Detekcija anomalija mrežnoga prometa temeljena na značajkama prometa i klasnoj pripadnosti uređaja

Cvitić, Ivan

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Ivan Cvitić

DETEKCIJA ANOMALIJA MREŽNOGA PROMETA TEMELJENA NA ZNAČAJKAMA PROMETA I KLASNOJ PRIPADNOSTI UREĐAJA

DOKTORSKI RAD

Zagreb, 2020.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Ivan Cvitić

DETEKCIJA ANOMALIJA MREŽNOGA PROMETA TEMELJENA NA ZNAČAJKAMA PROMETA I KLASNOJ PRIPADNOSTI UREĐAJA

DOKTORSKI RAD

Mentor: prof. dr. sc. Dragan Peraković

Zagreb, 2020.

University of Zagreb

Faculty of Transport and Traffic Sciences

Ivan Cvitić

NETWORK TRAFFIC ANOMALY DETECTION BASED ON TRAFFIC CHARACTERISTICS AND DEVICE CLASS AFFILIATION

DOCTORAL DISSERTATION

Supervisor: Full professor Dragan Peraković, PhD

Zagreb, 2020

INFORMACIJE O MENTORU: prof. dr. sc. Dragan Peraković

Dragan Peraković rođen je 12. travnja 1972. u Zagrebu. Nakon osnovne i srednje škole koju je završio u Grubišnom Polju upisuje studij na Fakultetu prometnih znanosti (u daljnjem tekstu Fakultet) Sveučilišta u Zagrebu i diplomira na PiT smjeru 1995. godine.

Poslijediplomski znanstveni studij „Tehničko-tehnološki sustavi u prometu i transportu“ pohađao je na Fakultetu, gdje je 2003. godine stekao akademski stupanj magistra znanosti iz područja tehničkih znanosti, polja Tehnologija prometa i transport, obranivši znanstveni magistarski rad "Mogućnost primjene mobilnog interneta u inteligentnim transportnim sustavima". Na temelju obrane doktorske disertacije pod naslovom "Model distribucije informacija korisnicima prometnog sustava", 2005. godine stekao je doktorat znanosti iz područja tehničkih znanosti, polja Tehnologija prometa i transport, na Fakultetu prometnih znanosti Sveučilišta u Zagrebu.

Od 1995. godine u stalnom je radnom odnosu na Fakultetu, prvo kao stručni suradnik, zatim mlađi asistent, a potom predavač i viši predavač. Od 2006. godine zaposlen je u znanstveno-nastavnom zvanju docent, 2011. godine izabran je u znanstveno-nastavno zvanje izvanrednog profesora. Godine 2017. izabran je u znanstveno-nastavno zvanje redoviti profesor, prvi izbor, u području tehničkih znanosti, polje: tehnologija prometa i transport.

Od 2010. godine imenovan je predstojnikom Zavoda za informacijsko-komunikacijski promet i voditeljem Katedre za upravljanje informacijsko-komunikacijskim uslugama.

Autor ili koautor je više od 130 znanstvenih radova objavljenih u međunarodnim časopisima i u zbornicima radova s međunarodnih znanstvenih skupova te 13 poglavlja u znanstvenim knjigama.

Trenutačno obnaša i nekoliko mentorstava na poslijediplomskom studiju iz područja tehničkih znanosti, polja Tehnologija prometa i transport. Uspješnost pri obavljanju funkcije mentora na doktorskom studiju očituje se u činjenici da je četiri (4) doktoranada uspješno obranilo doktorsku disertaciju. Četiri uspješno obranjena znanstvena magistarska rada govore u prilog uspješnom mentorstvu pri izradi znanstvenih magistarskih radova.

Suzani i Borni. Hvala za beskonačnu potporu i strpljenje.

Sažetak

Cilj zaštite informacijsko-komunikacijskog (IK) sustava podrazumijeva postizanje i održavanje zahtijevane razine osnovnih načela sigurnosti. Osnovna načela sigurnosti predstavljena su CIA (engl. *confidentiality, integrity, availability*) modelom koji obuhvaća cjelovitost, povjerljivost i dostupnost IK resursa. Jedan od čimbenika koji negativno utječu na načelo dostupnosti, a čiji trend je u kontinuiranom porastu posljednjih deset godina, mrežno je orijentirani distribuirani napad uskraćivanja usluge (engl. *Distributed Denial of Service*, DDoS), odnosno DDoS promet kao sredstvo provođenja napada. DDoS promet kao produkt DDoS napada predstavlja anomaliju u mrežnom prometu. Pojavom koncepta internet stvari (engl. *Internet of Things,* IoT) kao novog pravca tehnološkog razvoja i nove komunikacijske paradigme koja objedinjuje milijarde novih uređaja povezanih na internetsku mrežu, stvara se novi prostor sigurnosnih ranjivosti koje je moguće iskoristiti za neovlaštene i maliciozne aktivnosti. Predmet istraživanja u okviru ovog doktorskog rada je karakterističnost prometa generiranog IoT uređajima u okruženju pametnog doma kao osnove za detekciju anomalija koje nastaju kao rezultat provedbe DDoS napada. Ovim doktorskim radom prikazano je definiranje klasa unutar kojih je moguće dodijeliti IoT uređaje u okruženju pametnog doma. Klase se temelje na koeficijentu varijacije odnosa primljenog i poslanog prometa pojedinog uređaja. Jednako tako prikazan je i razvoj višeklasnog klasifikacijskog modela temeljen na *boosoting* metodi strojnog učenja koji uz visoku točnost (99,79 %) može klasificirati uređaje po osnovi karakteristika generiranog prometnog toka koristeći 13 značajki. Klasifikacijski model pruža mogućnost stvaranja profila legitimnog prometa pojedine klase uređaja nužnog u razvoju klasifikacijskog modela koji će omogućiti detekciju anomalija mrežnoga prometa. Radom je prikazan i razvoj modela detekcije anomalija mrežnoga prometa temeljenog na značajkama prometa i klasnoj pripadnosti uređaja. Model je razvijen uz korištenje metode logističkih stabala odluke pri čemu se za svaku klasu uređaja primjenjuje drugačija inačica modela koja se razlikuje u broju korištenih značajki i graničnim vrijednostima grananja stabla odluke. Prema rezultatima, visoka je točnost modela za sve četiri klase uređaja, od 99,92 % do 99,99 %. Navedeni pristup detekciji anomalija mrežnoga prometa predstavlja iskorak u istraživanju ovog problemskog područja jer se po prvi put koriste klase uređaja u svrhu detekcije DDoS prometa. Razvijeni model ima potencijal prepoznati do sada neviđene uređaje te ih dodijeliti pripadajućoj klasi za koju je poznat profil legitimnog prometa pri čemu postoji učinkovit model koji može prepoznati anomalije na temelju vrijednosti značajki prometnog toka koji takav uređaj generira.

Ključne riječi: DDoS, klase uređaja, značajke prometnog toka, strojno učenje, *boosting*

Summary

The development of a public, packet-oriented, communication network (Internet network), accompanied by an increase in the number of users and information and communication (IC) services, has also resulted in an increase in the amount of data transferred. Data stored, processed and transmitted through the IC system is often the target of illegitimate users whose goal is to gain unauthorized access or to prevent legitimate users from accessing IC system resources. This results in an increase in the need for research in the field of IC protection in recent decades.

The goal of protecting an IC system is to achieve and maintain the required level of basic security principles. The basic principles of security are presented by the CIA (confidentiality, integrity, availability) model, which embraces the integrity, confidentiality and availability of IC resources. The availability principle is defined as the probability that the requested service (or other IC system resource) will be available to a legitimate user at the required time. There are several factors to negatively impact the availability of IC resources. They can be classified according to the source of action (internal and external) and the executor (human, environment and technology). One of these factors with the steadily increasing trend over the last ten years is network-oriented Distributed Denial of Service (DDoS) attack, or DDoS traffic as a means of conducting attacks. The traffic generated by the DDoS attack is aimed at exploiting the deficiencies of the elements of the IC system in charge of processing and transmitting data such as communication links, active network equipment (routers, switches, firewalls, etc.) and devices intended for processing user requests and delivery of services (servers). The primary disadvantage that a DDoS attack exploits is the limitation of the capacity of the communication link, network equipment, or server.

Congestion can result from an increase in the intensity of legitimate inbound traffic that exceeds the total server and queue capacity, which negatively affects the quality of service (QoS). In doing so, it is necessary to apply traffic flow control methods which, between traffic flows of equal importance, will determine those that will be processed first.

Another way of creating congestion in a communications network may be the result of deliberately generating DDoS traffic. Such traffic has the characteristics of a legitimate user, and its primary objective is to exploit the previously identified shortcomings of the IC resources and to cause congestion resulting in degradation of quality or complete inaccessibility of the IC resources to the legitimate user. Using traffic flow control and congestion management methods

to solve DDoS traffic problems is not appropriate. The reason is that traffic flows are not of equal importance and it is therefore necessary to detect illegitimate traffic, which is an anomaly of network traffic at the level of individual network packets or traffic flow.

Network traffic anomaly detection is a dynamic and broad area of research. Any network traffic pattern that deviates from the sample of a previously defined profile of legitimate (normal) traffic and has the potential to disrupt the normal operation of the IC is considered an anomaly. The legitimate traffic profile is defined by the values of traffic features recorded over a period of time in which the traffic generating terminal device is not security compromised and operates in the manner defined by the manufacturer. The root causes of network traffic anomalies may be related to performance or IC system security. One of the growing causes of security-related network traffic anomalies is DDoS attacks. This type of attack utilizes a number of compromised terminal devices to generate legitimate, DDoS traffic to the destination. The consequences of DDoS attacks are degradation of quality or complete unavailability of IC services to legitimate users.

The emergence of the Internet of Things (IoT) concept as a new direction of technological development and a new communication paradigm that brings together billions of new devices connected to the Internet, creates a new space of security vulnerabilities that can be exploited for unauthorized and malicious activities. The continuous growth in the number of such devices, their inadequate protection and the ability to generate traffic on the network, makes them ideal candidates for the creation of a botnet network for the purpose of generating DDoS traffic of unprecedented traffic intensity. The concept of smart home as one of the fastest growing application areas of the IoT concept is becoming one of the most heterogeneous application areas in terms of number of IoT devices manufacturers. Such devices are often delivered with minimal or no protection, and the security of such devices is also reduced by the ease of use required by end users, who often do not have the adequate level of knowledge required to install and operate such devices. All of the above listed smart home devices are among the most vulnerable to a number of security threats, emphasizing the use of such devices to generate DDoS traffic.

The subject of this doctoral research is the traffic characteristics generated by IoT devices in a smart home environment as a basis for detecting anomalies resulting from DDoS attacks. Based on the research problems and the existing shortcomings, the following scientific hypotheses of the research were put forward:

(1) Based on the traffic features generated by IoT devices in a smart home environment, it is possible to define classes of IoT devices and associated profiles of legitimate traffic.

(2) Based on the defined profile of legitimate traffic of a particular class of IoT devices in a smart home environment, it is possible to detect with high accuracy the illegitimate traffic generated by such devices.

The concept of IoT offers numerous benefits in different fields of application, but from the point of security view, it also highlights a number of challenges that need to be adequately addressed. Research within this doctoral thesis considers the smart home environment as one of the fastest growing application areas within the IoT concept. Devices within this environment have many limitations and disadvantages that make them potential generators of DDoS traffic.

Despite the identified shortcomings, the communication of such devices generates traffic that possesses specific features and differences with respect to conventional devices. This research seeks to analyze the possibilities of applying such features for the purpose of classifying devices, regardless of their functionality or purpose. This kind of classification is necessary in a dynamic and heterogeneous environment such as a smart home where the number and types of devices grow daily, as it depends solely on the traffic features such devices generate.

Device classification allows defining the legitimate traffic profile of a particular class, based on which it is possible to determine deviations in the form of anomalies caused by the DDoS traffic generation of an individual device. Consequently, the aim of this research is to develop a model for detecting illegitimate DDoS traffic generated by IoT devices in a smart home environment based on specific traffic features and class affiliation of IoT devices.

Based on the above, the scientific contributions of the doctoral research are as follows:

(1) Identification of traffic features by which it is possible to classify IoT devices in a smart home environment for the purpose of detecting illegitimate DDoS traffic.

(2) Defining legitimate traffic profiles for each class of IoT device in a smart home environment.

(3) DDoS traffic detection model based on traffic features and class affiliation of IoT devices.

Despite the high accuracy of detection and the advantages shown by the methods used, there are some shortcomings in the research of DDoS traffic detection problems to date. The first drawback is reflected in the datasets used, that is, in traffic records, which are the basis for

the development of the detection model. Datasets containing traffic are often outdated, which reduces the accuracy of detection because they do not reflect the characteristics of current traffic that are changing as technological developments in new IK devices, concepts and services change. The previous research implies DDoS traffic generated solely through conventional terminal devices without considering devices for which human communication is not necessary for communication. The latter devices are unified under the IoT paradigm.

According to predictions, by the end of 2020, approximately 31 billion IoT devices will exist globally, and till 2025 75 billion. In this case, 41%, or 12.86 billion IoT devices will be installed within the concept of smart home (SH). The limitations of IoT devices in general, and thus SHIoT (smart home IoT) devices, are described in the previous researches, covering hardware constraints, high autonomy requirements and low cost of production, which reduces the ability to implement advanced security methods and increases the risk of numerous threats. Traffic generated by SHIoT devices or MTC (Machine Type Communication) traffic is different from traffic generated through conventional devices, HTC (Human Type Communication) traffic. Although SHIoT devices are characterized by heterogeneity, MTC traffic is homogeneous in contrast to HTC traffic, which means that devices of the same or similar purpose behave approximately equally, that is, generate traffic of similar characteristics.

The identified shortcomings of previous research, such as taking into account of SHIoT traffic features when detecting DDoS traffic, the consideration of classes of SHIoT devices that generate roughly equal values of traffic features, and the number of devices used in the study, will be sought to be remedied by planned research.

The importance of this research is also evident through the increasing number of research and projects in this field. An example of this is the project called Mitigating IoT-Based Distributed Denial Of Service (DDoS), implemented by NIST (National Institute of Standards and Technology) and NCCoE (National Cybersecurity Center of Exellence), which addresses the issue of generating DDoS traffic through an IoT device.

The research within this doctoral thesis formed the laboratory environment of the smart home. Such an environment is comprised of a variety of SHIoT devices, along with an accompanying communications infrastructure and software-hardware platform that enables traffic collection and data set to be applied in later stages of research and development of network traffic anomaly detection models. In addition to the primary data collected through the process described above, the research also included secondary data, encompassing a greater

variety of SHIoT devices. The reason for this is the heterogeneity of devices that can exist in the observed environment.

A total of 41 devices in a smart home environment were used for this doctoral research. According to statistics, there are differences in the estimation of the average number of SHIoT devices per household that has a certain form of smart home implemented. These estimates range from 6.53 to 14 SHoT devices per household. In the Republic of Croatia, smart home representation is still low, and telecom operators are assuming the role of smart home provider through the offering of end-user SHIoT devices. For example, Iskon Internet service provider offers customers the option of purchasing a smart home package that makes four SHIoT devices, while telecom operator A1 provides users with the ability to deploy a total of five SHIoT devices in a smart home environment. Despite mentioned, this research sought to achieve the greatest possible variety of SHIoT devices due to the need to define device classes based on the characteristics of the traffic generated. Therefore, the number of devices used is higher than the current statistical estimate of the average value of SHIoT devices per smart home in the Republic of Croatia and worldwide.

Predictability of IoT device behavior is a phenomenon that has been the result of communication activities of IoT devices observed in numerous studies. Given that SHIoT devices have a limited number of functionalities, certain devices will behave approximately the same in time according to the values of the observed traffic features. Unlike IoT devices, conventional devices (smartphones, desktops, laptops, etc.) support the installation of a large number of applications, where the communication activity of such devices depends on the end users and how the device is used. Accordingly, the index of the predictability level of the behavior of an IoT device, expressed by the coefficient of variation of the received and sent amount of data (C_u index), is a measure on the basis of which it is possible to determine the behavior of an SHIoT device over a period of time. The closer the index (C_u) to 0, the observed device has a smaller deviation with respect to the amount of data received and sent, and it is considered that the level of predictability of the behavior of such device is higher than the device whose index C_u is greater than 0.

For the purpose of developing a classification model based on the logistic regression method enhanced by the concept of supervised machine learning, a data set was created containing the values of extracted features of traffic flows of SHIoT devices and belonging to the class of individual device for each traffic flow in the set. Model development, testing and validation were performed using the WEKA software tool with the support of MS Excel 2016

during the preparation of the model development dataset. Since a total of 59 features were selected using the information gain method, during model development, the number of features was gradually reduced when the validation measures for each model were compared. The aim of this procedure is to develop a model that will use the least possible number of independent features that will not significantly affect its performance. Each model was validated by *k*-fold cross-validation at $k = 10$. This method is used to evaluate the behavior of the model over data not used in the learning phase. In doing so, the model is applied iteratively *k* times over the dataset. In each iteration, the data set is divided into *k* parts. One part of the set is used to validate the model while the remaining *k*-1 parts of the set are combined into a model learning subset. In order to develop DDoS traffic detection models based on predefined classes of SHIoT devices, it is necessary to define the legitimate traffic profile of each device class. When developing any anomaly detection model based on supervised machine learning methods, it is necessary to have a data set that will represent legitimate traffic and a data set that will represent illegitimate traffic. The defined classes of SHIoT devices allow the establishment of a legitimate traffic profile for each class of device, which is important in the later development of anomaly detection models. In doing so, the SHIoT device traffic feature values become part of the legitimate profile of the observed device class. The legitimate traffic profile of a particular class of SHIoT device is defined by the values of the features of those traffic flows that are assigned to a particular class of SHIoT device by the classification model. The Logistic Model Trees (LMT) method was used to develop a model for detecting illegitimate DDoS network traffic. The WEKA software tool was used to implement the method and process the data, and datasets that represent the profiles of normal traffic resulting from the SHIoT device classification model and illegitimate DDoS traffic datasets.

The work of the developed model of detection of illegitimate DDoS traffic takes place in two stages. The first phase is a prerequisite for the later detection of DDoS traffic in the second phase of operation and implies the classification of the SHIoT device based on the generated traffic flow. One of the basic metrics that indicate model performance is classification accuracy and kappa statistics. According to the classification accuracy, all models show high performance, which means that based on the observed flow, they can determine with high accuracy whether the traffic flow is the result of legitimate device communication or the device generates DDoS traffic. Thus, the LMT model for the C1 device class shows an accuracy of 99.9216%, or 56092 accurately classified traffic flows, as DDoS or traffic flow that legitimately belongs to a SHIoT device in class C1. A total of 44 traffic flows were misclassified, or

0.0784% in the total set of 56136. In addition to high accuracy, the LMT model for the C1 device class also exhibits a kappa coefficient ($\kappa = 0.9984$) indicating high model performance. The LMT model version developed for the C2 class shows high accuracy (99.9966%). This implies 59660 accurately classified traffic flows in a set consisting of 59662 traffic flows. The classification error is 0.0034%, or two traffic flows. The kappa coefficient is 0.9999, which indicates the high performance of these LMT models. The LMT classification model developed for the C3 class provides 99.9744% accuracy. Therefore, out of a total of 58661 traffic flows, 15 were misclassified, or 0.0256% while accurately classified, 58646. The kappa coefficient of 0.9995, as in previous versions of the LMT model, indicates its high performance. The latest version of the LMT model, developed for the C4 class, shows an accuracy of 99.9583% which implies 59879 correctly classified traffic flows. Accordingly, a total of 25 traffic flows were misclassified. The success of the model as measured by the kappa coefficient is 0.9992.

Research has shown that it is possible to define device classes based on the variation of the received and sent traffic ratio, and it is possible to classify devices into defined classes based on the traffic flow features such devices generate. Finally, depending on the affiliation of an individual device to a defined class, it is possible to determine whether the traffic flow that the device generates is an anomaly in the form of DDoS traffic or legitimate traffic.

Keywords: DDoS, device classes, traffic flow features, machine learning, boosting

SADRŽAJ

1 Uvod

Uvodnim poglavljem doktorskog rada opisan je i definiran predmet istraživanja kao i motivacija autora za provedbu istraživanja. Nadalje, određen je cilj istraživanja i očekivani znanstveni doprinosi kao produkti planiranog istraživanja. Prikazan je osvrt na dosadašnja istraživanja koji ukazuje na trenutne smjerove istraživanja problemskog područja, ali i ukazuje na nedostatke tih istraživanja te određuje prostor istraživanja u okviru ovog doktorskog rada.

1.1 Predmet istraživanja i znanstvene hipoteze

Razvoj javne, paketno orijentirane, komunikacijske mreže (internetske mreže) praćen povećanjem broja korisnika i informacijsko-komunikacijskih (IK) usluga, rezultirao je i povećanjem količine prenesenih podataka [1], [2]. Podatci koji se pohranjuju, obrađuju i prenose posredstvom IK sustava često su meta nelegitimnih korisnika čiji je cilj neovlašteni pristup ili onemogućavanje pristupa resursima IK sustava legitimnim korisnicima [3]. Navedeno rezultira povećanjem potrebe istraživanja u području zaštite IK sustava posljednjih desetljeća.

Cilj zaštite IK sustava podrazumijeva postizanje i održavanje zahtijevane razine osnovnih načela sigurnosti. Osnovna načela sigurnosti predstavljena su CIA (engl. *confidentiality, integrity, availability*) modelom koji obuhvaća cjelovitost, povjerljivost i dostupnost IK resursa [3]. Prema [4], načelo dostupnosti definirano je kao vjerojatnost da će tražena usluga (ili drugi resurs IK sustava) biti dostupan legitimnom korisniku u traženom vremenu. Brojni su čimbenici za negativan utjecaj na dostupnost IK resursa. Prema [5], moguće ih je klasificirati prema izvoru djelovanja (interni i eksterni) i izvršitelju (čovjek, okruženje i tehnologija). Jedan od tih čimbenika, čiji trend je u kontinuiranom porastu posljednjih deset godina, mrežno je orijentirani distribuirani napad uskraćivanja usluge (engl. *Distributed Denial of Service,* DDoS), odnosno DDoS promet kao sredstvo provođenja napada [6]. Promet generiran DDoS napadom usmjeren je na iskorištavanje nedostataka elemenata IK sustava zaduženih za obradu i prijenos podataka poput komunikacijskih linkova, aktivne mrežne opreme (usmjernici, preklopnici, vatrozidi i sl.) te uređaja namijenjenih obradi korisničkih zahtjeva i isporuci usluga (poslužitelji). Primarni nedostatak koji DDoS napad iskorištava je ograničenje kapaciteta komunikacijskog linka, mrežne opreme ili poslužitelja [7].

Ograničenja kapaciteta poslužitelja i repa sustava posluživanja predmet su istraživanja od pojave telekomunikacijskih sustava [8]. Odgovarajući opis problema pruža teorija podvorbenih sustava (TPS) koja je često korištena za modeliranje procesa obrade paketa u komunikacijskoj mreži i komunikacijskim čvorovima. Prema TPS, kapacitet poslužitelja predstavlja brzinu kojom poslužitelj obrađuje korisnike, a rep sustava posluživanja odnosi se na skup korisnika koji pred poslužitelj postavljaju zahtjev za posluživanjem [9]. Prometni problem u komunikacijskoj mreži moguće je definirati tako da postoji veći broj prostorno razmještenih mrežnih čvorova i izvorišta koji generiraju prometne tokove. Generirane prometne tokove potrebno je poslužiti uz prihvatljivu razinu usluge i troškove pri čemu zbroj svih prometnih tokova generiranih na izvorištima mora biti manji od kapaciteta odredišnog

poslužitelja [10]. U slučajevima kada prethodno navedeni zahtjev nije ispunjen, javlja se zagušenje u komunikacijskom čvoru ili nekom drugom segmentu IK sustava koji obnaša funkciju obrade dolaznog prometa (npr. poslužitelju).

Zagušenje može nastati kao posljedica povećanja intenziteta legitimnog dolaznog prometa koji prelazi ukupne kapacitete poslužitelja i repa što se negativno odražava na kvalitetu usluge (engl. *Quality of Service,* QoS). Pri tome je potrebno primijeniti metode kontrole toka prometa koji će, između prometnih tokova jednake važnosti, odrediti one koji će biti prvi obrađeni [11], [12].

Drugi način stvaranja zagušenja u komunikacijskoj mreži može biti rezultat namjernog generiranja DDoS prometa. Takav promet ima karakteristike legitimnog, a osnovni cilj mu je iskoristiti prethodno identificirane nedostatke IK resursa i izazvati zagušenje što za posljedicu ima degradaciju kvalitete ili potpunu nedostupnost IK resursa legitimnom korisniku. Korištenje metoda kontrole toka prometa i metoda upravljanja zagušenjem u rješavanju problema DDoS prometa nije prikladno. Razlog tome je što prometni tokovi nemaju jednaku važnost te je shodno tome nužno detektirati nelegitimni promet koji predstavlja anomaliju mrežnog prometa na razini pojedinačnih mrežnih paketa ili prometnog toka [7].

Detekcija anomalija mrežnog prometa predstavlja dinamično i široko područje istraživanja. Anomalijom se smatra svaki uzorak mrežnog prometa koji odstupa od uzorka prethodno definiranog profila legitimnog (normalnog) prometa te ima potencijal narušiti normalan rad IK sustava [13]. Profil legitimnog prometa definira se vrijednostima prometnih značajki zabilježenih u vremenskom periodu u kojemu terminalni uređaj koji generira promet nije sigurnosno kompromitiran i radi na način kojeg definira proizvođač. Prema [14], osnovni uzročnici anomalija u mrežnom prometu mogu biti povezani s performansama ili sa sigurnošću IK sustava. Jedan od rastućih uzročnika anomalija mrežnog prometa povezanih sa sigurnošću je DDoS napad. Ovakva vrsta napada koristi brojne kompromitirane terminalne uređaje s ciljem generiranja nelegitimnog, DDoS prometa prema odredištu. Posljedice DDoS napada su degradacija kvalitete ili potpuna nedostupnost IK usluga legitimnim korisnicima [15].

Pojavom koncepta internet stvari (engl. *Internet of Things,* IoT) kao novog pravca tehnološkog razvoja i nove komunikacijske paradigme koja objedinjuje milijarde novih uređaja povezanih na internetsku mrežu, stvara se novi prostor sigurnosnih ranjivosti koje je moguće iskoristiti za neovlaštene i maliciozne aktivnosti. Kontinuirani rast broja ovakvih uređaja, njihova neadekvatna zaštita i sposobnost generiranja prometa u mreži, čini ih idealnim

kandidatima za stvaranje *botnet*[1] mreže u svrhu generiranja DDoS prometa do sada nezabilježenog prometnog intenziteta. Koncept pametnog doma kao jedno od najbrže rastućih područja primjene koncepta IoT postaje i jedno od izrazito heterogenih područja primjene s aspekta broja proizvođača IoT uređaja. Takvi uređaji često se isporučuju uz minimalnu ili nepostojeću zaštitu, a sigurnost takvih uređaja smanjuje se i zbog jednostavnosti korištenja koju zahtijevaju krajnji korisnici, koji često nemaju adekvatnu razinu znanja potrebnu za instalaciju i upravljanje takvim uređajima. Sve navedeno ubraja uređaje objedinjene pod konceptom pametnog doma među najranjivije na brojne sigurnosne prijetnje pri čemu se izrazito ističe iskorištavanje takvih uređaja u svrhu generiranja DDoS prometa.

Predmet istraživanja u okviru ovog doktorskog rada su karakteristike prometa generiranog IoT uređajima u okruženju pametnog doma kao osnove za detekciju anomalija koje nastaju kao rezultat provedbe DDoS napada.

Na temelju problema istraživanja i postojećih nedostataka postavljene su sljedeće znanstvene hipoteze istraživanja:

(1) Na temelju značajki prometa koji generiraju IoT uređaji u okruženju pametnog doma moguće je definirati klase IoT uređaja i pripadajuće profile legitimnog prometa.

(2) Temeljem definiranog profila legitimnog prometa pojedine klase IoT uređaja u okruženju pametnog doma moguće je uz visoku točnost detektirati nelegitiman promet koji takvi uređaji generiraju.

1.2 Cilj istraživanja i znanstveni doprinos

Koncept IoT pruža brojne prednosti u različitim područjima primjene, ali gledano s aspekta sigurnosti aktualizira i brojne izazove koje je potrebno na adekvatan način adresirati. Istraživanje u okviru ovog doktorskog rada u obzir uzima okruženje pametnog doma kao jedno od najbrže rastućih područja primjene u okviru koncepta IoT. Uređaji u okviru tog okruženja posjeduju brojna ograničenja i nedostatke koji ih čine potencijalnim generatorima DDoS prometa.

Unatoč identificiranim nedostatcima, komunikacija takvih uređaja generira promet koji posjeduje specifične značajke i različitosti u odnosu na konvencionalne uređaje. Predmetno istraživanje nastoji analizirati mogućnosti primjene takvih značajki u svrhu klasifikacije uređaja, neovisno o njihovim funkcionalnostima ili namjeni. Takav način klasifikacije nužan je

[1] Mreža neovlašteno udaljeno kontroliranih i geografski dislociranih terminalnih uređaja.

u dinamičnom i heterogenom okruženju kao što je pametni dom u kojemu broj i vrste uređaja svakodnevno rastu, jer ovisi isključivo o prometnim značajkama koje takvi uređaji generiraju.

Klasifikacija uređaja omogućuje definiranje profila normalnog prometa pojedine klase na temelju kojega je moguće utvrditi odstupanja u obliku anomalija uzrokovanih generiranjem DDoS prometa pojedinog uređaja. Slijedom navedenoga, cilj predmetnog istraživanja je razvoj modela detekcije nelegitimnog DDoS prometa generiranog IoT uređajima u okruženju pametnog doma koji se temelji na specifičnim značajkama prometa i klasnoj pripadnosti IoT uređaja.

Temeljem navedenog, znanstveni doprinosi predmetnog istraživanja su sljedeći:

(1) Identifikacija značajki prometa temeljem kojih je moguće klasificirati IoT uređaje u okruženju pametnog doma u svrhu detekcije nelegitimnog DDoS prometa.

(2) Definiranje profila legitimnog prometa za pojedinu klasu IoT uređaja u okruženju pametnog doma.

(3) Model detekcije DDoS prometa temeljen na značajkama prometa i klasnoj pripadnosti IoT uređaja.

1.3 Osvrt na dosadašnja istraživanja

Posljednja dva desetljeća brojna istraživanja usmjerena su prema razvoju metoda, modela i sustava koji su u mogućnosti detektirati DDoS promet u stvarnom vremenu. Unatoč tome, broj DDoS napada i količina DDoS prometa u kontinuiranom je porastu, što predstavlja razlog za daljnja istraživanja u području detekcije sigurnosnih prijetnji ove vrste [16].

Istraživanja definiraju nekoliko pristupa detekciji DDoS prometa. Općenito ih je moguće podijeliti u tri osnovne kategorije, temeljene na specifikaciji komunikacijskih protokola, temeljene na uzorku i temeljene na anomalijama [15], [17]. Istraživanje [18], uz prethodna, identificira i pristup temeljen na entropiji, a istraživanje [19] navodi mogućnosti primjene hibridnog pristupa detekcije DDoS prometa.

Pristup temeljen na specifikaciji komunikacijskih protokola podrazumijeva komparaciju predodređenih profila opće prihvaćenih definicija legitimnih aktivnosti za svako stanje protokola. S tako definiranim stanjem uspoređuju se nova opažanja i utvrđuju potencijalne devijacije. Osnovni nedostatak navedenog pristupa je taj što zahtijeva značajne računalne resurse zbog kompleksnosti analize. Dodatni nedostatak je nemogućnost ovog

pristupa da prepozna napade koji ne narušavaju karakteristike prihvaćenog legitimnog ponašanja protokola [17].

Metode temeljene na uzorku primjenjuju komparaciju dolaznog prometa s prethodno definiranim profilima i uzorcima poznatih mrežnih anomalija [20]. Detekciju DDoS napada temeljenu na uzorku moguće je provoditi na tri načina: na temelju potpisa poznatih napada, na temelju pravila (ako-onda) i na temelju stanja i prijelaza [7]. Prednost ovakvog načina detekcije je visoka stopa detekcije već poznatih DDoS napada uz mali broj lažno pozitivnih i lažno negativnih rezultata. Nedostatak predstavlja nemogućnost detekcije novih i nepoznatih napada, odnosno onih napada koji se ne nalaze u bazi podataka sa čijim zapisima se uspoređuju uzorci dolaznog prometa. S obzirom na dinamičnost problemskog područja u pogledu rasta broja i raznovrsnosti uređaja, od velike je važnosti da su metode detekcije u mogućnosti detektirati nepoznate uzorke DDoS prometa [15].

Suprotno navedenome, pristup temeljen na detekciji anomalija mrežnog prometa koristi prethodno definirane modele normalnog prometa s kojima se zatim uspoređuje dolazni promet [19]. Spomenuti pristup detekciji razvijen je da bi se prevladali nedostatci pristupa detekcije temeljenog na uzorcima [18]. Ukoliko se dolazni promet značajno razlikuje od definiranog modela normalnog prometa, tada se dolazni promet identificira kao anomalija, odnosno kao DDoS promet [21]. Prednost detekcije anomalija mrežnog prometa u odnosu na detekciju temeljenu na uzorcima, mogućnost je otkrivanja nepoznatih napada. Osnovni nedostatak detekcije temeljene na anomalijama je problem određivanja graničnih vrijednosti (engl. *threshold)* između normalnog prometa i anomalije [19], [22]. Anomalije mrežnog prometa detektiraju se kada vrijednosti trenutnog prometnog toka ili drugih odabranih parametara prelaze prethodno definiranu graničnu vrijednost modela normalnog prometa. Nisko definirana granična vrijednost uzrokuje veliki broj lažno pozitivnih rezultata, a visoko definirana granična vrijednost dovodi do velikog broja lažno negativnih rezultata [23].

Brojne znanstvene metode korištene su u funkciji detekcije DDoS prometa. U aktualnoj znanstvenoj literaturi najčešće se primjenjuju statističke metode, metode strojnog učenja i *softcomputing* metode [24].

Statistička svojstva prometa moguće je iskoristiti za razlikovanje normalnog i DDoS prometa. Statistički temeljen pristup svodi se na primjenu statističkih metoda u utvrđivanju modela normalnog prometa nakon čega se statističkim zaključivanjem određuje odgovara li nova instanca prometa (tok, paket ili skup paketa) definiranom modelu [24]. Metode korištene

u detekciji DDoS prometa iz domene statistike i teorije informacija su devijacija, kumulativna suma, korelacija, entropija i kovarijanca [7].

Samosličnost (engl. *self-similarity*) i dugoročna ovisnost (engl. *long-range dependence* - LRD) mrežnog prometa su često korištena svojstva u statističkoj obradi i detekciji DDoS prometa što se uočava iz brojnih istraživanja poput [16], [21], [25], [26]. Podatkovni promet u normalnim uvjetima održava LRD svojstvo što implicira gubitak ili smanjenje stupnja LRD svojstva u slučaju anomalija u komunikacijskoj mreži kao što je pojava DDoS prometa [21]. Prema tome, analizom LRD svojstva dolaznog prometa moguće je detektirati DDoS promet. Svojstva LRD i samosličnosti izražavaju se Hurstovim parametrom (H) koji se još naziva i indeksom dugoročne ovisnosti, a mjeri se statističkim procjeniteljima poput autokorelacije, agregacije varijance, *wavelet,* R/S (engl. *rescaled range*) metoda i sl. [26]. Izazov pri određivanju LRD svojstva je određivanje vremenskog perioda unutar kojeg će se analizirati promet [21]. Ukoliko je vremenski period prekratak, rezultati analize neće biti valjani zbog nedovoljne količine prometa za određivanje stupnja LRD, dok će preveliki vremenski period uzrokovati nemogućnost detekcije anomalija kratkog trajanja [25]. Uz navedeno, nedostatak ovakvog načina detekcije je preddefinirana statična granična vrijednost Hurstovog parametra što rezultira detekcijom DDoS prometa samo kada njegov intenzitet uzrokuje promjenu vrijednosti Hurstovog parametra iznad definiranog praga.

Istraživanja poput [22], [27–29] koriste entropiju kao primarnu metodu detekcije DDoS prometa potpomognutu drugim statističkim metodama. Istraživanja [29] i [30] koriste entropiju i Pearsonov hi-kvadrat korelacijski test u funkciji mjerenja statističkih svojstava vrijednosti parametara zaglavlja paketa. Kao primjer u [29] navodi se primjena navedenih metoda nad analizom izvorišnih IP adresa u određenom skupu dolaznih paketa. U istraživanju su korištena četiri podatkovna skupa prikupljena u različitim IK okruženjima. Točnost detekcije značajno se razlikuje u ovisnosti o podatkovnom skupu. Nedostatak istraživanja vidljiv je u definiranju granične vrijednosti hi-kvadrat testa koja može rezultirati velikim brojem lažno negativnih ili lažno pozitivnih rezultata. Dodatni nedostatak, prema autorima istraživanja, odabir je parametara zaglavlja paketa čije će vrijednosti biti analizirane jer je potrebno dobro poznavati na koje parametre će utjecati DDoS promet. Uz navedeno, prema [31], korelacijske metode poput Pearsonove, Spearmanove i Kendallove smatraju se neodgovarajućim u detekciji DDoS prometa jer često pokazuju visoku stopu korelacije između različitih objekata ili instanci prometa. Detekcija DDoS prometa temeljena na entropiji korištena je u istraživanju [28]. Razvijeni model detekcije temelji se na agregaciji prometnog toka i primjeni metode brze

entropije (engl. *fast entropy*). Ukoliko vrijednost entropije padne ispod zadane granične vrijednosti promatrani prometni tok smatra se DDoS prometom. Određivanje granične vrijednosti u navedenom istraživanju je adaptivno i njegova prilagodba se temelji na srednjoj vrijednosti i standardnoj devijaciji broja prometnih tokova u promatranom vremenskom intervalu.

Često korištena statistička metoda u detekciji DDoS prometa je multivarijantna korelacijska analiza (MKA). Primjeri primjene MKA metode vidljivi su u istraživanjima [31–33]. Metoda MKA se primjenjuje zbog prednosti koje pruža nad ostalim statističkim metodama poput malog broja lažno pozitivnih rezultata [32]. Kao nedostatak ističu se granične vrijednosti koje su korisnički definirane [31]. Istraživanje [31] koristi dva podatkovna skupa: CAIDA DDoS 2007 i DARPA 2000 za validaciju predloženog modela detekcije, a istraživanje [32] koristi CAIDA DDoS 2007, KDD CUP 99 i TUIDS podatkovne skupove[2]. Točnost detekcije u oba modela značajno ovisi o postavljenoj graničnoj vrijednosti korelacije između legitimnog i DDoS prometa. Visoka točnost i mali broj lažno pozitivnih rezultata za svaki podatkovni skup zahtijeva drugačiji iznos granične vrijednosti pri čemu se nameće problem definiranja granične vrijednosti na novom skupu podataka. Uz navedeno, sva analizirana istraživanja podrazumijevaju povećanje broja lažno pozitivnih rezultata u ovisnosti o broju točno detektiranih instanci DDoS prometa [31–33]. Da bi detekcija DDoS prometa primjenom MKA, ali i primjenom drugih metoda bila učinkovita, veliku važnost ima odabir parametara prometa koji će biti analizirani jer nemaju svi parametri jednaku važnost u analizi i klasifikaciji mrežnog prometa [32]. Veći broj korištenih parametara može povećati i točnost detekcije, ali zahtijeva i više resursa za obradu što često onemogućava detekciju u stvarnom vremenu.

Primjena metoda strojnog učenja predstavlja jedan u nizu pristupa detekciji DDoS prometa. Razlozi za njihovu primjenu su prednosti u odnosu na metode detekcije temeljene na uzrocima jer se značajno umanjuje utjecaj ljudskog faktora u cjelokupnom procesu detekcije DDoS prometa [34]. Metode strojnog učenja mogu se klasificirati na nadzirane (koristi se postojeće znanje za klasifikaciju budućih nepoznatih instanci) i nenadzirane (nastoji odrediti pripadajuću klasu instance bez prethodnog znanja) [7]. Primjeri metoda nadziranog strojnog učenja često korištenih u detekciji DDoS prometa su stabla odluke, metoda *k*-najbližih susjeda (engl. *k-Nearest Neighbor*, kNN), potporni vektori (engl. *Suport Vector Machines*, SVM) i

[2] Navedeni podatkovni skupovi predstavljaju sintetički generirani promet (korištenjem simulacijskih alata) ili promet prikupljen u realnim okruženjima. Obje vrste podatkovnih skupova sadrže jedan ili više vrsta napada i/ili zapis normalnog prometa generiranog u komunikacijskoj mreži

naivni Bayes klasifikator. Metode nenadziranog strojnog učenja često korištene u detekciji DDoS prometa su *fuzzy* C srednjih vrijednosti i klasteriranje primjenom k-srednjih vrijednosti [35].

Primjena metoda stabla odluke i naivnog Bayesovog klasifikatora vidljiva je u istraživanju [36]. Autori koriste navedene metode za detekciju DDoS prometa u CAIDA podatkovnom skupu. Rezultati istraživanja dokazuju visok stupanj učinkovitosti primjene navedenih metoda. Točnost detekcije stabla odluke iznosi 99 %, a naivnog Bayes klasifikatora 97 %. Primjena istih metoda nad drugim skupom podataka (NSL KDD) pokazuje manju točnost detekcije naivnog Bayesovog klasifikatora (<90 %) dok je točnost detekcije stabla odluke jednaka kao u prethodnom istraživanju [37]. Istraživanje [38] analizira primjenu metoda *fuzzy* C srednjih vrijednosti, SVM, kNN, *k* srednjih vrijednosti, stabla odluke i naivnog Bayesovog klasifikatora na CAIDA podatkovnom skupu. Sve analizirane metode pokazuju visoku točnost detekcije (>95 %) pri čemu metode SVM, kNN i stablo odluke imaju visoku stopu lažno pozitivnih rezultata. Istraživanje [39] koristi metodu dekompozicije singularnih vrijednosti (engl. *Singular Value Decomposition,* SVD) u razvoju modela detekcije DDoS prometa. Model koristi ukupno 41 parametar temeljem kojih se provodi klasifikacija prometa na normalan i DDoS promet. Rezultati istraživanja pokazuju visoku točnost detekcije nad KDD-CUP 1999 skupom podataka i u usporedbi s primjenom metoda strojnog učenja poput kNN, slučajne šume (engl. *random forest*) i *bagging*. Granične vrijednosti između normalnog i DDoS prometa također su korisnički definirane kao i kod statističkog pristupa. Pri tome SVD metoda pokazuje manje promjene na točnost detekcije (98,4 % - 99,5 %) pod utjecajem granične vrijednosti, za razliku od ostalih korištenih metoda.

Prednosti *softcomputing* metoda u odnosu na prethodno opisane su tolerancija na nepreciznost, nesigurnost, djelomičnu istinitost i nepotpunost ulaznih podataka. Robusnost i učinkovitost ovakvih metoda dokazana je u rješavanju velikog broja kompleksnih problema poput detekcije podudarnosti uzoraka. *Softcomputing* pristup učinkovit je u rješavanju problema kod kojih su informacije o problemu nepotpune, a moguće rješenje problema nije egzaktno [7]. To je razlog česte primjene ove skupine metoda u detekciji DDoS prometa pri čemu su često korištene metode umjetnih neuronskih mreža (UNM) i neizrazita logika što je vidljivo iz brojnih istraživanja poput [40–44]. Učinkovitost primjene umjetnih neuronskih mreža vidljiva je iz istraživanja [40] i [42]. Istraživanjem [40] razvijen je model detekcije DDoS prometa SPUNNID (*Statistical Pre-Processor & Unsupervised Neural Net based Intrusion Detector*). Model koristi osam parametara mrežnih paketa za detekciju DDoS prometa velikog

intenziteta (UDP, SYN i ICMP preplavljivanje). Korišteni parametri odabrani su zbog utvrđene statističke promjene njihovih vrijednosti pod utjecajem DDoS prometa u odnosu na normalan promet. Na temelju odabranih parametara provedeno je učenje, testiranje i validacija umjetne neuronske mreže na podatkovnom skupu generiranom u simuliranom okruženju. Rezultati validacije modela pokazuju visoku točnost (94,9 %) i brzinu detekcije DDoS prometa (0,7 sekundi). Visoku točnost detekcije pokazuje i model temeljen na UNM u istraživanju [42]. Autori koriste pet parametara zaglavlja mrežnih paketa i četiri javno dostupna podatkovna skupa za učenje, testiranje i validaciju modela. Razvijeni model koristi metodu učenja propagacije unatrag (engl. *back-propagation*) i sigmoidnu aktivacijsku funkciju što se pokazalo učinkovitim i u istraživanju [41]. Model detektira i razlikuje tri klase DDoS prometa (DNS, UDP i Chargen) i normalni promet uz ukupnu točnost od 95,6 %. Rezultati istraživanja pokazuju najmanju točnost detekcije UDP DDoS prometa od 82.1 % zbog podudaranja vrijednosti parametara takvog prometa s vrijednostima parametara normalnog prometa.

Neizrazita logika u funkciji detekcije DDoS napada korištena je u istraživanju [43]. Autori istraživanja predlažu model detekcije TCP SYN DDoS prometa. Točnost detekcije i broj lažno pozitivnih i negativnih rezultata ovisan je o definiranoj graničnoj vrijednosti intenziteta prometa prema kojoj se određuje vjerojatnost DDoS prometa. Autori istraživanja [44] koriste neizrazitu logiku za detekciju intenziteta DDoS prometa s obzirom na to da ne postoji jasno definirana granica između DDoS prometa malog i jakog intenziteta. Neizrazita logika korištena je u kombinaciji s *wavelet procjenom* temeljenoj na Hurstovom parametru primijenjenoj u svrhu detekcije promjene svojstva samosličnosti mrežnog prometa. Detektirane promjene vrijednosti Hurstovog parametra predstavljaju ulazne podatke u model temeljen na neizrazitoj logici koji prema definiranim pravilima procjenjuje intenzitet DDoS prometa. Problem definiranja granične vrijednosti Hurstovog parametra iznad koje se promet smatra DDoS prometom, nastoji se riješiti uzimanjem u obzir stupnja samosličnosti normalnog prometa.

Unatoč visokoj točnosti detekcije i prednostima koje pokazuju primijenjene metode, uočavaju se određeni nedostatci u dosadašnjim istraživanjima problema detekcije DDoS prometa. Prvi nedostatak ogleda se u korištenim podatkovnim skupovima, odnosno u zapisima DDoS prometa koji predstavljaju temelj razvoja modela detekcije. Podatkovni skupovi koji sadrže DDoS promet često su zastarjeli što, prema [41], smanjuje točnost detekcije jer ne odražavaju karakteristike trenutnog prometa koje se mijenjaju pod utjecajem tehnološkog razvoja novih IK uređaja, koncepata i usluga. Prethodno navedena istraživanja podrazumijevaju DDoS promet generiran isključivo posredstvom konvencionalnih terminalnih uređaja ne

uzimajući u obzir uređaje za čiju međusobnu komunikaciju nije nužna ljudska intervencija. Potonji uređaji objedinjeni su pod paradigmom IoT.

Prema predviđanjima prikazanima u [45], do kraja 2020. godine globalno će u primjeni egzistirati približno 31 milijarda IoT uređaja. Pri tome će 41 %, odnosno 12.86 milijardi IoT uređaja biti instalirano unutar koncepta pametnog doma (engl. *smart home,* SH) [46]. Ograničenja IoT uređaja općenito, a time i SHIoT (*smart home* IoT) uređaja, opisani su u istraživanju [47], a obuhvaćaju hardverska ograničenja, zahtjeve za visokom autonomijom te nisku cijenu proizvodnje što smanjuje mogućnost implementacije naprednih metoda zaštite i povećava rizik od brojnih prijetnji prikazanih u [48].

Promet koji generiraju SHIoT uređaji ili MTC (engl. *Machine Type Communication*) promet razlikuje se od prometa generiranog posredstvom konvencionalnih uređaja, HTC (engl. *Human Type Communication*) prometa, što je prikazano istraživanjem [49]. Iako SHIoT uređaje karakterizira heterogenost, MTC promet je homogen za razliku od HTC prometa što znači da se uređaji iste ili slične namjene ponašaju približno jednako, odnosno generiraju promet sličnih obilježja [50].

Specifična obilježja MTC prometa korištena su za rješavanje brojnih problema u komunikacijskoj mreži. Istraživanje [51] promatra utjecaj MTC prometa na QoS tijekom integracije sa HTC prometom u LTE komunikacijskoj mreži. Identifikacija i klasifikacija IoT uređaja u pametnim gradovima i kampusima te u pametnim okruženjima korištenjem obilježja MTC prometa prikazana je istraživanjima [52] i [53]. Istraživanje [54] nastoji utvrditi nove zahtjeve i izazove u dizajnu i upravljanju mobilnom komunikacijskom mrežom nametnute generiranjem MTC prometa.

Istraživanja problema detekcije DDoS prometa generiranog IoT uređajima pretežno su preglednog karaktera ili tijekom istraživanja nisu korišteni realni skupovi podataka što je vidljivo u [55] i [56]. Istraživanje [57] je, prema navodima autora, prvo koje uzima u obzir SHIoT promet pri razvoju modela detekcije DDoS prometa. Istraživanjem je predložen model binarne klasifikacije prometa na legitiman i DDoS promet primjenom pet različitih metoda strojnog učenja. Specifična obilježja SHIoT prometa promatrana su kroz promjenu značajki prometa poput veličine paketa, međudolaznih vremena paketa, korištenih protokola te promjene broja odredišnih IP (engl. *Internet Protocol*) adresa s kojima SHIoT uređaji komuniciraju u različitim vremenskim intervalima. Istraživanje prikazano u [51] predlaže metodu detekcije DDoS prometa generiranog IoT uređajima u korporativnom okruženju primjenom *Deep Autoencoders* metode temeljene na umjetnim neuronskim mrežama. Autori u [58] navode da je

učinkovitost detekcije DDoS prometa veća ukoliko se provodi na rubu promatranog IoT okruženja. U svrhu detekcije korištena je softverski definirana mreža (engl. *Software Defined Network,* SDN) kao novo i fleksibilno rješenje u pogledu dinamičkog definiranja pravila i upravljanja prometnim tokovima.

Istraživanje [59] ističe porast utjecaja IoT uređaja na povećanje intenziteta DDoS prometa, a autori u [60] i [61] naglašavaju potrebu za istraživanjem mogućnosti detekcije DDoS prometa generiranog posredstvom SHIoT uređaja. Prema tome, kao prvi nedostatak uočava se vrlo ograničen broj istraživanja ovog specifičnog problema unatoč njegovoj izraženosti i tendenciji budućeg rasta. Uz navedeno, do sada provedena istraživanja ne uzimaju u obzir mogućnost detekcije DDoS prometa temeljem klasa SHIoT uređaja s približno jednakim karakteristikama generiranog prometa kod uobičajenog rada uređaja. Konačno, kao nedostatak prethodnih istraživanja uočava se brojnost i raznovrsnost SHIoT uređaja korištenih u prikupljanju prometa. Istraživanje [57] koristi tri uređaja pri čemu je promet prikupljan u periodu od 10 minuta, dok istraživanje [51] koristi devet uređaja od kojih su pet *web* ili sigurnosne kamere. Istraživanje [58] temelji se isključivo na podatcima prikupljenim emulacijom uređaja u laboratorijskom okruženju.

Identificirani nedostatci prethodnih istraživanja, poput uvažavanja značajki SHIoT prometa pri detekciji DDoS prometa, uzimanja u obzir klase SHIoT uređaja koje generiraju približno jednake vrijednosti značajki prometa te brojnost uređaja korištenih u istraživanju, nastojat će se otkloniti planiranim istraživanjem.

Značaj ovog istraživanja vidljiv je i kroz porast broja istraživanja i projekata u ovom području. Primjer za to je i projekt naziva *Mitigating IoT-Based Distributed Denial Of Service (DDoS)* koji provode NIST (engl. *National Institute od Standards and Technology*) i NCCoE (engl. *National Cybersecurity Center of Exellence*), a adresiraju upravo problematiku generiranja DDoS prometa posredstvom IoT uređaja.

1.4 Korištene znanstvene metode

Tijekom istraživanja u okviru ovog doktorskog rada korištene su znanstvene metode opisane u nastavku.

Metode kompilacije, sinteze i povijesna metoda korištene su pri preuzimanju tuđih opažanja, stavova i zaključaka te prikaza statističkih pokazatelja i trendova u domeni koncepta IoT. Na osnovi kompilacije korištena je induktivna metoda u svrhu donošenja zaključaka na temelju opažanja i stavova drugih istraživača.

Metodom deskripcije opisani su i pojašnjeni elementi i terminologija u doktorskom radu važni za razumijevanje problema istraživanja. Istom metodom objašnjeno je i formiranje laboratorijskog okruženja kao i metodologija prikupljanja podataka. Metodom analize identificirane su značajke prometa koje mogu biti korištene pri definiranju klasa i klasifikaciji SHIoT uređaja.

Tijekom prikupljanja podataka korištena je metoda mjerenja s obzirom da su mjerene određene značajke prometa kao što je brzina prijenosa podataka, vrijeme trajanja prometnog toka i slično. Metodom simulacije generiran je DDoS promet nužan za razvoj modela detekcije anomalija mrežnoga prometa.

U svrhu definiranja klasa SHIoT uređaja korištene su matematička, statistička i metoda klasifikacije. Metoda modeliranja korištena je pri razvoju modela višeklasne klasifikacije SHIoT uređaja kao i pri razvoju modela detekcije DDoS prometa. Matematička metoda korištena je i za razvoj modela s obzirom da se korištene metode strojnog učenja temelje na matematičkim metodama.

1.5 Struktura doktorskog rada

Struktura ovog doktorskog rada proizašla je iz uočenog i postavljenog problema istraživanja kao i znanstvenih hipoteza i cilja istraživanja te navedenih znanstvenih metoda.

U prvom poglavlju doktorskog rada opisan je i definiran predmet istraživanja kao i motivacija autora za provedbu istraživanja. Nadalje, određen je cilj istraživanja i znanstveni doprinosi kao produkti planiranog istraživanja. Prikazan je osvrt na dosadašnja istraživanja koji ukazuje na trenutne smjerove istraživanja problemskog područja, ali i ukazuje na nedostatke tih istraživanja te određuje prostor istraživanja u okviru ovog doktorskog rada.

S obzirom da će se istraživanje provoditi u okruženju koncepta IoT, u drugom poglavlju detaljno su objašnjene osnovne karakteristike ovog koncepta nužne za daljnje razumijevanje problemskog područja i istraživanja. Koncept IoT pojašnjen je kroz prikaz arhitekture, korištenih komunikacijskih tehnologija i mogućih područja primjene. Prikazana je analiza statističkih pokazatelja kao što su rast primjene i prihvaćenost te stupanj penetracije koncepta IoT u različitim vertikalnim područjima primjene.

U trećem poglavlju detaljno je pojašnjen koncept pametnog doma kao jedno od najbrže rastućih područja primjene koncepta IoT. S obzirom da je fokus istraživanja usmjeren upravo na to područje primjene, pobliže je razjašnjeno okruženje pametnog doma kroz skupine

korištenih uređaja, korištene komunikacijske tehnologije i arhitekture takvog okruženja. Opisane su karakteristike mrežne komunikacije u navedenom okruženju. Usporedno su naglašeni i sigurnosni aspekti pametnog doma kroz raznovrsne prijetnje i ranjivosti koje predstavljaju važan aspekt prihvaćanja i primjene ovog koncepta.

Budući da je istraživanje u okviru doktorskog rada usmjereno na detekciju anomalija mrežnoga prometa koje nastaju kao rezultat generiranja DDoS prometa SHIoT uređaja, u četvrtom poglavlju ovoga rada pojašnjen je termin anomalija u komunikacijskoj mreži kao i princip provedbe DDoS napada. Kompleksnost i raznovrsnost DDoS napada prikazani su taksonomijama te su analizom statističkih pokazatelja utvrđeni trenutni trendovi opsega napada, razine provedbe i protokola korištenih u provedbi DDoS napada. Istaknuta je i važnost pojave koncepta IoT i uređaja pod tim konceptom u porastu broja i intenziteta DDoS napada, gdje do izražaja dolaze upravo uređaji objedinjeni pod konceptom pametnog doma.

Petim poglavljem opisan je razvoj modela detekcije anomalija mrežnoga prometa temeljenog na značajkama prometa i klasnoj pripadnosti uređaja kroz više faza. Analizirane su i sustavno prikazane značajke prometa korištene u dosadašnjim istraživanjima u svrhu identifikacije IoT uređaja. Pojašnjen je proces formiranja laboratorijskog okruženja i prikupljanja podataka. Definirane su klase SHIoT uređaja te je razvijen višeklasni klasifikacijski model temeljen na *boosting* metodi strojnog učenja kao preduvjet za razvoj modela detekcije anomalija mrežnoga prometa. Konačno, prikazan je i pojašnjen razvoj modela detekcije anomalija mrežnoga prometa temeljen na značajkama prometa i klasnoj pripadnosti SHIoT uređaja. Za oba razvijena modela (višeklasni klasifikacijski model i model detekcije anomalija) provedena je *k*-struka unakrsna validacija te su izračunate mjere za ocjenu performansi modela. Ovim poglavljem prikazana je i diskusija o rezultatima provedenog istraživanja. Pojašnjen je značaj detekcije DDoS prometa na temelju klasa SHIoT uređaja kao i praktična primjenjivost razvijenog modela. Uz to, navedena su ograničenja provedenog istraživanja te uočeni potencijal za buduća istraživanja u okviru identificiranog problemskog područja.

U posljednjem, šestom poglavlju, dana su zaključna razmatranja temeljena na dobivenim rezultatima istraživanja kojima su dokazane postavljene znanstvene hipoteze predmetnog istraživanja te su ostvareni izvorni znanstveni doprinosi. Istaknuta je učinkovitost korištenog pristupa u razvoju modela detekcije anomalija mrežnoga prometa u IoT okruženju kao i učinkovitost primjene metoda strojnog učenja u promatranom problemskom području. Uz navedeno, dan je osvrt na potencijalne primjene razvijenog modela u praksi.

1.6 Faze i aktivnosti istraživanja

Istraživanje je provedeno kroz pet faza kako slijedi i kako je prikazano tablicom 1.1: (1) analiza i identifikacija specifičnih značajki MTC prometa generiranog SHIoT uređajima, (2) formiranje okruženja pametnog doma i prikupljanje podataka, (3) obrada i priprema prikupljenih podataka za daljnju analizu, (4) razvoj modela detekcije DDoS prometa, (5) validacija razvijenog modela detekcije DDoS prometa. Detaljan proces provedbe istraživanja i razvoja modela detekcije nelegitimnog prometa prikazan je UML dijagramom toka u prilogu 1.

U prvoj fazi istraživanja analizirana je aktualna znanstvena i stručna literatura s ciljem boljeg razumijevanja MTC prometa i razlika u odnosu na HTC promet. U ovoj fazi identificirat će se specifične značajke MTC prometa koje je moguće iskoristiti za klasifikaciju SHIoT uređaja. Identificirane značajke (npr. periodi aktivnosti uređaja, količina prometa koji uređaj generira u promatranom vremenskom periodu, broj javnih poslužitelja kojima uređaj pristupa, prosječna veličina paketa i sl.) bit će korištene za potrebe definiranja i određivanja klase SHIoT uređaja u kasnijim fazama istraživanja.

U drugoj fazi istraživanja prikupljani su primarni i sekundarni podatci potrebni za daljnju provedbu istraživanja. U svrhu prikupljanja primarnih podataka stvoreno je okruženje pametnog doma u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava Fakulteta prometnih znanosti pri čemu su implementirani SHIoT uređaji i povezani u lokalnu mrežu. Okruženje pametnog doma stvoreno je s ciljem prikupljanja realnih podataka međusobnom komunikacijom uređaj – uređaj i uređaj korisnik što je rezultiralo generiranjem legitimnog MTC prometa. SHIoT uređaji povezani su bežičnim putem na bežičnu pristupnu točku ili žičanim putem na preklopnik, ovisno o komunikacijskoj izvedbi uređaja. Generirani promet prikupljan je na preklopniku gdje su povezani SHIoT uređaji žičanim putem i putem bežične pristupne točke na koju su povezani SHIoT uređaji koji komuniciraju Wi-Fi tehnologijom. Za potrebe prikupljanja prometa korištena je metoda zrcaljenja porta koja je omogućila prikupljanje prometa bez unosa šuma, odnosno nenamjernog utjecaja na promet. Uz navedeno, tijekom vremenskog perioda prikupljanja prometa simulirano je generiranje DDoS prometa posredstvom SHIoT uređaja primjenom dostupnih programskih alata za generiranje takvog oblika prometa (poput BoNaSi, LOIC, XOIC, HULK i slični).

Tablica 1.1 Opis faza i aktivnosti istraživanja u svrhu razvoja modela detekcije anomalija mrežnoga prometa

R. br.	Faza	Aktivnosti	Korištene metode i programski alati	Očekivani rezultat	Ostvareni znanstveni doprinos
1.	Analiza literature	Analiza aktualne znanstveno-istraživačke i stručne literature u svrhu identifikacije značajki MTC prometa generiranog SHIoT uređajima.	Metode kompilacije, sinteze i analize	Identificirane značajke prometa specifične za MTC promet koji generiraju SHIoT uređaji.	
2.	Prikupljanje podataka	Formiranje SHIoT okruženja u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava		Istraživačko laboratorijsko okruženje namijenjeno generiranju MTC prometa korištenjem SHIoT uređaja.	
		Generiranje legitimnog prometa SHIoT uređaja.	Wireshark 2.6.3, zrcaljenje porta, metoda mjerenja	Prikupljeni podatkovni skup legitimnog SHIoT prometa za daljnju analizu.	
		Generiranje DDoS prometa simulacijom i/ili manipulacijom SHIoT uređaja.	BoNaSi, Wireshark 2.6.3, zrcaljenje porta, metoda simulacije	Prikupljeni podatkovni skup DDoS prometa za daljnju analizu.	
		Prikupljanje sekundarnih podataka i stvaranje jedinstvenog podatkovnog skupa		Jedinstveni podatkovni skup MTC prometa raznovrsnih SHIoT uređaja i DDoS prometa	
3.	Odabir podskupa značajki za razvoj modela detekcije anomalija mrežnoga prometa	Filtriranje i predobrada prometa za individualne SHIoT uređaje u podatkovnom skupu legitimnog prometa SHIoT uređaja.	Capinfos, splitcap, editcap i tcpdump programski alati za manipulaciju *.pcap* datoteka	Podatkovni podskup koji sadrži legitimni promet za individualne SHIoT uređaje.	
		Ekstrakcija značajki prometnog toka identificiranih u prvoj aktivnosti za legitiman i nelegitiman promet.	CICFlowMeter	Podatkovni podskup koji sadrži značajke prometa SHIoT uređaja i DDoS prometa.	
		Odabir i izračun zavisne značajke na temelju koje je moguće klasificirati SHIoT uređaje pri generiranju legitimnog prometa	Koeficijent varijacije	Odabrana i izračunata zavisna značajka u svrhu daljnje klasifikacije SHIoT uređaja	
4.	Razvoj modela detekcije anomalija mrežnog prometa temeljenog na značajkama prometa i klasnoj pripadnosti uređaja	Definiranje broja klasa SHIoT uređaja na temelju raspona vrijednosti odabrane značajke MTC prometa u funkciji definiranja profila legitimnog prometa.	Klasifikacija koeficijenata varijacije, Tukey metoda transformacije podataka, Shapiro-Wilk i Shapiro-Francia testovi normalnosti, min-max normalizacijska metoda, programski alat Stata	Broj klasa kojima SHIoT uređaji mogu pripadati te definirani profili normalnog prometa za pojedinu klasu na osnovi raspona vrijednosti značajki generiranog MTC prometa.	
		Izračunavanje stupnja povezanosti između nezavisnih i zavisne značajke primjenom metode informacijske dobiti u svrhu odabira najrelevantnijih nezavisnih značajki korištenjem WEKA programskog alata.	Metoda informacijske dobiti, programski alat WEKA 3.8	Odabrane nezavisne značajke MTC prometa SHIoT uređaja s najvećim stupnjem povezanosti.	Identifikacija značajki MTC prometa temeljem kojih je moguće klasificirati SHIoT uređaje u svrhu detekcije nelegitimnog DDoS prometa.
		Opisivanje faza razvoja modela UML dijagramom toka korištenjem MS Visio alata.	MS Visio 216	UML dijagram toka razvoja modela.	
		Određivanje pripadnosti SHIoT uređaja prethodno definiranim klasama nad podatkovnim skupom legitimnog MTC prometa generiranom u određenom vremenskom intervalu primjenom *logitboost* metode strojnog učenja.	*Logitboost* metoda, metoda poduzorkovanja, *k*-struka unakrsna validacija, metode ocjene performansi modela (*kappa*, točnost, TPR, FPR, F-mjera, preciznost, ROC, PRC, matrica konfuzije), programski alat WEKA 3.8	Izračun vjerojatnosti pripadanja SHIoT uređaja pojedinoj definiranoj klasi na temelju vrijednosti značajki generiranog MTC prometa, što označava inicijalnu klasnu pripadnost SHIoT uređaja i omogućuje definirati profile legitimnog prometa za svaku klasu.	Definirani profili legitimnog prometa za pojedinu klasu SHIoT uređaja.
		Analiza odabranih značajki nad mješovitim podatkovnim skupom koji sadrži legitiman i DDoS promet primjenom metode logističkih stabala odluke iz skupa metoda strojnog učenja korištenjem WEKA programskog okruženja.	Metoda logističkih stabala odluke, *k*-struka unakrsna validacija, metode ocjene performansi modela (*kappa*, točnost, TPR, FPR, F-mjera, preciznost, ROC, PRC, matrica konfuzije), programski alat WEKA 3.8	Utvrđen stupanj podudarnosti značajki MTC prometa generiranog SHIoT uređajem s profilom legitimnog prometa pripadajuće klase	Razvijeni model detekcije DDoS prometa temeljen na klasama SHIoT uređaja koji generiraju promet.

Drugi način generiranja DDoS prometa je manipulacijom SHIoT uređaja korištenjem javno dostupnih malicioznih programskih kodova kao što su Mirai i Bashlite (odnosi se na SHIoT uređaje koje je moguće kompromitirati). Pri tome su legitimni i DDoS uzorci prometa adekvatno označeni u svrhu stvaranja cjelovitog podatkovnog skupa generiranog prometa i daljnje obrade podataka.

Promet je prikupljan primjenom programskog alata Wireshark te je pohranjen u *.pcap* formatu čime će se omogućiti daljnja obrada prikupljenih podataka. Sekundarne podatke predstavljaju podatkovni skupovi SHIoT prometa generiranih za potrebe drugih istraživanja, a javno su dostupni i moguće ih je primijeniti u svrhu predmetnog istraživanja. U svrhu prikupljanja što je moguće većeg broja raznovrsnih SHIoT uređaja i prometa koji generiraju, korišteni su primarni i sekundarni skupovi podataka.

U trećoj fazi istraživanja provedene su aktivnosti pripreme podataka za daljnju obradu. To podrazumijeva filtriranje prikupljenih podataka i ekstrakciju značajki identificiranih u prvoj fazi istraživanja. Promatrane su isključivo vrijednosti zaglavlja paketa, odnosno statistička obilježja prometa, dok se sadržaj paketa nije razmatrao zbog primjene kriptografskih metoda u prijenosu. U ovoj fazi odabrane su zavisne i nezavisne značajke prometa. U tu svrhu određen je stupanj povezanosti između zavisnih i nezavisnih značajki primjenom dostupnih metoda za izračun koeficijenta korelacije te su odabrane one značajke s najvećim stupnjem povezanosti. Odabrane značajke korištene su za potrebe definiranja modela u sljedećoj fazi istraživanja.

Cilj četvrte faze istraživanja je definirati model detekcije DDoS prometa koji generiraju SHIoT uređaji i to kroz dva koraka. Prvi korak podrazumijeva definiranje broja klasa SHIoT uređaja na temelju vrijednosti odabranih prometnih značajki pojedinačno analiziranih uređaja. Pri tome je korištena istraživanjem utvrđena adekvatna metoda iz skupa metoda regresijske analize i strojnog učenja. Opisani pristup omogućuje definiranje profila legitimnog prometa koji generira pojedina klasa SHIoT uređaja. Drugim korakom analizirane su odabrane značajke prometa raznovrsnih SHIoT uređaja. Cilj ovog koraka je utvrditi inicijalnu pripadnost pojedinog uređaja prethodno definiranim klasama. Nakon utvrđivanja klasne pripadnosti uređaja u narednom vremenu provjeravana je podudarnost generiranog prometa promatranog uređaja s uzorkom legitimnog prometa pripadajuće klase. Pri tome granične vrijednosti i drugi parametri modela, kao i korištene nezavisne značajke, ovise o identificiranoj klasi uređaja. Nepodudarnost vrijednosti značajki prometa s vrijednostima značajki identificirane pripadajuće klase iznad definirane granične vrijednosti, podrazumijeva da uređaj generira DDoS promet u promatranom vremenskom intervalu. U svrhu provjere klasne pripadnosti korištena je,

istraživanjem utvrđena adekvatna klasifikacijska metoda iz skupa metoda strojnog učenja. Dosadašnji pristupi detekciji DDoS prometa nisu uzimali u obzir klase uređaja koje generiraju promet u mreži, već su promet promatrali neovisno o uređaju koji ga generira ili pojedinačno za svaki uređaj. U scenariju u kojem egzistiraju IoT uređaji, skupine uređaja se ponašaju različito s obzirom na namjenu i broj funkcionalnosti pri čemu generiraju različite uzorke prometa. Prema tome, ključno je identificirati klasnu pripadnost uređaja temeljem generiranog prometa i odstupanja od identificirane klase u narednim vremenskim intervalima.

Petom fazom istraživanja model je validiran te je provedena ocjena performansi modela korištenjem validacijskih mjera kao što su točnost, preciznost, specifičnost, matrica konfuzije te ROC (engl. *Receiver Operating Characteristics*) krivulja. Validacija i ocjena performansi su aktivnosti koje se odnose i na klasifikacijski model u prvom koraku četvrte faze kao i na model detekcije anomalija mrežnoga prometa u drugom koraku četvrte faze.

2 Razvoj i primjena koncepta internet stvari

S obzirom da je istraživanje provedeno u okruženju koncepta IoT, ovim poglavljem detaljno su objašnjene osnovne karakteristike ovog koncepta nužne za daljnje razumijevanje problemskog područja i istraživanja. Koncept IoT pojašnjen je kroz prikaz arhitekture, korištenih komunikacijskih tehnologija i mogućih područja primjene. Prikazana je analiza statističkih pokazatelja kao što su rast primjene i prihvaćenost te stupanj penetracije koncepta IoT u različitim vertikalnim područjima primjene.

2.1 Definicija koncepta internet stvari

Internet stvari predstavlja termin definiran brojnim izvorima stručne i znanstveno-istraživačke literature. IoT predstavlja novu komunikacijsku paradigmu u području IK tehnologija u kojemu se razlikuju dva pojma: internet i stvar (fizički objekt). Pojam internet podrazumijeva globalno rasprostranjeni sustav međupovezanih računalnih mreža i krajnjih uređaja koji koriste standardizirani internet protokol stog (TCP/IP) u svrhu međusobne komunikacije. Pojmom stvar obuhvaćeni su fizički objekti ili živa bića koja egzistiraju u stvarnom svijetu [62]. Objekti uključuju, ne samo svakodnevno korištene elektroničke uređaje i napredne tehnološke proizvode, već i one objekte koji nisu elektronički poput hrane, odjeće, namještaja, različitih materija, umjetnina, znamenitosti, i dugo [63].

Ideju koncepta IoT prvi je definirao Kevin Ashton, suvlasnik i izvršni direktor tvrtke Auto-ID Center 1999. godine. Tvrtka Auto-ID Center istraživala je i razvijala tehnologiju automatske identifikacije. Pri tome su predstavili koncept u kojemu svi objekti, neovisno o tome jesu li fizički ili elektronički, imaju dodijeljenu elektroničku identifikacijsku oznaku. Takva oznaka sadrži informacije o objektu kojemu je dodijeljena. Pri tome svaki fizički objekt s dodijeljenom oznakom postaje čvor u komunikacijskoj mreži čime je omogućen udaljeni, beskontaktni pristup informacijama vezanima uz promatrani objekt [64], [65].

Daljnjim razvojem i porastom primjene, koncept IoT definirala su brojna stručna standardizacijska tijela, organizacije i udruge iz područja IK tehnologija, ali i brojni istraživači. Prema tome, definiciju koncepta IoT moguće je razmatrati s aspekta stručnih organizacija u području IK tehnologija kao i sa znanstveno-istraživačkog aspekta.

Europski institut za telekomunikacijske standarde, ETSI (engl. *The European Telecommunications Standards Institute*) neovisno je i neprofitno tijelo koje donosi globalne standarde u području IK tehnologija te ga Europska Unija prepoznaje kao Europsku organizaciju za standarde. Iako ETSI ne definira egzaktno termin IoT, u dokumentu *Machine-to-Machine communications (M2M); Functional architecture* definira M2M (engl. *Machine to Machine*) kao sličan koncept koji se ujedno smatra i pretečom koncepta IoT. ETSI definira M2M kao komunikaciju između dva ili više entiteta koji ne zahtijevaju nužno ljudsku intervenciju, a M2M usluge imaju funkciju automatizacije odluka i komunikacijskih procesa [66].

Najveća svjetska organizacija u području elektrotehnike i elektronike IEEE (engl. *Institute of Electronical and Electronics Engineers*) 2014. godine prepoznaje koncept IoT kao

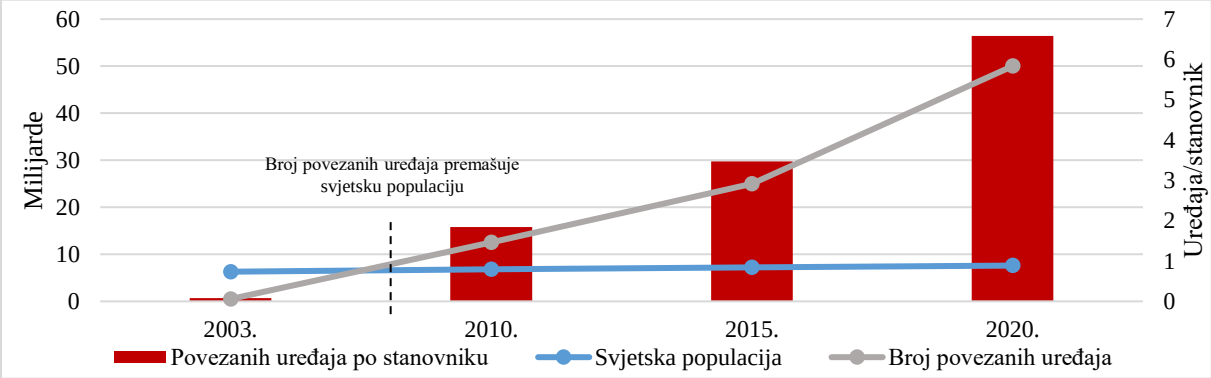
važan multidisciplinaran problem te pokreće *Internet of Things* inicijativu. Dokumentom [67] IEEE neslužbeno definira koncept IoT kao mrežu objekata pri čemu svaki posjeduje ugrađene senzore koji su povezani na internetsku mrežu.

Nadalje, Međunarodna telekomunikacijska unija ITU (engl. *International Telecommunication Union*) kao specijalizirano tijelo Ujedinjenih naroda (UN) za područje IK tehnologija, zajedno s Europskim istraživačkim klasterom za *Internet of Things* (engl. *European Research Cluster on Internet of Things*, IERC), nešto detaljnije definira IoT i to kao globalnu infrastrukturu informacijskog društva koja omogućuje napredne usluge kroz međupovezanost stvari (fizičkih i virtualnih) primjenom postojećih i nadolazećih interoperabilnih IK tehnologija [68].

Prema Europskom istraživačkom klasteru za Internet, ovaj koncept predstavlja globalni koncept i zahtijeva generičku definiciju. Prema dokumentu IERC-a definiranje koncepta IoT predstavlja zahtjevnu zadaću s obzirom na temelje koncepta i korištene tehnologije i tehnološke procese, od senzorskih uređaja, komunikacijskih sustava, agregacije i predprocesiranja podataka pa do pružanja usluge krajnjem korisniku [69]. Prema tome, IERC definira koncept IoT kao dinamičku globalnu mrežnu infrastrukturu sa sposobnošću samostalne konfiguracije, a temeljena je na standardnim i interoperabilnim komunikacijskim protokolima gdje fizički i virtualni objekti imaju identitete, fizičke atribute i virtualne osobnosti te koriste inteligentna sučelja i integrirana su u komunikacijsku mrežu.

Definicija koncepta IoT koju pruža tvrtka Cisco Systems Inc., kao jedan od globalno vodećih proizvođača mrežne opreme, razlikuje se od definicija ostalih organizacija. Prema Cisco-u, koncept IoT predstavlja trenutak u vremenu gdje broj objekata povezanih na internetsku mrežu premašuje svjetsku populaciju, kako je prikazano grafikonom 2.1 [70]. Međutim, isti izvor ističe IoT kao prvu evoluciju internetske mreže koja dovodi do revolucionarnih primjena koje će značajno unaprijediti način života, učenja, rada i ostalih aspekata ljudskog života.

Grafikon 2.1 Broj povezanih uređaja



Izvor: [70]

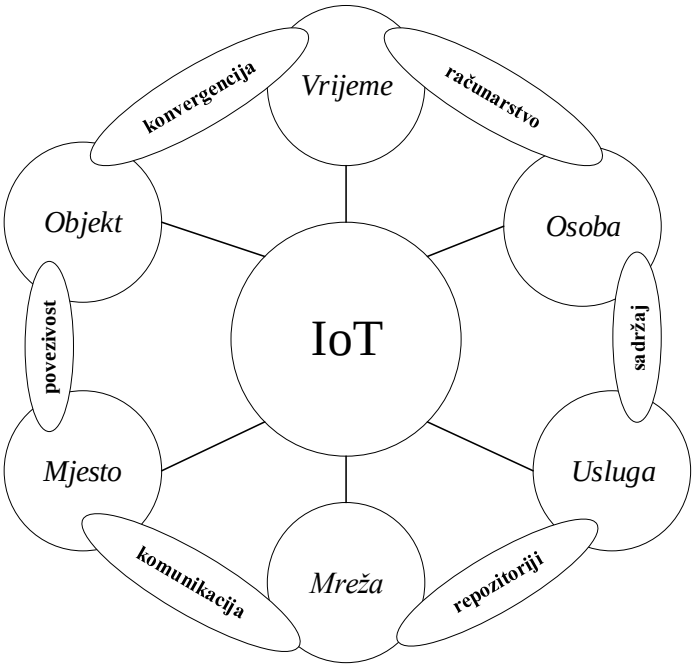
Također i telekom operatori prepoznaju potencijal i identificiraju ključne karakteristike ovog koncepta koje se prema [71] mogu promatrati kroz:

- potencijal da koncept IoT omogući niz novih usluga koje će unaprijediti kvalitetu života korisnika kroz više temeljnih sektora gospodarstva,
- zahtjeve za globalnim distribucijskim modelima i konzistentnim globalnim uslugama s ciljem zadovoljavanja korisničkih potreba,
- prilike za razvoj novih komercijalnih modela koji će pružati podršku globalnim implementacijama,
- raznovrsne zahtjeve postavljene pred razvoj mobilnih mreža kao rezultat ponašanja IoT uređaja i povezanih aplikacija.

Iz navedenoga moguće je zaključiti da brojna stručna tijela i organizacije u području IK tehnologija prepoznaju IoT kao važan koncept u daljnjem razvoju IK tehnologija koji ima potencijal automatizacije odvijanja različitih procesa, donošenja odluka i pružanja novih oblika usluga kao i omogućavanja dodane vrijednosti za krajnjeg korisnika.

Uz stručna tijela, koncept IoT predmet je istraživanja brojnih istraživača koji su pružili različite, ali međusobno preklapajuće definicije i objašnjenja ovog koncepta. Europski istraživački klaster za internet stvari predstavlja jedno od najznačajnijih udruženja u području istraživanja koncepta IoT. Ovo udruženje definira IoT kao koncept koji omogućuje čovjeku i objektima povezanost u bilo koje vrijeme (engl. *Anytime*), na bilo kojem mjestu (engl. *Any place*) sa bilo kojim drugim čovjekom (engl. *Anyone*) i objektom (engl. *Anything*) koristeći bilo koju mrežu (engl. *Any network*) i uslugu (engl. *Any service*). To implicira prisutstvo elemenata

poput konvergencije, sadržaja, repozitorija, obrade, komunikacije i povezivanja u kontekstu međupovezanosti objekata i ljudi ili objekata i objekata tako da su prisutni svi prethodno navedeni elementi i zahtjevi kako je prikazano slikom 2.1 [72].



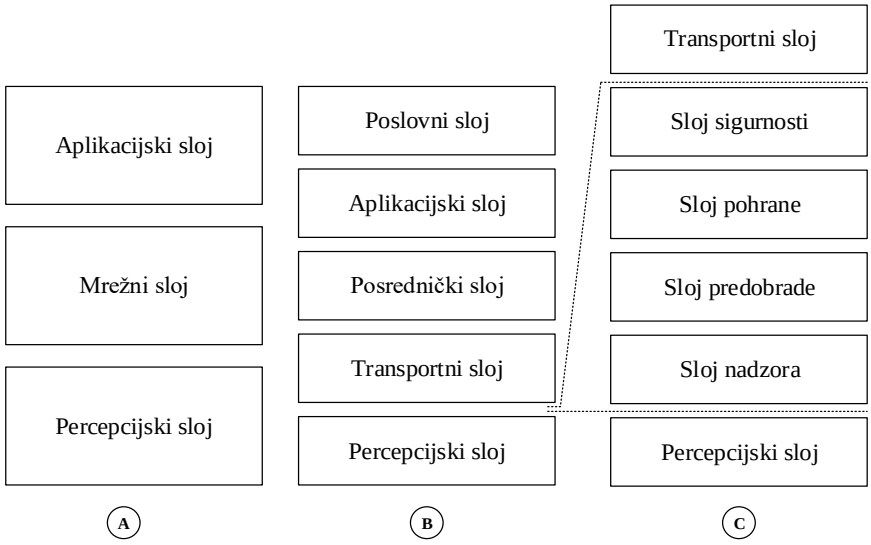
Slika 2.1 Elementi koncepta IoT [72]

Patel i ostali u istraživanju [63] prepoznali su važnost koncepta IoT te ga definiraju kroz tri načina međusobne komunikacije čovjeka i objekta: čovjek - čovjek, čovjek – objekt i objekt – objekt. Prema istom istraživanju objekti imaju mogućnost međusobnog prepoznavanja i međusobne komunikacije, a ugrađena inteligencija im omogućuje donošenje odluka temeljem konteksta i razmijenjenih informacija. Prema istraživanju [73], IoT adresira i potencijalno ima ključnu ulogu pri suočavanju s globalnim društvenim izazovima definiranim radnim okvirom Horizon 2020, a odnose se na zdravstvo, demografske promjene, održivu agrokulturu, sigurnu, čistu i učinkovitu energiju, pametan i integrirani promet i transport, klimatske promjene, okoliš i sigurno i inovativno društvo.

2.2 Arhitektura koncepta IoT

Arhitektura koncepta IoT od iznimne je važnosti za njegov razvoj i primjenu s obzirom na potencijalnu brojnost uređaja, količinu podataka koje takvi uređaji generiraju, potrebu za prijenosom generiranih podataka te njihovu obradu i isporuku krajnjem korisniku posredstvom raznovrsnih usluga. Različite arhitekture predlažu različiti istraživači [74]. Troslojna arhitektura predstavlja elementarnu arhitekturu definiranu početnim istraživanjima ovog područja [75].

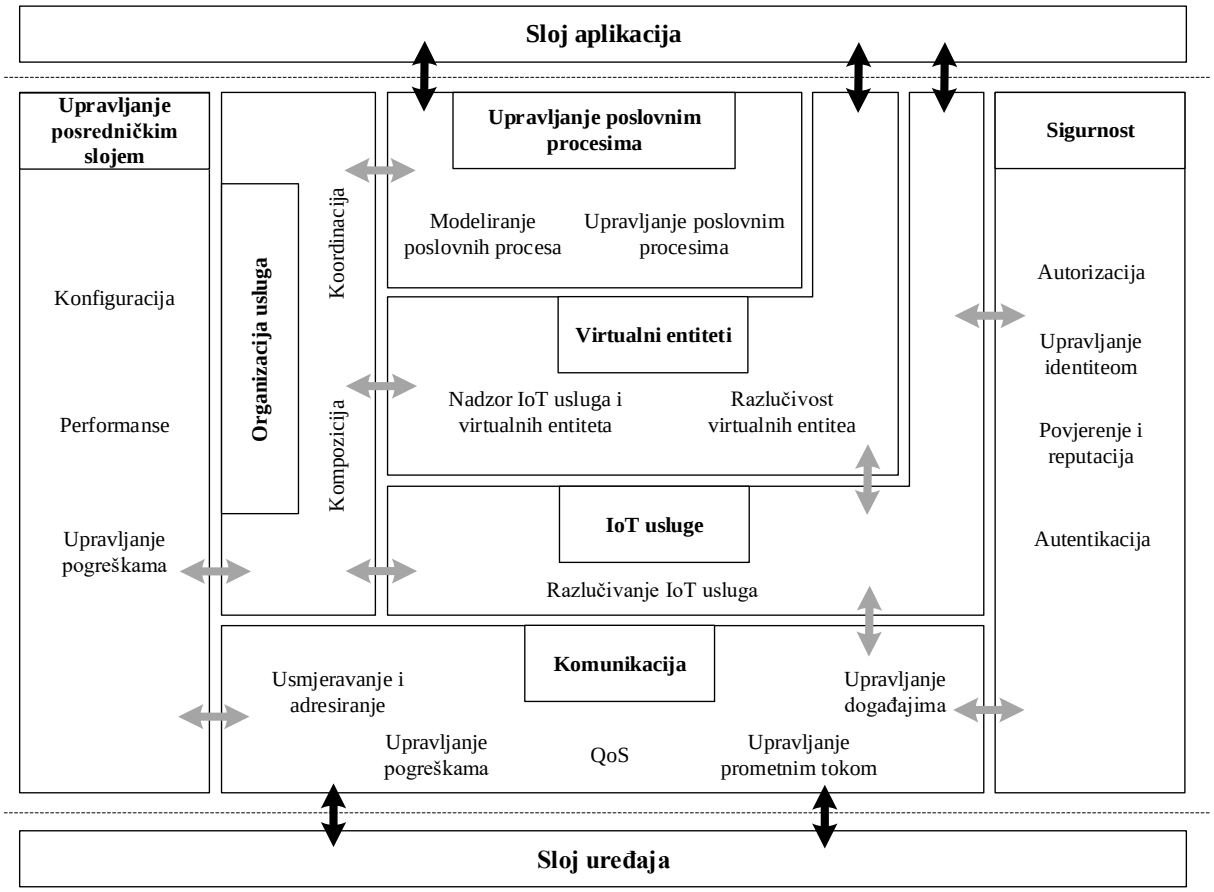
Troslojna arhitektura, prikazana slikom 2.2 a), sastoji se od percepcijskog, mrežnog i aplikacijskog sloja. Pri tome, percepcijski sloj ili sloj uređaja čine senzori čija je svrha prikupljanje informacija (vrijednosti fizičkih parametara) ili identifikacija drugih objekata u okruženju. Ključne tehnologije korištene u ovom sloju su senzorske tehnologije, RFID, 2D barkode, i dr. Mrežni sloj, koji predstavlja jezgru komunikacije koncepta IoT, obuhvaća konvergenciju komunikacijskih tehnologija kao i upravljanje komunikacijskom mrežom, a svrha mu je prijenos informacija prikupljenih na percepcijskom sloju prema aplikacijskom sloju i obrnuto. Aplikacijski sloj zadužen je za integraciju informacija i njihovu isporuku krajnjim korisnicima putem aplikacija. Pod utjecajem brzog razvoja koncepta IoT troslojna arhitektura postaje nedovoljna te se zamjenjuje s peteroslojnom arhitekturom, prikazanom slikom 2.2 (b) koja sadrži dodatna dva sloja: posrednički i poslovni sloj [76].



Slika 2.2 (a) troslojna, (b) peteroslojna arhitektura IoT koncepta i c) arhitektura temeljena na konceptu *Fog Computing* [74]

Sveprisutno računarstvo (engl. *ubiquitous computing*) predstavlja temeljnu zamisao koncepta IoT što podrazumijeva pridruživanje komunikacijskih mogućnosti i mogućnosti obrade podataka u sve fizičke objekte u okruženju. Interoperabilnost takvih heterogenih uređaja zahtijeva posrednički sloj koji će veliku količinu podataka (koju IoT uređaji generiraju) sažeti i učiniti iskoristivima za aplikacije koje koriste takve podatke. Arhitektura posredničkog sloja, kao ključnog segmenta arhitekture IoT koncepta, prikazana je slikom 2.3. Poslovni sloj namijenjen je upravljanju aktivnostima i uslugama cjelovitog sustava temeljenog na konceptu IoT uključujući aplikacije, privatnost korisnika te upravljanje ekonomskim aspektima. Osnovna funkcija ovog sloja je generiranje i izgradnja poslovnog modela i vizualizacija podataka (grafovi, dijagrami toka) temeljenim na podatcima prikupljenim iz aplikacijskog sloja. Na taj

način omogućuje se podrška procesima odlučivanja temeljenim na analizi velike količine podataka (engl. *Big Data*).



Slika 2.3 Arhitektura posredničkog sloja koncepta IoT [77]

Značajna i često korištena arhitektura je ona temeljena na računarstvu u oblaku (engl. *Cloud Computing*, CC). Razlog tome je količina podataka generiranih IoT uređajima i obrada takvih podataka gdje se CC rješenje pokazalo dovoljno fleksibilnim i skalabilnim u takvim poslovima. Unatoč karakteristikama i prednostima koje pruža CC, određene primjene koncepta IoT postavile su zahtjeve za čije ispunjenje je potreban novi pristup što je uvjetovalo razvoj koncepta *Fog Computing*. Novi zahtjevi koje nameću specifične primjene koncepta IoT odnose se na smanjenje latencije, povećanje kapaciteta obrade podataka, brzinu prijenosa podataka, brzinu odgovora na zahtjeve, i sl. Prema [78], *Fog Computing* predstavlja geografski distribuiranu arhitekturu čiji je cilj približiti resurse obrade podataka percepcijskim slojevima, odnosno izvoru generiranih podataka, da bi se ispunili prethodno navedeni zahtjevi. Arhitektura koncepta IoT temeljena na konceptu *Fog Computing* prikazana je slikom 2.2 c) pri čemu se uočavaju dodatni slojevi između percepcijskog i transportnog sloja koji pružaju funkcionalnosti nadzora, obrade, pohrane i zaštite podataka bez potrebe za njihovim prijenosom u CC okruženje. Uz termin *Fog*, često se primjenjuje i termin *Dew* čija je namjena korisniku dodatno

približiti resurse za obradu u svrhu stvarnovremene obrade i isporuke ključnih podataka te stvaranja redundancije sa *Fog* resursima [79].

S obzirom da je namjena koncepta IoT povezivanje velikog broja uređaja, razvoj fleksibilne slojevite arhitekture nametnulo se kao ključna potreba daljnjeg razvoja ovog koncepta. Unatoč jednostavnosti troslojne i peteroslojne arhitekture, kao osnovnih arhitekturnih modela, funkcionalnosti mrežnog i aplikacijskog sloja postaju raznovrsne i kompleksne. Pa tako mrežni sloj, osim usmjeravanja i prijenosa podataka pruža i podatkovne usluge poput agregacije podataka, obrade i sl. Aplikacijski sloj, uz pružanje usluge korisnicima i uređajima, pruža i podatkovne usluge kao što su rudarenje podataka, analitika i sl. Upravo zbog toga, s ciljem uspostave generičke i fleksibilne višeslojne arhitekture za koncept IoT, potreban je sloj usluge kao posrednik između mrežnog i aplikacijskog sloja. Sloj usluge omogućuje pružanje podatkovnih usluga kod primjene koncepta IoT. Navedeno je rezultiralo razvojem usluge orijentirane prema arhitekturi (engl. *Service Oriented Architecture*, SoA) kao podrške za IoT [80], [81]. Prema [82], usvajanje SoA arhitekture omogućava dekompoziciju kompleksnih sustava u primjene koje se sastoje od ekosustava jednostavnijih i dobro definiranih komponenata. Ovakav pristup omogućava višestruku primjenu istih softverskih i hardverskih komponenata jer se ne forsira primjena specifičnih tehnologija za implementaciju usluga. Kod primjene SoA arhitekture, imperativ za pružatelje i tražitelje usluga postaje jasna međusobna komunikacija neovisno o heterogenoj prirodi informacijskih struktura, poslovnih artefakata i drugih dokumenata. Spomenuto se često naziva i semantička interoperabilnost. Prema prethodno navedenome, ključni zahtjevi pri dizajnu sustava temeljenih na konceptu IoT su skalabilnost, modularnost, proširivost i interoperabilnost između heterogenih objekata i njihovih okruženja.

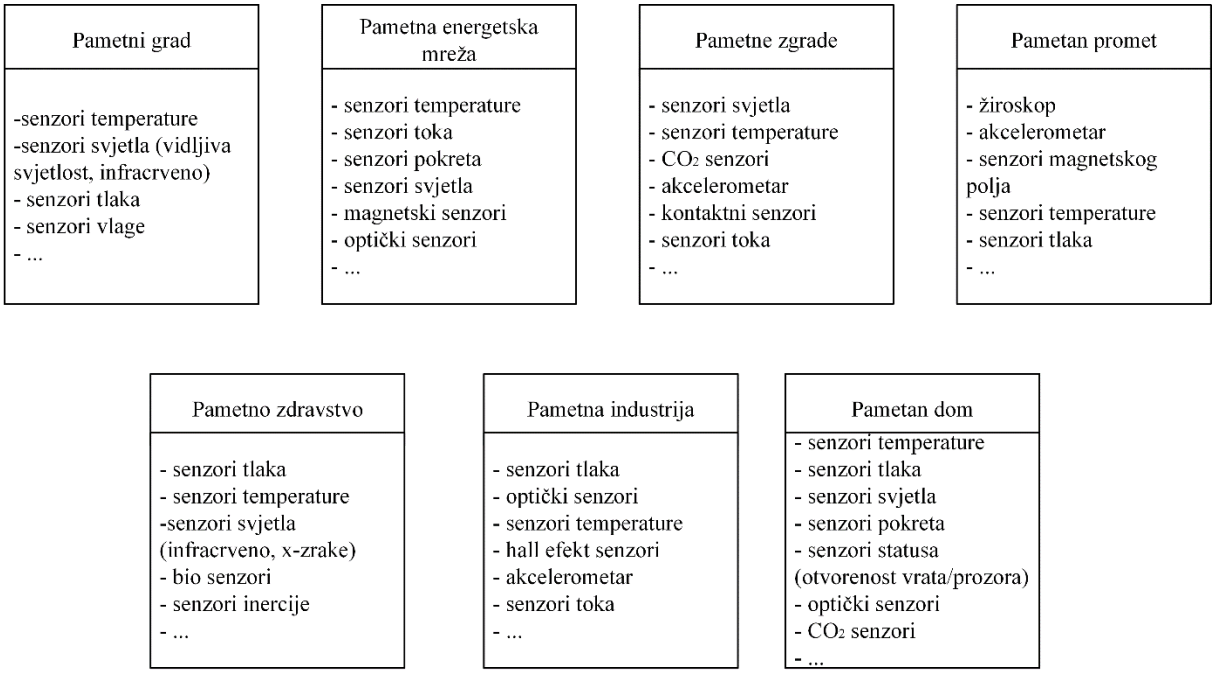
Arhitekturno gledano, koncept IoT za pravilno funkcioniranje zahtijeva brojne tehnologije na različitim slojevima arhitekture. Unatoč tome, percepcijski sloj, sastavljen od senzora, aktuatora i pristupnih komunikacijskih tehnologija, čini ovaj koncept različitim od konvencionalnih IK sustava.

2.2.1 Senzorske tehnologije

Korištenje senzorskih uređaja ključno je u okviru koncepta IoT. Prethodno prikazane arhitekture koncepta IoT sadrže percepcijski sloj čija je osnovna funkcija detekcija fizički mjerljivih svojstava fizičkog objekta ili okruženja. Senzori predstavljaju uređaje koji mjere fizičku vrijednost određene pojave i pretvaraju tu vrijednost u signal ili digitalnu vrijednost

koju naknadno može pročitati promatrač ili drugi uređaj. Senzor je uređaj koji detektira ili mjeri vanjski podražaj te ga pohranjuje, ukazuje ili na drugi način reagira na njega. S obzirom na prirodu vanjskog podražaja koji se detektira, postoje dvije kategorije senzora, fizikalni i kemijski [83].

Prema [84], fizikalni senzori općenito mjere fizikalne veličine poput duljine, tlaka zraka, temperature, struje, težine, zvuka i sl. Prema tome, moguće ih je definirati kao uređaje koji reagiraju na fizikalna svojstva ili podražaje na temelju kojih generiraju korespondentni električni signal. Za razliku od fizikalnog senzora, uređaj koji reagira na određenu kemijsku reakciju te koji može biti korišten za kvantitativno ili kvalitativno određivanje njezine promjene, kemijski je senzor. Takvi uređaji namijenjeni su mjerenju specifične kemijske supstance ili skupa kemijskih podražaja. Korištene vrste senzora ovise o području primjene koncepta IoT pri čemu pojedini senzor može biti korišten u više područja, ovisno o zahtjevima konkretne usluge što je vidljivo iz slike 2.4.



Slika 2.4 Vrste senzora korištene u vertikalnim područjima primjene koncepta IoT

Senzori korišteni u IoT uređajima mogu biti klasificirani u tri osnovne kategorije: senzori pokreta, senzori okoline i senzori pozicije. Najčešće korišteni senzori u IoT uređajima, ovisno o kategoriji, prikazani su tablicom 2.1.

Tablica 2.1 Često korišteni senzori u IoT uređajima

Vrsta senzora	Naziv senzora	Opis
Senzori pokreta	Akcelerometar	Elektromehanički uređaj koji može mjeriti promjene akceleracijske sile duž x, y i z osi
	Senzor linearne akceleracije	Vrsta akcelerometra koji detektira akceleraciju duž jedne osi bez uzimanja u obzir utjecaja gravitacijske sile
	Žiroskop	Mjeri stopu promjene kutnog momenta u sve tri osi
Senzori okoline	Senzor svjetla	Foto dioda koja mijenja karakteristike sukladno promjeni intenziteta svjetlosti
	Senzor blizine	Infracrveni senzor koji detektira prisutnost objekta u blizini bez fizičkog kontakta
	Senzor temperature	Mjeri temperaturu uređaja ili ambijenta
	Audiosenzor	Dvije vrste - 1) mikrofon - detektira akustički signal; 2) zvučnik - reproducira audiosignal
	Kamera	Slike i videozapisi
	Barometar	Mjeri tlak zraka ili uređaja
	Senzor otkucaja srca	Mjeri otkucaje srca
Pozicijski senzori	GPS	Prima signal sa satelita na temelju čega računa poziciju
	Magnetski senzor	Mjeri magnetsko polje uređaja u odnosu na Zemljino magnetsko polje

Izvor: [83]

Uz senzorske tehnologije, u konceptu IoT nužna je i primjena aktuatora. Za razliku od senzora, aktuator je uređaj koji pretvara energiju u pokret ili mehaničku energiju. Prema tome, u literaturi se još koristi termin elektromehanički transduktori. Za rad aktuatora potrebna je hidraulična tekućina, struja ili neki drugi izvor napajanja. Aktuatori mogu generirati pravocrtno gibanje, kružno gibanje ili oscilatorno gibanje. Najčešće korišteni aktuatori su termalni (pretvaraju termalnu energiju u gibanje korištenjem efekta termalne ekspanzije), električni (pretvaraju električnu energiju u gibanje, npr. elektromotori) i mehanički (pretvaraju mehaničku, najčešće rotacijsku energiju u linearno gibanje) [85].

2.2.2 Komunikacijske tehnologije

Područja primjene i način implementacije koncepta IoT zahtijeva bežični način povezivanja IoT uređaja zbog njihove brojnosti, heterogenosti i lokacijske disperziranosti [86]. Posljedično tome, jedan od ključnih elemenata ovog koncepta je bežična senzorska mreža (engl. *Wireless Sensor Network,* WSN) ili bežična senzorska i aktuatorska mreža (engl. *Wireless Sensor and Actuator Network,* WSAN) koja objedinjuje senzore i aktuatore (koji predstavljaju čvorove komunikacijske mreže). Čvorovi imaju mogućnost mjerenja određene pojave i

izvršavanja aktivnosti temeljem izmjerenih vrijednosti pri čemu komunikacijska infrastruktura omogućuje kooperaciju između senzora, resursa za obradu podataka i aktuatora [87].

Komunikacijske tehnologije koje omogućavaju komunikaciju i kooperaciju IoT uređaja dijele se na tehnologije kratkog i tehnologije dugog dometa. Komunikacijske tehnologije kratkog dometa koje omogućuju komunikaciju uređaja u PAN (engl. *Personal Area Network*), BAN (engl. *Body Area Network*) i LAN (engl. *Local Area Network*) mrežama kao i njihove karakteristike vidljive su u tablici 2.2.

Tablica 2.2 Komunikacijske tehnologije kratkog dometa u IoT konceptu

Tehnologija	Frekvencijski pojas	Domet	Brzina prijenosa	Trajanje baterije uređaja	Topologija	Standardizacija	Upravljačko tijelo
RFID	varijabilan (niska/visoka/ultra visoka frekvencija)	1 cm – 100 m	1 - 100 kb/s	N/A (pasivni način rada) / 3-5 godina (aktivni način rada)	P2P	otvoreni standard	više nadležnih tijela
NFC	13.56 MHz	0.2 m	424 kb/s	N/A (pasivni način rada) / 3-5 godina (aktivni način rada)	P2P	otvoreni standard	ISO/IEC
BLE	2.4 GHz	10 – 100 m	1 Mb/s	nekoliko mjeseci - nekoliko godina	P2P / Zvijezda	otvoreni standard	Bluetooth SIG
Ant	2.4 GHz	30 m	1 Mb/s	nekoliko godina	P2P / Zvijezda / Hijerarhijska / Mješovita	vlasnički	Garmin
EnOcean	ispod 1 GHz	30 – 300 m	125 kb/s	N/A (samonapajajući uređaji)	Mješovita	vlasnički	EnOcean Alliance
Z-Wave	ispod 1 GHz	40 – 200 m	100 kb/s	nekoliko mjeseci - nekoliko godina	Mješovita	vlasnički	Z-Wave Alliance
Insteon	ispod 1 GHz	30 – 50 m	37.5 kb/s	nekoliko mjeseci - nekoliko godina	Mješovita	vlasnički	Smartlabs
ZigBee	ispod 1 GHz, 2.4 GHz	10 – 100 m	250 kb/s	nekoliko mjeseci - nekoliko godina	Zvijezda / Hijerarhija / Mješovita	otvoreni standard	ZigBee Alliance
MiWi	ispod 1 GHz, 2.4 GHz	10 – 100 m	250 kb/s	nekoliko mjeseci - nekoliko godina	Zvijezda / Hijerarhija / Mješovita	vlasnički	Microchip Technology
DigiMesh	ispod 1 GHz, 2.4 GHz	10 – 100 m	250 kb/s	nekoliko godina	P2P / Mješovita	vlasnički	Digi Internation
WirelessHART	ispod 1 GHz, 2.4 GHz	10 – 100 m	250 kb/s	nekoliko godina	Mješovita	otvoreni standard	HART Communication Foundation
Thread	ispod 1 GHz, 2.4 GHz	10 – 100 m	250 kb/s	nekoliko mjeseci - nekoliko godina	Zvijezda / Hijerarhija / Mješovita	otvoreni standard	Thread Group Alliance
6LowPAN	ispod 1 GHz, 2.4 GHz	10 – 100 m	250 kb/s	nekoliko mjeseci - nekoliko godina	Zvijezda / Hijerarhija / Mješovita	otvoreni standard	IETF
Wi-Fi	2.4 GHz, 5 GHz; ispod 1 GHz (Wi-Fi HaLow)	100 m; 1 km (Wi-Fi HaLow)	varijabilna (Mb/s - Gb/s)	nekoliko dana - nekoliko godina	Zvijezda	otvoreni standard	Wi-Fi Alliance
NB – IoT	450 MHz – 3.5 GHz (2G/3G/4G spectrum)	10 – 15 km	250 kb/s	10 + godina	Zvijezda	otvoreni standard	3GSTR
eMTC	450 MHz – 3.5 GHz (kao LTE)	10 – 15 km	1 Mb/s	10 + godina	Zvijezda	otvoreni standard	3GSTR
EC-GSM-IoT	850 – 900 MHz, 1800 – 1900 MHz (kao GSM)	10 – 15 km	70 – 240 kb/s	10 + godina	Zvijezda	otvoreni standard	3GSTR
LoRaWAN	Ispod 1GHz	10 – 15 km	50 kb/s	10 + godina	Zvijezda zvijezda	otvoreni standard	LoRa Alliance
Symphony Link	Ispod 1GHz	10 – 15 km	50 kb/s	10 + godina	Zvijezda	vlasnički	Link labs
Wightless	Ispod 1 GHz, televizijski spektar	2 – 5 km	100 kb/s – 10 Mb/s	3 – 10 godina	Zvijezda	otvoreni standard	Weightless SIG proprietary
SIGFOX	Ispod 1GHz	10 - 50 km	100 b/s	10 + godina	Zvijezda	Vlasnički	Sigfox
DASH7	Ispod 1 GHz	2 – 5 km	167 kbps	10 + godina	Zvijezda / hijerarhija	Otvoreni standard	Dash7 Alliance

Izvor: [86–89]

Promatrano s aspekta prikazanih komunikacijskih tehnologija i standarda, uočavaju se razlike u dometu pojedine tehnologije, ali i brzine prijenosa, topologije povezivanja krajnjih uređaja i energetske učinkovitosti. Primjerice, u usporedbi s dobro poznatim standardima kao što je Wi-Fi (IEEE 802.11), ZigBee standard (IEEE 802.15.4) dizajniran je kao energetski učinkovita tehnologija s malom brzinom prijenosa podataka i niskom cijenom implementacije. Prema tome, pojedine komunikacijske tehnologije dizajnirane su kao odgovor na potrebe i zahtjeve nametnute konceptom IoT i specifičnostima uređaja koji egzistiraju u tom konceptu, dok su druge, već postojeće tehnologije, našle prostor primjene zbog karakteristika koje posjeduju.

Odabir i primjena komunikacijske tehnologije ovisit će o brojnim čimbenicima kao što su specifičnosti područja primjene koncepta IoT i specifičnosti pojedine usluge koja nameće različite komunikacijske zahtjeve. Pojedine usluge zahtijevaju nisku latenciju dok druge zahtijevaju sigurnu vezu i komunikaciju ili visoku autonomiju rada uređaja [87].

2.3 Vertikalna područja primjene koncepta IoT

Koncept IoT moguće je promatrati kroz proširenje postojeće interakcije između ljudi i aplikacija kroz novu dimenziju integracije i komunikacije koju predstavljaju objekti. Potencijal koji koncept IoT nudi omogućuje njegovu implementaciju i primjenu u različitim područjima koja obuhvaćaju društvo, okoliš i industriju, čiji su opisi i indikativni primjeri prikazani tablicom 2.3 [90].

Tablica 2.3 Područja primjene IoT koncepta

Područje primjene	**Opis**	**Indikativni primjeri**
Industrija	Aktivnosti koje uključuju financijske ili komercijalne transakcije između tvrtki, organizacija i ostalih entiteta.	Proizvodnja, logistika, uslužni sektor bankarstvo, posredništvo, i dr.
Okoliš	Aktivnosti povezane sa zaštitom, nadzorom ili razvojem svih prirodnih resursa	Agrikultura i uzgoj, recikliranje, usluge upravljanja okolišem, upravljanje energijom i dr.
Društvo	Aktivnosti/inicijative povezane s razvojem i uključivanjem društava, gradova i ljudi	Vladine usluge prema građanima i ostale društvene strukture, e-uključivanje (starije osobe i osobe s invaliditetom), itd.

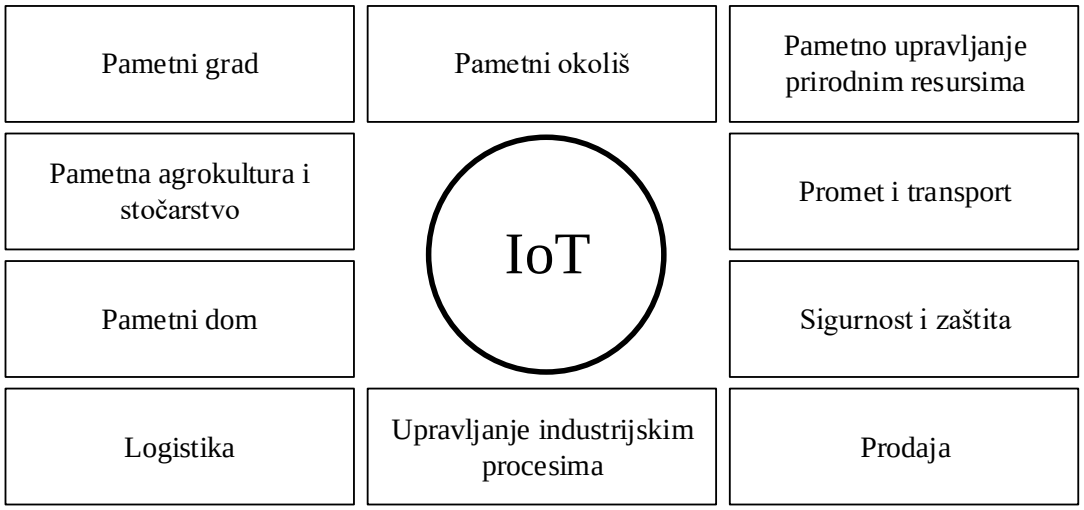
Izvor: [90]

S obzirom na područje primjene, objekti mogu biti različito percipirani. Primjerice, objekti u području industrije mogu predstavljati proizvode, opremu, sredstva prijevoza i sve što sudjeluje u životnom ciklusu proizvoda. U području okoliša objekt može predstavljati građevinske objekte, uređaje za mjerenje uvjeta u okolišu i sl. Konačno, u području društva objekt se može odnositi na uređaje na javnim prostorima, uređaje u kućanstvu i sl. U primjeni koncepta IoT gotovo je nemoguće izolirati jedno područje primjene, već je pojedina usluga često primijenjena na razini koja obuhvaća više od jednog područja. Primjerice, usluga nadzora opasnog otpada ne odnosi se samo na industriju kao područje primjene, već je potrebno u razmatranje uzeti okoliš i društvo.

Brojni autori i istraživanja identificiraju različite primjene IoT koncepta. U sklopu projekta IoT-I provedenog 2010. godine identificirano je ukupno 65 konkretnih primjena koncepta IoT pri čemu su one grupirane u 14 vertikalnih područja (pametni gradovi, pametni okoliš, pametna vodoopskrba, pametno mjerenje, sigurnost, prodaja, logistika, industrijska kontrola, pametna agrokultura, pametno stočarstvo, automatizacija doma i pametno zdravstvo).

Za razliku od navedenog, istraživanje [86] klasificira primjenu koncepta IoT na sedam vertikalnih područja koja se nazivaju još i pametna okruženja, odnosno pametni grad, pametni

dom, pametna energetska mreža, pametne zgrade, pametan promet, pametno zdravstvo i pametna industrija, prikazanih slikom 2.5. Međusobna komunikacija uređaja u okruženju, automatizacija pojedinih procesa i donošenja odluka bez ljudske intervencije rezultirala je i čestom primjenom termina „pametno“ uz pojedino područje primjene. Pa tako skup usluga temeljenih na IoT konceptu u okruženju grada rezultira konceptom nazvanim pametni grad, primjena za upravljanje okolišem rezultira konceptom pametnog okoliša i sl.



Slika 2.5 Područja primjene koncepta IoT

Slijedom navedenog, moguće je zaključiti da skup usluga koje se temelje na konceptu IoT, a primjenjuju se u specifičnom okruženju, čini takvo okruženje pametnim u kontekstu komunikacije, obrade podataka, donošenja odluka i odvijanja aktivnosti.

Pametni grad (engl. *Smart* City) predstavlja okruženje u kojemu su svi gradski resursi virtualno povezani i udaljeno upravljani [81]. Koncept IoT uvodi nove mogućnosti, kao što je mogućnost daljinskog nadzora i upravljanja uređajima, analize i poduzimanja aktivnosti na temelju informacija primljenih iz različitih tokova podataka u stvarnom vremenu. Kao rezultat toga, primjena koncepta IoT mijenja gradove poboljšanjem infrastrukture, stvaranjem učinkovitijih komunalnih usluga, poboljšanjem usluga prijevoza smanjenjem zagušenja cestovnog prometa i poboljšanjem sigurnosti građana. Prema [91], usluge koje su obuhvaćene u kontekstu pametnoga grada prikazane su tablicom 2.4.

Tablica 2.4 Usluge temeljene na IoT-u u okviru koncepta pametnoga grada

Naziv usluge	**Opis usluge**
Pametno parkiranje	Nadzor popunjenosti parkirnih mjesta u gradu
Strukturalna ispravnost	Nadzor vibracija i stanja materijala građevinskih objekata, mostova, prometne infrastrukture i sl.
Mape gradske buke	Nadzor buke u stvarnom vremenu.

Upravljanje prometnim zagušenjem	Praćenje vozila i pješaka u svrhu optimizacije rute vožnje ili pješačkih ruta.
Pametna rasvjeta	Inteligentno i vremenu prilagodljivo upravljanje uličnom rasvjetom.
Upravljanje otpadom	Detekcija popunjenosti kontejnera u svrhu optimiziranja rute odvoza.
Inteligentni transportni sustavi	Pametne ceste i autoceste uz primjenu dinamičnih znakova upozorenja i diverzije u ovisnosti o vremenskim uvjetima i neočekivanim događajima poput nesreća ili zagušenja.

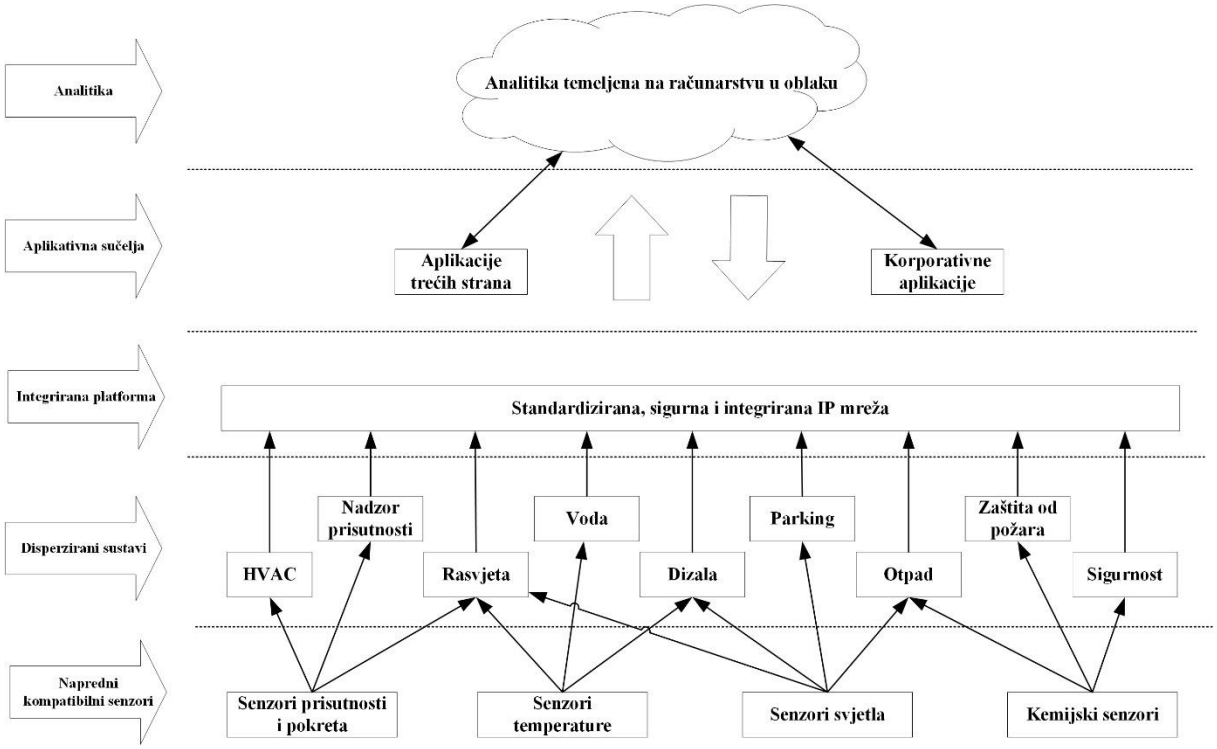
Izvor: [91]

Prema prethodno navedenom, pametni gradovi moraju ispunjavati dva ključna cilja. Prvi je pružanje napredne infrastrukture koja omogućava prikupljanje i obradu podataka korištenjem i međusobnom interakcijom IK tehnologija i na njima temeljenim uslugama navedenim tablicom 2.4. Drugi cilj predstavlja mogućnost interakcije korisnika s okruženjem koristeći aplikacije u svrhu pozitivnog utjecaja na okoliš i smanjenje zagađenja što će povećati kvalitetu života u gradovima.

S obzirom na kontinuirani rast potrošnje električne energije u privatnim kućanstvima i porast broja korisnika električne energije te povećanje ekoloških i regulatornih ograničenja, potreba za unaprjeđenjem ukupne učinkovitosti električnih mreža jedno je od današnjih ključnih problema [92]. Usluge okruženja pametne energetske mreže imaju svoju primjenu u generiranju, prijenosu, distribuciji i potrošnji električne energije. Integracija naprednih usluga temeljenih na konceptu IoT povećava učinkovitost tradicionalne energetske mreže pružanjem veće razine automatizacije, pouzdane predikcije opterećenja energetske mreže i sigurnijeg rada električnih uređaja, što rezultira povećanjem kvalitete usluge isporuke energije i većim zadovoljstvom korisnika. Također se očekuje niža fluktuacija opterećenja i naknadno smanjenje dinamike mreže, veća stabilnost, manji gubitci u linijama i niži operativni troškovi u smislu usklađivanja potražnje za energijom s ponudom [93].

Tijekom godina, stambene zgrade i građevinski objekti postali su kompleksniji i dinamičniji s višestrukim sustavima i uređajima koji podržavaju brojne aktivnosti i procese. Kompleksnost često dovodi do neučinkovitosti upravljanja takvim okruženjima. Okruženje pametne zgrade u određenoj mjeri postoji već duži niz godina, a primjeri toga vidljivi su u rasvjeti aktiviranoj pokretom te programibilnom sustavu upravljanja grijanjem, hlađenjem i ventilacijom (engl. *Heating, Ventilation, Air-Condition,* HVAC). Primjena koncepta IoT u okruženju pametne zgrade omogućuje upraviteljima bolju vidljivost komponenata zgrade, veću kontrolu i učinkovitost upravljanja [94]. Slikom 2.6 prikazana je arhitektura okruženja pametne zgrade s primjenom koncepta IoT. Pri tome je vidljiva višestruka primjena raznovrsnih senzora

u svrhu praćenja brojnih parametara (pokret, tlak zraka, osvjetljenje, temperatura, protok vode) u različitim scenarijima da bi se omogućilo autonomno prikupljanje relevantnih podataka, njihov prijenos, analiza i izvršavanje aktivnosti na temelju dobivenih informacija.



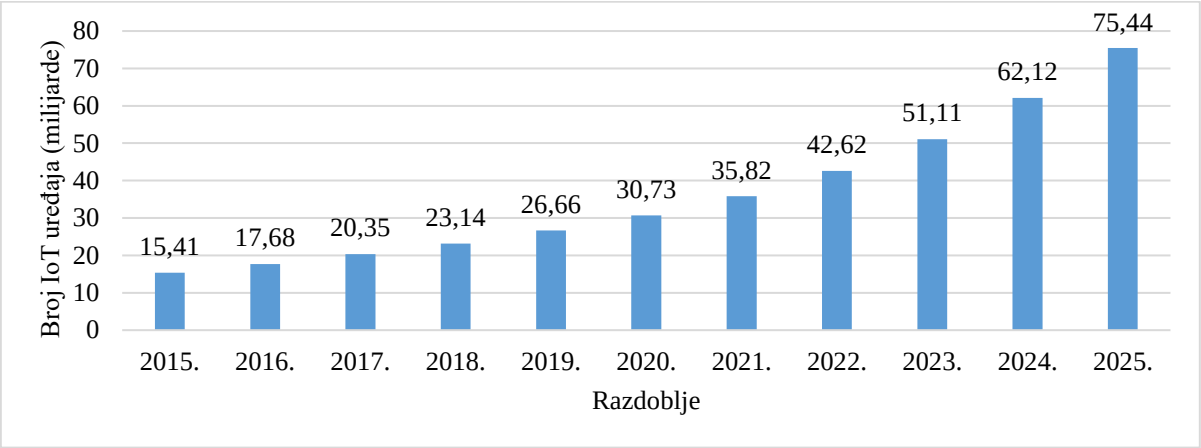
Slika 2.6 Arhitektura primjene koncepta IoT u okruženju pametne zgrade [95]

Vlasnicima građevinskih objekata omogućuje se jasnije upravljanje troškovima i resursima adresirajući neučinkovitosti i poboljšavajući iskorištavanje prostora. Problem vlasnika građevinskih objekata predstavlja holistički uvid u sve procese koji se događaju unutar građevinskog objekta. Rješenja pametnih zgrada omogućuju dionicima brže uočavanje problema, korektivno održavanje, unaprjeđenje procesa, uštedu resursa te prilagodbu različitim zahtjevima dionika [96].

2.4 Statistički pokazatelji primjene koncepta IoT

Broj IoT uređaja u kontinuiranom je porastu posljednje desetljeće. Točan broj uređaja i stopa rasta razlikuje se ovisno o istraživanju. Prema [97], do 2020. godine predviđa se približno 20.5 milijardi IoT uređaja dok istraživanje [45] predviđa do iste godine približno 30.7 milijardi IoT uređaja, a do 2025. godine 75 milijardi IoT uređaja, vidljivo na grafikonu 2.2.

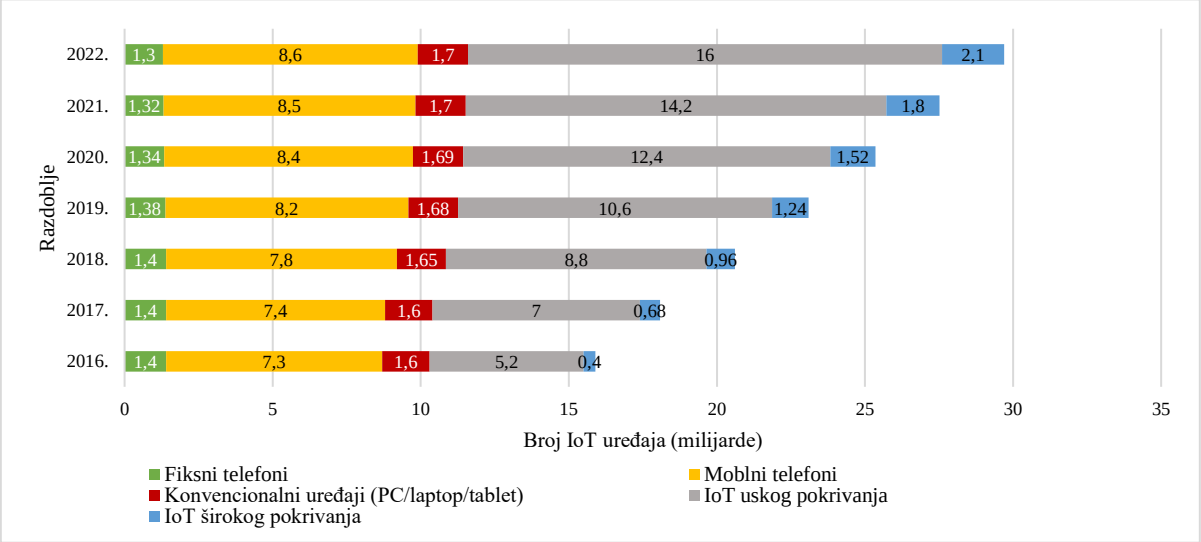
Grafikon 2.2 Predikcija ukupnog broja IoT uređaja do 2025. (globalno)



Izvor: [45]

Prema globalnim statističkim pokazateljima tvrtke Ericsson, koji se odnose na zastupljenost pojedine kategorije povezanih uređaja, uočava se dominacija IoT uređaja u odnosu na do sada dominantne mobilne uređaje. Grafikonom 2.3 prikazan je broj povezanih uređaja prema kategorijama za vremenski period od 2015. do 2021. godine. Prema predviđanjima očekuje se godišnja stopa rasta IoT uređaja (CAGR) od 23 % za vremenski period od 2016. do 2021. godine [98].

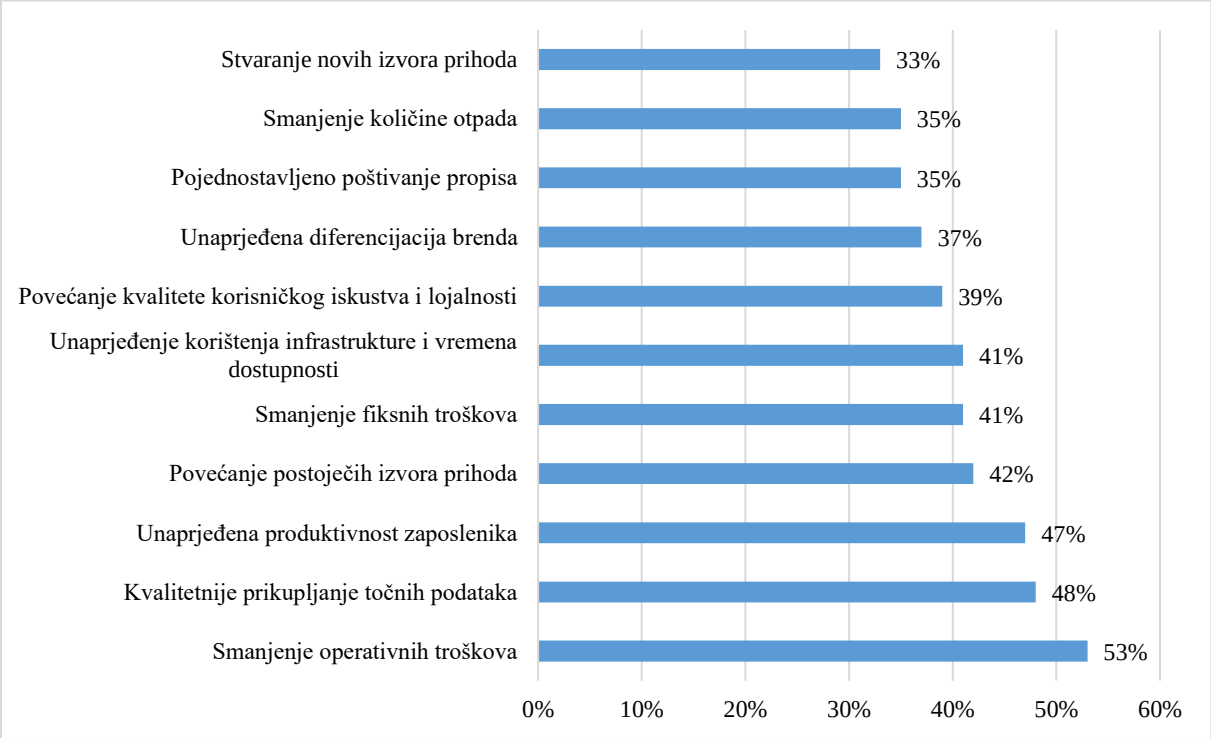
Grafikon 2.3 Broj povezanih uređaja prema kategorijama od 2016. do 2021. godine



Izvor: [98]

Primjena koncepta IoT u različitim gospodarskim sektorima postaje ključan faktor za unaprjeđenje poslovanja. Prema [99], 92 % tvrtki smatra da će koncept IoT biti važan za njihovo poslovanje do 2020. godine. Posljedično, tvrtke smatraju da sigurnost, privatnost, troškovi i regulativna pitanja predstavljaju najveće izazove implementacije i primjene koncepta IoT. Istraživanje [100] provedeno nad 1430 tvrtki (male, srednje i velike) ukazuje na brojne prednosti koje uviđa velika većina (95 %) usvojitelja IoT koncepta. Pri tome više od polovine (53 %) ispitanih potvrđuju značajne prednosti implementacije koncepta IoT u poslovanju dok 79 % ispitanih smatra da primjenom koncepta IoT ostvaruju pozitivne rezultate na različitim područjima rada koje u suprotnom ne bi mogli ostvariti. Neke od istaknutijih prednosti prikazane su grafikonom 2.4.

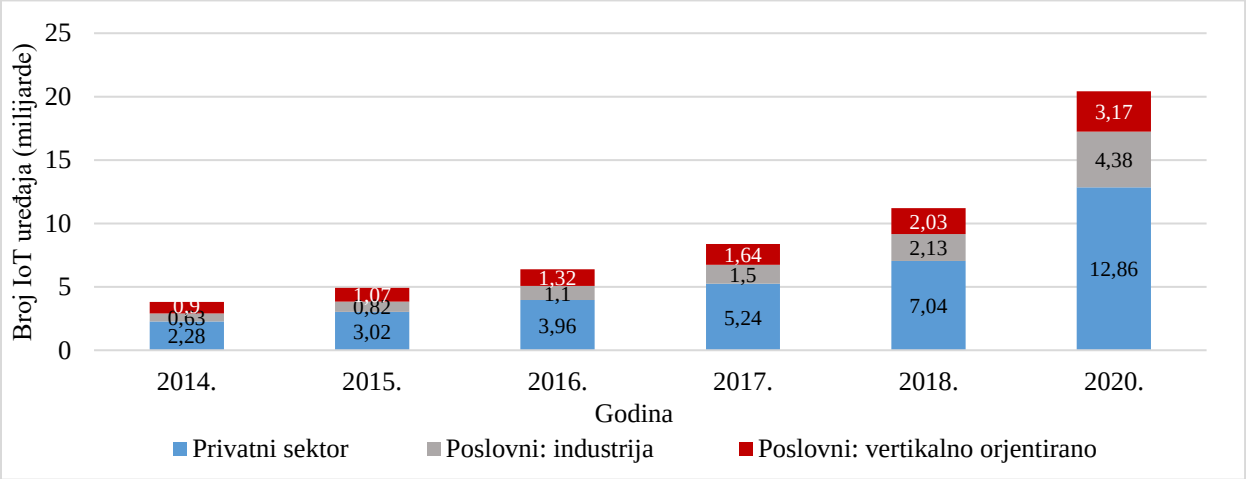
Grafikon 2.4 Prednosti implementacije koncepta IoT u poslovnom okruženju



Izvor: [100]

Prema Gartneru, najveća zastupljenost i primjena koncepta IoT prema broju korištenih IoT uređaja do 2017. godine bilo je u području okruženja pametnih zgrada. Nakon 2017. koncept pametnog doma je okruženje koje objedinjuje najveći broj IoT uređaja [95]. Zastupljenost IoT uređaja prema kategorijama primjene prikazano je grafikonom 2.5 pri čemu se uočava dominacija IoT uređaja u privatnom sektoru koji podrazumijeva okruženje pametnog doma, u odnosu na poslovne sektore.

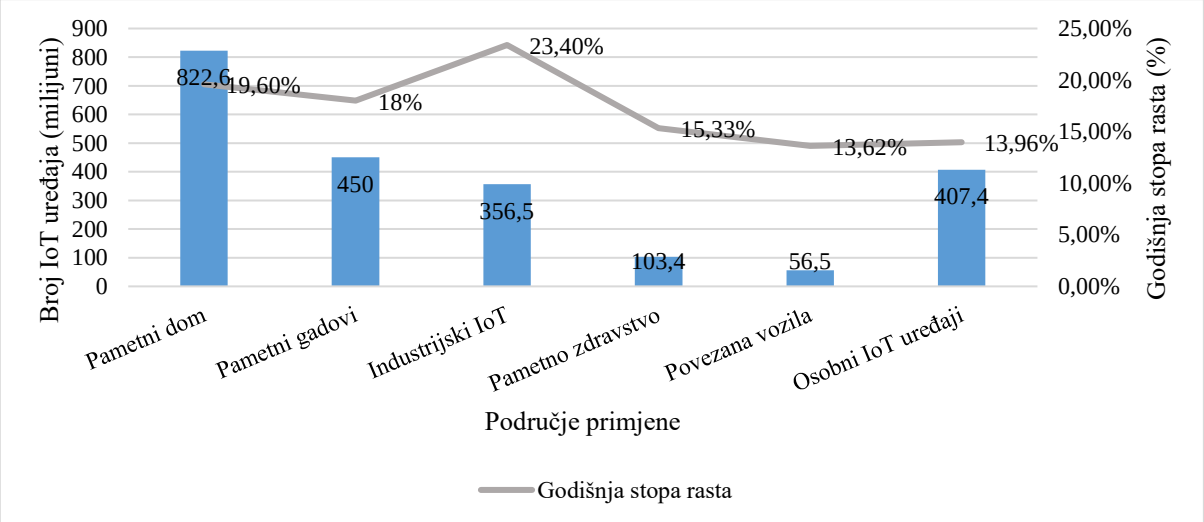
Grafikon 2.5 Broj implementiranih uređaja prema kategoriji primjene



Izvor: [45], [97]

Jasniji uvid u zastupljenost IoT uređaja prema pojedinom području primjene pruža istraživanje tvrtke IHS Markit [101]. Iz grafikona 2.6 vidljivo je da koncept pametnog doma bilježi najveći broj instaliranih IoT uređaja (822,6 milijuna) u odnosu na ostala područja primjene. Godišnja stopa rasta (predikcija do 2021. godine) iznosi 19,6 %, što koncept pametnog doma, uz koncept industrijskog IoT (CAGR 23,4 %), čini najbrže rastućim područjem primjene koncepta IoT.

Grafikon 2.6 Broj IoT uređaja i godišnja stopa rasta prema području primjene



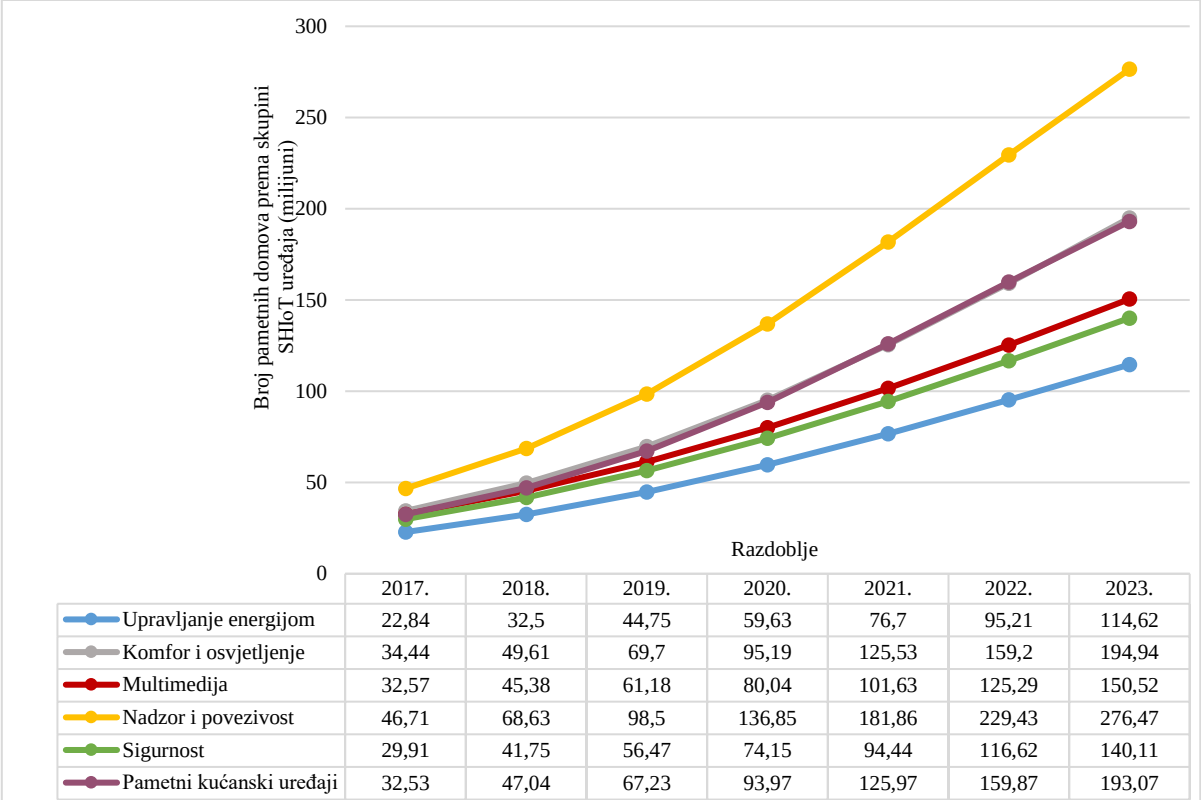
Izvor: [101]

Broj pametnih domova koji imaju implementirane SHIoT uređaje iz pojedine skupine, prikazan je grafikonom 2.7. Na prikazanom grafu vidljiva je predikcija kontinuiranog rasta implementacije uređaja iz svih navedenih kategorija do 2023. godine. Prema [102], najveći porast očekuje se za domove s implementiranim SHIoT uređajima iz skupine „nadzor i

povezivost“ koja podrazumijeva uređaje poput pametnih utičnica, prekidača i zvučnika. Statistički pokazatelji prikazani u [103] ukazuju na kontinuirani porast prihoda ove skupine uređaja do 2023. godine prema regijama. Predikcija za područje Azije (odnosi se na Kinu) ukazuje na stopu godišnjeg rasta prihoda od 35 % dok je za područje SAD-a i Europe u rasponu od 17 % - 25 %.

Drugi najbrže rastući pametni domovi su oni koji implementiraju SHIoT uređaje iz skupine „komfor i osvjetljenje“ koja podrazumijeva uređaje poput rasvjetnih tijela kao najzastupljenije uređaje u ovoj skupini, ali i senzore prozora i vrata kao i uređaje za kontrolu primjerice garažnih vrata. S obzirom na jednostavnost implementacije uređaja ove kategorije, što se prvenstveno odnosi na rasvjetna tijela, često predstavljaju ulaznu točku za korisnike u implementacije koncepta pametnog doma. Prema [104], globalna tržišna vrijednost ove skupine u 2023. godini iznosit će približno 14,32 milijarde dolara. Očekivana stopa godišnjeg rasta prihoda za Kinu je 41 %, te za Europu i SAD u rasponu od 19 % do 27 %.

Grafikon 2.7 Broj pametnih domova koji imaju implementirane SHIoT uređaje iz pojedine skupine (2018-2023.)



	2017.	2018.	2019.	2020.	2021.	2022.	2023.
Upravljanje energijom	22,84	32,5	44,75	59,63	76,7	95,21	114,62
Komfor i osvjetljenje	34,44	49,61	69,7	95,19	125,53	159,2	194,94
Multimedija	32,57	45,38	61,18	80,04	101,63	125,29	150,52
Nadzor i povezivost	46,71	68,63	98,5	136,85	181,86	229,43	276,47
Sigurnost	29,91	41,75	56,47	74,15	94,44	116,62	140,11
Pametni kućanski uređaji	32,53	47,04	67,23	93,97	125,97	159,87	193,07

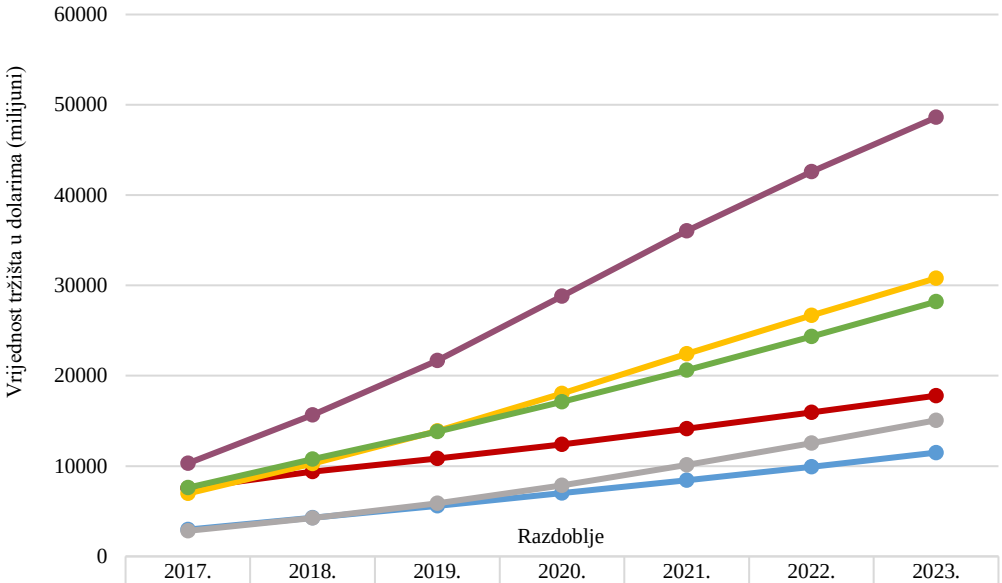
Izvor: [102]

Broj domova s implementiranim SHIoT uređajima iz skupine „pametni kućanski uređaji“ približno je jednak broju domova s implementiranim uređajima iz prethodne skupine. Ova skupina objedinjuje uređaje kao što su perilice rublja, hladnjaci, aparati za kavu i sl.

Grafikonom 2.8 prikazana je tržišna vrijednost za pojedinu skupinu uređaja po godinama izražena u milijardama dolara. Komparacijom vrijednosti i trenda pojedine skupine uređaja na grafikonu 2.7 i 2.8 uočljiv je nesrazmjer vrijednosti tržišta u odnosu na broj pametnih domova koji imaju ili će imati implementirane uređaje ove skupine. Uočeni nesrazmjer rezultat je cijene uređaja ove kategorije koja je veća nego što je to cijena uređaja ostalih kategorija.

Pametni domovi koji implementiraju SHIoT uređaje iz skupine „multimedija“, „sigurnost“ i „upravljanje energijom“ zastupljeni su u manjoj mjeri nego prethodne dvije skupine. Unatoč tome, i za navedene tri kategorije predviđa se kontinuirani rast i značajna tržišna vrijednost.

Grafikon 2.8 Vrijednost tržišta prema pojedinoj skupini SHIoT uređaja (2018. - 2023.)



	2017.	2018.	2019.	2020.	2021.	2022.	2023.
Upravljanje energijom	2968	4263,4	5577,2	6995,7	8441,3	9933,5	11491,6
Komfor i osvjetljenje	2831	4228,6	5864,5	7872,6	10142,1	12555,4	15069,1
Multimedija	7534,5	9366,8	10826,8	12412,7	14138,5	15936,74	17793,4
Nadzor i povezivost	6965,7	10254,9	13876,8	18049,1	22420,1	26684,2	30796,4
Sigurnost	7607	10754,6	13801,3	17107,4	20633,1	24350,5	28198,8
Pametni kućanski uređaji	10304	15654,6	21682,2	28808,6	36039,6	42608,6	48605,2

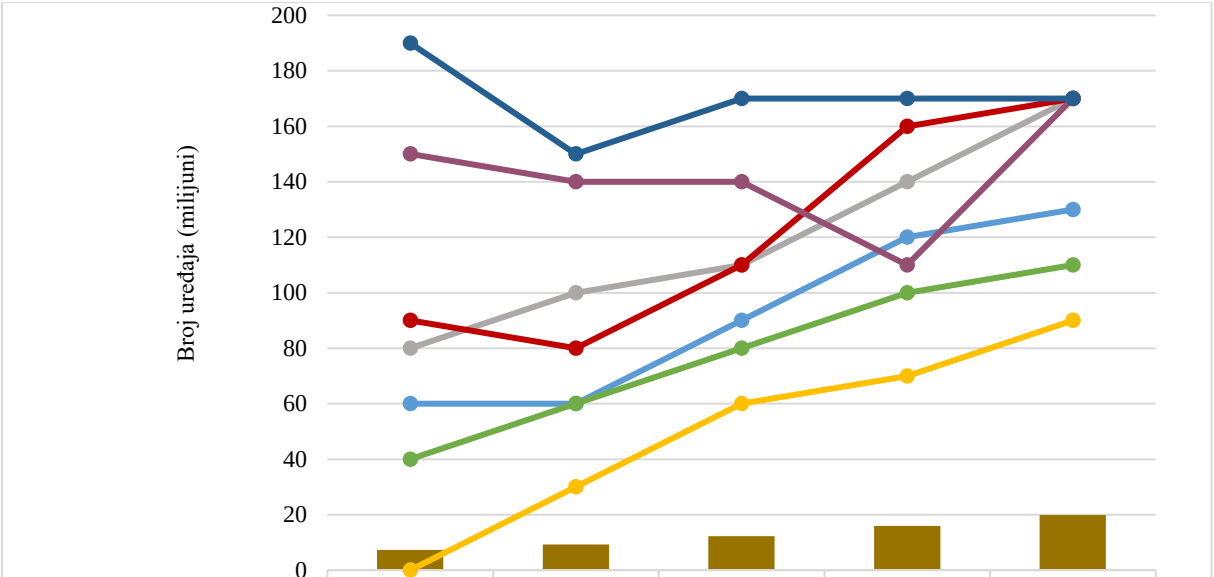
Izvor: [102]

Važan pokazatelj rasta i važnosti koncepta pametnog doma predstavlja broj SHIoT uređaja po kućanstvu. Predviđanja se razlikuju u ovisnosti o izvoru pa tako tvrtka Kaspersky navodi da trenutno prosječno kućanstvo posjeduje 6,3 povezana uređaja, pri čemu se podrazumijevaju sve vrste uređaja (konvencionalni i SHIoT) koji ostvaruju vezu na internetsku mrežu [105].

Grafikonom 2.9 prikazani su skupni podatci tvrtke Statista i Forrester pri čemu je u odnos stavljen broj pametnih domova i ostalih povezanih uređaja među kojima su i SHIoT

uređaji. Prema prikazanom grafikonu, predviđa se da će 2020. godine egzistirati 19,9 milijuna pametnih domova te 130 milijuna implementiranih SHIoT uređaja što čini prosječno 6,53 SHIoT uređaja po pametnom domu.

Grafikon 2.9 Odnos predikcije broja pametnih domova, SHIoT i ostalih povezivih uređaja

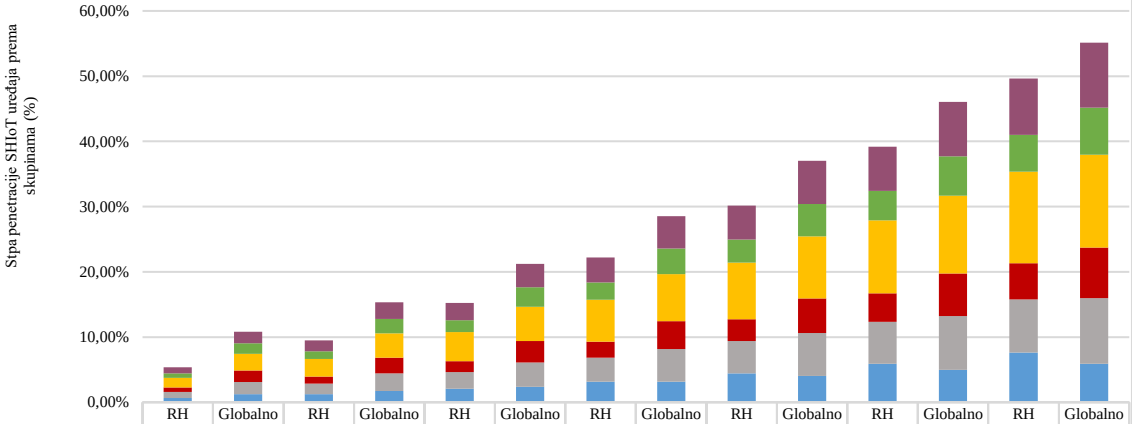


	2016.	2017.	2018.	2019.	2020.
Broj pametnih domova	7,3	9,3	12,2	15,9	19,9
SHIoT uređaji	60	60	90	120	130
Pametni STB	80	100	110	140	170
Pametni TV	90	80	110	160	170
360° kamere	0	30	60	70	90
VR uređaji	40	60	80	100	110
Nosivi uređaji	150	140	140	110	170
Ostali mobilni uređaji	190	150	170	170	170

Izvor: [106], [107]

Istraživanje tvrtke Telsyte na području Australije ukazuje da prosječno kućanstvo posjeduje 13,7 povezanih uređaja, a predviđa da će ih 2021. godine biti 30,7 od kojih će 14 biti SHIoT uređaji [108]. S obzirom na ograničeni broj statističkih pokazatelja koji ukazuju na prosječan broj SHIoT uređaja instaliranih po pametnom domu, indikatore utjecaja ovakvih uređaja moguće je promatrati i kroz trenutni broj i predikciju budućeg trenda broja povezanih uređaja (konvencionalni + SHIoT) po korisniku. Tako istraživanja tvrtke Cisco predviđaju da će 2021. godine biti četiri povezana uređaja po korisniku (globalno), pri čemu će najveći broj povezanih uređaja (13) biti u Sjevernoj Americi, u Europi 6,5 (prosječna vrijednost), dok se najmanji broj povezanih uređaja po korisniku predviđa za područje Bliskog istoka i Afrike (1) [109].

Grafikon 2.10 Usporedba stope penetracije SHIoT uređaja u Republici Hrvatskoj i globalno



	RH 2017.	Globalno 2017.	RH 2018.	Globalno 2018.	RH 2019.	Globalno 2019.	RH 2020.	Globalno 2020.	RH 2021.	Globalno 2021.	RH 2022.	Globalno 2022.	RH 2023.	Globalno 2023.
Pametni kućanski uređaji	0,96%	1,76%	1,66%	2,53%	2,64%	3,58%	3,83%	4,97%	5,21%	6,60%	6,79%	8,31%	8,64%	9,96%
Sigurnost	0,67%	1,62%	1,16%	2,24%	1,83%	3,01%	2,63%	3,92%	3,51%	4,95%	4,51%	6,06%	5,63%	7,22%
Nadzor i povezivost	1,49%	2,53%	2,71%	3,69%	4,43%	5,25%	6,47%	7,24%	8,72%	9,53%	11,22%	11,93%	14,05%	14,25%
Multimedija	0,66%	1,77%	1,10%	2,44%	1,69%	3,26%	2,43%	4,23%	3,31%	5,33%	4,33%	6,51%	5,52%	7,76%
Komfor i osvjetljenje	0,93%	1,87%	1,60%	2,67%	2,54%	3,72%	3,68%	5,03%	4,97%	6,58%	6,44%	8,28%	8,14%	10,05%
Upravljanje energijom	0,67%	1,24%	1,24%	1,75%	2,08%	2,39%	3,16%	3,15%	4,43%	4,02%	5,91%	4,95%	7,64%	5,91%

Izvor: [102], [110]

Usporedba globalnog tržišta s onim u Republici Hrvatskoj (RH) s aspekta stope penetracije pojedine kategorije SHIoT uređaja vidljiva je na grafikonu 2.10. Stopa penetracije označava odnos broja pametnih domova i ukupnog broja privatnih domova. Unatoč pokazateljima koji predviđaju nižu stopu penetracije u RH u odnosu na globalno tržište, predviđa se kontinuirani rast. Prema [110], ukupna vrijednost tržišta pametnog doma 2018. godine u RH je iznosila 40 milijuna dolara, a do 2023. godine predviđa se linearan rast i vrijednost od 151 milijun dolara. Trenutna zastupljenost pametnih domova u RH je 0,14 milijuna uz prosječnu cijenu implementiranih SHIoT uređaja od 441,94 dolara po pametnom domu, a do 2023. godine predviđa se 0,36 milijuna pametnih domova uz prosječnu cijenu od 419,27 dolara po pametnom domu.

Prema prikazanim statističkim pokazateljima zaključuje se da broj uređaja u konceptu IoT eksponencijalno raste. Primjena koncepta IoT dominira u privatnom sektoru, odnosno u okruženju pametnog doma kao području primjene, gdje je implementiran najveći broj IoT uređaja. Broj IoT uređaja u konceptu pametnog doma, uz područje industrijskog IoT-a, ima najveću godišnju stopu rasta. Koncept pametnog doma ima pozitivan trend promatrano s aspekta penetracije uređaja na globalnom tržištu, broja kućanstava unutar kojih su implementirani SHIoT uređaji te vrijednosti tržišta neovisno o skupinama uređaja objedinjenih pod ovim konceptom. Analizirani pokazatelji egzaktno i jednoznačno ukazuju da je koncept pametnog doma trenutno najzastupljenije i najbrže rastuće područje primjene koncepta IoT.

3 Analiza koncepta pametnog doma

Trećim poglavljem detaljno je pojašnjen koncept pametnog doma kao jedno od najbrže rastućih područja primjene koncepta IoT. S obzirom da je fokus istraživanja usmjeren upravo na to područje primjene, pobliže je razjašnjeno okruženje pametnog doma kroz skupine korištenih uređaja, korištene komunikacijske tehnologije i arhitekture takvog okruženja. Opisane su karakteristike mrežne komunikacije u navedenom okruženju. Usporedno su naglašeni i sigurnosni aspekti pametnog doma kroz raznovrsne prijetnje i ranjivosti koje predstavljaju važan aspekt prihvaćanja i primjene ovog koncepta.

3.1 Okruženje pametnog doma

Pametni dom predstavlja koncept primjene sveprisutnog računartva u okruženju kućanstva. Prema [111], nekoliko je sinonima prihvaćeno u znanstveno-istraživačkoj i stručnoj literaturi za termin pametni dom poput automatizacija doma (engl. *Home automation*), inteligentni dom (engl. *Intelligent home*), prilagodljivi dom (engl. *Adaptive home*) i sl.

Europski standard EN 15232 i Direktiva o energetskim svojstvima zgrada 2010/31 / EU, koja je u skladu s Direktivom 2009/72 / EZ, kao i Energetskim planom za 2050., promiču usvajanje tehnologija pametnog doma da bi se smanjila potrošnja energije u stambenom sektoru [92]. Prema istraživanju [112], okruženje pametnog doma moguće je razmatrati kao skup SHIoT uređaja, komunikacijskih tehnologija i usluga. Pri tome su SHIoT uređaji hardverske jedinice koje objedinjuju senzore, aktuatore. Komunikacijske tehnologije omogućuju povezivost SHIoT uređaja u jedinstvenu komunikacijsku mrežu, a usluge pružaju različite funkcionalnosti krajnjim korisnicima kroz korištenje aplikativnih rješenja.

Iako je pojava i brzo širenje širokopojasnog pristupa internetu krajem 1990-ih godina pružilo tehnološke temelje za razvoj kućnih mreža, koncept pametnog doma počeo se implementirati u drugoj polovini 2000-ih godina, prikazano tablicom 3.1. Tome su pridonijeli razvoj i popularizacija pametnih telefona. Nakon 2010. godine ovaj koncept počinje se ubrzano razvijati i temeljiti na kombinaciji tehnologija kao što su IoT i umjetna inteligencija što je rezultiralo okruženjem koje je svjesno situacije i konteksta [113].

Tablica 3.1 Evolucija okruženja pametnog doma

Godina	Faza	Tehnološki temelji	Primarne funkcionalnosti
1990.-2000.	Automatizacija doma	Širokopojasni pristup internetskoj mreži	Automatizacija doma
2000.-2010.	Kućna mreža	Pametni telefoni i aplikacije	Udaljeni nadzor i upravljanje
2010. – danas	Pametni dom	IoT i umjetna inteligencija (AI)	Upravljanje, nadzor i automatizacija temeljena na kontekstu

Izvor: [113]

Koncept pametnog doma implicira automatizaciju procesa koji se odvijaju unutar kućanstva. U tu svrhu primjenjuje se mreža međupovezanih mehaničkih i elektroničkih uređaja koji komuniciraju međusobno i s korisnikom s ciljem stvaranja interaktivnog prostora [92]. Prema tome, pametni dom podrazumijeva kućanstvo opremljeno komunikacijskom mrežom, tehnološki inovativnim uređajima i senzorima kojima je moguće udaljeno pristupiti, nadzirati i

njima upravljati te koji mogu pružiti usluge koje odgovaraju korisničkim zahtjevima i potrebama [113]. S obzirom na nisku razinu konsenzusa znanstvene zajednice o definiciji koncepta pametnog doma, postoje brojne interpretacije ovog koncepta. Tako istraživanje [114] opisuje pametni dom kao okruženje koje posjeduje ambijentalnu inteligenciju i automatiziranu kontrolu sposobnu reagirati na temelju ponašanja korisnika te omogućiti različite prilagodbe prostora. Stoga koncept pametnog doma predstavlja okosnicu koja omogućava upravljanje i nadzor različitih područja unutar doma povezujući četiri osnovna stupa ljudskog života unutar doma: (1) udobnost i skrb, (2) fizički integritet i sigurnost objekata, (3) racionalno upravljanje energijom i (4) pružanje zdravstvenih usluga korisnicima [115].

Osnovne mogućnosti pametnog doma prikazane su u istraživanju [116], a moguće ih je svesti na:

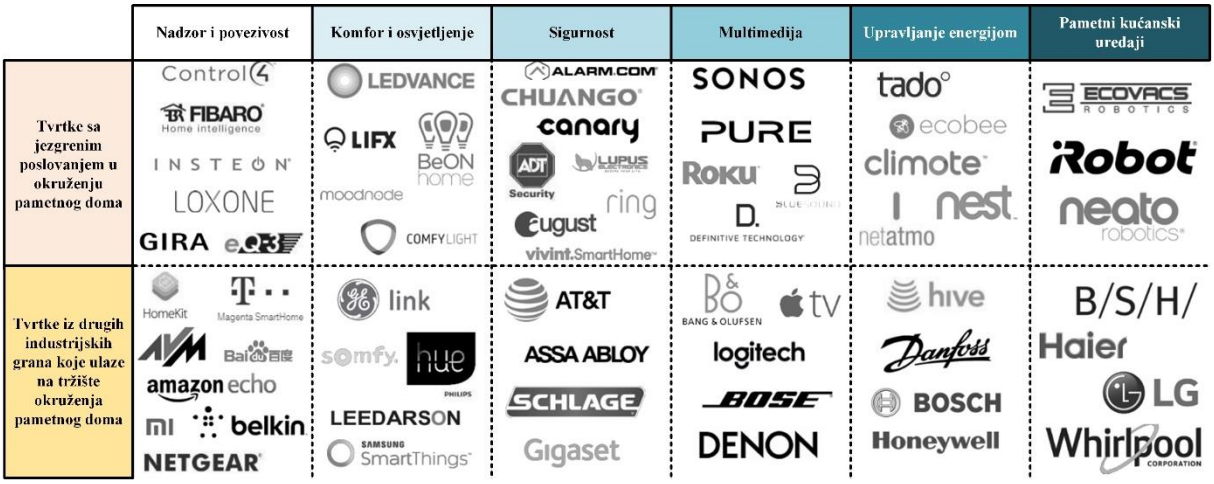
1) Povezivost između korisnika i energetske mreže, dohvat informacija o potrošnji električne energije i trošku, uspostavu plana potrošnje električne energije, omogućavanje racionalnog korištenja električne energije s ciljem uštede i zaštite okoliša.
2) Mogućnost unaprjeđenja razine komfora, sigurnosti, praktičnosti i interaktivnosti kućanstva.
3) Podršku za provedbu udaljenih novčanih transakcija.
4) Udaljen nadzor i interakcija s domom putem terminalnih uređaja.
5) Ostvarivanje stvarnovremenskih sigurnosnih usluga kroz implementaciju senzora za mjerenje prisutnosti i razine vode, električne energije i plina.

Ključni aspekt funkcioniranja pametnog doma kao okosnice je razvoj pouzdane i jednostavne komunikacijske arhitekture. Iz te perspektive pametni dom moguće je sagledavati kao koncentrator i diseminator informacija i usluga s ciljem pokrivanja sveobuhvatnih funkcionalnih područja u području doma. Funkcija pametnog doma ne odnosi se samo na komunikaciju između određenih elemenata unutar fizičkog doma s ciljem unaprjeđenja razine udobnosti i kvalitete života, već podrazumijeva i obnašanje uloge mrežnog prolaza[3] (engl. *gateway*) ili sučelja prema javnoj komunikacijskoj mreži u svrhu komunikacije s drugim konceptima kao što su pametna energetska mreža i pametni grad s ciljem razmjene informacija [115].

[3] Mrežni prolaz (engl. *gateway*) – hardverski mrežni uređaj čija je osnovna uloga povezivanje dviju ili više vrsta komunikacijske mreže.

3.1.1 Skupine uređaja u okruženju pametnog doma

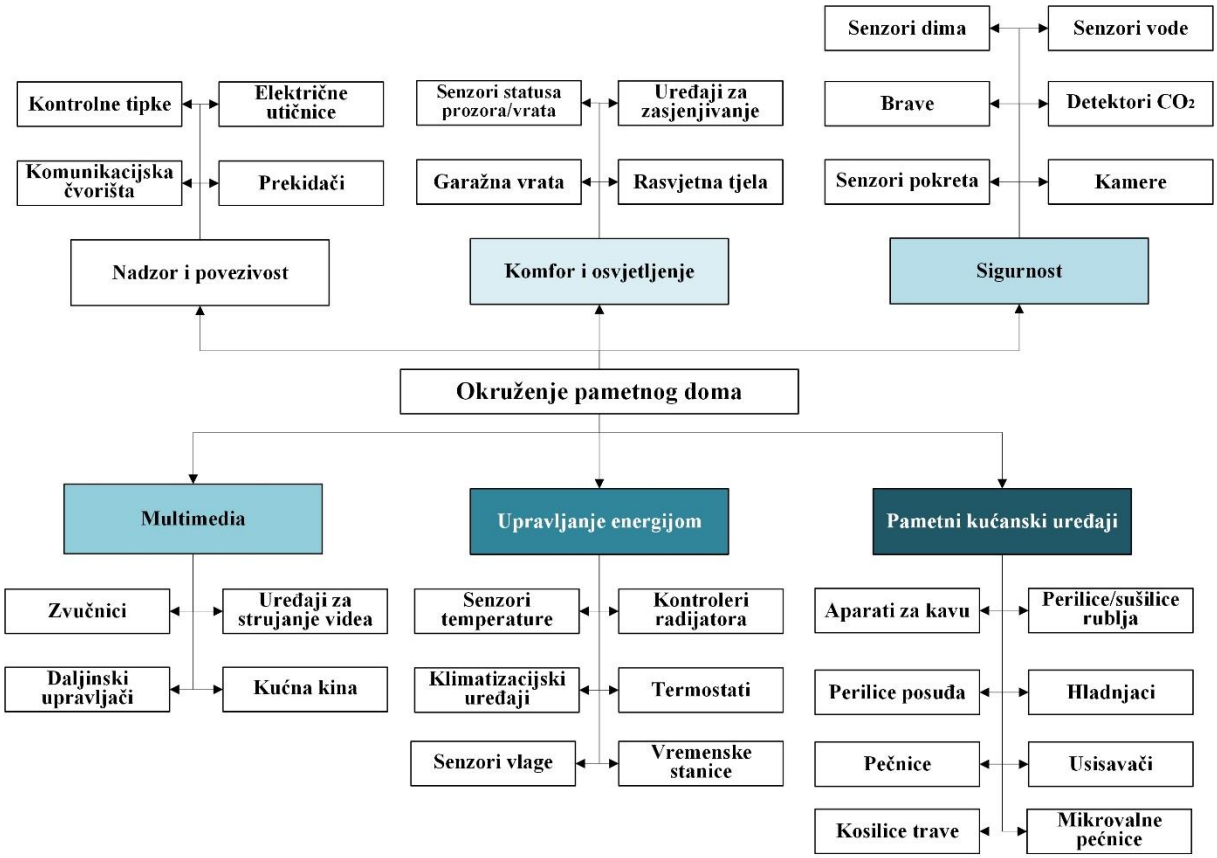
Rastuća uloga i prihvaćenost koncepta pametnog doma u posljednjem desetljeću rezultirala je razvojem brojnih SHIoT uređaja koji pružaju raznovrsne funkcionalnosti i vrijednosti za krajnjeg korisnika. Brojnost i raznolikost SHIoT uređaja praćena je i brojem proizvođača koji nastoje stvoriti vlastiti ekosustav SHIoT uređaja što je vidljivo iz slike 3.1. Određena istraživanja, poput [117], pod okruženjem pametnog doma podrazumijevaju i osobna računala, prijenosna računala, pametne telefone, tablete i nosive uređaje. Međutim, pametni telefoni, tableti i nosivi uređaji pripadaju skupini potrošačke elektronike (engl. *consumer electronic*) dok osobna i prijenosna računala pripadaju skupini konvencionalnih terminalnih uređaja.



Slika 3.1 Heterogenost proizvođača i pružatelja usluga u okruženju pametnog doma [118]

Jednostavna i egzaktna podjela SHIoT uređaja pružena je u [118] i to u šest skupina: (1) nadzor i povezivost, (2) komfor i osvjetljenje, (3) sigurnost, (4) multimedija, (5) upravljanje energijom i (6) pametni kućanski uređaji. Navedene skupine uz primjere uređaja koji pripadaju pojedinoj kategoriji prikazane su slikom 3.2. Istraživanje [115] razlikuje SHIoT uređaje prema četiri kategorije: (1) energetska učinkovitost i upravljanje, (2) zdravstvena skrb, (3) zabava i (4) sigurnost.

Istraživanje [119], identificira pojedine skupine funkcionalnosti u okruženju pametnog doma. Standardna skupina predstavlja funkcionalnosti koje su ključne u okruženju pametnog doma, a zadovoljavaju osnovne potrebe korisnika i omogućavaju automatizaciju rutinskih aktivnosti (upravljanje svjetlima, kontrola temperature prostorije, upravljanje roletama i sl.). Pomoćnu skupinu predstavljaju proširene funkcionalnosti standardne skupine, a zadovoljavaju potrebe specifičnih skupina korisnika (detekcija CO_2, prilagodba programa rekreacije na temelju zdravstvenog stanja, i sl).



Slika 3.2 Skupine SHIoT uređaja [120]

Skupina funkcionalnosti za povećanje razine komfora uključuje one funkcionalnosti koje nisu nužne za normalan rad pametnog doma, a njihova implementacija zahtijeva dodatna financijska ulaganja (zatamnjenje prozora, samočisteći prozori, i sl.). Navedene funkcionalnosti moguće je promatrati i kroz sljedeća područja primjene: osvjetljenje, sustavi za zasjenjenje prostora, upravljanje kućanskim uređajima, HVAC (engl. *heating, ventilation, air-conditioning*), sigurnost objekta, multimedija, zdravlje, kuhinja, navodnjavanje, čišćenje, upravljanje. Za pružanje pojedine skupine funkcionalnosti nužni su SHIoT uređaji.

Iz slike 3.2 vidljiva je heterogenost s aspekta brojnosti i raznovrsnosti SHIoT uređaja koji potencijalno mogu egzistirati u okruženju pametnog doma. Uz navedeno, brojni su i proizvođači koji su prisutni na tržištu SHIoT uređaja kao i pružatelji usluga u okruženju pametnog doma, prikazano slikom 3.1 što dodatno utječe na povećanje heterogenosti.

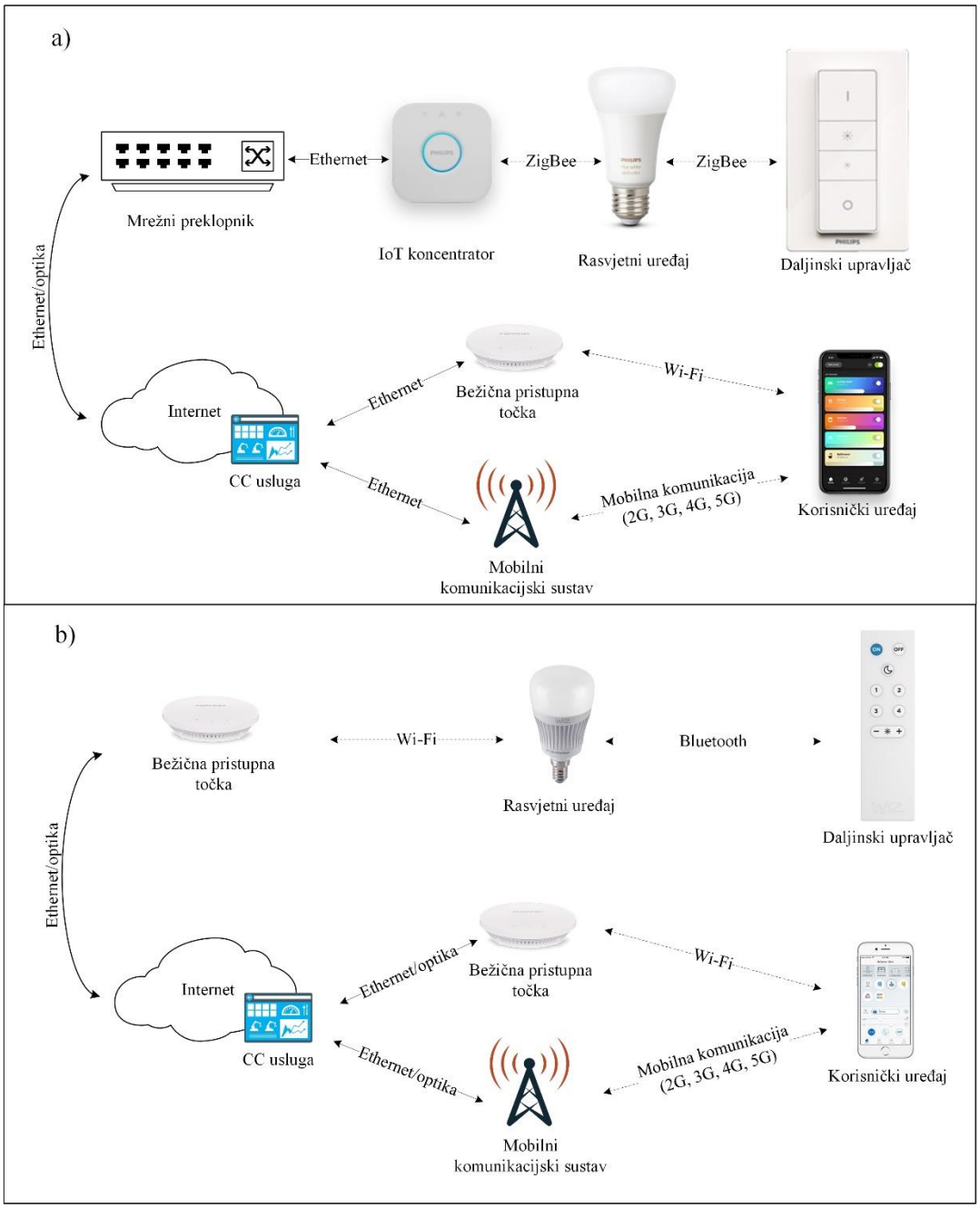
3.1.2 Komunikacijske tehnologije korištene u okruženju pametnog doma

Uređaji u okruženju pametnog doma mogu ostvariti određene funkcionalnosti lokalnim upravljanjem, međutim cjelovite funkcionalnosti ostvaruju udaljenim upravljanjem za što je nužna povezanost SHIoT uređaja na lokalnu i javnu komunikacijsku mrežu [120]. Komunikacijska infrastruktura korištena u funkciji povezivanja SHIoT uređaja naziva se još i

HAN (engl. *Home Area Network*). S obzirom na područje djelovanja, HAN obuhvaća LAN i PAN ili BAN komunikacijske mreže i pripadajuće komunikacijske tehnologije. Većina korištenih komunikacijskih tehnologija u HAN mreži razvijene su prije pojave okruženja pametnog doma te većina proizvođača SHIoT uređaja s ciljem ostvarenja njihove mrežne komunikacije koristi tehnologije poput Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4), Z-Wave, *Bluetooth* (IEEE 802.15.1) [115]. Prema [121], navedene tehnologije trenutno predstavljaju temelj komunikacije u HAN mreži što će se nastaviti i nakon 2020. godine.

Primjena određene komunikacijske tehnologije ovisit će o izvedbi SHIoT uređaja, njegovoj namjeni i funkcionalnostima koje podržava. Tako će SHIoT uređaji (npr. pametni termostat) koji kao izvor energije koriste bateriju, koristiti i energetski učinkovitu komunikacijsku tehnologiju (ZigBee ili Z-Wave) i komunicirat će putem IoT koncentratora. IoT koncentrator je mrežni uređaj koji se koristi kao posrednik u komunikaciji između dviju različitih komunikacijskih tehnologija. U navedenom primjeru omogućit će komunikaciju uređaja koji koristi ZigBee ili Z-Wave tehnologiju s bežičnom pristupnom točkom koja koristi Wi-Fi tehnologiju. SHIoT uređaji koji su povezani na neprekidan izvor energije (pametne utičnice, pametne žarulje) najčešće će koristiti i Wi-Fi komunikacijsku tehnologiju.

Bluetooth tehnologija koristit će se u scenariju lokalnog povezivanja i upravljanja SHIoT uređaja. Primjer takvog scenarija je pametna ključanica koja detektira blizinu korisnika korištenjem *Bluetooth* tehnologije i izvršava odgovarajuću aktivnost (npr. otključavanje vrata). Zbog dimenzija SHIoT uređaja te njihovog potencijalnog broja u okruženju pametnog doma prvenstveno su korištene bežične komunikacijske tehnologije zbog praktičnosti i jednostavnosti povezivanja uređaja u HAN mreži. Međutim, određeni proizvođači u određenim segmentima HAN infrastrukture koriste i žičani način povezivanja (*ethernet*). Slikom 3.3 prikazana su dva scenarija povezivanja pametnih rasvjetnih tijela. Na dijelu a) iste slike vidljiva je primjena IoT koncentratora i njegova žičana komunikacija s mrežnim preklopnikom dok je između IoT koncentratora, rasvjetnog uređaja i daljinskog upravljača komunikacija izvedena korištenjem ZigBee tehnologije.

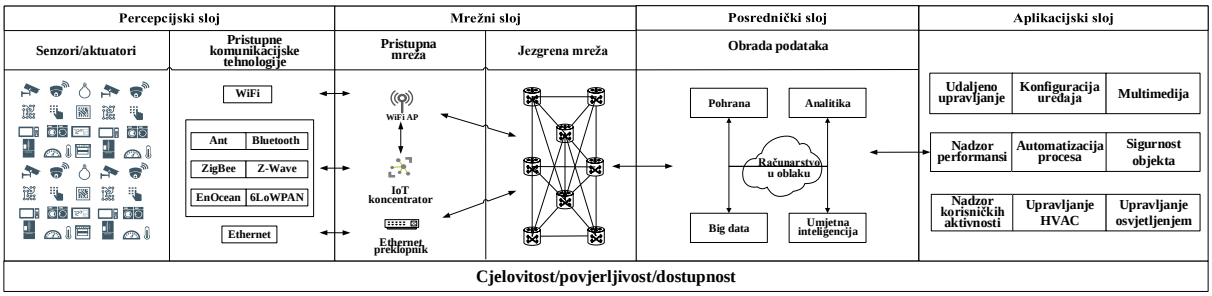


Slika 3.3 Scenariji povezivanja SHIoT uređaja u okruženju pametnog doma; a) uz IoT koncentrator i žičanu komunikaciju i b) bez IoT koncentratora i isključivo bežičnom komunikacijom

Svrha IoT koncentratora je povezivanje većeg broja uređaja istog proizvođača kroz isto čvorište. Cilj ovakvog pristupa bio je stvoriti homogeno okruženje pametnog doma pri čemu bi sve funkcionalnosti pružali SHIoT uređaji istog proizvođača. Rezultat je to tržišnog natjecanja i stjecanja konkurentske prednosti. Međutim, prema istraživanju [103], spomenuti trend je u padu i u budućnosti se očekuje integracija takvih uređaja u *gateway* uređaj. Stoga je u budućnosti realniji scenarij povezivanja prikazan slikom 3.3 b) gdje se SHIoT uređaj povezuje s bežičnom pristupnom točkom bez potrebe za posredničkim komunikacijskim uređajima.

3.1.3 Arhitektura okruženja pametnog doma

Heterogenost okruženja pametnog doma zahtijeva jasnu i jednostavnu arhitekturu koja omogućuje jednostavniji razvoj pojedinih elemenata u svrhu interoperabilnosti uređaja i razvoja novih usluga [122]. Polazna točka razvoja i definiranja arhitekture pametnog doma predstavlja generički slojeviti model arhitekture koncepta IoT. Prilagodba i konkretizacija takvog generičkog modela arhitekture za produkt ima razvoj arhitekture pametnog doma u kojoj su jasno razlučivi pojedini elementi i njihova uloga u ovom konceptu [116]. Generički model arhitekture pametnog doma prikazan je slikom 3.4.



Slika 3.4 Generički model slojevite arhitekture pametnog doma [120]

Iz prikaza generičkog modela jasno su razlučivi elementi pametnog doma prema slojevima. Percepcijski sloj objedinjuje SHIoT uređaje zajedno s pripadajućim pristupnim komunikacijskim tehnologijama. Takvi uređaji se, korištenjem komunikacijskih tehnologija, povezuju u HAN mrežu s ciljem lokalne komunikacije (neposredno između uređaja) ili komunikacije s poslužiteljima u CC okruženju. U takvoj komunikaciji mrežni sloj ima ključnu ulogu jer predstavlja točku povezivanja lokalne s javnom mrežom i omogućuje prijenos podataka prema posredničkom sloju.

Posrednički sloj obnaša ulogu obrade podataka i pruža interoperabilnost platformi različitih proizvođača, a time i SHIoT uređaja. Primjer je povećanje intenziteta osvjetljenja u trenutku detekcije smanjene vanjske razine svjetla pri čemu se proizvođači senzora razine vanjskog osvjetljenja i rasvjetnog tijela mogu razlikovati.

Aplikacijski sloj pruža sučelje krajnjem korisniku u vidu aplikacije (mobilne ili *web*) koje mu omogućuje korištenje raznovrsnih usluga [120]. Element arhitektura koji se proteže kroz sve spomenute slojeve arhitekture je sigurnost svih IK resursa. Sigurnost kao ključni čimbenik svakog IK sustava potrebno je implementirati i kontinuirano održavati na zahtijevanoj razini neovisno o promatranom elementu arhitekture pametnog doma.

Prikazana arhitektura pruža interoperabilnost različitih uređaja, usluga i potporne IK infrastrukture neovisno o proizvođaču uređaja, pružatelju usluga, pružatelju sadržaja i o

aplikaciji uz potrebnu razinu sigurnosti svih navedenih elemenata. Na taj način korisniku se pruža fleksibilnost pri odabiru SHIoT uređaja i usluga te se omogućuje jednostavniji razvoj pojedinih elemenata arhitekture i smanjenje krajnje cijene proizvoda.

3.2 Mrežna komunikacija SHIoT uređaja

3.2.1 Karakteristike mrežne komunikacije SHIoT uređaja

Istraživanje načina komunikacije uređaja objedinjenih pod konceptom IoT, što podrazumijeva i SHIoT uređaje, postaje rastući istraživački problem promatrano s više aspekata. U svrhu razlikovanja komunikacije takvih uređaja i konvencionalnih uređaja brojni istraživači, poput [49] i [123], usvojili su termine MTC i HTC. Razlog za to su razlike u karakteristikama i načinu rada SHIoT i konvencionalnih uređaja što je i uzrok razlika u karakteristikama prometa koji generiraju ove dvije skupine uređaja. MTC način komunikacije rezultat je aktivnosti SHIoT uređaja s obzirom da komunikacija takvih uređaja često ne zahtijeva ljudsku intervenciju. Komparativno s IoT uređajima, HTC komunikacija posljedica je aktivnosti konvencionalnih uređaja.

Razlike MTC u odnosu na HTC komunikaciju moguće je promatrati iz više aspekata (usmjerenost prometa, pristupno kašnjenje, periodičnost prijenosa, količina uređaja i sigurnost) [124], [125]. Prvi aspekt promatranja je usmjerenost prometa. Općenito MTC komunikaciju karakterizira dominacija *uplink*[4] prometa u scenariju gdje senzor prenosi prikupljene informacije prema odredištu (npr. kamera ili senzor temperature). Određene SHIoT uređaje može karakterizirati i simetrična količina prometa u *uplinku* i *downlinku*[5] u scenariju kada je senzor i aktuator implementiran unutar istog SHIoT uređaja (npr. termostat). HTC komunikaciju karakterizira dominacija *downlink* prometa kao rezultat klijentsko-poslužiteljske arhitekture koja je još uvijek najzastupljenija kod ovog oblika komunikacije (ne razmatraju se P2P i slični oblici komunikacije).

Sljedeći važan aspekt, kada je u pitanju diferencijacija MTC i HTC komunikacije, odnosi se na pristupno kašnjenje (engl. *access delay*[6]). SHIoT uređaji često se temelje na radnim ciklusima (uređaj je u stanju mirovanja iz kojeg periodički izlazi u svrhu slanja podataka) kada se zahtijeva kratko vrijeme pristupnog kašnjenja da bi se osigurao brzi pristup mreži i slanje podataka te povratak u stanje mirovanja koje doprinosi povećanju autonomije uređaja. Iako su

[4] Odlazni promet (od uređaja)
[5] Dolazni promet (prema uređaju)
[6] Odražava vrijeme od kada je mrežni paket generiran dok ne napusti mrežno sučelje promatranog uređaja

brojne aplikacije koje generiraju HTC promet vrlo zahtjevne (u kontekstu mrežnih performansi), nakon uspostave veze, dulje vrijeme pristupnog kašnjenja se tolerira [126].

Vrlo važna karakteristika MTC komunikacije, prema istraživanju [125], je periodičnost prijenosa podataka. Iako pojedini IoT uređaji prenose podatke mrežom rjeđe nego konvencionalni uređaji, brojni su IoT uređaji koji će ovu aktivnost izvršavati periodički što rezultira periodičkim uzorcima prometa. HTC promet po prirodi je stohastičan i asinkron što rezultira problemima pri razlikovanju uređaja koji generiraju ovakav promet dok SHIoT uređaji iste ili slične namjene generiraju isti ili približno isti uzorak prometa. Uz navedeno, s ciljem osiguranja potrebnih performansi prijenosa, HTC promet sadrži i visok udio signalizacijskog prometa. Konvencionalni uređaji posjeduju mogućnost instalacije različitih operativnih sustava i aplikacija koje proširuju funkcionalnosti takvih uređaja što se odražava i u karakteristikama HTC komunikacije. SHIoT uređaji za razliku od konvencionalnih uređaja podržavaju ograničen i ne proširiv broj funkcionalnosti. Primjer je pametna utičnica koja može poprimiti dva stanja (uključeno/isključeno) pa će način komunikacije takvog uređaja biti nepromjenjiv.

Brojnost uređaja također ima značajan utjecaj na karakteristike komunikacije. Promatrano s aspekta okruženja pametnog doma, broj SHIoT uređaja veći je od broja konvencionalnih uređaja. Broj SHIoT uređaja koji komuniciraju u HAN mreži može sezati od nekoliko desetaka do nekoliko stotina dok je broj konvencionalnih uređaja u HAN mreži najčešće do deset [88].

S aspekta sigurnosti, SHIoT uređaji nemaju implementirane mehanizme detekcije i upozoravanja u slučaju neispravnog funkcioniranja ili neovlaštene izmjene načina rada uređaja. Konvencionalnim uređajima upravlja korisnik koji može detektirati nepravilan rad takvog uređaja ili uređaji imaju implementirane mehanizme detekcije nepravilnog i neovlaštenog rada [124].

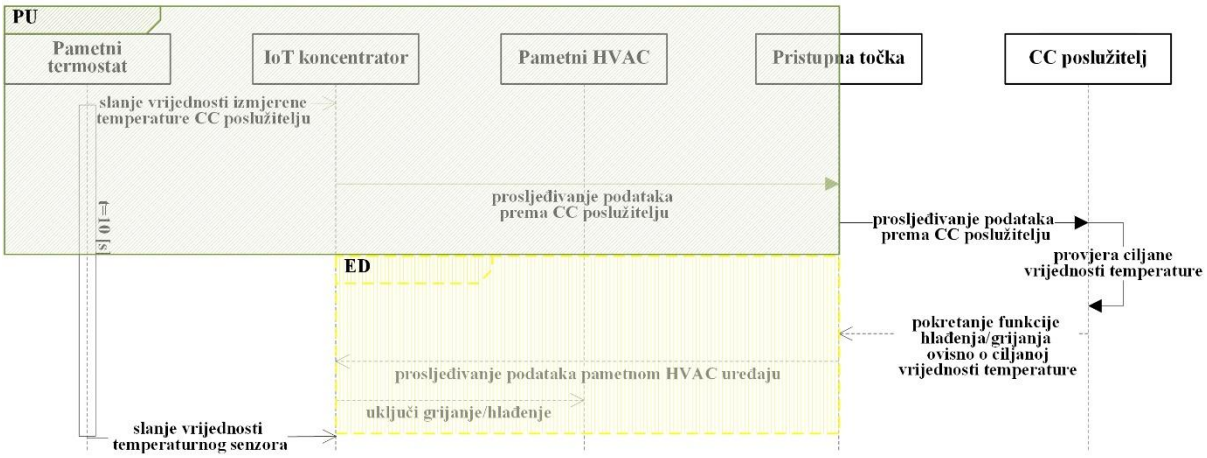
3.2.2 Uzorci prometa generiranog SHIoT uređajima

Ograničeni broj funkcionalnosti SHIoT uređaja čini njihovu komunikaciju do određene razine predvidivom što je moguće zaključiti i iz ograničenog broja uzoraka MTC prometa koje generiraju u procesu komunikacije. Istraživanjima [127] i [128] prepoznata su dva uzorka MTC prometa: uzorak periodičkog ažuriranja (engl. *Periodic Update,* PU) i uzorak uzrokovan događajem (engl. *Event Driven*, ED). Dodatni, treći uzorak utvrđen je istraživanjima [123] i [50], a određen je razmjenom sadržaja (engl. *Payload Exchange,* PE). Periodičko ažuriranje predstavlja uzorak prometa uzrokovan prijenosom, senzorom izmjerene vrijednosti prema IoT

koncentratoru, odnosno prema poslužitelju. Ovakva vrsta prijenosa podataka nije stvarnovremena i karakterizira ju jednaki vremenski intervali prijenosa podataka kao i konstantna količina podataka tijekom svakog prijenosa [129].

Zeleno označeno područje slike 3.5, korištenjem UML dijagrama međudjelovanja, prikazuje komunikacijski proces tijekom kojega se generira PU uzorak prometa. U prikazanom scenariju pametni termostat periodički prenosi vrijednost temperaturnog senzora IoT koncentratoru kojim je povezan. IoT koncentrator taj podatak prosljeđuje pristupnoj točki koja predstavlja izlazni mrežni čvor prema internetskoj mreži te se temperaturna vrijednost prosljeđuje CC usluzi na CC poslužitelju. CC usluga provjerava ciljanu temperaturu koju zadaje korisnik ili drugi proces te uspoređuje izmjerenu temperaturu sa ciljanom.

Žutim područjem slike 3.5 prikazan je ED uzorak prometa. Ukoliko postoji odstupanje, upućuje se zahtjev pametnom HVAC uređaju za uključenjem funkcije grijanja ili hlađenja. Zahtjev prema HVAC uređaju upućuje se posredstvom pristupne točke i IoT koncentratora na koji je uređaj povezan. Pri tome se generira ED uzorak prometa. ED uzorak prometa nastaje pojavom događaja koji predstavlja okidač za aktuator (pametni HVAC uređaj). Okidač može predstavljati senzorom izmjerena vrijednost (u prikazanom scenariju to je temperaturna vrijednost izmjera pametnim termostatom) ili naredba proslijeđena IoT koncentratoru u svrhu upravljanja aktuatorom.

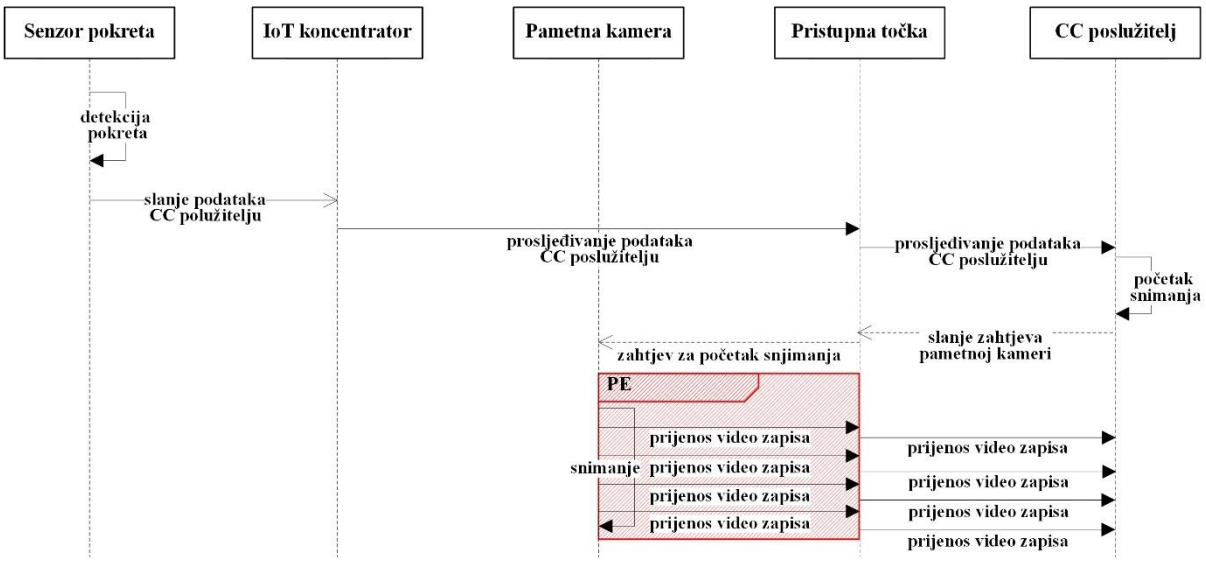


Slika 3.5 UML dijagram međudjelovanja komunikacijskog procesa u kojemu se generiraju PU i ED uzorci prometa

PE uzorak prometa rezultat je komunikacijskih procesa koji generiraju prethodna dva uzorka i podrazumijeva prijenos većih količina podataka između SHIoT uređaja i poslužitelja. Ovaj uzorak prometa karakteriziran je dominacijom odlaznog prometa čiji intenzitet može biti

konstantan (tijekom prijenosa telemetrijskih podataka) ili varijabilan (tijekom prijenosa slike ili videozapisa).

UML dijagramom međudjelovanja na slici 3.6 prikazan je komunikacijski proces između SHIoT uređaja (detektora pokreta i pametne kamere) posredstvom IoT koncentratora, pristupne točke i CC poslužitelja. Primjer generiranja PE uzorka prometa prikazan je crvenim područjem slike 3.6 tijekom prijenosa podatkovnog prometa generiranog pametnom kamerom (videozapis).



Slika 3.6 UML dijagram međudjelovanja komunikacijskog procesa u kojemu se generira PE uzorak prometa

Predvidivost MTC prometa naglašena je u [86], primjer mogućnosti primjene te karakteristike vidljiv je u istraživanju [123]. Autori istraživanja ukazuju da SHIoT uređaji u realnim implementacijama često generiraju promet koji sadrži kombinaciju navedenih uzoraka zbog čega predlažu radni okvir za modeliranje MTC prometa temeljen na ON/OFF strukturi. Pri tome se predlaže integracija takve strukture u Markovljev lanac koji ima četiri različita stanja (OFF, PU, ED i PE). Na ovaj način moguće je optimizirati mrežu u ovisnosti o karakteristikama MTC komunikacije.

3.3 Sigurnosni aspekti primjene koncepta pametnog doma

Različiti autori istražuju sigurnosne izazove koji se pretežno odnose na sveobuhvatno područje koncepta IoT. Prema [130], koncept IoT nasljeđuje sigurnosne izazove prisutne u senzorskim mrežama, mobilnim komunikacijskim mrežama i internetskoj mreži. Međutim, dodatno posjeduje i sigurnosne izazove povezane s privatnošću, autentikacijom, kontrolom pristupa i dostupnošću koje ističu brojna relevantna istraživanja [47], [74], [130–133]. Istraživanje [134] dokazuje kako osnovna načela sigurnosti (povjerljivost, cjelovitost i dostupnost) ili CIA trijada nisu dostatna pri uvažavanju novih prijetnji koje se javljaju kao rezultat primjene koncepta IoT. Prema tome, uz CIA trijadu, predlaže se razmatranje dodatnih načela: neporecivost, privatnost, revizija, odgovornost i vjerodostojnost prikazanih tablicom 3.2.

Tablica 3.2 Proširena načela sigurnosti nužna u okruženjima primjene koncepta IoT

Načelo sigurnosti	Obrazloženje	Resursi IK sustava na koje se načelo odnosi					
		Podatci	Korisnici	Procesi	Hardver	Softver	Mreža
Povjerljivost	Isključivo autorizirani korisnici/procesi imaju pravo uvida i pristupa resursima IK sustava		●				
Cjelovitost	Isključivo autorizirani korisnici imaju pravo izmjene podataka u IK sustavu			●			
Dostupnost	IK resursi moraju biti dostupni legitimnom korisniku/procesu u traženo vrijeme i prema zadanim uvjetima	●	●	●	●	●	●
Neporecivost	Sudionici transakcije koja se odvija posredstvom IK sustava ne mogu poreći provedbu transakcije	●	●	●	●	●	●
Privatnost	Sposobnost IK sustava da provodi definirana pravila privatnosti omogućavajući korisniku kontrolu nad osjetljivim podatcima	●					
Revizija	Sposobnost IK sustava da omogući provedbu revizije aktivnosti u slučaju nepoželjnog događaja	●	●	●	●	●	●
Odgovornost	Sposobnost IK sustava da nametne odgovornost korisniku za poduzete aktivnosti	●		●			
Vjerodostojnost	Sposobnost IK sustava da jednoznačno utvrdi identitet i osigura povjerenje između trećih strana (korisnika/procesa)	●	●				

Izvor: [134]

Jednako tako, u okruženjima kao što je pametan dom, dostupnost je načelo sigurnosti od ključne važnosti za krajnjeg korisnika. Prema tome, osnovna načela sigurnosti primjenjiva u navedenom okruženju moguće je prikazati i kao ACI pri čemu redoslijed označava prioritete u implementaciji mehanizama zaštite [135].

Okruženje pametnog doma, kao područje primjene koncepta IoT, pruža brojne prednosti korisnicima s različitih aspekata i kroz raznovrsne mogućnosti primjene. Paralelno s trendom rasta broja pametnih domova, penetracijom SHIoT uređaja i rastom investicija u ovaj koncept, dolazi do porasta sigurnosnih prijetnji. Ovo okruženje čine SHIoT uređaji koji prema istraživanjima različitih autora posjeduju ograničene funkcionalnost i hardverske resurse[7]. Prema [47], [112] i [136], ograničenja SHIoT uređaja rezultat su sljedećih zahtjeva i karakteristika:

- Veličina i dizajn uređaja – često se zahtijevaju male dimenzije uređaja što za posljedicu ima implementaciju hardverskih komponenti još manjih dimenzija i ograničenih mogućnosti.
- Cijena uređaja – zbog heterogenosti tržišta i brojnosti proizvođača zahtijeva se proizvodnja uređaja po što nižoj cijeni što rezultira korištenjem komponenata loše kvalitete, pouzdanosti i ograničenih mogućnosti.
- Energetski zahtjevi – uređaji moraju zadovoljiti visoke zahtjeve u autonomiji pri čemu se implementiraju energetski učinkovite komponente.
- Heterogenost – veliki broj uređaja koji koriste različite komunikacijske tehnologije i vlasničke protokole.

Ograničeni hardverski resursi u SHIoT uređajima koji su rezultat navedenih zahtjeva, onemogućuju implementaciju adekvatnih metoda zaštite kao što su primjerice napredni kriptografski algoritmi. Pri tome SHIoT uređaji ostaju izloženi brojnim prijetnjama koje imaju potencijal narušiti osnovna načela sigurnosti (povjerljivost, cjelovitost i dostupnost) takvih uređaja. Sigurnosnim izazovima doprinosi i činjenica da današnji objekti nisu građeni i dizajnirani kao pametni domovi, već se SHIoT uređaji retrogradno implementiraju u postojeće okruženje. Uz to, ne postoji stručna podrška pri dizajnu pametnog doma ili operativnog rada SHIoT uređaja u okruženju doma [137]. Dodatni čimbenik koji utječe na nisku razinu sigurnosti SHIoT uređaja je i njihova prilagođenost krajnjim korisnicima. Da bi SHIoT uređaji bili

[7] Resursi za obradu i pohranu podataka – CPU (engl. *Central Processing Unit*), RAM (engl. *Random Access Memory*), ROM (engl. *Read Only Memory*), itd.

dostupni što većem broju korisnika, proizvođači su morali pojednostaviti njihovu konfiguraciju da bi zahtijevala minimalnu interakciju korisnika poput povezivanja uređaja na pristupnu točku korištenjem WPS (engl. *Wi-Fi Protected Setup*) čije ranjivosti su poznate i dokazane [138]. Posljedica toga su SHIoT uređaji koji ne posjeduju osnovne mehanizme zaštite kao što je kriptirana komunikacija u procesu povezivanja i konfiguracije uređaja ili kao što su to podatci za pristup uređaju (korisničko ime i zaporka) [139].

SHIoT uređaji prikupljaju, obrađuju, pohranjuju i prenose podatke različitih razina osjetljivosti. U slučaju neovlaštenog pristupa, takvi podatci mogu biti iskorišteni u različite svrhe kao što je krađa identiteta, neovlašteni uvid u privatne podatke korisnika i praćenje ponašanja korisnika [140]. Uz navedeno, javlja se i mogućnost djelomičnog ili potpunog onemogućavanja rada SHIoT uređaja čime se gube funkcionalnosti pametnog doma. Neispravno funkcioniranje SHIoT uređaja može dovesti i do narušavanja fizičke sigurnosti čovjeka ili objekata zbog sve većeg oslanjanja korisnika na informacije pružene takvim uređajima [141]. Primjer je neispravno funkcioniranje detektora požara koji alarmira žurne službe. Konačno, SHIoT uređaje moguće je i koristiti kao posrednike ili sredstvo za provedbu drugih oblika napada (DDoS napadi) [112]. Istraživanja poput [142] pružaju detaljnu taksonomiju mogućih prijetnji na različitim slojevima koncepta pametnog doma, dok istraživanje [139] objedinjuje sigurnosne prijetnje okruženja pametnog doma na način prikazan tablicom 3.3 i to prema vrsti prijetnje, utjecaju i cilju prijetnje.

Tablica 3.3 Pregled prijetnji okruženju pametnog doma

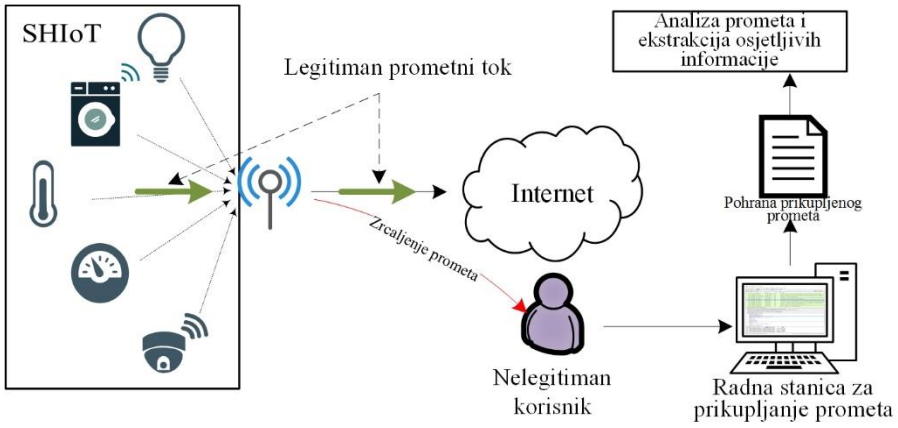
Vrsta prijetnje	**Prijetnja**	**Utjecaj**	**Cilj**
Pasivna	Prisluškivanje	Povjerljivost	Korisnik/SHIoT uređaj
Pasivna	Prisluškivanje	Privatnost	Korisnik
Pasivna	Iskorištavanje ranjivosti softvera	Povjerljivost	Korisnik/SHIoT uređaj
Pasivna	Iskorištavanje ranjivosti softvera	Privatnost	Korisnik
Pasivna	Iskorištavanje ranjivosti softvera	Integritet	Korisnik
Pasivna	Iskorištavanje ranjivosti softvera	Dostupnost	SHIoT uređaj
Aktivna	DDoS	Dostupnost	Korisnik/SHIoT uređaj
Aktivna	Lažno predstavljanje	Integritet	Korisnik
Aktivna	Lažno predstavljanje	Dostupnost	Korisnik/SHIoT uređaj
Aktivna	Lažno predstavljanje	Neovlašteni pristup	Korisnik

Izvor: [139]

Vrste prijetnji navedene tablicom ne mogu se smatrati konačnima, ali predstavljaju neke od najznačajnijih prijetnji pretpostavljenih okruženju pametnog doma.

3.3.1 Prijetnje prisluškivanja prometa

Prisluškivanje prometa predstavlja pasivnu nelegitimnu aktivnost kojom se narušava povjerljivost kao jedno od osnovnih načela sigurnosti pri čemu ne dolazi do izmjene podataka. Uz narušavanje povjerljivosti, ovakva vrsta prijetnje ima potencijal narušiti privatnost korisnika što je posebice izraženo u okruženju pametnog doma. Prisluškivanjem nelegitiman korisnik pasivno zrcali promet koji generiraju SHIoT uređaji čija analiza omogućava ekstrakciju osjetljivih informacija kako je prikazano slikom 3.7.

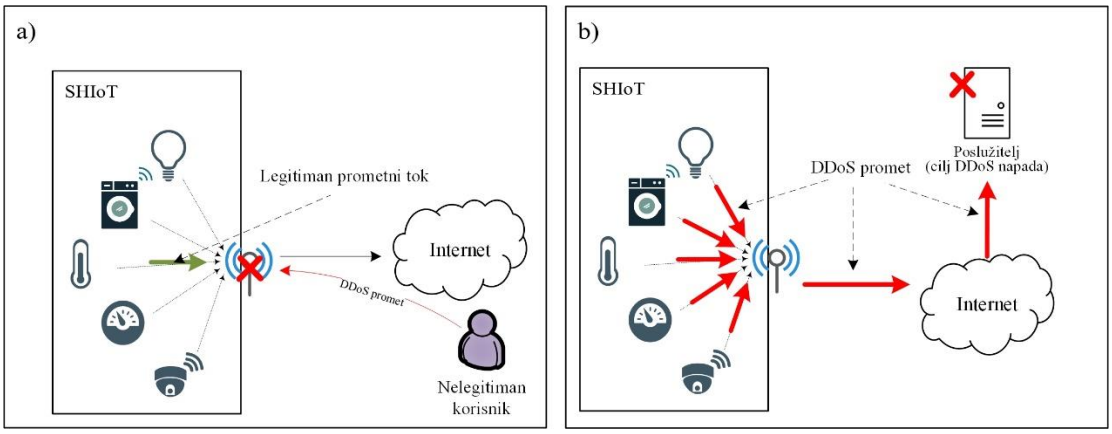


Slika 3.7 Princip prisluškivanja prometa

Prema istraživanju [143] SHIoT uređaji prikupljaju i prenose brojne informacije o okruženju korisnika kao i njegovim navikama. Analizom podataka prikupljenih neovlaštenim prisluškivanjem SHIoT uređaja poput senzora dima i ugljičnog monoksida moguće je, primjerice, utvrditi sa 90 postotnom sigurnošću nalazi li se korisnik u objektu [144]. Dobivenu informaciju moguće je iskoristiti za druge nelegitimne radnje kao što je fizička provala i sl. Ovakvu vrstu prijetnje nelegitiman korisnik ima mogućnost ostvariti povezivanjem na bežičnu pristupnu točku koja predstavlja točku agregiranja prometa svih SHIoT uređaja u okruženju.

3.3.2 DDoS prijetnje

DDoS napadi posebno su izražena prijetnja u okruženju pametnog doma. Statistički pokazatelji ukazuju na najnižu razinu zaštite SHIoT uređaja od ove vrste napada [145]. Uloga SHIoT uređaja u ovakvim napadima može biti promatrana s dva aspekta kako je prikazano slikom 3.8. Prvi aspekt podrazumijeva SHIoT uređaje kao cilj napada, slika 3.8 a).

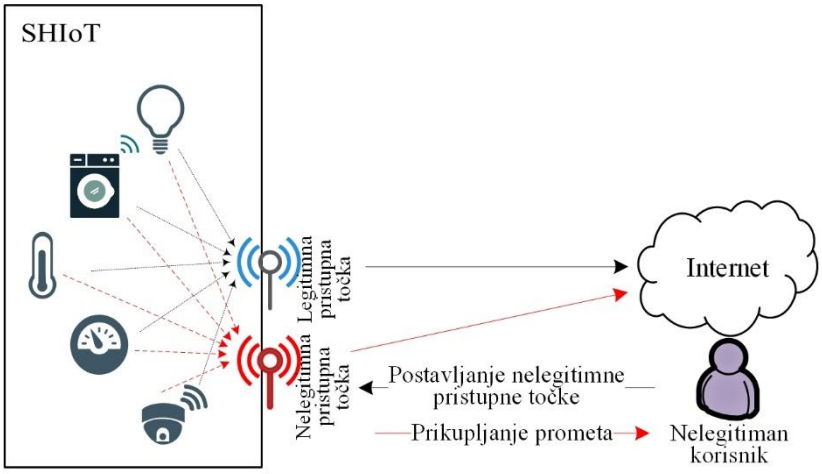


Slika 3.8 Provedba DDoS napada u okruženju pametnog doma, a) pametni dom kao cilj napada, b) pametni dom kao izvor napada

U ovakvom scenariju legitimnim korisnicima se nastoji onemogućiti pristup uslugama i funkcionalnostima koje pružaju SHIoT uređaji u okruženju pametnog doma kroz onemogućavanje rada bežične pristupne točke. Drugi scenarij odnosi se na korištenje SHIoT uređaja kao generatora DDoS prometa koji se prosljeđuje prema drugom odredištu s ciljem onemogućavanja pristupa legitimnim korisnicima, prikazano slikom 3.8 b) [59]. Ova prijetnja prema brojnim autorima, poput [146], predstavlja prijetnju najvećeg rizika.

3.3.3 Prijetnje lažnog predstavljanja

Lažno predstavljanje kao prijetnja podrazumijeva aktivnosti nelegitimnog korisnika kojima se nastoji oponašati legitiman korisnik ili uređaj s ciljem pristupa podatcima u okruženju pametnog doma. Provedba prijetnje podrazumijeva implementaciju nelegitimnog uređaja kao što je bežična pristupna točka ili IoT koncentrator koji obnaša funkciju legitimnog te na taj način predstavlja točku povezivanja SHIoT uređaja, vidljivo iz slike 3.9.



Slika 3.9 Princip provedbe prijetnje lažnog predstavljanja

Provedba prijetnje na opisani način pruža mogućnost prikupljanja osjetljivih podataka koje SHIoT uređaji prenose ili čak upravljanje radom SHIoT uređaja.

3.3.4 Prijetnje iskorištavanja ranjivosti softvera

Prijetnje koje iskorištavaju ranjivosti softvera implementiranog u SHIoT uređaje jednostavno je realizirati korištenjem malicioznog softvera[8] (engl. *malware*). Razlog je činjenica da SHIoT uređaji koriste prilagođene inačice poznatih operativnih sustava (najčešće linux distribucije) pri čemu nelegitimni korisnici nastoje iskoristiti njihove ranjivosti u svrhu nelegitimnog pristupa podatcima takvih uređaja ili samim uređajima. Prema [139], postoji više načina za korištenje malicioznog softvera u svrhu provedbe nelegitimnih aktivnosti nad SHIoT uređajima. Prvi način odnosi se na kupnju uređaja. Pri tome postoji rizik od nabave uređaja s prethodno implementiranim malicioznim softverom (nelegitiman korisnik implementira maliciozni kod u uređaj nakon čega ga prodaje putem različitih platformi za e-trgovanje poput *E-bay* trgovine). Drugi način podrazumijeva iskorištavanje nedostataka u operativnom sustavu SHIoT uređaja koji omogućavaju udaljeni pristup i nadogradnju *firmware*-a[9] inačicom koja sadrži implementiran maliciozni kod [147]. Treći način odnosi se na aplikativna rješenja instalirana na mobilne uređaje korisnika namijenjene upravljanju SHIoT uređajima. Takve aplikacije imaju pristup uređajima što znači da maliciozni kod instaliran na mobilni uređaj korisnika također može imati pristup SHIoT uređajima putem tih aplikacija [148].

[8] Dio programskog koda koji se izvršava na uređaju ili operativnom sustavu uređaja bez znanja i privole korisnika s ciljem provedbe nelegitimnih aktivnosti poput uzrokovanja neželjenog načina rada uređaja, izmjene ili preuzimanja podataka, širenja na druge uređaja, omogućavanja udaljenog pristupa ili udaljenu kontrolu uređaja.

[9] Programski kod koji se izvršava na razini sklopovlja te omogućava osnovno funkcioniranja uređaja i osigurava pristup višim funkcijama

4 Problem anomalija mrežnoga prometa

Budući da je istraživanje u okviru doktorskog rada usmjereno na detekciju anomalija mrežnoga prometa koje nastaju kao rezultat generiranja DDoS prometa posredstvom SHIoT uređaja, četvrtim poglavljem ovoga rada pojašnjen je termin anomalija u komunikacijskoj mreži kao i princip provedbe DDoS napada. Kompleksnost i raznovrsnost DDoS napada prikazani su taksonomijama te su analizom statističkih pokazatelja utvrđeni trenutni trendovi opsega napada, razine provedbe i protokola korištenih u provedbi DDoS napada. Istaknuta je i važnost pojave koncepta IoT i uređaja pod tim konceptom u porastu broja i intenziteta DDoS napada, gdje do izražaja dolaze upravo uređaji objedinjeni pod konceptom pametnog doma.

4.1 Anomalije u komunikacijskoj mreži

Anomalija predstavlja uzorke u podatcima koji ne odgovaraju prethodno definiranom normalnom ponašanju promatrane pojave. Podatci se općenito generiraju iz jednog ili više procesa koji mogu odražavati aktivnost u sustavu ili opažanja prikupljena o entitetima [149]. Neuobičajeno ponašanje procesa koji generira podatke stvara anomalije u podatcima. Prema tome, anomalija u podatcima često sadrži korisne informacije o abnormalnim karakteristikama sustava ili entiteta koji utječe na proces generiranja podataka. Prepoznavanje takvih značajki koje nisu uobičajene pruža korisne uvide u različitim primjenama. Primjeri primjene detekcije anomalija vidljivi su kroz brojna istraživanja, u različitim područjima primjene [150], [149]:

- **Sustavi detekcije nelegitimnih aktivnosti** (engl. *Intrusion detection systems*). U mnogim IK sustavima prikupljaju se različite vrste podataka o radu operativnog sustava, mrežnom prometu ili korisničkoj aktivnosti. Takvi podatci mogu ukazati na neuobičajeno ponašanje, odnosno anomalije uzrokovane nelegitimnim aktivnostima.
- **Otkrivanje prijevara s kreditnim karticama**. Prijevara s kreditnim karticama postaje sve češća zbog veće lakoće s kojom se mogu ugroziti osjetljivi podatci kao što je broj kreditne kartice. U mnogim slučajevima, neovlašteno korištenje kreditne kartice može pokazivati različite obrasce, kao što je iznenadno povećanje potrošnje s određenih lokacija (engl. *buying sprees*) ili kao što su vrlo velike transakcije. Takvi se obrasci mogu koristiti za otkrivanje ekstremnih vrijednosti u podatcima o transakcijama s kreditnim karticama.
- **Detekcija događaja putem senzora**. Senzori se često koriste za praćenje različitih parametara okoliša i lokacije u mnogim stvarnim aplikacijama. Iznenadne promjene temeljnih obrazaca mogu predstavljati događaje od interesa. Detekcija događaja jedna je od primarnih motivacijskih primjena u području senzorskih mreža.
- **Medicinske dijagnoze**. U brojnim medicinskim primjenama, podatci se prikupljaju primjenom različitih uređaja kao što su skeniranja korištenjem magnetske rezonance (MR), pozitronske emisijske tomografije (PET) ili vremenske serije elektrokardiograma (ECG). Neuobičajeni uzorci ili anomalije u takvim podatcima reflektiraju stanje bolesti pacijenta.

U svim navedenim primjerima primjene iz prikupljenih podataka definira se model normalnih podataka pri čemu su anomalije identificirane kao devijacije od takvog modela. Određene primjene poput detekcije neovlaštenog upada u IK sustav ili otkrivanje prijevara

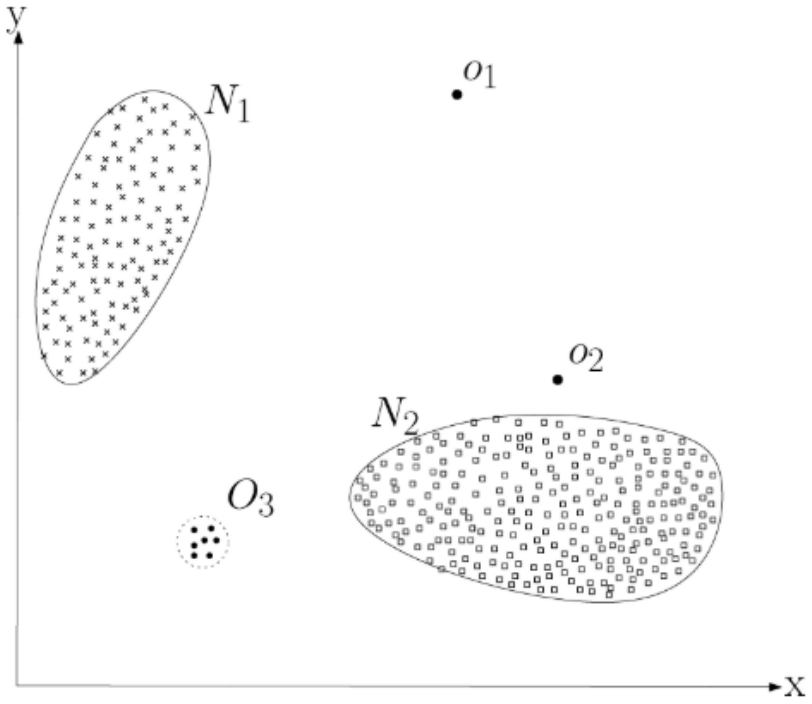
anomalije odgovaraju slijedu višestrukih podatkovnih točaka umjesto pojedinačnoj podatkovnoj točki. Specifičnost slijeda relevantna je za identifikaciju događaja koji predstavljaju anomaliju. Takve se anomalije u literaturi još nazivaju i kolektivne anomalije jer se mogu kolektivno izvesti iz skupa ili slijeda podatkovnih točaka.

Detekcije anomalija u podatcima općenito daju dvije vrste rezultata (ishoda):

1) razina anomalije i
2) binarne oznake.

Većina metoda detekcije anomalija vrednuje razinu anomalije svake podatkovne točke. Dobivene razine mogu služiti za rangiranje podatkovnih točaka prema njihovoj tendenciji da postanu anomalije. Binarne oznake indiciraju je li podatkovna točka anomalija ili ne. Razine anomalije također mogu biti transformirane u binarne oznake korištenjem graničnih vrijednosti koje se odabiru na temelju, primjerice, statističke distribucije razina dodijeljenih svim podatcima u promatranom skupu.

Slikom 4.1 prikazan je primjer anomalija podataka u dvodimenzionalnom podatkovnom skupu. Pri tome podatci imaju dvije normalne regije označene sa N_1 i N_2 s obzirom da većina opažanja leži u navedenim regijama. Točke koje su dovoljno daleko od označenih regija, poput o_1 i o_2 i skupa točaka u regiji O_3 predstavljaju anomalije [13].



Slika 4.1 Prikaz anomalije u dvodimenzionalnom podatkovnom skupu [13]

Promatrano s aspekta komunikacijske mreže, anomalije se mogu pojaviti u mrežnom podatkovnom prometu koji nastaje kao posljedica odvijanja komunikacijskih aktivnosti terminalnih ili mrežnih uređaja. Prema [1], uzroci anomalija u komunikacijskoj mreži mogu se pojaviti kao rezultat neočekivanih komunikacijskih aktivnosti, iznenadnog povećanja zahtjeva za uslugom legitimnih korisnika (engl. *flash crowd*) ili nelegitimnih aktivnosti. Prema [151], anomalije je moguće promatrati kroz tri osnovne kategorije, (1) individualne anomalije, (2) kontekstualne anomalije i (3) kolektivne anomalije.

Individualne anomalije su one u kojima pojedinačni podatak predstavlja anomaliju u odnosu na ostale podatke. Ovakve predstavljaju najjednostavniji oblik anomalije i brojna rješenja za detekciju anomalija pretpostavljaju upravo ovu vrstu anomalije. Izraz kontekstualne anomalije odnosi se na odstupanje značajki koje predstavljaju podatke zadanog konteksta. Kontekst može biti vremenski, prostorni ili zadan u ovisnosti o problemskom području [152]. Prema [153] i [154], kolektivna anomalija predstavlja skupine podataka koje se na pojedinačnoj razini ponašaju normalno, ali kao skupina predstavljaju anomaliju.

Detekcija različitih anomalija uzrokovanih nelegitimnim aktivnostima i sigurnosnim incidentima u računalnoj mreži predstavlja jedan od značajnijih izazova za istraživače, ali i za mrežne administratore i stručnjake IK sigurnosti. Jedan od rastućih uzročnika anomalija mrežnog prometa je prema brojnim istraživanjima DDoS napad. DDoS napadi predmetom su istraživanja od početka 2000. godine kada su ciljem tih napada postali Yahoo, Ebay, Amazon i slični portali u vlasništvu multinacionalnih kompanija koje su i tada velike resurse ulagale u sigurnost svojih IK sustava. DDoS napadi već su tada pokazali kako se radi o vrsti napada koje je teško detektirati i od kojih se teško zaštititi [155].

4.2 Značaj distribuiranih napada uskraćivanja usluge pri generiranju anomalija u komunikacijskoj mreži

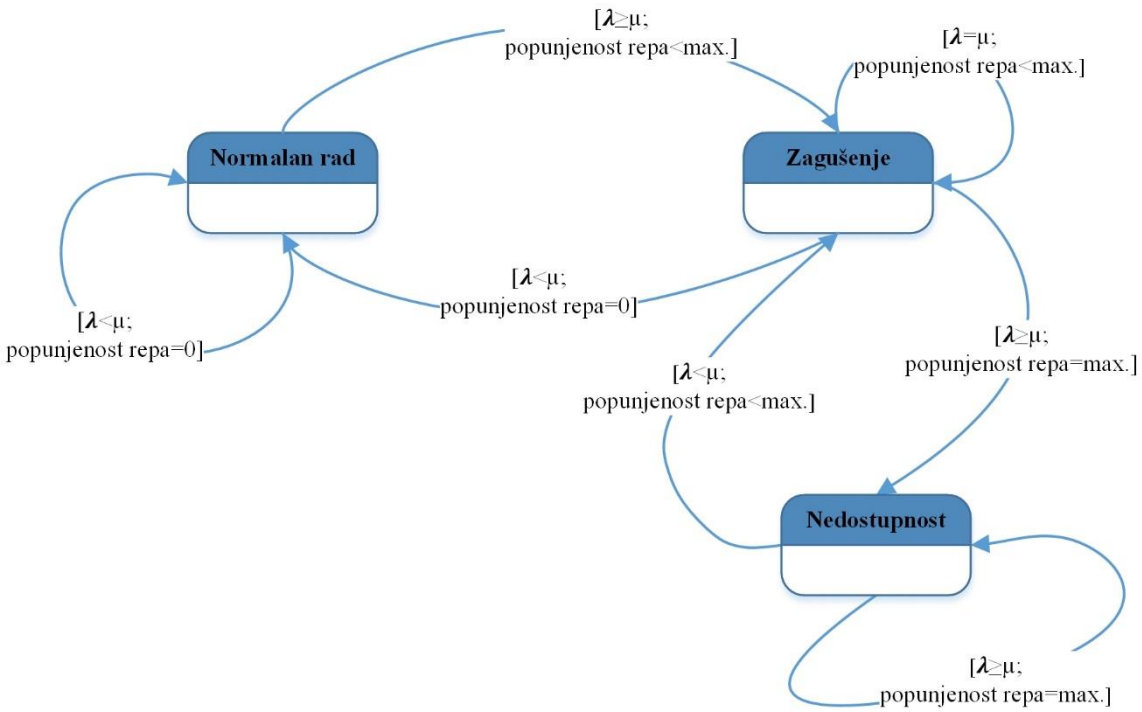
Većina nelegitimnih aktivnosti koje se odvijaju u IK sustavu nastoje narušiti jedno od tri osnovna načela sigurnosti pri čemu narušavanje načela dostupnosti podrazumijeva onemogućavanje pristupa IK usluzi, sustavu ili bilo kojem resursu legitimnim korisnicima [156]. Pri tome je legitimni korisnik predstavljen kao korisnik koji ima određenu razinu ovlasti korištenja resursa IK sustava i te ovlasti ne prelazi neovlaštenim aktivnostima. Napad uskraćivanja usluge (engl. *Denial of Service,* DoS) podrazumijeva općenitu klasu napada usmjerenih na dostupnost IK resursa.

Prema načinu distribucije, DoS napade moguće je podijeliti u dvije kategorije [157]:

- napadi s jednim izvorištem, SDoS (engl. *Single Source Denial of Service*) i
- napadi s više izvorišta ili distribuirani napad uskraćivanja usluge, DDoS.

Izvor SDoS napada je jedno računalo ili uređaj u mreži. Distribuirani napad uskraćivanja usluge predstavlja koordiniranu nelegitimnu aktivnost čija je svrha iskoristiti dostupne kapacitete uređaja za obradu ili prijenos mrežnog prometa s ciljem onemogućavanja pristupa IK resursima legitimnim korisnicima. Prema navedenome, DDoS napad usmjeren je narušavanju dostupnosti kao jednom od tri osnovna načela sigurnosti IK sustava. U svrhu provedbe napada koristi se veliki broj uređaja u mreži (najčešće terminalni uređaji) čiji komunikacijski resursi se koriste za generiranje nelegitimnog DDoS prometa prema cilju napada.

UML dijagramom stanja i prijelaza, na slici 4.2 prikazana su stanja u kojima se IK sustav ili usluga mogu nalaziti kao i uvjeti koji dovode do prelaska u pojedina stanja ili zadržavanja postojećeg stanja. Normalan rad je stanje koje se održava u uvjetima gdje je intenzitet prometa ili zahtjeva ($\boldsymbol{\lambda}$) manji od kapaciteta poslužitelja, odnosno manji od brzine obrade pristiglih zahtjeva (μ). Ukoliko je intenzitet prometa veći od kapaciteta poslužitelja, sustav prelazi u stanje zagušenja i ostaje u tom stanju sve dok popunjenost repa poslužitelja ne dosegne maksimum ili dok se ne smanji intenzitet dolaznog prometa. U prvom slučaju, kad se dosegne maksimum popunjenosti repa posluživanja, sustav prelazi u stanje nedostupnosti dok se u drugom slučaju sustav vraća u stanje normalnog rada.

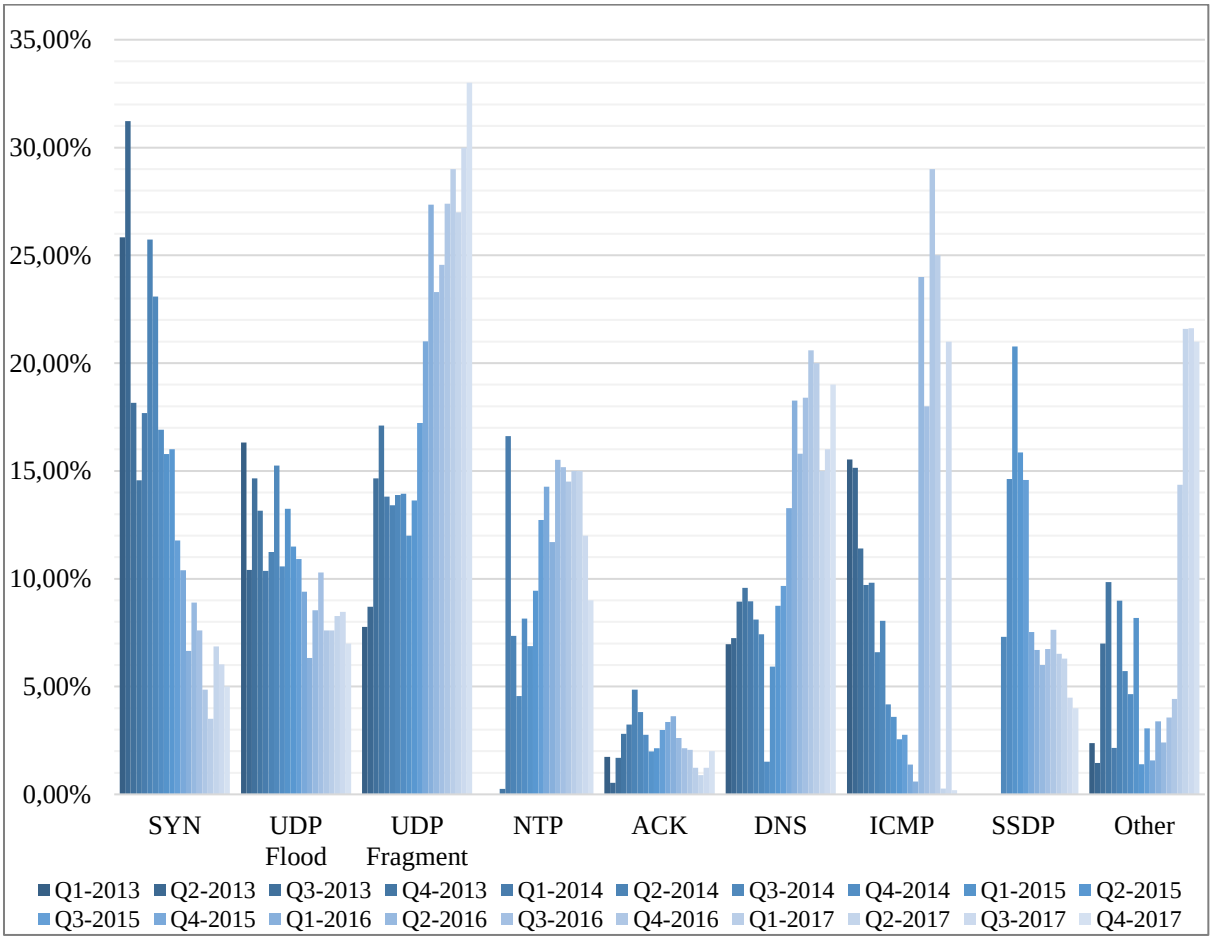


Slika 4.2 UML dijagram stanja IK resursa i usluga

DDoS napad koristi nedostatke arhitekture internetske mreže. Internetska mreža dizajnirana je za pružanje funkcionalnosti pri čemu sigurnost komunikacije nije razmatrana. Istraživanja [19], [158] i [159] ističu nedostatke dizajna internetske mreže koji omogućuju uspješnu provedbu DDoS napada. Prvi nedostatak ogleda se u ograničenom kapacitetu uređaja povezanih u mrežu koji mogu biti u potpunosti iscrpljeni. Također, kao jedan od problema ističe se da ranjivost na DDoS napad ne ovisi o razini zaštite uređaja u mreži koji je cilj napada, već ovisi o sigurnosti globalne internetske mreže. Porast broja uređaja i količine prometa koji se prenosi mrežom rezultiralo je nadogradnjom linkova visoke propusnosti u jezgrenom segmentu komunikacijske mreže. Navedeno je omogućilo iskorištavanje takve konfiguracije za isporuku intenziteta prometa koji prelazi 1Tb/s prema krajnjem cilju napada. Neprovođenje autentikacije pojedinog IP paketa omogućilo je provedbu DDoS napada s lažnim izvorišnim IP adresama što čini snažan mehanizam anonimizacije izvora napada. Konačno, kao jedan od značajnijih problema ističe se distribuirani način upravljanja i kontrole u internetskoj mreži. Svaka lokalna mreža povezana na internetsku mrežu može funkcionirati prema politici koju definira administrator. Posljedično, ne postoji način implementacije i provedbe globalnih sigurnosnih mehanizama ili politika što onemogućava istraživanje ponašanja prometa između raznovrsnih mreža.

Istraživanje i razvoj metoda detekcije DDoS prometa zahtijeva kontinuiranu analizu trendova korištenih protokola i intenziteta prometa s ciljem pravovremene reakcije na buduće napade. Najveći broj napada povezanih s infrastrukturnim slojem 2013. i 2014. godine izveden je posredstvom TCP protokola uz iskorištavanje SYN[10] oznake (31,22 % i 25,73 %). Nakon 2014. godine uočavaju se promjene u učestalosti korištenja pojedinih protokola infrastrukturnog sloja. Od trećeg kvartala 2014. godine udio napada temeljenih na SYN-u je u padu, a vidljiv je porast primjene drugih protokola poput UDP, NTP (engl. *Network Time Protocol*) i DNS (engl. *Domain Name System*). Grafikonima 4.1 i 4.2 prikazana je učestalost korištenja pojedinih protokola u provođenju DDoS napada, kvartalno za vremensko razdoblje od prvog kvartala 2013. do četvrtog kvartala 2017. godine.

Grafikon 4.1 Učestalost primjene protokola infrastrukturnog sloja u provođenju DDoS napada

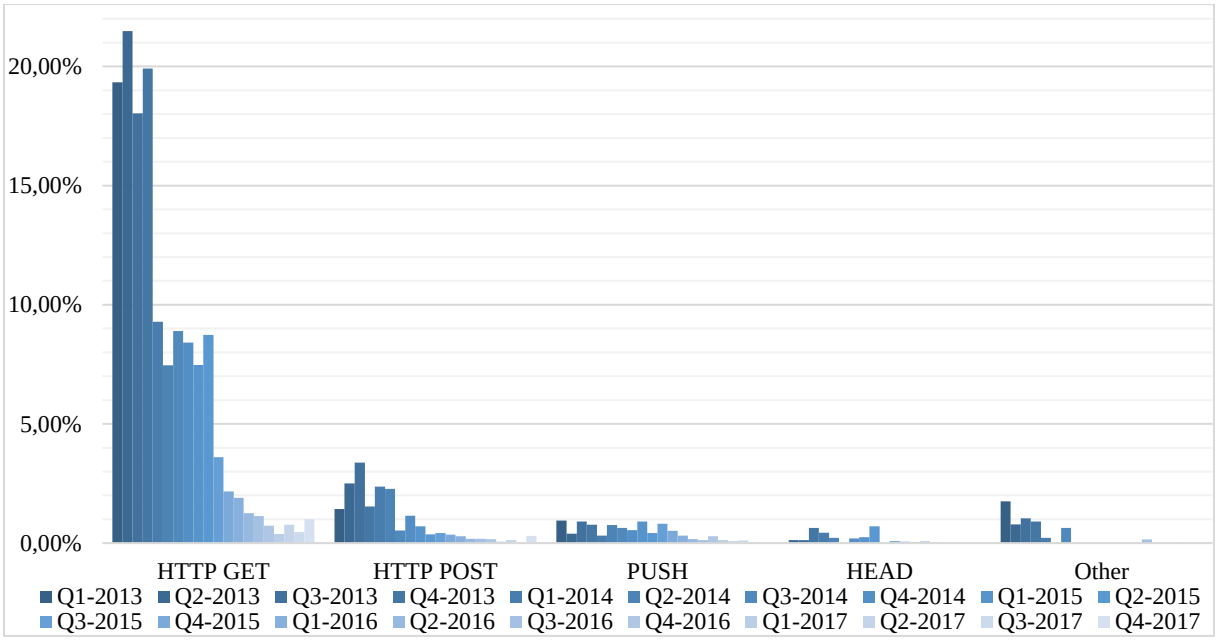


Izvor: [160]

[10] SYN predstavlja jednu od šest mogućih oznaka TCP zaglavlja (ACK, SYN, URG, FIN, RST, PSH, CWR, ECE i NS) čija je funkcija sinkroniziranje slijednih brojeva paketa prilikom iniciranja TCP sjednice

Iz prikazanih grafikona vidljivo je da su napadi infrastrukturnog sloja učestaliji u svih 20 analiziranih kvartala i imaju kontinuirani trend rasta (76,54 % - 99,43 %), za razliku od napada aplikacijskog sloja (23,46 % - 0,57 %) čiji je trend u padu.

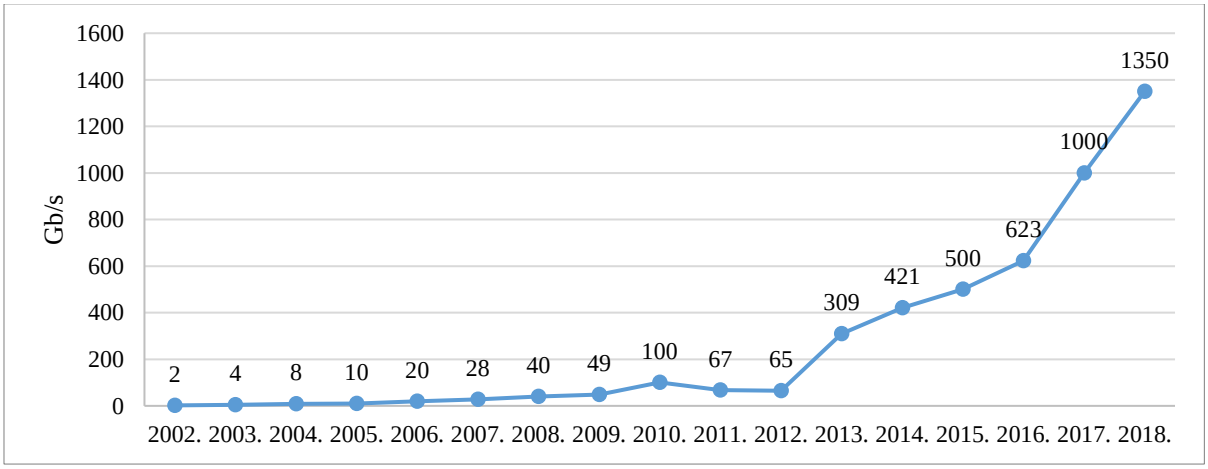
Grafikon 4.2 Učestalost primjene protokola aplikacijskog sloja u provođenju DDoS napada



Izvor: [160]

Iz podataka prikazanih grafikonom 4.3 uočava se skokoviti trend rasta intenziteta prometa generiranog DDoS napadima od 2013. godine. Napad s najvećim intenzitetom DDoS prometa zabilježen je krajem 2018. godine te je iznosio 1,35 Tb/s. Uzrok prikazanog trenda je razvoj koncepata kao što su IoT i CC. Novi IK koncepti omogućavaju stvaranje *botnet* mreže koju čini veći broj uređaja te koji u sumi mogu generirati veći intenzitet DDoS prometa prema odredištu nego što su to mogli *botnet* mreže sačinjene od konvencionalnih uređaja.

Grafikon 4.3 Intenzitet generiranog DDoS prometa u vremenskom periodu 2002.-2018.



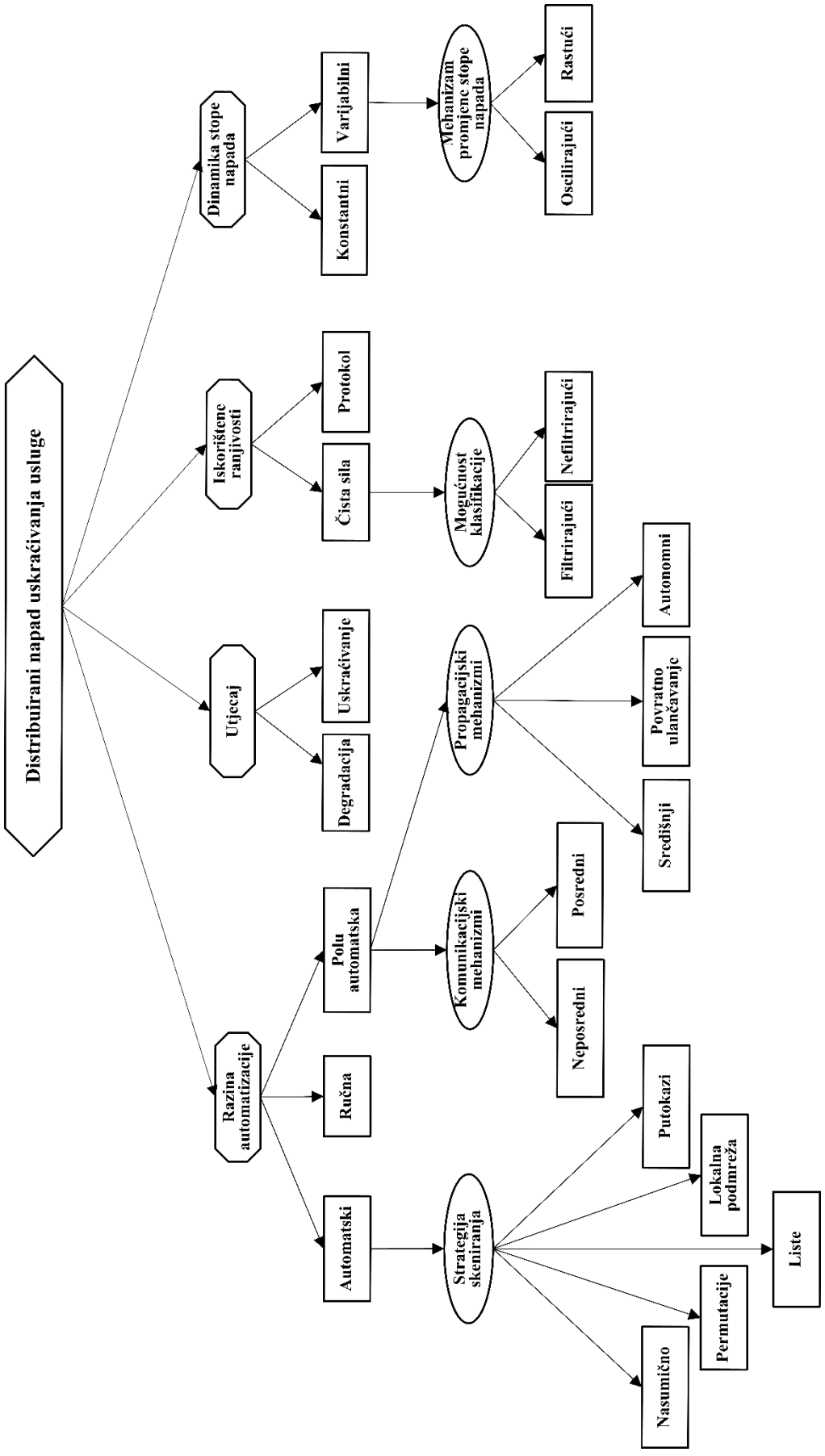
Izvor: [59], [161], [162]

Jednako tako, potreba za većim DDoS prometnim intenzitetom nametnuta je CC okruženjem u kojemu se brojni IK resursi i usluge danas nalaze. Takva okruženja posjeduju i veće kapacitete za obradu prometa i zahtjeva što, za uspješno narušavanje dostupnosti IK resursa u CC okruženju, implicira generiranje većeg intenziteta DDoS prometa [163].

4.2.1 Taksonomija DDoS napada

Postoje brojni načini provedbe DDoS napada što zahtijeva razvoj taksonomije s ciljem boljeg razumijevanja ovakve vrste napada i razvoja metoda zaštite. Istraživanja poput [19], [164], [159], [165] i [166] predlažu različite taksonomije DDoS napada. Istraživanje [19] definira jednu od prvih taksonomija DDoS napada 2004. godine, prikazanu slikom 4.3 koja u obzir uzima sredstva potrebna za pripremu i provođenje napada, karakteristike napada i utjecaja koji napad ima na cilj ili žrtvu kao osnovne klase.

Istraživanje [165] predlaže taksonomiju temeljenu na osnovnim metodama provedbe napada. Predložene su dvije osnovne klase napada: iskorištavanje propusnosti i iskorištavanje resursa za obradu podataka. Taksonomija definirana u [167] detaljnije klasificira DDoS napade i to sa četiri aspekta napada: iskorištavanje propusnosti komunikacijskog linka, iskorištavanje dostupnih resursa za obradu podataka, napadi na infrastrukturu i *Zero-day* napadi. Pri tome autori ističu napad na infrastrukturu kao najdestruktivniju klasu napada s obzirom da je cilj takvog napada prouzročiti nedostupnost ključne infrastrukture za normalno odvijanje komunikacije putem internetske mreže. Primjer cilja napada na infrastrukturu je *root* DNS poslužitelj čija nedostupnost može onemogućiti komunikaciju putem internetske mreže na globalnoj razini.



Slika 4.3 Taksonomija DDoS napada [19]

Navedene taksonomije predložene su prije razvoja koncepta IoT koji pruža nove mogućnosti provedbe ovakvih napada u pogledu jednostavnosti provedbe napada i intenziteta DDoS prometa koji je moguće generirati prema odredištu. Istraživanje [158] prikazuje taksonomiju DDoS napada, prikazanu tablicom 4.1.

Tablica 4.1 Upotpunjena taksonomija DDoS napada temeljena na novim IK okruženjima

Cilj napada	Infrastrukturni		
	Mrežni		
	Host[11]		
	Aplikacijski		
Arhitektura napada	Agent-rukovatelj		
	Refleksijski		
	IRC temeljen		
	WEB temeljen		
Iskorištavanje ranjivosti	Mrežna propusnost	Poplavljivanje	
		Amplifikacija	
	Resursi	Iskorištavanje protokola	
		Neispravno formirani paketi	IP adresa
			Opcije IP paketa
Razina protokola	Mrežna razina		
	Aplikacijska razina		
Stupanj automatizacije	Ručni		
	Automatski		
	Poluautomatski	Posredni	
		Neposredni	
Skeniranje	Nasumično		
	Liste		
	Putokazi		
	Permutacije		
	Lokalna podmreža		
Propagacija	Centralni izvor		
	Povratno ulančavanje		
	Autonomno		
Utjecaj na cilj napada	Degradacija		
	Uskraćivanje	Oporavljiv	
		Ne oporavljiv	
Stopa napada	Varijabilna	Oscilirajući	
		Povećavajući	
	Kontinuirana		
Mogućnost klasifikacije	Klasificirajući	Filtrirajući	
		Nefiltrirajući	
	Neklasificirajući		
Skup agenata	Varijabilni		
	Konstantni		
Izvorišna adresa	Stvarana		
	Lažirana	Usmjerljivost	Usmjerljiva
			Neusmjerljiva
		Tehnike lažiranja	Podmreža
			Na ruti
			Nasumična
Distribucija prometa	Jednako distribuiran		
	Nejednako distribuiran		
Resursi uključeni u napad	Simetrično		
	Asimetrično		

Izvor: [158]

[11] Uređaj povezan na računalnu mrežu (računalo, poslužitelj, IoT uređaj, i sl.)

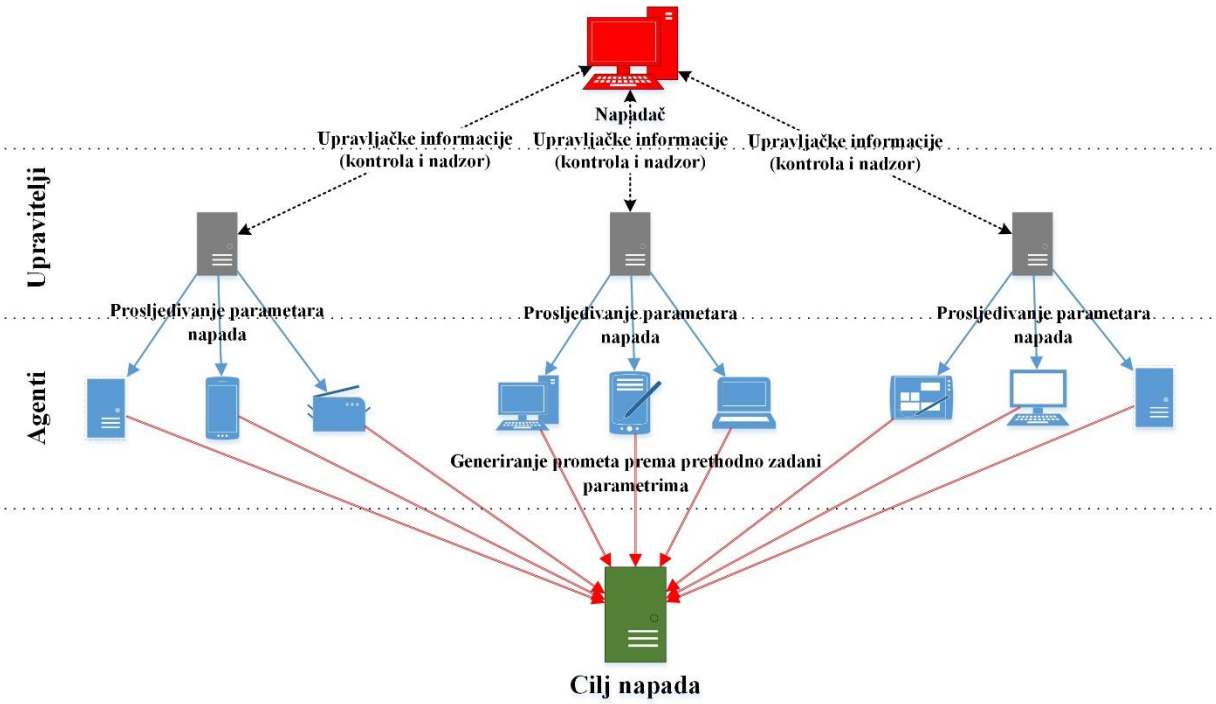
Prikazana taksonomija objedinjuje saznanja i zaključke prethodnih istraživanja te ih nadopunjuje novim klasama u svrhu proširenja baze znanja o trenutno dostupnim načinima provedbe DDoS napada koji postaju rastuća prijetnja upravo zbog sve češće primjene koncepta IoT i heterogenosti IoT uređaja s niskom razinom zaštite.

4.2.2 Princip provođenja DDoS napada

Distribuirani DoS napadi najčešće se provode posredstvom mreže udaljeno kontroliranih i geografski dislociranih uređaja. Mreža takvih uređaja naziva se još i *botnet*, a uređaji unutar *botneta* nazivaju se „zombi“ uređaji [168]. Za formiranje *botnet* mreže koriste se dva osnovna elementa, prikazani slikom 4.4 [169]:

- agenti (engl. *Agents*) i
- upravitelji (engl. *Handlers*) ili C&C poslužitelji (engl. *Command and Control*).

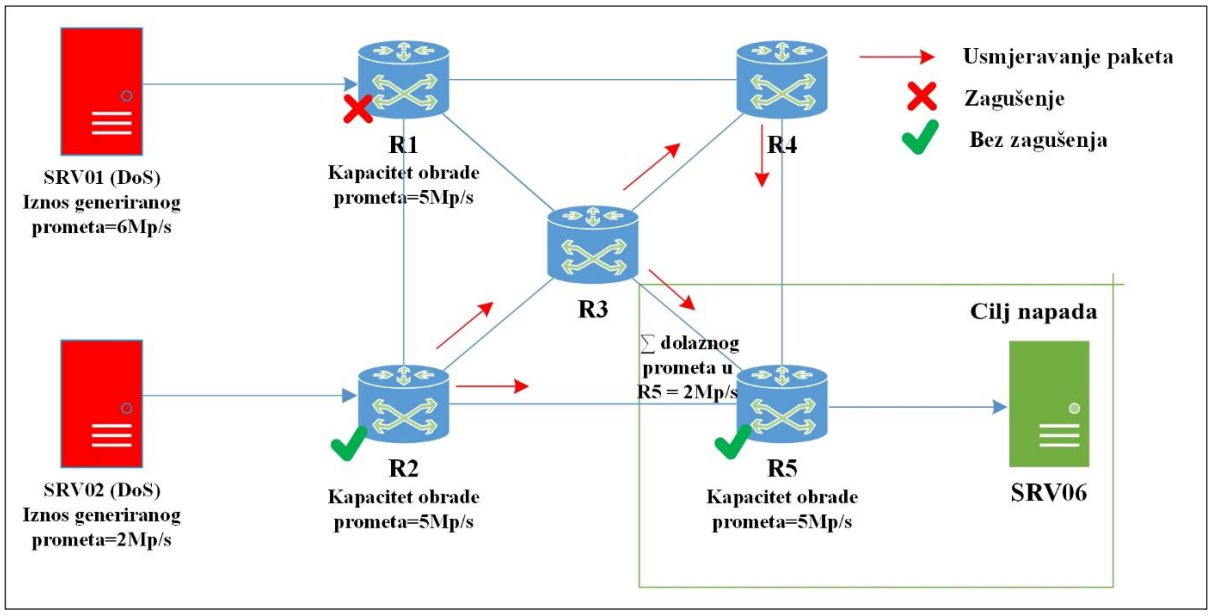
Agenti se izvršavaju na kompromitiranim uređajima i generiraju promet korišten za napad, dok su upravitelji programske strukture koje se izvršavaju na uređajima zaduženima za definiranje cilja, vremena, duljine i ostalih parametara napada koje prosljeđuju agentima. Agenti na temelju zadanih vrijednosti parametara generiraju DDoS promet i prosljeđuju ga prema cilju napada.



Slika 4.4 Arhitektura provedbe DDoS napada

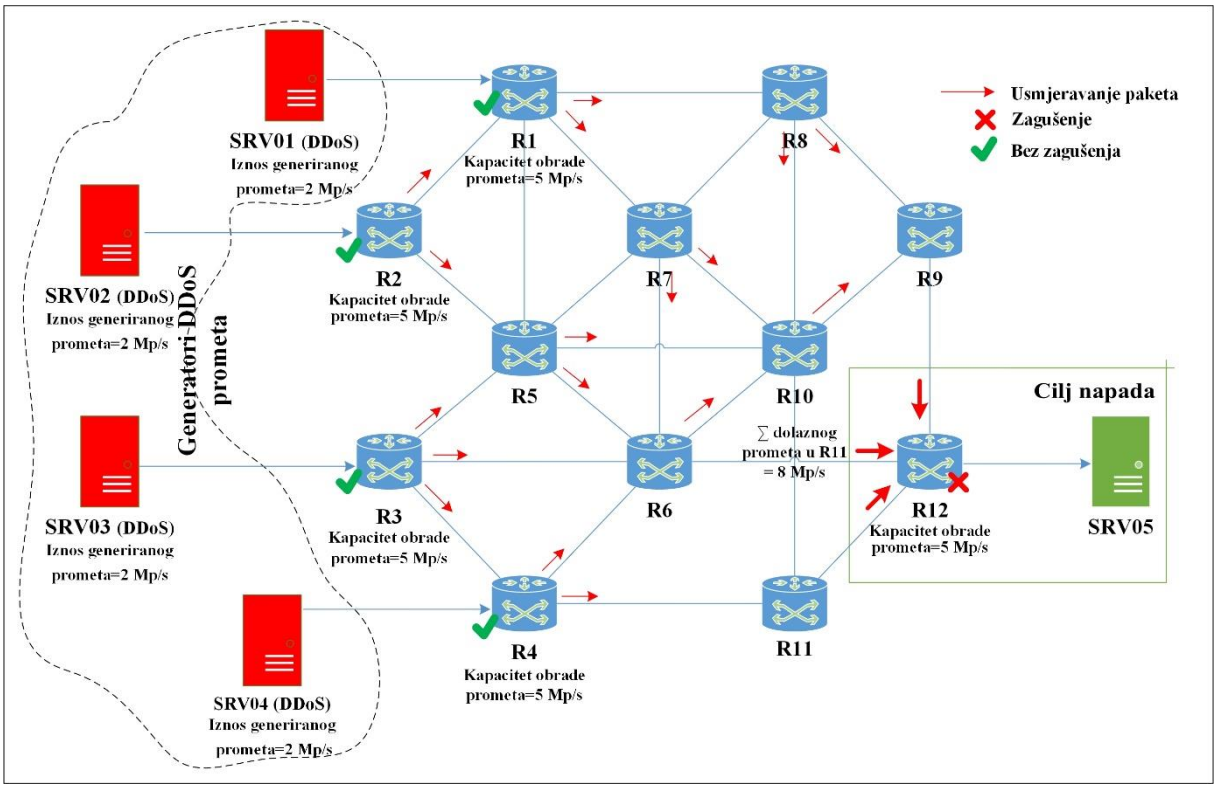
Razlog pojave DDoS metode napada je povećanje brzine obrade paketa unutar usmjerivača i krajnjih uređaja (poslužitelja) uslijed čega jedan uređaj u mreži često nije bio u mogućnosti generirati dovoljan intenzitet prometa da bi stvorio zagušenje u mreži. Drugi razlog jest maskiranje stvarnog izvora napada primjenom velikog broja, najčešće geografski dislociranih, uređaja za generiranje napada. Dodatni razlog primjene DDoS napada jest velika vjerojatnost stvaranja zagušenja u neželjenom segmentu mreže primjenom SDoS metode napada.

Slikom 4.5 prikazan je primjer izvođenja SDoS napada kroz dva slučaja. U prvom slučaju uređaj u mreži (SRV01) kao izvor napada generira promet iznosa 6 Mp/s (mega paketa po sekundi) koji je veći od kapaciteta obrade pristupnog usmjerivača (R1) što rezultira stvaranjem prometnog zagušenja u neželjenoj točki mreže za napadača. U drugom slučaju, uređaj u mreži (SRV02) kao izvor SDoS napada generira promet iznosa 2 Mp/s koji je manji od kapaciteta obrade pristupnog usmjerivača (R2), ali je manji i od kapaciteta obrade usmjerivača R5 koji je u domeni cilja napada. Drugim slučajem nije postignut željeni učinak prometnog zagušenja u željenom segmentu mreže.



Slika 4.5 Pojednostavljeni prikaz SDoS napada

Pojednostavljeni prikaz DDoS napada vidljiv je iz slike 4.6. Uređaji u mreži (SRV01 – SRV04) generiraju promet tako da ne stvaraju prometno zagušenje u pristupnim usmjerivačima (R1 – R4) jer je iznos generiranog prometa pojedinačnog uređaja manji od kapaciteta obrade pojedinog usmjerivača. Budući da je cjelokupni promet usmjeren prema uređaju SRV05, odnosno usmjerivaču R12 koji je u domeni cilja napada, prometno zagušenje nastat će upravo u toj točki kao rezultat sume generiranog prometa pojedinog uređaja na izvorišnoj strani.



Slika 4.6 Pojednostavljeni prikaz DDoS napada

Prometno zagušenje u usmjerivačima R5 – R11 nije razmatrano zbog postojanja mehanizama kontrole zagušenja i usmjeravanja paketa kroz mrežu u ovisnosti o stanju u pojedinoj točki. Kao točke interesa (i višeg stupnja ranjivosti), promatrani su isključivo pristupni usmjerivači (R1 – R4) te granični usmjerivač u domeni cilja napada (R5).

Prethodno su navedeni neki od razloga primjene DDoS napada pri čemu se provode posredstvom dviju osnovnih metoda [19]:

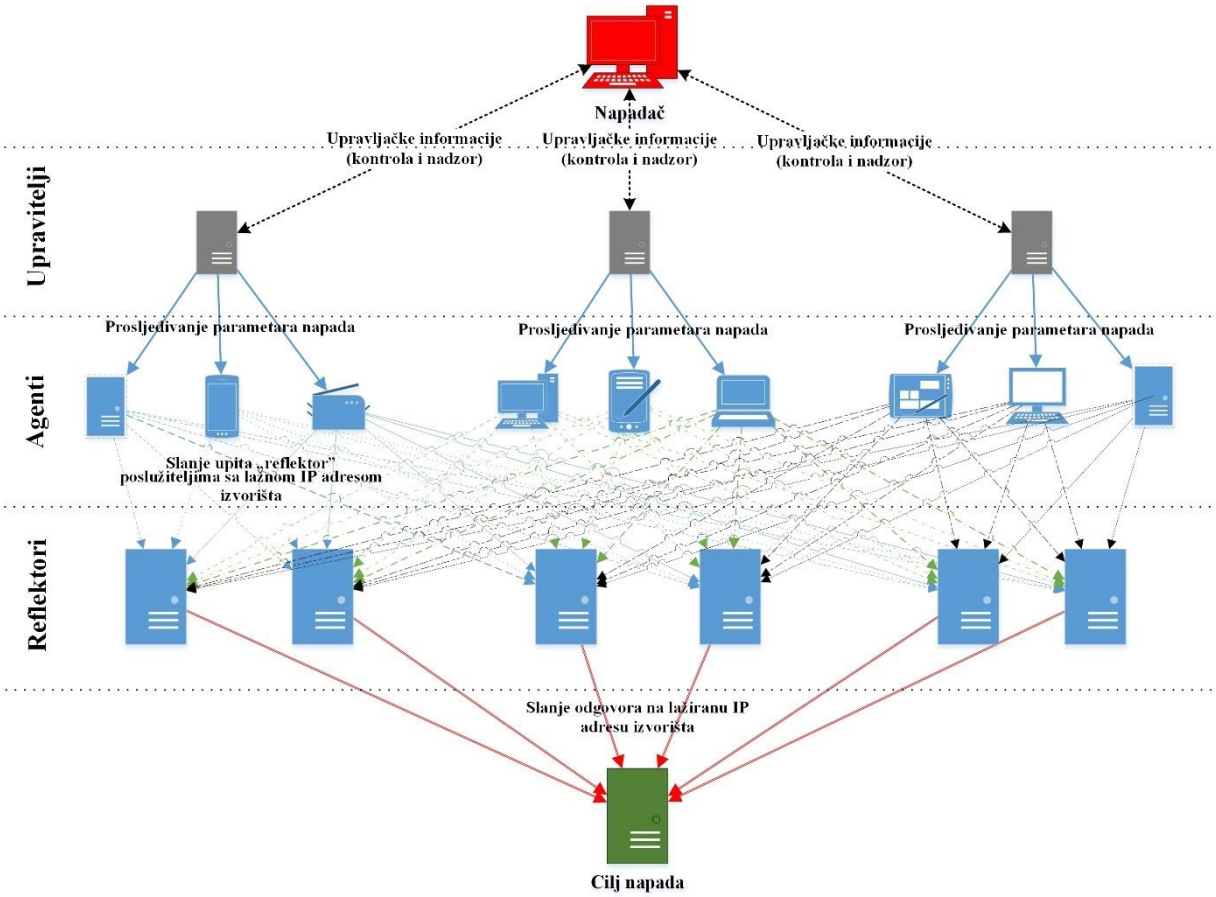
1) Slanje modificiranih mrežnih paketa s ciljem uzrokovanja nepravilnog rada mrežnih protokola.
2) Uskraćivanje povezivosti legitimnih korisnika iscrpljivanjem kapaciteta komunikacijskog linka ili kapaciteta resursa za obradu unutar usmjerivača (napadi poplavljivanjem na mrežnom i transportnom OSI sloju, često nazivani i infrastrukturni napadi) ili uskraćivanje usluge legitimnim korisnicima iscrpljivanjem resursa poslužitelja (napadi „poplavljivanjem“ na aplikacijskom OSI sloju).

4.2.2.1 Reflektivni i amplifikacijski napadi

Reflektivni napad (engl. *Distributed Reflected Denial of Service,* DRDoS) je vrsta DDoS napada koji posredstvom reflektora višestruko uvećava korištenu pojasnu širinu i prometni volumen upućen prema cilju. Uz standardne komponente klasičnog DDoS napada,

koriste se tzv. „reflektori“ kao dodatni sloj između napadača i cilja napada. Reflektori su uređaji (poslužitelji) izvan *botnet* mreže koji pružaju odgovore na postavljeni upit. Agenti koji upućuju upit, lažiraju IP adresu izvorišta (adresa cilja napada) što rezultira slanjem odgovora reflektora na IP adresu cilja napada [170]. Prikaz izvođenja DRDoS vidljiv je na slici 4.7.

Često korišteni „reflektor“ poslužitelj u izvođenju DRDoS napada je DNS poslužitelj s ciljem preplavljivanja cilja napada DNS *reply* prometom. Napadač u zahtjevima upućenim DNS poslužitelju navodi opciju „ANY“ što rezultira odgovorom koji sadrži sve dostupne informacije o domeni specificiranoj unutar upita [171]. Na upit veličine 64 *Byte* moguće je generirati odgovor veličine 3000 *Byte*, odnosno prosječno 1200 *Byte* kao što je prikazano u [172].



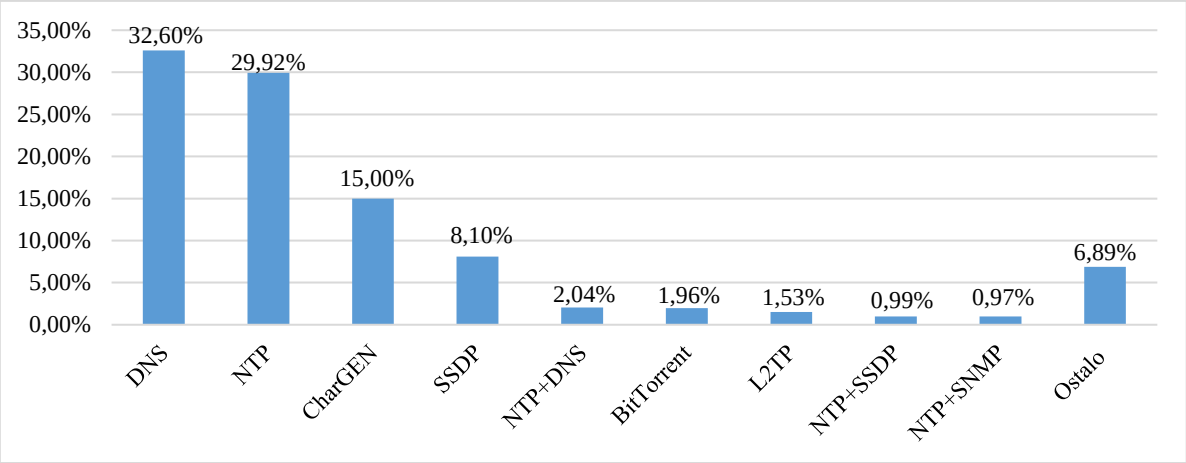
Slika 4.7 Izvođenje DDoS napada posredstvom "reflektor" poslužitelja

Prema istraživanju [173], DNS DRDoS metodom, 2016. godine, uspješno je generiran napad intenziteta 623 Gb/s i najopsežniji je do tada zabilježeni napad, što potvrđuje učinkovitost DRDoS metode napada.

Grafikonom 4.4 prikazani su protokoli korišteni pri izvođenju DRDoS napada. Uz DNS i NTP protokole (32,6 % i 29,92 %), često su korišteni CharGEN i SSDP protokoli (15 % i 8,1

%). Njihova primjena ima potencijal generiranja napada velikog intenziteta i stvaranja značajnih zagušenja u mreži te uskraćivanja pristupa ciljanom uređaju ili segmentu mreže.

Grafikon 4.4 Protokoli korišteni u DRDoS napadima



Izvor: [174]

Za razliku od reflektivnih, amplifikacijski napadi iskorištavaju faktor pojačanja generiranog prometa. Kao primjer, moguće je iskoristiti usmjerivač kao pojačalo posredstvom *broadcast* adrese. Zahtjev poslan na *broadcast* adresu usmjerivač prosljeđuje svim uređajima u podmreži, pri čemu svi uređaji u mreži šalju odgovor na adresu specificiranu unutar zahtjeva kao izvorišnu. Lažiranjem IP adrese izvorišta postiže se prosljeđivanje višestrukih odgovora na adresu koja predstavlja cilj napada. Primjeri takvih napada su *Smurf* i *Fraggle* vrste napada [175–177].

4.2.2.2 Napadi manipulacijom TCP protokola

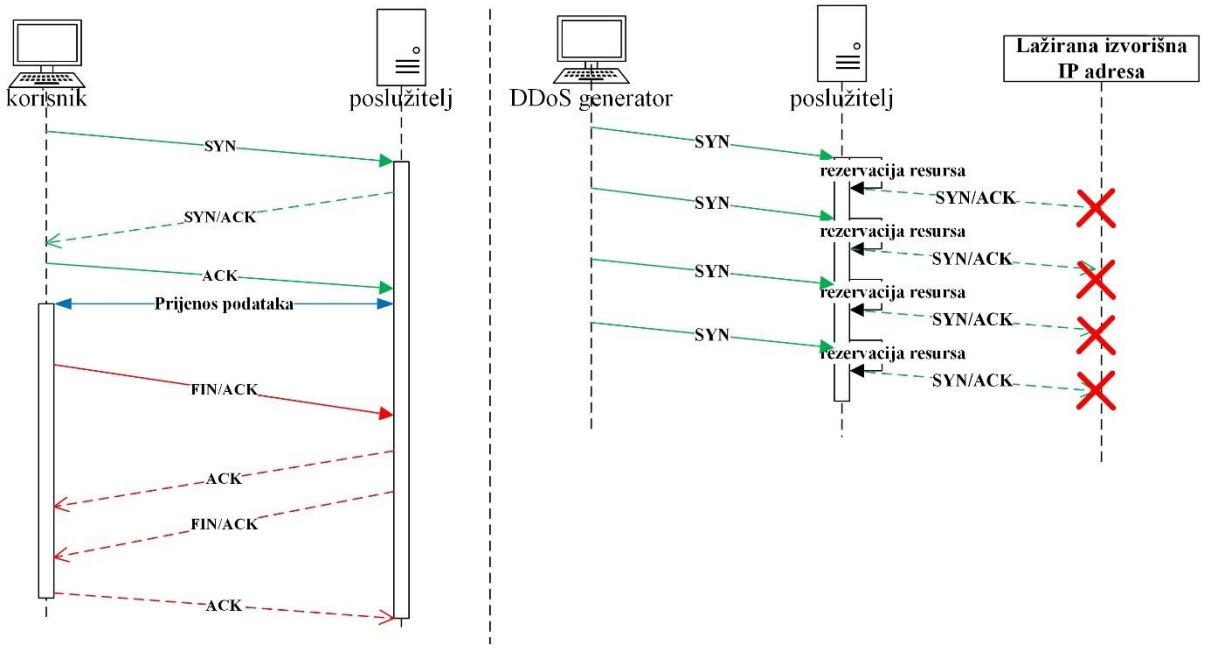
Jedan od temeljnih protokola TCP/IP protokolnog stoga jest spojno orijentirani TCP protokol koji pruža garanciju isporuke paketa od izvorišta do odredišta prethodnom uspostavom veze. Proces uspostave veze često je predmetom manipulacije u svrhu izvođenja DDoS napada poplavljivanjem resursa pri čemu se manipulira oznakama unutar protokola (SYN, ACK, RST, PSH, FIN, URG, CWR, ECE i NS) [176].

Slikom 4.8 prikazan je proces uspostave TCP veze (engl. *Three-way handshake*) i proces prekida TCP veze. Istom slikom (desno) prikazan je primjer iskorištavanja TCP protokola za provedbu DDoS napada. Postoji nekoliko vrsta DDoS napada čije izvođenje podrazumijeva manipulaciju prethodno spomenutim procesom [178]:

- napad poplavljivanjem posredstvom SYN oznake (engl. SYN *Flood*),
- napad poplavljivanjem posredstvom ACK oznake (engl. ACK *Flood*),

- napad poplavljivanjem posredstvom RST oznake (engl. RST *Flood*),
- itd.

Izvođenje DDoS napada poplavljivanjem posredstvom SYN oznake iskorištava ranjivost procesa uspostave TCP veze tako da se poslužitelju uputi veliki broj zahtjeva za uspostavom TCP veze koji sadrže SYN oznaku i nepostojeću (lažiranu) adresu izvorišta. Nakon što poslužitelj primi dolazni zahtjev, unutar odgovora umeće oznaku SYN/ACK i rezervira potrebne resurse. Zbog lažirane IP adrese izvorišta, odgovor poslužitelja ne vraća se stvarnom inicijatoru TCP veze i poslužitelj ne prima potvrdu uspostave veze (ACK) što rezultira zadržavanjem rezerviranih resursa. Veliki broj takvih zahtjeva uzrokuje iscrpljivanje svih dostupnih resursa poslužitelja nakon čega prelazi u stanje nedostupnosti [178], [179].



Slika 4.8 UML dijagram međudjelovanja procesa legitimne uspostave TCP sesije (lijevo) i manipulacije TCP protokola za provedbu DDoS napada (desno)

DDoS napad poplavljivanjem posredstvom ACK oznake temelji se na slanju velikog broja TCP poruka s oznakom ACK. Kada uređaj zaprimi takav paket, u osnovi mora provesti dvije radnje: prvo mora provjeriti postoji li inicirana TCP veza, a nakon toga (ukoliko inicijacija TCP veze postoji), slijedi provjera ispravnosti paketa da bi se mogao proslijediti aplikacijskom sloju. Ukoliko se utvrdi neispravnost paketa (npr. odredišni komunikacijski port je zatvoren), pošiljatelju se šalje RST paket koji označava prekid veze. Slanjem velikog broja mrežnog prometa koji sadrži ACK oznaku, zbog dviju radnji koje primatelj mora odraditi, mrežno sučelje primatelja prelazi u stanje nedostupnosti uslijed preopterećenja resursa [179].

Iskorištavanje oznake RST u TCP RST napadu temeljen je na „pogađanju“ slijednog broja TCP veze između dva entiteta u mreži i slanjem RST oznaka što uzrokuje prekid TCP veze. U ovom napadu često se koriste *botnet* mreže koje šalju veliki broj takvih paketa poslužitelju s različitim slijednim brojevima s ciljem pogađanja ispravnog. Kada se to dogodi, poslužitelj prihvaća RST paket i prekida vezu s klijentom [176].

4.2.2.3 Napadi manipulacijom UDP protokola

Uz TCP, jedan od osnovnih protokola TCP/IP protokolnog stoga je UDP protokol. Protokol UDP je nekonekcijski orijentiran što podrazumijeva pružanje transportne usluge bez uspostave veze kao što je slučaj kod TCP protokola te time i ne jamči isporuku niti omogućuje retransmisiju neisporučenih paketa. Struktura zaglavlja UDP-a jednostavnija je od TCP zaglavlja i sastoji se od četiri polja (izvorišni i odredišni komunikacijski port, kontrolna suma i duljina). Zbog jednostavnosti i nekonekcijske orijentiranosti, često se koristi u DDoS napadima poplavljivanja mrežnih resursa [12], [180].

DDoS napad posredstvom UDP protokola najčešće se provodi slanjem velike količine UDP paketa s lažiranih IP adresa na nasumične komunikacijske portove ciljanog uređaja. Uređaj koji prima UDP pakete nema dovoljan kapacitet za obradu dolazećeg prometnog volumena pri čemu pokušava odgovoriti velikim brojem ICMP paketa o nedostupnosti odredišta koji stvaraju dodatno zagušenje u mreži. Protokol je često korišten u reflektivnim napadima [176].

4.2.2.4 Napadi manipulacijom ICMP protokola

Za razliku od TCP i UDP protokola, ICMP (engl. *Internet Control Messeging Protocol*) je protokol mrežnog OSI sloja, ali je poput UDP protokola nekonekcijski orijentiran. Primjena ICMP protokola ogleda se u razmjeni dijagnostičkih poruka između uređaja u mreži i nije namijenjen prijenosu korisničkog sadržaja. Protokol se koristi u DDoS napadima poplavljivanja (engl. *Smurf*) slanjem velikog broja *echo* zahtjeva posredstvom *botnet* mreže ili amplifikacijskim uređajem na veliki broj IP adresa i uz lažiranu adresu odredišta [181].

4.3 DDoS promet generiran posredstvom SHIoT uređaja

Pojavom SHIoT uređaja sa svim poznatim nedostatcima javlja se novi moment u generiranju DDoS prometa, ali i u njegovoj detekciji. SHIoT uređaji jednostavno postaju dijelom različitih *botnet* mreža. Prema [59], SHIoT uređaji imaju značajan utjecaj na povećanje intenziteta DDoS prometa generiranog prema krajnjem odredištu. DDoS napadi generirani

SHIoT uređajima su kontinuirano rastući problem s aspekta razmjera, učestalosti i kompleksnosti i mogu predstavljati veliku prepreku daljnjem usvajanju koncepta pametnog doma, ali i ostalih oblika primjene koncepta IoT [155]. Promatrano s aspekta mogućnosti detekcije, SHIoT uređaji pripadaju skupini uređaja koji generiraju MTC promet. Takav promet posjeduje određenu razinu predvidivosti što omogućava razvoj metoda detekcije DDoS prometa kao anomalije na njegovom izvorištu [120].

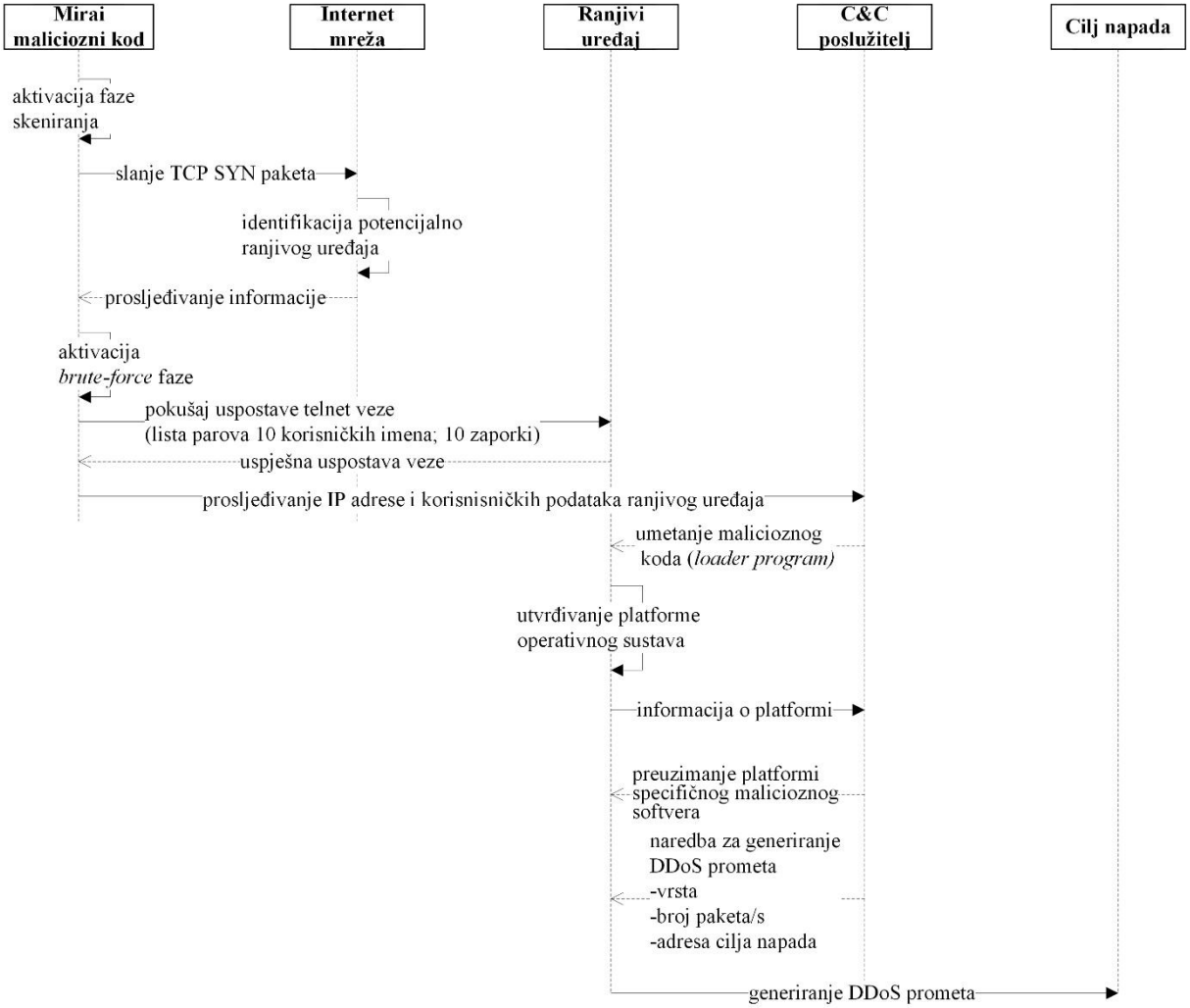
4.3.1 Mreže udaljeno kontroliranih SHIoT uređaja u funkciji generiranja DDoS prometa

Koncept *botnet*-a kao mreže udaljeno upravljanih ranjivih uređaja poznat je više od 20 godina, međutim njegova primjena u okruženju koncepta IoT je relativno nova. Stvaranje *botnet* mreže zahtijeva implementaciju malicioznog softvera u ciljani uređaj koji će omogućiti udaljeno upravljanje. Prema [55], zbog poznatih ograničenja SHIoT uređaja, brojni su maliciozni softveri usmjereni upravo na ovu vrstu uređaja s ciljem stvaranja *botnet* mreže posredstvom koje je moguće provesti DDoS napade koji generiraju DDoS promet velikog intenziteta (iznad 1Tb/s). Prema istraživanju tvrtke Bitdefender, u 2018. godini 78 % nelegitimne aktivnosti predvođene su IoT *botnet* mrežama [182]. Iako je mogućnost formiranja *botnet* mreže korištenjem SHIoT uređaja poznata od 2009. godine kada je izveden prvi takav DDoS napad, tek 2016. godine realiziran je prvi javno eksponiran DDoS napad *botneta* pod nazivom Mirai [183]. Mirai je maliciozni softver iz klase računalnih crva koji otkriva ranjive uređaje u mreži, iskorištava njihove ranjivosti u svrhu instalacije malicioznog koda i daljnje propagacije mrežom. Nekoliko istraživanja analiziralo je Mirai maliciozni softver i *botnet* mrežu u svrhu otkrivanja načina funkcioniranja i učinaka na uređaje i DDoS promet koji je generiran putem tog *botneta*. Istraživanje [173] prikazuje princip rada Mirai *botnet*-a, prikazano slikom 4.9.

Prema prikazanoj slici, Mirai maliciozni softver funkcionira u dvije faze: skeniranje i *brute-force*[12]. U provedbi prve faze skenira se pseudoslučajni opseg IPv4 adresa korištenjem TCP SYN[13] metode na komunikacijskim portovima koje koristi telnet mrežna usluga (TCP 23 i TCP 2323). Nakon što se otkrije aktivan SHIoT uređaj u mreži koji ima otvoreni komunikacijski port 23 ili 2323, započinje druga faza rada.

[12] Vrsta napada pri kojemu se iskušavaju dostupne kombinacije pristupnih podataka (korisničko ime i zaporka) s ciljem otkrivanja valjane kombinacije.

[13] Metoda koja koristi proces uspostave TCP sesije u svrhu otkrivanja aktivnih uređaja u mreži.



Slika 4.9 UML dijagram principa rada Mirai *botnet*-a [173]

U drugoj fazi koristi se *brute-force* pokušaj nelegitimnog pristupa ranjivom uređaju putem telnet usluge i liste od 62 potencijalna korisnička imena i zaporke. Nakon uspješnog pristupa uređaju, Mirai šalje IP adresu uređaja i povezane pristupne podatke kontrolnom poslužitelju. Kontrolni poslužitelj u ranjivi uređaj implementira programski kod (*loader program*) čija je uloga detekcija operativnog sustava uređaja na temelju kojega se implementira maliciozni softver specifičan za identificirani operativni sustav. Implementirani maliciozni kod omogućuje kontrolnom poslužitelju udaljeno upravljanje uređajem u vidu prosljeđivanja uputa za generiranje DDoS prometa (vrsta napada, intenzitet prometa, protokol, cilj napada) [173], [184].

Prema istraživanju [55], Mirai *botnet* sačinjavalo je približno 500 000 SHIoT uređaja iz 164 države čija je svrha bila generiranje DDoS prometa prema brojnim odredištima od kojih su najistaknutija: *web*-poslužitelj bloga *KerbsOnSecurity.com*, Dyn[14] DNS usluga i francuski

[14] Jedan od vodećih upravljanih pružatelja DNS usluga u svijetu

pružatelj usluge smještaja *web*-stranica (engl. *hosting provider*) OVH [147], [183]. Karakteristike DDoS napada korištenjem Mirai *botnet-a* prikazane su tablicom 4.2.

Tablica 4.2 Najznačajniji DDoS napadi provedeni posredstvom Mirai *botnet*-a

Cilj napada	**Broj SHIoT uređaja**	**Intenzitet DDoS prometa**	**Botnet**
KrebsOnSecurity.com	24000	623 Gb/s	Mirai
Dyn DNS	100000	1,2 Tb/s	Mirai
OVH	145607	1,1 – 1,5 Tb/s	Mirai/Bashlight

Uz Mirai *botnet,* kao najznačajnijeg predstavnika i pokazatelja važnosti i utjecaja na DDoS napade temeljene na SHIoT uređajima, istraživanja ukazuju i na brojne druge *botnet*-e koji za generiranje DDoS prometa koriste SHIoT uređaje [55], [60], [147], [183–186].

Tablicom 4.3 prikazani su postojeći maliciozni softveri čija je namjena stvaranje SHIoT *botnet*-a u svrhu generiranja DDoS prometa. Uz maliciozne softvere, navedene su i vrste DDoS prometa s aspekta korištenih protokola koje pojedine *botnet* mreža može generirati.

Tablica 4.3 Maliciozni softver korišten za kreiranje SHIoT *botnet* mreže u svrhu generiranja DDoS prometa

Maliciozni softver	**Vrsta generiranog DDoS prometa**
Linux.Hydra	SYN Flood, UDP Flood
Psyb0t	SYN Flood, UDP Flood, ICMP Flood
Tsunami, Kaiten	SYN Flood, UDP Flood, ACK Flood
Aidra, LightAidra, Zendran	SYN Flood, UDP Flood, ACK-PUSH Flood, HTTP Layer 7 Flood, TCP XMAS
Spike, Dofloo, MrBlack, Wrkatk, Sotdas, AES.DDoS	SYN Flood, ACK Flood
BASHLITE, Lizkebab,	SYN Flood, UDP Flood, ICMP Flood, DNS Query Flood, HTTP Layer 7 Flood
Elknot, BillGates	SYN Flood, UDP Flood, ACK Flood
XOR.DDoS	SYN Flood, UDP Flood, ICMP Flood, Flood, DNS Amplification, HTTP Layer 7 Flood, other TCP Floods
LUABOT	HTTP Layer 7 Flood
Remaiten, KTN-RM	SYN Flood, UDP Flood, ACK Flood, HTTP Layer 7 Flood
NewAidra, Linux.IRCTelne	SYN Flood, ACK Flood, ACK-PUSH Flood, TCP XMAS, TCP Floods
Mirai	SYN Flood, UDP Flood, ACK Flood, VSE Query Flood, DNS Water Torture, GRE IP Flood, GRE ETH Flood, HTTP Layer 7 Flood

Izvor: [147]

Iz svega navedenog moguće je zaključiti kako su, generički gledano, DDoS napadi pa time i DDoS promet kao produkt takvih napada, rastuća sigurnosna prijetnja dostupnosti IK resursa i usluga. Navedeno potvrđuju brojna istraživanja koja ukazuju na porast sofisticiranosti ove prijetnje gledano s aspekta raznovrsnosti protokola korištenih za generiranje DDoS

prometa, raznolikosti i kompleksnosti malicioznog softvera korištenog za stvaranje *botnet* mreža i konačno vrsta DDoS napada prikazanih taksonomijama (slika 4.3 i tablica 4.1).

Dodatni čimbenik rasta ovog problema nepobitno predstavlja pojava te rast i razvoj koncepta pametnog doma i SHIoT uređaja koji zbog svojih ograničenja i sigurnosnih nedostataka omogućavaju stvaranja *botnet* mreža sa znatno većim brojem udaljeno kontroliranih uređaja koji imaju potencijal generirati DDoS promet sve većeg intenziteta.

4.3.2 Detekcija DDoS prometa generiranog SHIoT uređajima

Općenito, kada se promatra DDoS promet, moguće ga je prevenirati, detektirati ili njime upravljati. Da bi se moglo upravljati DDoS prometom, potrebno ga je prvo detektirati uz visoku točnost te uz što manji udio lažno pozitivnih i lažno negativnih rezultata. To je razlog važnosti i čestog istraživanja problema detekcije DDoS prometa.

Detekciju DDoS prometa moguće je provoditi na izvorištu i odredištu. Prvotno podrazumijeva detekciju DDoS prometa na uređaju ili točki u mreži na koju je uređaj povezan, dok se posljednje odnosi na detekciju DDoS prometa na uređaju ili mreži koja predstavlja cilj DDoS napada [7]. Istraživanja koja su orijentirana na detekciju DDoS prometa često takav promet nastoje detektirati na njegovom izvorištu promatrajući pri tome individualne uređaje nastojeći utvrditi promjene u prometu koji pojedini IoT uređaj generira i na taj način detektirati anomaliju kao što je DDoS promet. Primjeri istraživanja DDoS prometa u IoT okruženju prikazani su tablicom 4.4. Pristup detekciji DDoS prometa na izvorištu vidljiv je u istraživanju [51] gdje se nastoji utvrditi generira li IoT uređaj DDoS promet korištenjem metode dubokih autoenkodera (engl. *deep autoencoders*). Jednako tako istraživanje [57] nastoji detektirati DDoS promet na temelju značajki mrežnih paketa koje individualni IoT uređaji generiraju.

Tablica 4.4 Primjeri istraživanja usmjerenih na detekciju DDoS prometa

Istraživanje	IoT okruženje	Točka detekcije	Korištene metode	Broj korištenih uređaja	Točnost modela
[51]	Okruženje pametnog doma	Detekcija DDoS prometa na izvorištu	Duboki autoenkoderi	9 SHIoT uređaja	≈100 %
[57]	Okruženje pametnog doma	Detekcija DDoS prometa na izvorištu	k-najbližih susjeda, strojevi potpornih vektora, Stabla odluke, Umjetne neuronske mreže	4 SHIoT uređaja (491 855 paketa)	91 % - 99 %
[58]	Općenito IoT okruženje	Detekcija DDoS prometa na izvorištu	Softverski definirane mreže	-	-

[187]	Općenito IoT okruženje	Detekcija DDoS prometa na izvorištu	Konvolucijske neuronske mreže, rekurzivna neuronska mreža	N/A; 266,160 prometnih tokova	>98 %

Navedeno istraživanje predstavlja i jedno od prvih istraživanja usmjerenih na detekciju DDoS prometa u okruženju pametnog doma. Temeljeno je na razlikama između MTC i HTC prometa i na pretpostavci da SHIoT uređaji koji generiraju MTC promet mogu poprimiti fiksan broj stanja te je time takav promet deterministčan i strukturiran. U svrhu detekcije DDoS prometa korišteno je nekoliko metoda strojnog učenja poput KNN, SVM, stabala odluke, nasumičnih šuma te metode umjetnih neuronskih mreža.

Iz navedenih istraživanja uočavaju se nedostatci kao što su brojnost i raznovrsnost SHIoT uređaja korištenih u istraživanju. Isto tako sva istraživanja temelje se na prethodnom poznavanju legitimnog prometa svakog pojedinog uređaja, što implicira ponovno učenje modela ili čak razvoj novoga s pojavom novog SHIoT uređaja na tržištu.

5 Razvoj modela detekcije anomalija mrežnoga prometa temeljen na značajkama prometa i klasnoj pripadnosti uređaja

Ovim poglavljem prikazan je razvoj modela detekcije anomalija mrežnoga prometa temeljen na značajkama prometa i klasnoj pripadnosti uređaja kroz više faza. Analizirane su i sustavno prikazane značajke prometa korištene u dosadašnjim istraživanjima u svrhu identifikacije IoT uređaja. Pojašnjena je metodologija formiranja laboratorijskog okruženja i prikupljanja podataka. Definirane su klase SHIoT uređaja te je razvijen višeklasni klasifikacijski model temeljen na *boosting* metodi strojnog učenja kao preduvjet za razvoj modela detekcije anomalija mrežnoga prometa. Konačno, prikazan je i pojašnjen razvoj modela detekcije anomalija mrežnoga prometa temeljen na značajkama prometa i klasnoj pripadnosti SHIoT uređaja pri čijem razvoju je korištena metoda logističkih stabala odluke iz skupa metoda strojnog učenja. Za oba razvijena modela (višeklasni klasifikacijski model i model detekcije anomalija) provedena je *k*-struka unakrsna validacija te su izračunate mjere za ocjenu performansi modela. Ovim poglavljem prikazana je i diskusija o rezultatima provedenog istraživanja. Pojašnjen je značaj detekcije DDoS prometa na temelju klasa SHIoT uređaja kao i praktična primjenjivost razvijenog modela. Uz to, navedena su ograničenja provedenog istraživanja te uočeni potencijal za buduća istraživanja u okviru identificiranog problemskog područja.

5.1 Identifikacija značajki prometa generiranog IoT uređajima u okruženju pametnog doma

SHIoT promet moguće je promatrati kroz mrežnu aktivnost i to kroz značajke kao što su volumen prometnog toka (zbroj ukupnog preuzetog prometa i ukupnog prenesenog prometa), trajanje prometnog toka (vrijeme između prvog i posljednjeg paketa u prometnom toku) i vrijeme neaktivnosti uređaja (vremenski period u kojemu uređaj nema aktivni prometni tok). Modeliranje mrežnog ponašanja (engl. *network behavioral modeling*) često je korišten pristup za rješavanje izazova u komunikacijskoj mreži poput detekcije nelegitimnih događaja na temelju prometa koji generiraju uređaji u mreži. Općenito, aktualni pristupi nastoje identificirati karakteristike prometa na razini mrežnih paketa i razini prometnog toka [188]. Identificirane značajke prometa na razini prometnog toka ili mrežnoga paketa prikazane su tablicom 5.1.

Brojni istraživači nastoje identificirati karakteristike prometa generiranog kao produkt komunikacije SHIoT uređaja. Karakteristike prometa koji generiraju pojedini SHIoT uređaji mogu biti ključan čimbenik u istraživanju uzročno-posljedičnih veza generiranog prometa na određene procese u komunikacijskoj mreži. Često se takve karakteristike koriste u svrhu identifikacije SHIoT uređaja u mreži [52], [53] i [189], identifikaciju vrste korištenih usluga [187], detekcije neautoriziranih uređaja u mreži [190] i detekcije anomalija u prometu [51]. Karakteristike prometa koje istraživači promatraju ovise o cilju istraživanja. Intenzitet prometa korišten je u [52] i [53] u svrhu razlikovanja MTC i HTC prometa i identifikacije IoT uređaja. Interpretacija rezultata istraživanja ukazuje na činjenicu da je intenzitet prometa koji generiraju IoT uređaji znatno manji (prosječno 66 Kb/s, vršno 1 Mb/s) nego kod konvencionalnih uređaja (prosječno 400 Kb/s, vršno 17 Mb/s za istraživanje) [52]. Razlike između MTC i HTC prometa vidljive su i iz duljine trajanja sesije (95 % svih promatranih sesija IoT uređaja traje kraće od 5 sekundi). Trajanje sesije utječe i na količinu prometa koji se prenese po sesiji (u 75 % promatranih sesija količina prometa je manja od 1KB, a u 1 % sesija količina prometa je veća od 10 KB).

Tablica 5.1 Značajke prometa generiranog SHIoT uređajima

Oznaka	Značajka prometa	Objašnjenje značajke	Razina	Istraživanje
int_traff	Intenzitet prometa	Količina prometa prenesena u jedinici vremena	Prometni tok	[52]
s_dur	Trajanje sesije	Vremenski period u kojemu uređaj generira promet	Prometni tok	[52]

sleep_time	Vrijeme neaktivnosti uređaja	Vremenski period u kojemu za promatrani uređaj ne postoje aktivni tokovi	Prometni tok	[52], [53]
flow_dur	Trajanje toka	Vremenski period između prvog i zadnjeg paketa prometnog toka	Prometni tok	[53]
flow_vol	Volumen prometa	Ukupna količina dolaznog i odlaznog prometa po prometnom toku	Prometni tok	[53]
avg_flow_rate	Prosječna brzina prijenosa podataka prometnog toka	Odnos prometnog volumena toka i trajanja toka	Prometni tok	[53]
pack_size	Veličina paketa	Veličina paketa u prometnom toku, može biti promatrana kroz statističke mjere poput srednje vrijednosti, standardne devijacije te minimalne ili maksimalne vrijednosti	Prometni tok	[51], [52], [189], [191]
port_no	Korišteni protokoli	Korišteni komunikacijski protokoli	Prometni tok	[53]
no_pack	Broj paketa	Broj paketa prenesen za vrijeme trajanja prometnog toka	Prometni tok	[51]
iat	Međudolazna vremena paketa	Vrijeme između dolaska dva uzastopna paketa u prometnom toku	Prometni tok	[51], [191]
proto	Prisutnost protokola	Provjera korištenjem pojedinih protokola u promatranom paketu	Mrežni paket	[57], [192]
ttl	Broj čvorova koje paket prolazi	Vrijednost u IP paketu koji govori mrežnim čvorovima trebaju li proslijediti paket idućem čvoru ili ga odbaciti.	Mrežni paket	[190]
p_size	Veličina paketa	Veličina pojedinačno promatranog paketa	Mrežni paket	[57]
ip_addr	IP addresa paketa	Izvorišna i odredišna IP adresa zapisana u zaglavlju paketa	Mrežni paket	[57]

Uz diferencijaciju uređaja koji generiraju MTC i HTC promet prema prethodnim karakteristikama prometa vidljiva je i razlika između pojedinih uređaja ili skupina uređaja koji generiraju MTC promet. Prema istraživanju [53] pojedini IoT uređaji razlikuju se prema količini prometa prenesenog po prometnom toku. Tako je, primjerice za LiFX pametnu rasvjetu količina prenesenih podataka u većini prometnih tokova između 130 i 140 *byte*-a, dok je za Belkin senzor pokreta u većini prometnih tokova količina prenesenih podataka između 2800 i 3800 *byte*-a. Istim istraživanjem utvrđene su i dodatne značajke prema kojima je moguće razlikovati pojedine IoT uređaje poput brzine prijenosa podataka. Pa tako LiFX pametna rasvjeta, u 60 % prometnih tokova, prenosi podatke prosječnom brzinom od 18 bit/s dok Belkin senzor pokreta u 40 % prometnih tokova podatke prenesi brzinom od 59-60 bit/s. Mala količina podataka prenesena za vrijeme trajanja prometnog toka vidljiva je u istom istraživanju pri čemu je analiza ove karakteristike provedena na razini individualnih uređaja. Isto istraživanje analizira i trajanje prometnog toka gdje je utvrđeno da LiFX pametna rasvjeta generira većinu

prometnih tokova (50 %) u trajanju od 60 sekundi dok Belkin senzor pokreta generira 21 % prometnih tokova u istom trajanju.

Istraživanje [189] nastoji klasificirati IoT uređaje prema semantičkim obilježjima (IoT čvorovi, elektronički uređaji, kamere i prekidači) koristeći značajke prometnog toka poput statistike duljine paketa, broja paketa, i korištenih komunikacijskih protokola. Istraživanjem je pretpostavljeno da svi uređaji pojedine skupine imaju jednake ili približno jednake karakteristike što nužno ne mora biti istinito. Dokaz tome je i točnost detekcije razvijenog modela od 74,8 %. Veličinu paketa i međudolazno vrijeme paketa u prometnom toku razmatraju i autori istraživanja [191] u kojemu se nastoje identificirati IoT uređaji u okruženju pametnog doma.

Pojedina istraživanja, za potrebe identifikacije IoT uređaja, detekciju anomalija ili rješavanje drugih klasifikacijski orijentiranih problema, fokusiraju se na razmatranje značajki prometa takvih uređaja na razini mrežnih paketa. Istraživanjem prikazanim u [190] nastoje se detektirati neautorizirani IoT uređaji u komunikacijskoj mreži. Pri tome su identificirane tri značajke na razini paketa kao relevantne u klasifikaciji uređaja. Sve tri značajke odnose se na TTL (engl. *Time to Live*) pojedinog paketa (minimalna vrijednost, prosječna vrijednost i vrijednost prvog kvartila).

Istraživanja [191] i [192] u svrhu identifikacije individualnih IoT uređaja koriste značajke mrežnih paketa koje takvi uređaji generiraju na različitim TCP/IP slojevima. Vrijednosti značajke su binarni, odnosno označavaju prisutnost promatrane značajke poput IP adresa, izvorišnih i odredišnih komunikacijskih portova, korištenje određenih protokola (ARP, LLC, IP, ICMP, HTTP, SSDP). Isto tako, promatrane su značajke poput veličine paketa, klase komunikacijskih portova i brojača odredišne IP adrese. Značajke mrežnih paketa korištene su i u istraživanju [57] gdje su u svrhu detekcije DDoS prometa promatrane značajke poput veličine paketa, protokola te izvorišne i odredišne IP adrese.

Iz analiziranih istraživanja uočava se učestalije razmatranje i korištenje značajki prometa na razini prometnog toka, nego na razini mrežnih paketa. Isto tako, navedena istraživanja koriste prikazane značajke za identifikaciju individualnih uređaja ili njihovu klasifikaciju koja se temelji na semantičkim obilježjima promatranih uređaja.

5.2 Formiranje okruženja pametnog doma i prikupljanje podataka

Prema [193], jedan od osnovnih problema u području istraživanja detekcije anomalija mrežnoga prometa s fokusom na DDoS promet predstavlja nedostatak podatkovnih skupova

koji sadrže realan promet[15] generiran u komunikacijskoj mreži. Nekoliko je razloga ovom problemu [194]. Kao prvi razlog nameće se problem anonimnosti podataka unatoč postojanju primjenjivih metoda anonimizacije. Idući razlog predstavlja cjelovitost i točnost označavanja prometa u podatkovnom skupu što podrazumijeva oznake legitimnog prometa i anomalije što je nužno pri razvoju modela detekcije anomalija posebice kod primjene metoda nadziranog strojnog učenja. Konačno, stvaranje realnog podatkovnog skupa predstavlja izazov zbog potrebnih resursa koje je potrebno osigurati u tu svrhu (okruženje, oprema, vrijeme, financijska sredstva) zbog čega istraživači često koriste već dostupne podatkovne skupove unatoč njihovim nedostatcima.

Postojeći podatkovni skupovi razlikuju se prema načinu njihovog generiranja. Prema [20], razlikuju se sintetički, simulirani i realni podatkovni skupovi. Sintetički podatkovni skupovi generirani su s ciljem zadovoljavanja specifičnih zahtjeva i uvjeta koje zadovoljavaju i realni podatkovni skupovi. Ovakvi skupovi korisni su za teorijsku analizu i pronalaženje osnovnog rješenja te kreiranja različitih vrsta scenarija. Simulirani podatkovni skupovi generirani su korištenjem simuliranog IK okruženja. Primjeri takvih skupova su KDDcup99 koji je najčešće korišten za validaciju metoda i modela detekcije anomalija, zatim NSL-KDD koji nastoji ispraviti nedostatke prethodnog skupa. Također, često korišteni su još i DEFCON, CAIDA te LBLN. Realni podatkovni skupovi generirani su u stvarnom okruženju, a trenutno dostupni istraživačkoj zajednici su UNIBS koji se sastoji od prometa generiranog u tri uzastopna dana korištenjem 20 konvencionalnih terminalnih uređaja, zatim ISCX-UNB skup koji se primarno sastoji od prometa temeljenog na HTTP, SMTP, SSH, IMAP, POP3 i FTP protokolima te TUIDS skup koji sadrži promet označen kao legitiman ili anomalija.

Svi navedeni podatkovni skupovi često su korišteni u brojnim istraživanjima problema detekcije anomalija u prometu (pa tako i DDoS prometa). Isto tako, navedeni skupovi stvoreni su između 1998. i 2012. godine pa je moguće zaključiti da se promet u tim skupovima razlikuje od prometa koji se generira u današnjim komunikacijskim mrežama s obzirom na dinamičnost razvoja IK područja s aspekta broja, raznovrsnosti, namjene i funkcionalnosti uređaja i prometa koji generiraju. Tako niti jedan od skupova ne sadrži promet generiran posredstvom SHIoT uređajima. S obzirom na ograničen broj istraživanja problema DDoS prometa generiranog SHIoT uređajima, problem dostupnosti podatkovnih skupova još je izraženiji. Tako je trenutno istraživačkoj zajednici dostupan podatkovni skup istraživača sa Sveučilišta New South Wales (Sydney, Australia) primarno prikupljenog u svrhu identifikacije SHIoT uređaja [53].

[15] Promet koji generiraju stvarni uređaji u promatranom okruženju

Istraživači u [51], za potrebe vlastitog istraživanja, kreirali su podatkovni skup koji sadrži promet generiran korištenjem devet IoT uređaja u korporativnom okruženju, ali podatkovni skup nije javno dostupan u izvornom obliku, već kao *.csv* datoteka koja sadrži već ekstrahirane značajke prometa. Ovakav skup je ograničavajući za druge istraživače jer ne posjeduje generirani promet u izvornom obliku pohranjen u formatu koji bi istraživačima omogućio ekstrakciju i izračun značajki koje se razlikuju od onih koje su ekstrahirane za potrebe navedenog istraživanja. Iz prikazanog, jasno se uočava problem nedostatka podatkovnih skupova dostupnih istraživačima koji bi se koristili u razvoju novih metoda i modela detekcije DDoS prometa općenito, a do još većeg izražaja ovaj problem dolazi u okruženju pametnog doma čiji uređaji su sve češće generatori DDoS prometa.

Istraživanjem u okviru ovog doktorskog rada formirano je laboratorijsko okruženje pametnog doma. Takvo okruženje čine raznovrsni SHIoT uređaji zajedno s popratnom komunikacijskom infrastrukturom i softversko-hardverskom platformom koja omogućava prikupljanje prometa i stvaranje podatkovnog skupa primjenjivog u kasnijim fazama istraživanja i razvoja modela detekcije anomalija mrežnoga prometa. Osim primarnih podataka prikupljenih prethodno opisanim procesom, istraživanjem su obuhvaćeni i sekundarni podatci prikupljeni istraživanjem [53] čime je obuhvaćen veći broj raznovrsnih SHIoT uređaja. Razlog tome je heterogenost uređaja koji mogu egzistirati u promatranom okruženju.

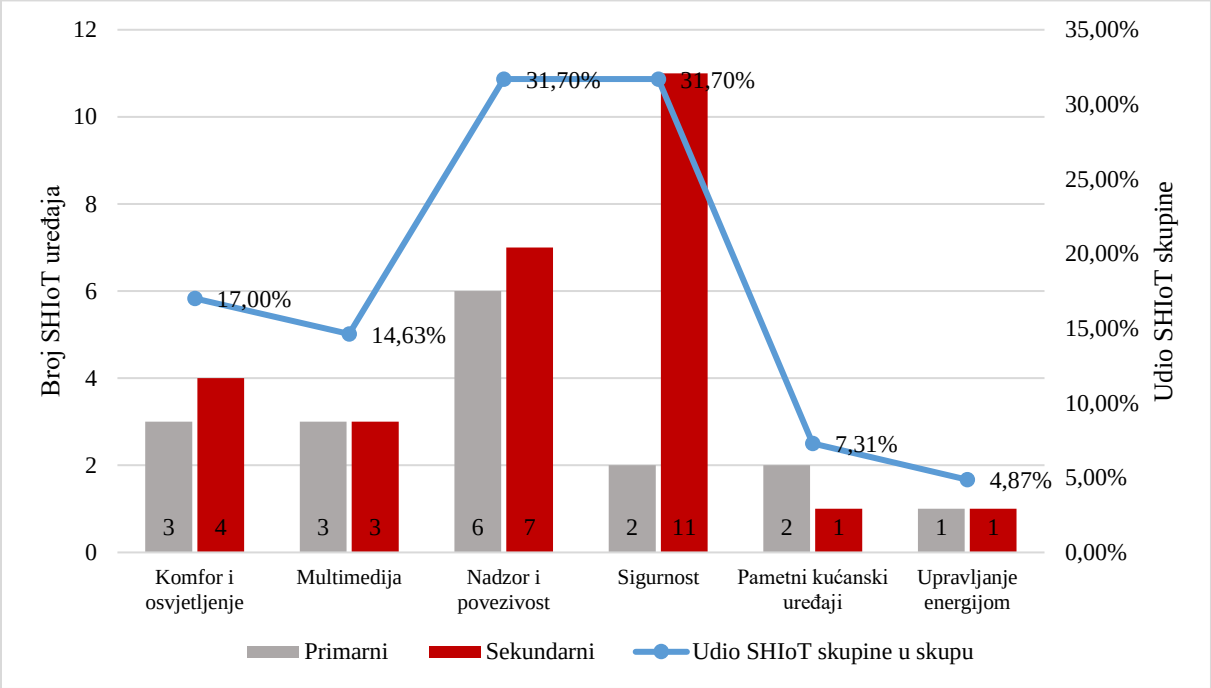
5.2.1 SHIoT uređaji korišteni u svrhu prikupljanja podataka

U svrhu prikupljanja primarnih podataka formirano je laboratorijsko okruženje pametnog doma koje sadrži SHIoT uređaje komercijalno dostupne na tržištu s obzirom da, prema statističkim pokazateljima, takvi uređaji imaju kontinuirani rast primjene.

Grafikonom 5.1 prikazana je distribucija SHIoT uređaja, odnosno zastupljenost pojedine skupine u ukupnom broju uređaja te broj uređaja koji će biti korišteni za prikupljanje primarnih i sekundarnih podataka. Cjelovita lista SHIoT uređaja obuhvaćena ovim istraživanjem prikazana je tablicom 5.2.

Laboratorijsko okruženje pametnog doma formirano je u sklopu Laboratorija za sigurnost i forenzičku analizu informacijsko-komunikacijskog sustava Zavoda za informacijsko-komunikacijski promet Fakulteta prometnih znanosti. Uz SHIoT uređaje namijenjene prikupljanju primarnih podataka, za potrebe predmetnog istraživanja korišteni su i sekundarni podatci već prikupljeni posredstvom raznovrsnih SHIoT uređaja u okviru postojećih istraživanja [53], [195], [196].

Grafikon 5.1 Distribucija skupina SHIoT uređaja



U tablici 5.2 naznačene su MAC (engl. *Media Access Control*) adrese kao jedinstvene oznake identifikacije SHIoT uređaja u mreži, naziv uređaja, oznaka P/S koja ukazuje je li promatrani uređaj korišten u svrhu prikupljanja primarnih ili sekundarnih podataka te kojoj skupini promatrani SHIoT uređaj pripada prema segmentaciji prikazanoj u poglavlju 3.

Tablica 5.2 SHIoT uređaji za potrebe prikupljanja podataka

r.br.	Uređaj	Oznaka	MAC adresa	Naziv uređaja	Namjena uređaja	Izvor prikupljanja podataka	Funkcionalna skupina SHIoT uređaja
1.	ph_hue_2	u10	00:17:88:78:0a:cb	Phillips Hue Starter kit 2xE26	Pametno upravljanje rasvjetnim tijelima	P	KO
2.	ph_hue_4	u33	00:17:88:2b:9a:25	Phillip Hue Starter kit 4xE26		S	KO
3.	wiz_F3	u2	a8:bb:50:05:31:f3	WiZ Colors ESP_0531F3		P	KO
4.	wiz_B0	u4	a8:bb:50:05:06:b0	WiZ Colors ESP_0506B0		P	KO
5.	lifx	u20	d0:73:d5:01:83:08	Light Bulbs LiFX Smart Bulb		S	KO
6.	wit_aura	u14	00:24:e4:20:28:c6	Withings Aura Sleep Tracking Mat	Nadzor i analiza ciklusa spavanja, nadzor otkucaja srca, detekcija turbulencija u dišnim putevima	S	KO
7.	google_chr	u36	7c:2e:bd:3d:4f:cb	Google Chromecast	Strujanje video sadržaja	P	M
8.	triby	u39	18:b7:9e:02:20:44	Invoxia Triby Speaker	Zvučnik s ugrađenom podrškom za Amazon Alexa uslugu, glasovna interakcija s korisnikom, strujanje i reprodukcija internetskog audiosadržaja	S	M
9.	pix	u34	e0:76:d0:33:bb:85	PIX-STAR Photo-frame	Reprodukcija slikovnog sadržaja s *online* usluga (google fotografije, Instagram, FlickR), prikaz vremenske prognoze	S	M
10.	amz_dot	u17	fc:65:de:31:69:d6	Amazon Alexa Dot	Zvučnik s mogućnošću glasovne interakcije s korisnikom, strujanje i reprodukcija internetskog audiosadržaja, povezivanje i glasovno upravljanje SHIoT uređajima	P	M
11.	amz_echo	u30	44:65:0d:56:cc:d3	Amazon Alexa Echo		S	M
12.	google_mini	u41	20:df:b9:21:fd:79	Google Home mini		P	M
13.	hs110	u12	ac:84:c6:5d:97:bc	TPlink Smart Plug HS110	Upravljanje i nadzor potrošnje električne energije i elektroničkih uređaja priključenih na strujnu utičnicu	P	NP
14.	hs105	u3	50:c7:bf:00:56:39	TPlink Smart Plug HS105		S	NP
15.	my_strom	u24	30:ae:a4:57:2d:54	MyStrom switch		P	NP
16.	w245	u15	74:da:da:5f:a8:19	D-link DSP-W245 plug		P	NP
17.	w115	u6	18:0f:76:cc:c0:e9	D-link DSP-W115 plug		P	NP
18.	ihome	u7	74:c6:3b:29:d7:1d	iHome Power Plug		S	NP
19.	belk_sw	u13	ec:1a:59:79:f4:89	Belkin Wemo switch		S	NP

20.	sams_st	u5	d0:52:a8:00:67:5e	Samsung Smart Things	Povezivanje i upravljanje pametnim SHIoT uređajima	S	NP
21.	bc_blood	u26	74:6a:89:00:2e:25	Blipcare Blood Pressure meter	Nadzor krvnog tlaka	S	NP
22.	aw_aq	u40	70:88:6b:10:0f:c6	Awair air quality monitor	Nadzor kvalitete zraka (temperatura, vlaga, CO2)	S	NP
23.	i896	u23	40:9f:38:e9:28:08	iRoobot Roomba 896	Robotski usisavač	P	PKU
24.	i895	u22	80:c5:f2:bb:17:95	iRoobot Roomba 895		P	PKU
25.	wit_body	u35	00:24:e4:1b:6f:96	Withings Body	Mjerenje mase i indeksa težine	S	PKU
26.	smartw_cam	u21	e8:ab:fa:9b:f0:9e	Smartwares C923IP Camera	Snimanje audio/videosadržaja, prijenos i pohrana sadržaja u CC okruženje	P	S
27.	blink_cam	u18	00:03:7f:27:2c:c3	Blink XT2 Camera		P	S
28.	cana_cam	u11	7c:70:bc:5d:5e:dc	Canary View Camera		S	S
29.	net_cam	u32	70:ee:50:18:34:43	Netatmo Welcome Camera		S	S
30.	tp_cam	u1	f4:f2:6d:93:51:f1	TPlink Day Night Cloud NC220 camera		S	S
31.	sams_cam	u19	00:16:6c:ab:6b:88	Samsung SmartCam		S	S
32.	nest_cam	u38	30:8c:fb:2f:e4:b2	Nest Dropcam		S	S
33.	belk_cam	u25	00:03:7f:27:2c:c3	Belkin NetCam Camera		S	S
34.	inst_cam	u28	00:62:6e:51:27:2e	Insteon HD WiFi Camera		S	S
35.	wit_baby	u8	00:24:e4:11:18:a8	Withings Smart Baby Monitor	Snimanje audio i video sadržaja, nadzor temperature, vlage, zvuka i pokreta u prostoru	S	S
36.	belk_mot	u31	ec:1a:59:83:28:11	Belkin Wemo Motion Sensor	Detekcija pokreta u prostoru	S	S
37.	nest_smoke	u9	18:b4:30:25:be:e4	NEST Protect Smoke Alarm	Detekcija razine CO2 u prostoru	S	S
38.	aug_door	u29	e0:76:d0:3f:00:ae	August Doorbell Cam	Pametno zvono, videonadzor ulaza, audiokomunikacija	S	S
39.	ring_vd	u37	88:4a:ea:31:66:9d	Ring Video Doorbell		S	KO
40.	net_therm	u16	70:ee:50:0c:14:c2	Netatmo smart thermostat	Nadzor i upravljanje temperaturom u prostoru	P	UE
41.	net_weath	u27	70:ee:50:03:b8:ac	Netatmo Smart Weather Station	Nadzor temperature zraka, vlažnosti, kvalitete zraka, razine CO2 i zvuka	S	UE

*P – Primarni; KO – Komfor i osvjetljenje; M – Multimedija; NP – Nadzor i povezivost; S – Sigurnost; PKU – Pametni kućanski uređaji;
S – Sekundarni; UE – Upravljanje energijom;

Za potrebe istraživanja u sklopu ovog doktorskog rada korišten je ukupno 41 uređaj u okruženju pametnog doma. Prema statističkim podatcima prikazanima u 2.4, uočavaju se razlike u procjeni prosječnog broja SHIoT uređaja po kućanstvu koje ima implementiran određeni oblik pametnog doma. Te procjene kreću se od 6,53 do 14 SHoT uređaja po kućanstvu. U Republici Hrvatskoj zastupljenost pametnih domova još uvijek je niska, a telekom operatori preuzimaju ulogu pružatelja usluge pametnog doma kroz ponudu paketa SHIoT uređaja za krajnje korisnike. Primjerice, pružatelj internetskih usluga Iskon Internet u svojoj ponudi pruža korisnicima mogućnost kupnje *smarthome* paketa koji čini četiri SHIoT uređaja [197] dok telekom operator A1 pruža korisnicima mogućnost implementacije ukupno pet SHIoT uređaja u okruženju pametnog doma [198].

Unatoč navedenome, ovim istraživanjem nastojala se postići što veća raznolikost SHIoT uređaja zbog potrebe definiranja klasa uređaja na temelju karakteristika generiranog prometa. Zbog toga je i broj korištenih uređaja veći nego što je trenutna statistička procjena srednje vrijednosti SHIoT uređaja po pametnom domu u Republici Hrvatskoj i svijetu. Predikcije prikazane u 2.4 odnose se na vremenski period do 2023., no s obzirom na uzlazni trend rasta broja uređaja za pretpostaviti je da će broj uređaja u dogledno vrijeme doseći 40 po pametnom domu.

5.2.2 Način prikupljanja podataka

Prikupljanje podataka obuhvaća procese prikupljanja legitimnog mrežnog prometa generiranog SHIoT uređajima kao i DDoS prometa koji takvi uređaji mogu generirati. Stoga će u nastavku biti detaljnije pojašnjen proces prikupljanja podataka.

5.2.2.1 Prikupljanje legitimnog prometa generiranog SHIoT uređajima

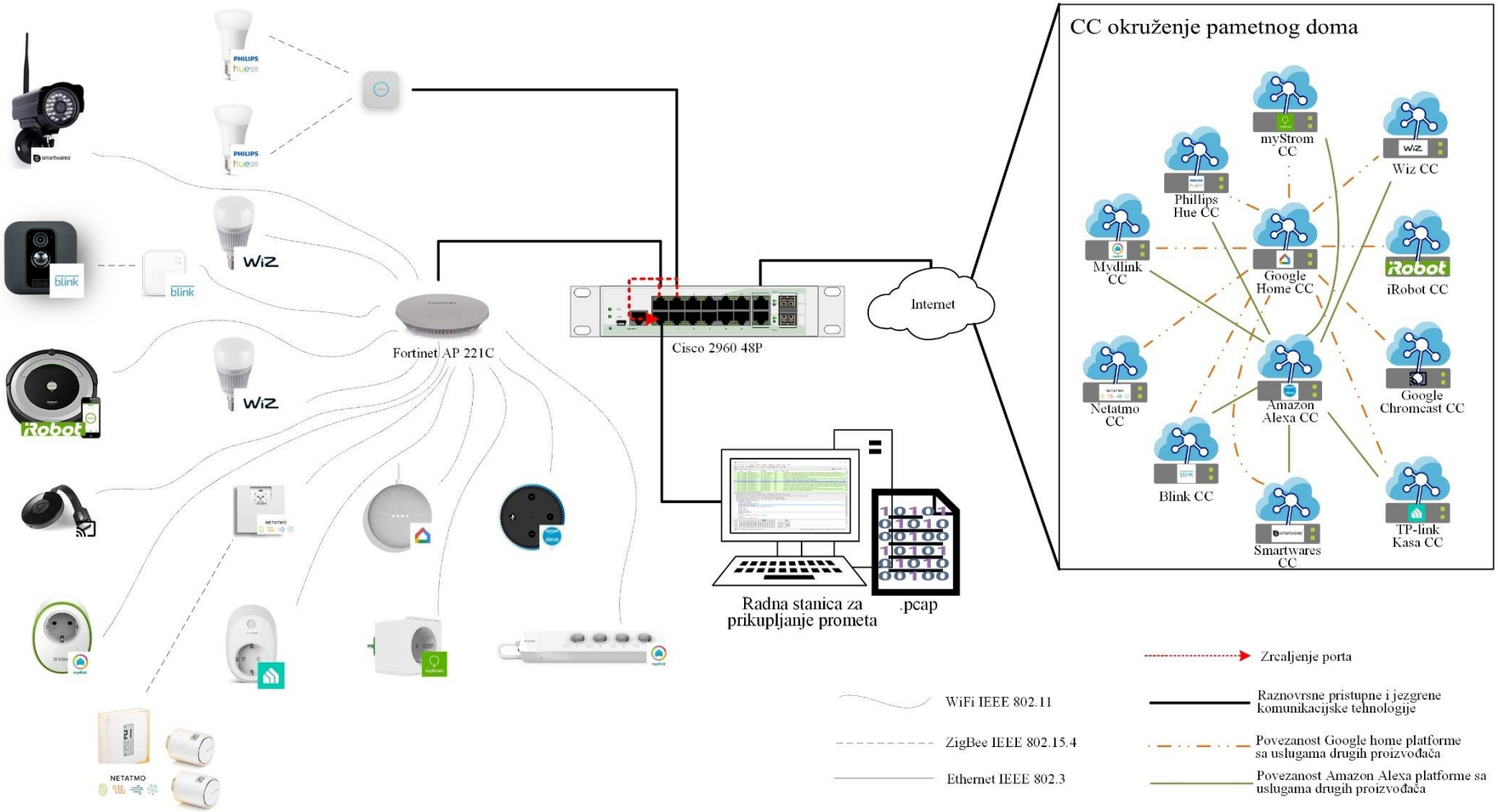
Svrha uspostave laboratorijskog okruženja pametnog doma jest povezivanje SHIoT uređaja različitih namjena s ciljem generiranja legitimnog prometa pojedinog uređaja. SHIoT uređaji dobavljeni su od ovlaštenih distributera i zastupnika pojedinog proizvođača uređaja te su priključeni i povezani u komunikacijsku mrežu onako kako preporučuje proizvođač pri čemu ni na koji način uređaji nisu modificirani na softverskoj i hardverskoj razini. Prema tome, pretpostavlja se da uređaji korišteni za prikupljanje legitimnog prometa u okviru ovog istraživanja rade onako kako su dizajnirani te da ni na koji način nisu prethodno sigurnosno kompromitirani.

Topologija mreže kao i karakteristike okruženja pametnog doma vidljive su na slici 5.1. Uređaji su povezani, posredno ili neposredno, Wi-Fi komunikacijskom tehnologijom s

bežičnom pristupnom točkom Fortinet AP 221C, uz izuzetak uređaja Phillips Hue koji s ostatkom lokalne mreže komunicira putem Ethernet (IEEE 802.3) komunikacijskog standarda. Pojedini uređaji, poput Blink pametne kamere, Netatmo pametnog termostata i Philips Hue pametnih rasvjetnih tijela, koriste IoT koncentrator s kojim ostvaruju bežičnu komunikaciju, ali ZigBee tehnologijom. Razlog je energetska učinkovitost uređaja s obzirom da koriste bateriju kao izvor napajanja krajnjeg uređaja što im pruža prednosti s aspekta mobilnosti i neovisnosti uređaja o električnoj energiji kao izvoru napajanja. IoT koncentrator povezan je Wi-Fi (ili Ethernet u slučaju Phillips Hue uređaja) tehnologijom s bežičnom pristupnom točkom. Na temelju navedenog, kao adekvatna točka prikupljanja prometa koji SHIoT uređaji generiraju, određena je bežična pristupna točka.

Zbog poznatih načina rada i karakteristika računalnih, pa time i bežičnih Wi-Fi mreža, promet u komunikacijskoj mreži nije moguće prikupljati neposredno. Nekoliko je metoda dostupno za prikupljanje prometa pri čemu je često korišteno zrcaljenje fizičkog porta na preklopniku. Spomenuta metoda pokazala se učinkovitom u više istraživanja kao što su [51], [117], [190], [199], što pruža uporište za primjenu iste metode pri provedbi ovog istraživanja.

Za potrebe prikupljanja prometa metodom zrcaljenja porta postavljena je softversko-hardverska platforma koja se sastoji od bežične pristupne točke Fortinet AP 221C, preklopnika Cisco 2960 Catalyst 48 PoE (engl. *Power over Ethernet*) te radne stanice HP Pavillion dm1 (Microsoft Windows 10 10.0.17134 build 17134, x64 procesorska arhitektura, AMD E-350, 1600MHz 2 jezgre, 4 GB RAM) s instaliranim programskim alatom Wireshark inačice 2.6.3.



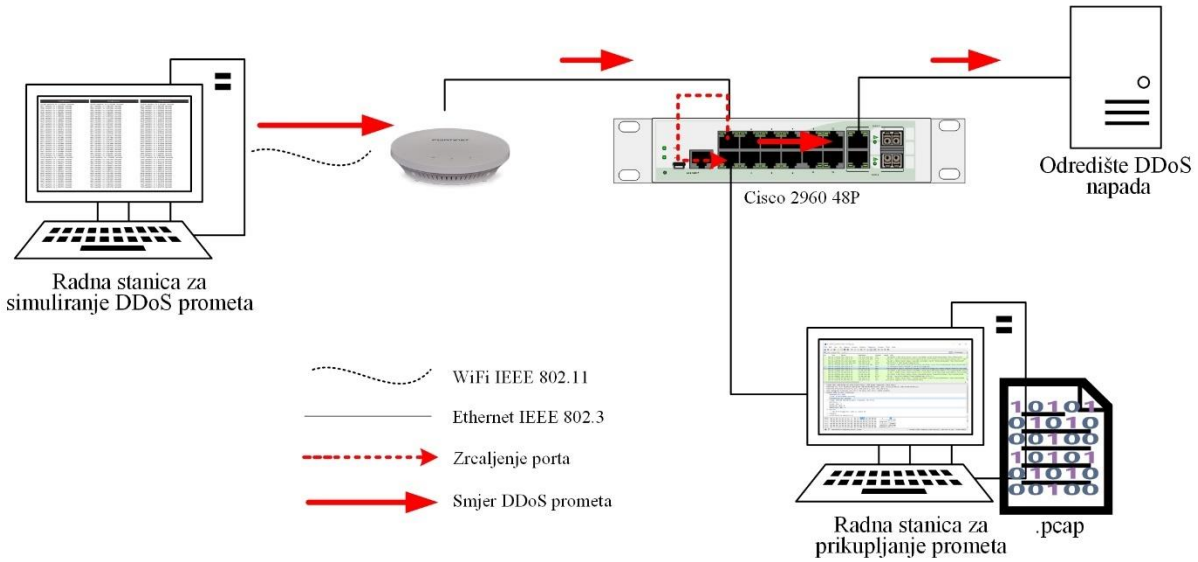
Slika 5.1 Laboratorijsko okruženje pametnog doma formirano u svrhu prikupljanja podataka

Kako je prikazano slikom 5.1, zrcaljenje porta konfigurirano je za fizičke komunikacijske portove (FA0/1 i FA0/3) preklopnika na koji je povezana bežična pristupna točka i IoT koncentrator za Phillips Hue uređaj. Navedeni portovi konfigurirani su kao izvorišni što označava da će cjelokupni promet koji dolazi prema tim portovima ili s njih odlazi, biti zrcaljen (preslikan) na odredišni komunikacijski port (FA0/2). Na taj port povezana je radna stanica za prikupljanje prometa.

5.2.2.2 Generiranje i prikupljanje DDoS prometa

Uz legitiman profil prometa SHIoT uređaja ključno je posjedovati skup podataka koji će predstavljati DDoS promet. Takva dva skupa predstavljaju temelj razvoja učinkovitog modela detekcije anomalija mrežnoga prometa koji SHIoT uređaji generiraju. S obzirom da skup legitimnog prometa proizlazi iz primarnog i sekundarnog izvora pri čemu autor nema pristup uređajima sekundarnog izvora, veliki izazov predstavlja manipulacija SHIoT uređaja da bi oni generirali DDoS promet. Stoga će se u ovom istraživanju kao rješenje navedenog izazova koristiti alat za generiranje DDoS prometa BoNeSi (engl. *DDoS Botnet Simulator*). BoNeSi je programski alat otvorenog koda koji ima mogućnost simuliranja DDoS prometa na infrastrukturnom i aplikacijskom sloju kao i mogućnost prilagodbe različitih parametara poput korištenog protokola, brzine slanja paketa, broja izvorišta DDoS prometa i slično [200]. Prema navodima autora programskog alata, on je učinkovit i u provedbi realnih DDoS napada pri čemu je uspješno testiran na mrežnom i aplikacijskom sloju te je dokazana njegova učinkovitost naspram postojećih, komercijalnih sustava zaštite od DDoS napada. Za potrebe ovog istraživanja BoNeSi je korišten za simuliranje DDoS prometa na izvorištu, odnosno na SHIoT uređajima. DDoS promet generiran je u izoliranom okruženju, prikazanom slikom 5.2, da bi se izbjegla mogućnost narušavanja sigurnosti javno dostupnih IK resursa te da ne bi provedba istraživanja narušavala važeće legislativne okvire Republike Hrvatske i Europske Unije.

S obzirom da je konačan cilj istraživanja razviti model detekcije anomalije mrežnoga prometa koji generiraju SHIoT uređaji (na izvorištu), ključna aktivnost je generirati DDoS promet i prikupiti ga za potrebe daljnje obrade i analize, dok je samo odredište takvog prometa u ovakvom scenariju manje važan čimbenik. Za potrebe generiranja DDoS prometa i stvaranje podatkovnog skupa nelegitimnog prometa korištena je virtualna radna stanica definirana Linux Ubuntu 19.04 operativnim sustavom s dediciranih 4 GB RAM memorije i Inter Core i7-5500U procesoru (4x2,40GHz).



Slika 5.2 Prikaz topologije korištene za potrebe generiranja DDoS prometa

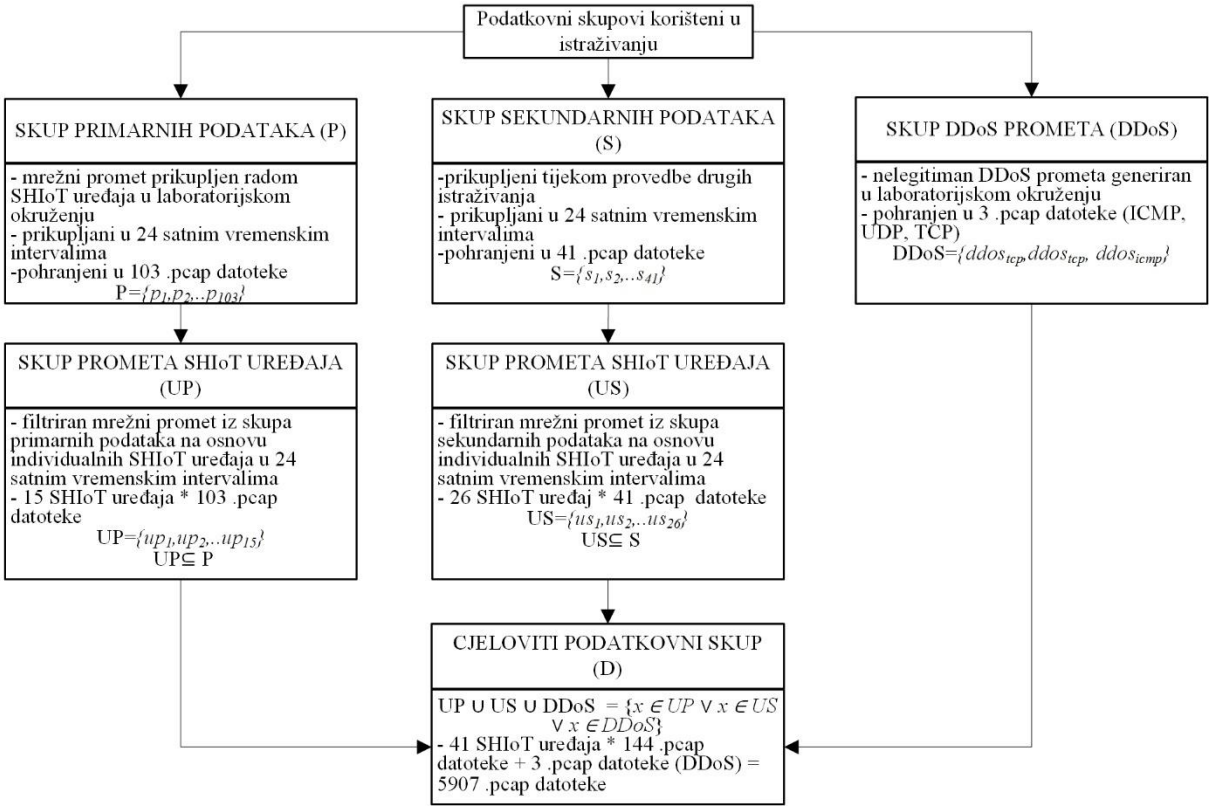
Za potrebe virtualizacije operativnog sustava korištena je platforma VMware Workstation 15 Player. Razlog korištenja virtualizacije i operativnog sustava temeljenog na Linux-u, veća je fleksibilnost u kontroli generiranog mrežnog prometa, odnosno minimiziranje mrežnog prometa koji bi bio rezultat različitih aplikacija i mrežnih usluga na Microsoft Windows operativnom sustavu.

Korištenjem BoNeSi programskog alata generiran je DDoS promet infrastrukturnog sloja temeljen na TCP, UDP i ICMP protokolima jer su DDoS napadi infrastrukturnog sloja učestaliji i intenzivniji nego napadi aplikacijskog sloja što je obrazloženo u poglavlju 4.2.

5.2.3 Deskriptivna statistička analiza prikupljenih podataka

Proces formiranja cjelovitog podatkovnog skupa korištenog za razvoj i validaciju modela detekcije anomalija mrežnog prometa prikazan je slikom 5.3. Inicijalni, univerzalni podatkovni skup (*U*) sadrži tri podskupa. Prvi podskup (*P*) predstavlja skup primarnih podataka koji sačinjavaju *.pcap* datoteke koje sadrže zapise legitimnog mrežnog prometa generiranog SHIoT uređajima u laboratorijskom okruženju u vremenskom intervalu od 24 sata.

Pri tome jedna *.pcap* datoteka sadrži kombinirane zapise mrežnog prometa 15 SHIoT uređaja. Dodatnom obradom generiran je novi podskup (UP) kojeg sačinjavaju *.pcap* datoteke mrežnog prometa u vremenskim intervalima od 24 sata za individualne SHIoT uređaje. Drugi podskup (S) odnosi se na podatke prikupljene u svrhu provedbe drugih istraživanja, a biti će korišteni u ovom istraživanju.



Slika 5.3 Formiranje cjelovitog podatkovnog skupa mrežnog prometa

Jednako kao i kod skupa primarnih podataka, skup sekundarnih podataka sadržan je u *.pcap* datotekama koje sadrže objedinjene zapise mrežnoga prometa za više SHIoT uređaja. Prema tome, i skup (S) dodatno je obrađen što je rezultiralo generiranjem novog podskupa (US) koji sadrži filtrirani mrežni promet prema SHIoT uređajima. To čini mrežni promet u 24-satnim vremenskim intervalima prikupljen od ukupno 26 uređaja i pohranjen u *.pcap* datoteke. Uz podatkovne skupove koji sadrže legitimni mrežni promet SHIoT uređaja, stvoren je i podatkovni skup koji sadrži nelegitiman DDoS promet u ukupnom trajanju od 36,62 sata, a koji će biti korišteni u fazi razvoja modela detekcije anomalija mrežnog prometa.

Primarni podatkovni skup formiran za potrebe ovog istraživanja sastoji se od ukupno 103 datoteke u *.pcap* formatu koje sadrže cjeloviti zapis mrežnog prometa. Sekundarni podatkovni skup sastoji se od 41 datoteke istog formata kao i primarni skup što čini ukupno 144 datoteke mrežnog prometa generiranog raznovrsnim SHIoT uređajima i predstavlja legitiman mrežni promet. Svaka od 144 datoteke sadrži promet generiran u vremenskom intervalu od 24 sata. Detaljan prikaz prikupljenih podataka prema pojedinoj *.pcap* datoteci prikazan je prilogom 2 ovog rada.

Tablicom 5.3 prikazan je statistički opis podatkovnog skupa kroz statističke mjere standardne devijacije, minimalne, maksimalne i srednje vrijednosti na razini 24-satnih intervala prikupljanog prometa za primarne i sekundarne podatke te za objedinjeni podatkovni skup.

Tablica 5.3 Statistički opis prikupljenih podataka legitimnog prometa

Statistička mjera	Broj prikupljenih paketa	Veličina datoteke (Byte)	Količina prikupljenih podataka (Byte)	Prosječna brzina prijenosa podataka (B/s)	Prosječna brzina prijenosa paketa (paketa/s)	Prosječna veličina paketa (Byte)
Primarni podatci						
Standardna devijacija	2613702,8	2503780307	2462270632	28498,13	30,25	175,48
Minimalna vrijednost	1019339	288056862	271747414	3145,21	11,8	252,5
Maksimalna vrijednost	14815959	13562522315	13325466947	154232,8	171,48	899,4
Srednja vrijednost	4428879,6	3416448737	3345586639	38721,71	51,25	677,782
Sekundarni podatci						
Standardna devijacija	1646515,4	804291290,1	765130504,3	12047,91	186,6204	20,69
Minimalna vrijednost	527035	89615024	71959664	832,87	136,54	6,1
Maksimalna vrijednost	7720905	3483660828	3322027939	60188,48	910,56	730,47
Srednja vrijednost	2365097,3	986887232,4	908751070	11565,99	330,12	45,21
Ukupno						
Standardna devijacija	2557564,5	2429423670	2396969893	27864,11	165,57	329,45
Minimalna vrijednost	527035	89615024	71959664	832,87	11,8	6,1
Maksimalna vrijednost	14815959	13562522315	13325466947	154232,8	910,56	899,4
Srednja vrijednost	3835384,1	2714894474	2641775718	30881,53	132,6931	492,9182

Karakteristike inicijalno prikupljenih podataka prikazane su tablicom 5.4 te su izražene kroz broj prikupljenih datoteka koje sadrže 24-satne intervale generiranog prometa, broj prikupljenih paketa, veličine datoteke, količine prikupljenih podataka te ukupan vremenski period prikupljanja podataka.

Tablica 5.4 Karakteristike inicijalnog podatkovnog skupa legitimnog prometa

	Broj datoteka	Broj prikupljenih paketa	Veličina datoteke (GB)	Količina prikupljenih podataka (GB)	Vremenski period prikupljanja (sati)
Primarni (suma)	103	456174601	351,89	344,59	2472,01
Sekundarni (suma)	41	99334088	41,44	38,16	986,45
Ukupno	144	555508689	393,33	382,75	3458,47

Alat za prikupljanje prometa (*Wireshark*) koristi određene metapodatke koje zapisuje unutar datoteka s prikupljenim prometom što čini razliku u veličini datoteke i količine prikupljenih podataka (prometa) koji se u datoteci nalazi.

Tablicom 5.5 prikazan je statistički opis prikupljenih podataka o DDoS prometu kroz broj prikupljenih paketa, veličinu datoteka, količinu prikupljenih podataka, prosječnu brzinu prijenosa podataka paketa te kroz prosječnu veličinu paketa.

Tablica 5.5 Statistički opis prikupljenih podataka DDoS prometa

Vrsta DDoS prometa	Statistička mjera	Broj prikupljenih paketa	Veličina datoteke (Byte)	Količina prikupljenih podataka (Byte)	Prosječna brzina prijenosa podataka (B/s)	Prosječna brzina prijenosa paketa (paketa/s)	Prosječna veličina paketa (Byte)
UDP	Minimalna vrijednost	240	16882	13018	703,86	12,98	54,24
	Maksimalna vrijednost	1112489	100000089	82226887	556885,96	7536,84	74,02
	Standardna devijacija	94456,78	8497712,45	6986412,60	36802,27	497,38	1,25
	Srednja vrijednost	1101250,5	99079803	81459770,61	514242,08	6952,01	73,88
TCP	Minimalna vrijednost	812406	68990117	55991597	2365,05	32,85	68,14
	Maksimalna vrijednost	1188524	100000088	81818196	223844,98	3251,73	72
	Standardna devijacija	47416,73	4028133,54	3276899,25	25364,99	367,79	0,44
	Srednja vrijednost	1169498,64	99357347,4	80645345,15	211751,48	3072,55	68,95
ICMP	Minimalna vrijednost	1007306	90667603	74550683	256103,23	3460,41	74
	Maksimalna vrijednost	1111091	100000089	82674753	587427,26	7936,74	76,35
	Standardna devijacija	7747,91	664900,17	548387,59	51604,32	698,04	0,19
	Srednja vrijednost	1110170,6	99952428	82189674,86	517835,22	6994,68	74,03

Podatkovni skup izražen je kroz mjere minimalne, maksimalne te srednje vrijednosti i standardne devijacije za DDoS promet temeljen na ICMP, TCP i UDP protokolima, odnosno na infrastrukturnoj razini.

Tablica 5.6 Karakteristike podatkovnog skupa DDoS prometa

Vrsta DDoS prometa	Broj datoteka	Broj prikupljenih paketa	Veličina datoteke (GB)	Količina prikupljenih podataka (GB)	Vremenski period prikupljanja (sati)
UDP	245	269806374	24,27	19,95	10,75
TCP	73	85373401	7,25	5,88	17,12
ICMP	195	217593439	19,59	16,1	8,75
Ukupno	513	572773214	51,11	41,93	36,62

Uz navedeno, prikupljeni podatci izraženi su i kroz ukupan broj prikupljenih datoteka, broj paketa, količinu prikupljenih podataka i kroz vrijeme prikupljanja za pojedinu vrstu DDoS prometa i sumarno, kako je prikazano tablicom 5.6.

5.3 Predobrada prikupljenih podataka i ekstrakcija identificiranih značajki prometa

U svrhu razvoja modela klasifikacije SHIoT uređaja proveden je proces filtriranja prometa iz pojedine *.pcap* datoteke prema MAC adresi uređaja. Razlog takvog načina filtriranja je dodjeljivanje IP adrese uređajima putem DHCP poslužitelja, zbog čega se ona može promijeniti tijekom vremena pa ne predstavlja pouzdanu značajku prema kojoj je moguće precizno filtrirati promet prema pojedinom uređaju u duljem vremenskom periodu.

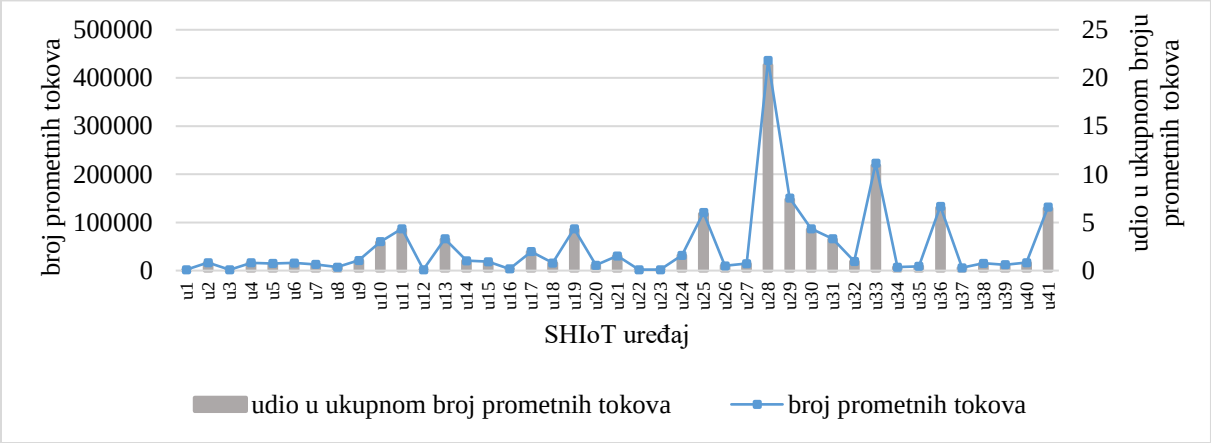
Predmetno istraživanje promatra značajke prometa za pojedinačne SHIoT uređaje obuhvaćene istraživanjem (41 uređaj) na razini prometnog toka. Prometni tok definiran je slijedom paketa s jednakim vrijednostima izvorišne IP adrese, odredišne IP adrese, izvorišnog komunikacijskog porta, odredišnog komunikacijskog porta i korištenog protokola (TCP ili UDP) [201]. Razlog odabira prometnog toka kao razine promatranja i analize značajki prometa je taj što predstavlja agregirane (statističke) podatke zaglavlja paketa za komunikaciju između izvorišta i odredišta. Analiza značajki prometa na razini paketa obuhvaća veći broj informacija kao što je sadržaj paketa, a isto tako zahtijeva više računalskih resursa za njihovu pohranu i obradu. Primjer odnosa broja prometnih tokova i broja paketa u vremenskom periodu od 24 sata vidljiv je za uređaj Google Chromcast (obuhvaćen ovim istraživanjem) gdje je generirano 11 877 zasebnih prometnih tokova dok je broj paketa 2 459 538. S obzirom na to da većina uređaja i aplikacija u današnje vrijeme koristi kriptografske metode za komunikaciju, sadržaj paketa nije moguće promatrati i analizirati na ekonomski, vremenski i legalno prihvatljiv način. Prema tome, promatranje i analiza značajki prometa na razini prometnog toka predstavlja prihvatljiv i često korišten pristup u brojnim istraživanjima.

U svrhu ekstrakcije značajki prometnog toka, korišten je programski alat CICFlowMeter. CICFlowMeter je alat razvijen na kanadskom institutu za kibernetičku sigurnost sveučilišta New Brunswick [202]. Alat je razvijen u Java programskom jeziku što pruža fleksibilnost u odabiru značajki prometnog toka koje je moguće izračunati kao i dodavanje novih značajki. Primjenom navedenog alata provedena je ekstrakcija ukupno 83 značajke prometnog toka prikazanih prilogom 3 ovog rada. Ekstrahirane značajke prometnog toka rezultat su analize i identifikacije relevantnih značajki prometa za MTC promet proizašle iz prve faze istraživanja prikazane u 5.1 kao i izračuna dodatnih značajki i statističkih mjera (standardna devijacija, minimalna i maksimalna vrijednost te srednja vrijednost). Razlog je prikupljanje što većeg broja značajki u inicijalnom skupu da bi se u kasnijim fazama istraživanja (klasifikacija SHIoT uređaja i detekcija anomalija) utvrdilo koje nezavisne značajke imaju najveći utjecaj na promjenu odabrane zavisne značajke.

Grafikonom 5.2 prikazana je distribucija prometnih tokova (vektora značajki[16]), odnosno udio prometnih tokova ekstrahiranih iz prikupljenog prometa SHIoT uređaja obuhvaćenih predmetnim istraživanjem.

[16] Vektor značajki – opažanje/primjer koje predstavlja numeričku reprezentaciju promatranih značajki

Grafikon 5.2 Distribucija broja prometnih tokova prema SHIoT uređaju



Ukupan broj prikupljenih prometnih tokova iznosi 2 045 052. Prikazani vektori značajki korišteni su u kasnijim fazama koje podrazumijevaju definiranje klasa SHIoT uređaja te razvoj modela klasifikacije SHIoT uređaja i razvoj modela detekcije DDoS prometa.

5.4 Definiranje klasa IoT uređaja temeljenih na identificiranim značajkama prometa

Identifikacija uređaja u IoT okruženju predstavlja važan korak i osnovu za aktivnosti povezane sa sigurnošću okruženja u kojima takvi uređaji egzistiraju kao što je detekcija neovlaštenih aktivnosti, nedozvoljenih uređaja unutar mreže, malicioznog programskog koda i sl. Autori u istraživanju [52] koriste klaster metodu u svrhu klasifikacije 21 IoT uređaja pri čemu uređaje klasificiraju zasebno na temelju 11 značajki. Na temelju identifikacije uređaja, istraživanje [190] nastoji detektirati neovlaštene uređaje povezane na promatranu mrežu. U tu svrhu korišteno je ukupno 11 IoT uređaja koji su klasificirani prema semantičkim karakteristikama uređaja, odnosno njihovoj namjeni (uređaji za nadzor djece, senzori pokreta, hladnjaci, sigurnosne kamere, senzori dima, utičnice, termostati, televizori, satovi). Sličan način klasifikacije, temeljen na semantičkim karakteristikama uređaja, prikazan je i u istraživanju [189] u kojem autori koriste sekundarni podatkovni skup prikupljen u [52]. Istraživanjem je obuhvaćeno ukupno 15 uređaja koji su klasificirani u četiri kategorije s obzirom na namjenu pojedinog uređaja (koncentratori, elektronički uređaji, kamere i utičnice). Autori na temelju analize provedene istraživanjem ističu kako je za klasifikaciju SHIoT uređaja važnija raznovrsnost uređaja obuhvaćenih u fazi prikupljanja podataka, nego veličina samog podatkovnog skupa (vremenskog perioda prikupljanja i količine prikupljenog prometa).

Iz dosadašnjih istraživanja uočljivo je da su pristupi klasifikaciji do sada temeljeni pretežno na semantičkim obilježjima što znači da su klase uređaja definirane prema primjeni takvih uređaja ili njihovim funkcionalnostima. Nedostatak takvog pristupa pri definiranju klasa moguće je promatrati s aspekta dinamičnosti okruženja pametnog doma. Prema statističkim pokazateljima prikazanima u poglavlju 2.4, broj SHIoT uređaja je u kontinuiranom porastu što je praćeno i porastom broja tvrtki koje razvijaju nova rješenja i nove SHIoT uređaje. Prema tome, klase SHIoT uređaja potrebno je definirati na način koji će biti moguće primijeniti na nadolazeće SHIoT uređaje koji će se prema funkcionalnostima i primjeni razlikovati od trenutno dostupnih uređaja.

5.4.1 Određivanje značajke prometnog toka u svrhu definiranja klasa SHIoT uređaja

Predvidivost ponašanja IoT uređaja je fenomen koji je rezultat komunikacijskih aktivnosti IoT uređaja uočen u istraživanjima [51], [117], [203]. S obzirom da SHIoT uređaji posjeduju ograničen broj funkcionalnosti, određeni uređaji ponašat će se približno jednako u vremenu prema vrijednostima promatranih značajki prometa. Za razliku od IoT uređaja,

konvencionalni uređaji (pametni telefoni, stolna računala, prijenosna računala, i sl.) podržavaju instalaciju velikog broja aplikacija pri čemu komunikacijska aktivnost takvih uređaja ovisi o krajnjim korisnicima i načinu korištenja uređaja. Prema navedenome, indeks razine predvidivosti ponašanja IoT uređaja izražen koeficijentom varijacije primljene i poslane količine podataka (indeks C_u) predstavlja mjeru na temelju koje je moguće odrediti ponašanje SHIoT uređaja u određenom vremenskom periodu. Što je indeks (C_u) bliži 0, promatrani uređaj ima manje odstupanje u odnosu na količinu primljenih i poslanih podataka i smatra se da je razina predvidivosti ponašanja takvog uređaja veća u odnosu na uređaj čiji je indeks C_u dalji od 0.

Indeks C_u izračunat je za srednje vrijednosti uzastopnih prometnih tokova pojedinog SHIoT uređaja u vremenskom periodu od 30 dana prema izrazu (1).

$$C_u = CVar_u = \frac{\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}}{\frac{1}{N}\sum_{i=1}^{N} x_i} \tag{1}$$

Gdje je:

$C_u = CVar_u$ – indeks razine predvidivosti prometa SHIoT uređaja u

N – ukupan broj srednjih vrijednosti odnosa primljene i poslane količine prometa za uzastopne prometne tokove u vremenskom periodu T

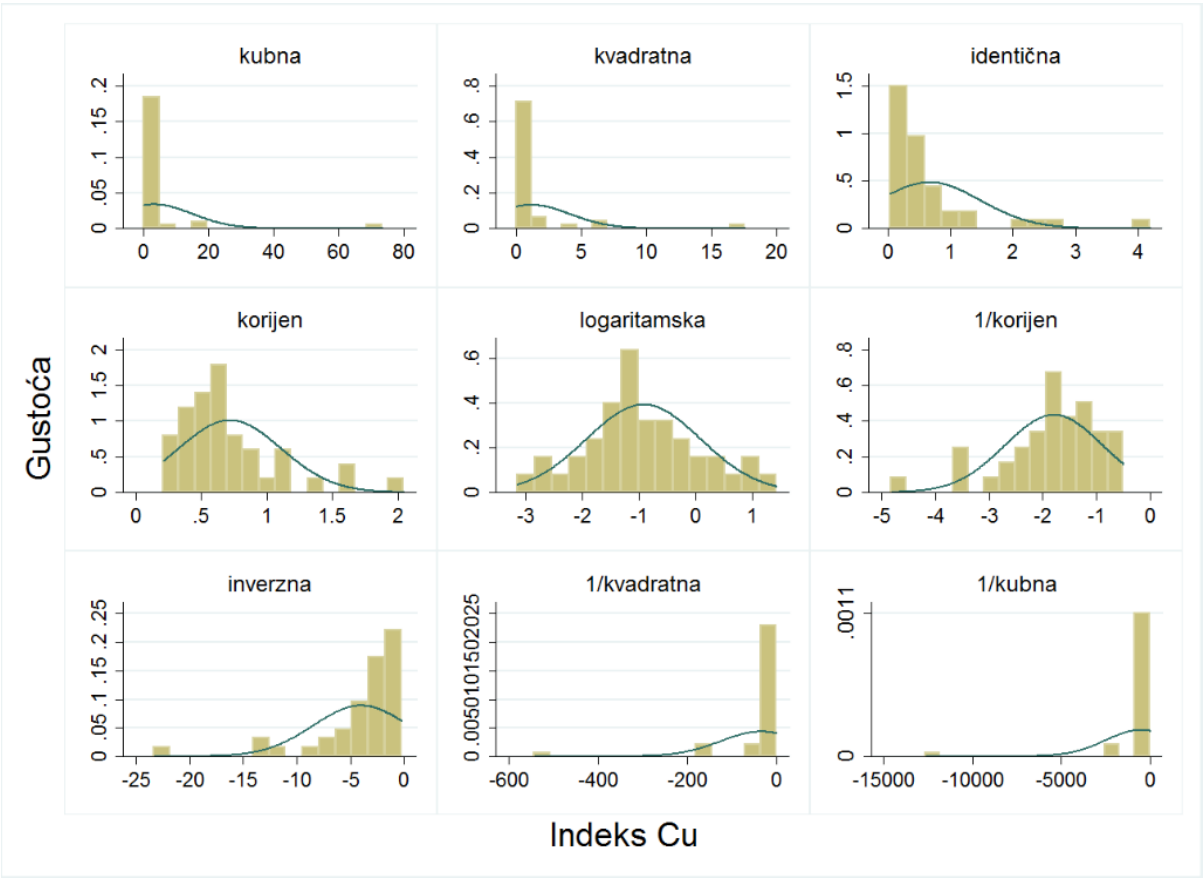
x_i – iznos srednje vrijednosti odnosa primljene i poslane količine prometa za uzastopne prometne tokove

Kako bi se izbjeglo da srednje vrijednosti teže 0, što predstavlja problem primjene metode koeficijenta varijacije, kao normalizirane vrijednosti disperzije, iz podatkovnog skupa uklonjeni su prometni tokovi u kojima je odnos količine primljenih i poslanih podataka jednak 0.

5.4.2 Definiranje klasa IoT uređaja na osnovi koeficijenata varijacije

Za definiranje klasa uređaja na temelju vrijednosti indeksa C_u korištena je metoda klasifikacije koeficijenata varijacije primijenjena u istraživanjima [204–207] koja pretpostavlja normalnu distribuciju podataka. S obzirom da je distribucija dobivenih vrijednosti (Indeks C_u) asimetrične prirode (ukošena ulijevo), podatci su transformirani. Metoda transformacije podataka odabrana je korištenjem metode *Ladder of powers* (Tukey metoda) koja jasno

prikazuje prikladnu funkciju transformacije podataka Da bi se postigla normalna distribucija [208].



Slika 5.4 Histogramski prikaz razdiobe podataka u ovisnosti o korištenoj funkciji transformacije

Iz slike 5.4 uočava se prikladnost primjene logaritamske funkcije u svrhu transformacije podataka s obzirom da u ovom slučaju rezultira normalnom distribucijom. Uz grafički prikaz, tablicom 5.7 prikazane su chi^2 vrijednosti pojedine funkcije transformacije.

Tablica 5.7 Rezultati provedbe *Ladder of Powers* (Tukey) metode

Transformacija	**Izraz**	**chi^2**	**P(chi^2)**
Kubna	C_u^3	*50,29*	*0*
Kvadratna	C_u^2	42,42	0
Identična	C_u	25,18	0
Korijen	$\sqrt{C_u}$	12,08	0,002
Logaritamska	**log(Cu)**	**0,44**	**0,804**
1/korijen	$\sqrt{\frac{1}{C_u}}$	9,48	0,009
Inverzna	$\frac{1}{C_u}$	25,07	0
1/kvadratna	$\frac{1}{C_u^2}$	43,37	0
1/kubna	$\frac{1}{C_u^3}$	51,08	0

Pri tome je distribucija podataka najbliže normalnoj što je chi^2 bliži vrijednosti 0, odnosno što je P(chi^2) bliži vrijednosti 1. Normalna distribucija dobivenih podataka potvrđena je i Shapiro-Wilk i Shapiro-Francia testom normalnosti, vidljivo u tablici 5.8, pri čemu u oba slučaja, p>0,05 i nul hipotezu (da vrijednosti varijable *log(C_u)* prate normalnu razdiobu) nije moguće odbaciti. Parametri W i V predstavljaju koeficijente koji označavaju odstupanje od normalne razdiobe podataka pri čemu vrijednost W ≈ 1 indicira normalnu razdiobu podataka, dok *z* predstavlja z-statistiku koja označava koliko standardnih devijacija su promatrani podatci udaljeni od srednje vrijednosti [209].

Tablica 5.8 Rezultati Shapiro-Wilk i Shapiro-Francia testova normalnosti

Varijabla	**Promatranja**	**W**	**V**	**z**	**p>z**
log(C_u) – Shapiro-Wilk	41	0,98831	0,471	-1,588	0,94382
log(C_u) – Shapiro-Francia	41	0,98887	0,495	-1,367	0,91420

U svrhu primjene metode klasifikacije koeficijenata varijacije, logaritamske vrijednosti indeksa C_u normalizirane su min-max metodom prema izrazu (2):

$$C_{u(norm)} = \frac{\log (C_u) - \log (C_{u_{min}})}{\log (C_{u_{max}}) - \log (C_{u_{min}})} \tag{2}$$

Gdje je:

$C_{u(norm)}$ – normalizirana vrijednost logaritamski transformirane vrijednosti C_u u intervalu [0,1]

$\log (C_u)$ – logaritamska vrijednost C_u uređaja u

$\log (C_{u_{min}})$ – minimalna logaritamska vrijednost C_u svih uređaja

$\log (C_{u_{max}})$ – maksimalna logaritamska vrijednost C_u svih uređaja

Nakon uspostave normalne distribucije podataka i njihove normalizacije, primijenjena je metoda definiranja klasa na temelju koeficijenata varijacije kao rezultat srednjih vrijednosti koeficijenata varijacije i njihove standardne devijacije.

Srednja vrijednost koeficijenta varijacije izračunata je prema izrazu (3):

$$A_{C_{u(norm)}} = \frac{1}{N} \sum_{u=1}^{n} \frac{C_{1(norm)} + C_{2(norm)} + \cdots + C_{n(norm)}}{N} \tag{3}$$

Gdje je:

$A_{C_{u(norm)}}$ – aritmetička sredina koeficijenata varijacije svih uređaja

N – broj uređaja

$C_{u(norm)}$ – koeficijent varijacije uređaja u

Standardna devijacija koeficijenata varijacije izračunata je prema izrazu (4):

$$\sigma_{C_{u(norm)}} = \sqrt{\frac{1}{N-1}\sum_{u=1}^{n}(C_{u(norm)} - \bar{C})^2} \quad (4)$$

Gdje je:

$\sigma_{C_{u(norm)}}$ – standardna devijacija koeficijenata varijacije svih uređaja

N – broj uređaja

$C_{u(norm)}$ – koeficijent varijacije uređaja u

$\bar{C}$ – aritmetička sredina koeficijenata varijacije svih uređaja

Na temelju prethodno provedene obrade podataka definirane su ukupno četiri klase IoT uređaja prema metodi korištenoj u istraživanju [206]. Prvom klasom obuhvaćeni su uređaji kod kojih je zadovoljen uvjet $C_{u(norm)} \leq A_{C_{u(norm)}}$-$\sigma_{C_{u(norm)}}$. Drugom klasom obuhvaćeni su uređaji koji zadovoljavaju uvjet $A_{C_{u(norm)}}$-$\sigma_{C_{u(norm)}} < C_{u(norm)} \leq \frac{A_{C_u}+\sigma_{C_u}}{2}$. Trećom klasom obuhvaćeni su uređaji koji zadovoljavaju uvjet $\frac{A_{C_u}+\sigma_{C_u}}{2} < C_{u(norm)} \leq A_{C_u} + \sigma_{C_u}$, dok su posljednjom klasom obuhvaćeni uređaji koji zadovoljavaju uvjet $C_{u(norm)} > A_{C_u} + \sigma_{C_u}$.

Vrijednosti C_u, logaritamski transformirane vrijednosti te min-max normalizirane vrijednosti za svaki analizirani uređaj prikazane su tablicom 5.9. Prema podatcima prikazanim tablicom 5.9, definirane su ukupno četiri klase uređaja na temelju vrijednosti indeksa C_u. Prvoj klasi (C1) pripadaju svi uređaji čija je logaritamski transformirana i normalizirana vrijednost $C_{u(norm)} \leq 0{,}253722$. Drugoj klasi (C2) pripadaju uređaji za koje vrijedi $0{,}253722 < C_{u(norm)}$ 0,354866. Trećoj klasi (C3) pripadaju uređaji za koje vrijedi $0{,}354866 < C_{u(norm)} \leq 0{,}709732$ dok u posljednju klasu (C4) pripadaju uređaji za koje vrijedi $C_{u(norm)} > 0{,}709732$.

Klasa C1 označava IoT uređaje s vrlo visokom razinom predvidivosti ponašanja s obzirom da je koeficijent varijacije odnosa primljenih i poslanih podataka najbliži vrijednosti 0. To znači da se takvi uređaji tijekom vremena ponašaju približno jednako s aspekta promatrane značajke. Ako IoT uređaj klase C1 koristi korisnik, drugi uređaj ili okolina, neće biti značajnog utjecaja na promjenu vrijednosti indeksa C_u.

Tablica 5.9 Definirane klase uređaja prema vrijednosti indeksa C_u

r.br.	Uređaj	Indeks C_u	log(C_u) transformacija	min-max normalizacija ($C_{u(norm)}$)	Definicija klase	Naziv klase
1.	tp_cam	0,042916917	-1,36737	0	$C_{u(norm)} \leq A_{C_u} - \sigma_{C_u}$	**C1**
2.	wiz_F3	0,075820416	-1,12021	0,124242056		
3.	hs105	0,076231674	-1,11786	0,125423008		
4.	wiz_B0	0,08086321	-1,09225	0,138299504		
5.	sams_st	0,123562483	-0,90811	0,230861447		
6.	w115	0,142241675	-0,84697	0,261595627		
7.	ihome	0,148887517	-0,82714	0,271564558	$A_{C_u} - \sigma_{C_u} < C_{u(norm)} \leq \frac{A_{C_u} + \sigma_{C_u}}{2}$	**C2**
8.	wit_baby	0,176239975	-0,7539	0,308384178		
9.	nest_smoke	0,192606687	-0,71533	0,327771139		
10.	ph_hue_2	0,200187894	-0,69856	0,336199355		
11.	cana_cam	0,209863653	-0,67806	0,346504073		
12.	hs110	0,24742122	-0,60656	0,382445795	$\frac{A_{C_u} + \sigma_{C_u}}{2} < C_{u(norm)} \leq A_{C_u} + \sigma_{C_u}$	**C3**
13.	belk_sw	0,254614637	-0,59412	0,388702406		
14.	wit_aura	0,261184872	-0,58305	0,394264423		
15.	w245	0,27041724	-0,56797	0,401848085		
16.	net_therm	0,290797956	-0,53641	0,417711253		
17.	amz_dot	0,318918293	-0,49632	0,437862868		
18.	blink_cam	0,344500361	-0,46281	0,454707915		
19.	sams_cam	0,34686605	-0,45984	0,456201948		
20.	lifx	0,346886878	-0,45981	0,456215056		
21.	smartw_cam	0,357559305	-0,44665	0,462830477		
22.	i895	0,358681004	-0,44529	0,463514273		
23.	i896	0,379012744	-0,42135	0,475551248		
24.	my_strom	0,432393144	-0,36412	0,5043173		
25.	inst_cam	0,479119397	-0,31956	0,526719365		
26.	bc_blood	0,479127026	-0,31955	0,526722841		
27.	net_weath	0,543491131	-0,26481	0,554240633		
28.	belk_cam	0,565787022	-0,24735	0,563017747		
29.	aug_door	0,610206124	-0,21452	0,579517618		
30.	amz_echo	0,632948837	-0,19863	0,587506285		
31.	belk_mot	0,724907331	-0,13972	0,617121319		
32.	net_cam	0,764635407	-0,11655	0,628769456		
33.	ph_hue_4	0,791347539	-0,10163	0,636265899		
34.	pix	0,958787396	-0,01828	0,678167108		
35.	wit_body	1,140461786	0,057081	0,716048538	$C_{u(norm)} > A_{C_u} + \sigma_{C_u}$	**C4**
36.	google_chr	1,267801595	0,103051	0,739157175		
37.	ring_vd	1,370122066	0,136759	0,756101612		
38.	nest_cam	1,985562839	0,297884	0,837096166		
39.	triby	2,468462951	0,392427	0,884621355		
40.	aw_aq	2,553917945	0,407207	0,89205118		
41.	google_mini	4,187473486	0,621952	1		

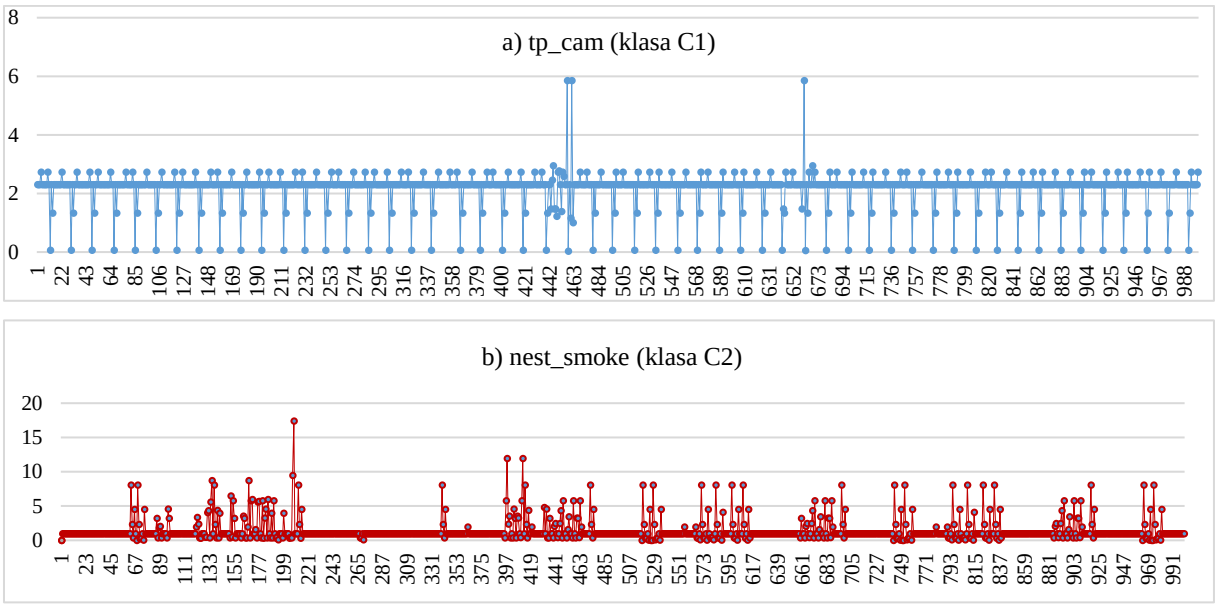
Klasa C2 objedinjuje uređaje s visokom razinom predvidivosti ponašanja. Ako uređaj iz navedene klase koristi korisnik, drugi uređaj ili okolina, to može rezultirati manjim

promjenama odnosa primljenih i poslanih podataka. Uređaji objedinjeni klasom C3 predstavljaju uređaje sa srednjom razinom predvidivosti ponašanja. Utjecaj interakcije korisnika, drugih uređaja ili okoline na odnos primljenih i poslanih podataka može biti značajan. Rezultat ovakvog ponašanja mogu biti dodatne funkcionalnosti uređaja koje u određenim trenutcima rezultiraju većom količinom podataka u dolaznom ili odlaznom smjeru.

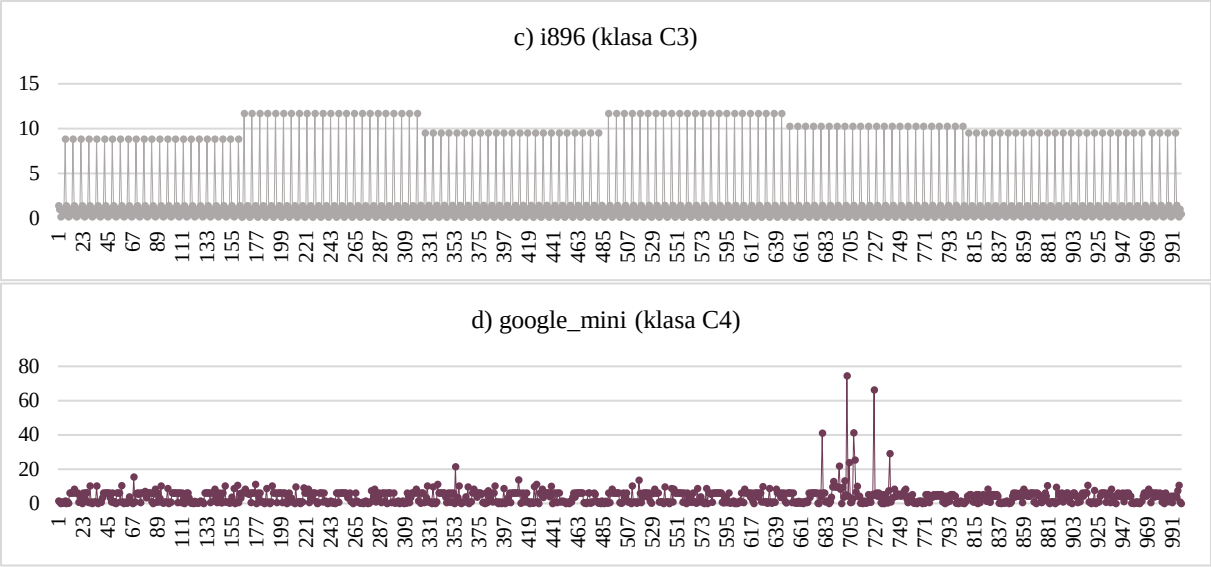
Posljednja klasa C4, objedinjuje SHIoT uređaje niske razine predvidivosti ponašanja. Korištenje takvih uređaja i njihova interakcija s korisnikom, drugim uređajima ili okolinom značajno utječe na odnos primljenih i poslanih podataka. Kao razlog uočava se značajno veća količina podataka u dolaznom smjeru (preuzimanje) kao rezultat zahtjeva korisnika. Primjer je vidljiv kod uređaja kao što je Google Chromcast gdje se na zahtjev korisnika reproducira videosadržaj što zahtijeva njegovo preuzimanje putem Youtube[17] usluge za pregled videosadržaja. Ovoj klasi pripada i uređaj Google Home mini, pametni zvučnik koji na upit korisnika može pružiti različite audiosadržaje što također uzrokuje veću varijaciju odnosa primljenog i poslanog prometa.

Grafikonom 5.3 prikazan je primjer odnosa ponašanja četiri SHIoT uređaja (TPlink Day Night Cloud NC220 camera, NEST Protect Smoke Alarm, iRoobot Roomba 896 i Google Home mini) koji pripadaju različitim klasama za 1000 uzastopnih prometnih tokova.

Grafikon 5.3 Prikaz razlike ponašanja četiri SHIoT uređaja u vremenu prema odnosu primljenog i poslanog prometa za 1000 uzastopnih prometnih tokova



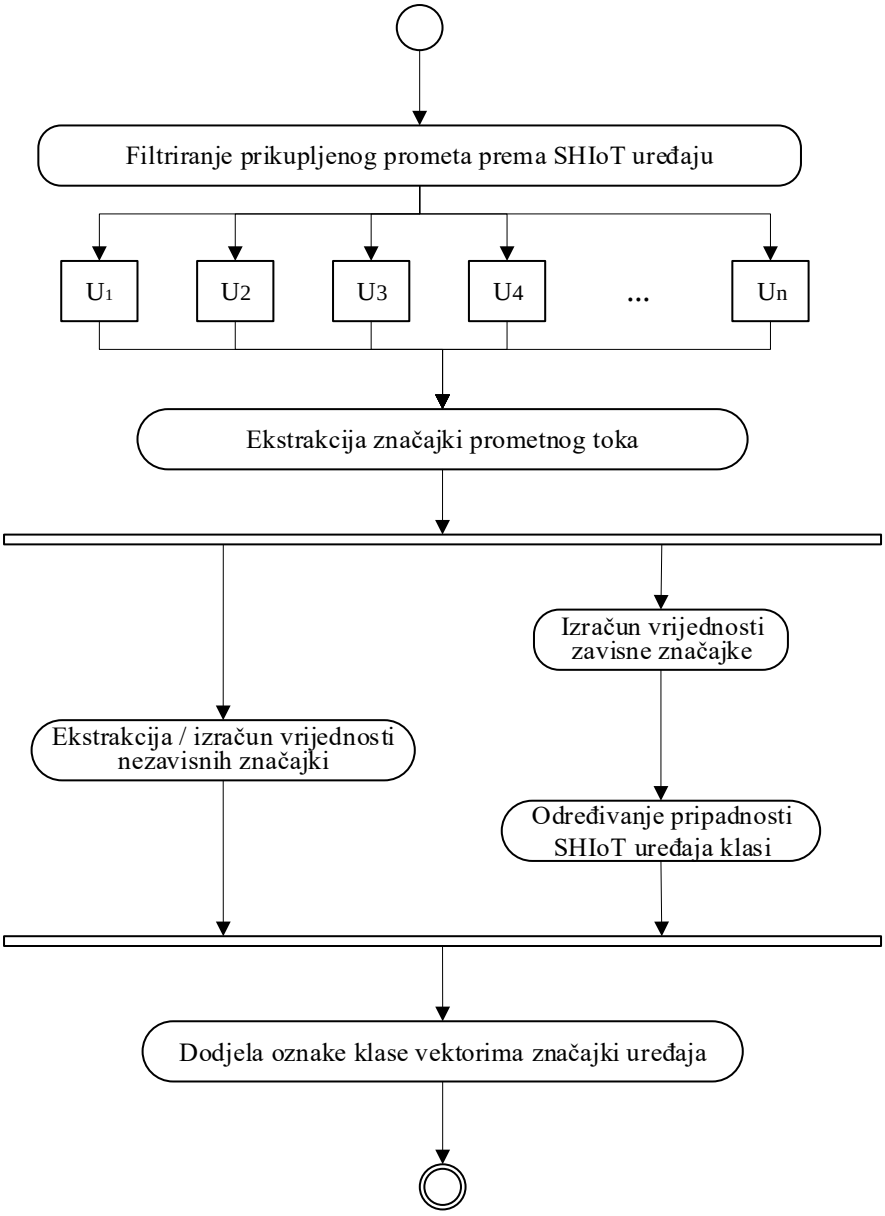
[17] https://www.youtube.com



Pri tome se kod uređaja Google Home mini uočava razlika varijacije odnosa primljenog i poslanog prometa (C_{google_mini}=4,18) u odnosu na uređaje TPlink Day Night Cloud NC220 camera (C_{tp_link}=0,042), NEST Protect Smoke Alarm (C_{nest_smoke}=0,19) te iRoobot Roomba 896 (C_{i896} =0,37).

5.4.3 Formiranje podatkovnog skupa s obzirom na definirane klase SHIoT uređaja

Za potrebe razvoja klasifikacijskog modela temeljenog na metodi logističke regresije unaprijeđene konceptom nadziranog strojnog učenja, formiran je podatkovni skup koji sadrži vrijednosti ekstrahiranih značajki prometnih tokova SHIoT uređaja te pripadnost klasi pojedinog uređaja za svaki prometni tok u skupu. Proces formiranja podatkovnog skupa koji sadrži združene podatke o vrijednostima značajki pojedinog prometnog toka i pripadnosti prometnog toka definiranim klasama, prikazan je UML dijagramom toka na slici 5.5.



Slika 5.5 UML dijagram aktivnosti procesa stvaranja podatkovnog skupa

Svaki prometni tok generiran je SHIoT uređajem koji pripada određenoj klasi prema klasifikaciji prikazanoj u tablici 5.9. Prema tome svakom prometnom toku pridružena je odgovarajuća klasa kojoj pripada uređaj koji generira promatrani prometni tok kako je prikazano tablicom 5.10.

Tablica 5.10 Primjer združivanja prometnih tokova i oznaka klase

r.br.	uređaj	z8	z9	z10	z11	z12	z13	z14	z15	z16	z17	z18	…	z83	klasa
1.	u6	110176901	5	4	372	648	186	0	74	102	186	154	…	54900000	C1
2.	u6	110117149	5	4	372	648	186	0	74	102	186	154	…	54800000	C1
3.	u4	113285202	30	23	2012	3831	267	0	67	78	1460	0	…	5740188	C1
4.	u4	8334253	3	2	96	80	32	32	32	0	48	32	…	5269207	C1
5.	u4	79698183	25	21	1805	4905	267	0	72	83	1460	0	…	5767895	C1

6.	u4	1234276	1	2	69	69	69	69	69	0	69	0	…	0	C1
7.	u4	1269831	1	2	32	80	32	32	32	0	48	32	…	0	C1
8.	u5	110119161	5	4	372	648	186	0	74	102	186	154	…	54900000	C1
9.	u5	4307304	12	1	366	40	40	21	31	10	40	40	…	0	C1
10.	u1	55120696	3	3	186	494	186	0	62	107	186	154	…	54900000	C1
11.	u1	110105251	5	4	372	648	186	0	74	102	186	154	…	54900000	C1
12.	u11	9383	7	1	2156	308	308	308	308	0	308	308	…	0	C2
13.	u11	1649	3	1	924	308	308	308	308	0	308	308	…	0	C2
14.	u10	4785250	17	1	5104	296	305	296	300	4	296	296	…	0	C2
15.	u10	4795180	17	1	5104	296	305	296	300	4	296	296	…	0	C2
16.	u10	90304076	4	5	0	74	0	0	0	0	39	0	…	30000000	C2
17.	u10	90314494	4	5	0	74	0	0	0	0	39	0	…	30000000	C2
18.	u10	101406974	23	1	7203	309	318	309	313	4	309	309	…	101000000	C2
19.	u10	90310934	4	5	0	74	0	0	0	0	39	0	…	30000000	C2
20.	u10	251936	11	1	3447	309	318	309	313	4	309	309	…	0	C2
21.	u9	2949318	6	7	634	943	528	0	106	209	680	0	…	0	C2
22.	u9	4921095	12	14	1873	1906	527	0	156	169	677	0	…	0	C2
23.	u19	2461	1	3	33	143	33	33	33	0	61	33	…	0	C3
24.	u19	2337	1	3	33	143	33	33	33	0	61	33	…	0	C3
25.	u30	108109786	4	1	596	149	149	149	149	0	149	149	…	27000000	C3
26.	u30	108113739	4	1	636	159	159	159	159	0	159	159	…	27000000	C3
27.	u30	119577279	9	11	164	246	41	0	18	22	41	0	…	29100000	C3
28.	u30	104123962	2	4	96	192	48	48	48	0	48	48	…	49300000	C3
29.	u30	2090	1	3	33	143	33	33	33	0	61	33	…	0	C3
30.	u30	2126	1	3	33	143	33	33	33	0	61	33	…	0	C3
31.	u41	141088	4	7	454	2881	357	28	114	162	1350	16	…	0	C4
32.	u42	68231	1	3	32	140	32	32	32	0	60	32	…	0	C4
33.	u43	15158091	9	9	6181	3268	1350	23	687	660	1350	20	…	14900	C4
34.	u44	15125583	8	8	4966	3058	1350	23	621	657	1350	20	…	14900	C4
35.	u45	75000643	3	4	26	26	26	0	9	15	26	0	…	29800	C4
36.	u46	116337	4	7	454	2881	357	28	114	162	1350	16	…	0	C4
37.	u47	15122480	5	7	910	3100	792	23	182	341	1350	20	…	14900	C4
38.	u48	36187	1	3	33	275	33	33	33	0	145	33	…	0	C4
39.	u49	15148222	5	7	1084	3284	966	23	217	419	1350	20	…	14900	C4
40.	u50	116586	4	7	454	2881	357	28	114	162	1350	16	…	0	C4
41.	u51	140798	4	7	454	2881	357	28	114	162	1350	16	…	0	C4
42.	u40	97777	1	3	32	140	32	32	32	0	60	32	…	0	C4

Ekstrakcija značajki prometnih tokova generiranih pojedinim SHIoT uređajem, opisana u podpoglavlju 5.3 i definiranje klasa SHIoT uređaja opisano u podpoglavlju 5.4, osnova su za formiranje podatkovnog skupa prometnih tokova SHIoT uređaja kojima su pridružene oznake klase.

5.5 Odabir značajki prometnog toka u svrhu razvoja modela klasifikacije SHIoT uređaja

Odabir značajki prometa generiranog SHIoT uređajima predstavlja ključni korak u postupku razvoja modela klasifikacije SHIoT uređaja. Važnost odabira značajki dokazana je u brojnim istraživanjima koja koriste statističke metode i metode strojnog učenja, posebice u području klasifikacije i regresije. Cilj je utvrditi podskup izvornog skupa značajki koje su relevantne za klasifikacijski problem koji se nastoji riješiti, a ukloniti one značajke koje su irelevantne ili redundantne te na taj način reducirati dimenzionalnost prostora značajki kao i cjelokupnog podatkovnog skupa. Odabir značajki pozitivno se odražava na točnost klasifikacijskog modela, brzinu klasifikacije te može smanjiti pojavu prenaučenosti modela (engl. *overfitting*) koja često dovodi do loših rezultata u postupku validacije [210].

Iz inicijalnog skupa značajki preventivno su uklonjene značajke koje se odnose na identifikaciju prometnog toka (z1,..,z7) da bi se kod razvoja klasifikacijskog modela smanjila njegova pristranost (engl. *bias*), odnosno pojava koja uzrokuje „krive pretpostavke“ tijekom faze učenja modela i rezultira neuočavanjem relevantnih relacija između nezavisnih i zavisnih značajki. Primjerice, učestala pojava jedne IP adrese u skupu prometnih tokova koji pripadaju jednoj klasi uređaja može rezultirati modelom koji je naučen da ta IP adresa predstavlja važan element promatrane klase. Posljedično tome, pojava uređaja s drugačijom IP adresom uzrokovat će njegovo svrstavanje u pogrešnu klasu. Prema tome, inicijalni skup nezavisnih značajki reduciran je s 83 na 76.

U svrhu odabira značajki u predmetnom istraživanju korištena je metoda informacijske dobiti (engl. *information gain, IG*). Odabrana metoda temelji se na entropiji i pripada skupu metoda rangiranja značajki (engl. *feature ranking*). Ovu skupinu metoda karakterizira jednostavnost i dobri rezultati u praktičnim primjenama zbog čega se često koristi u procesu odabira značajki u različitim domenama poput kategorizacije teksta, analize genoma, detekcije anomalija u komunikacijskim mrežama i bioinformatici [211–214].

Prema [215], *IG* metoda pripada mjerama temeljenima na korelaciji i služi za izračun stupnja korelacije između odabrane nezavisne značajke i zavisne značajke (klase uređaja) te za evaluaciju prikladnosti značajke u svrhu klasifikacije (engl. *goodness of feature*). Prema [216], nezavisna značajka je prikladna ukoliko je relevantna za promatranu zavisnu značajku, ali ujedno i nije redundantna s ostalim relevantnim nezavisnim značajkama. *IG* izražava mjeru redukcije neizvjesnosti identifikacije zavisne značajke u slučaju kada je vrijednost nezavisne značajke nepoznata. Izračun neizvjesnosti temeljen je na teoriji informacija i Shannonovoj

entropiji s ciljem odabira onih nezavisnih značajki koje imaju najznačajniji utjecaj na zavisnu značajku. Entropija zavisne značajke *X* definirana je izrazom (5) [216].

$$H(X) = -\sum_{i=1}^{n} P(x_i) log_2(P(x_i)) \tag{5}$$

Gdje je:

H(X) – entropija zavisne značajke *X*

$P(x_i)$ – vjerojatnost pojave vrijednosti x_i značajke *X*

Entropija zavisne značajke *X*, nakon opažanja vrijednosti nezavisne značajke *Y*, definirana je izrazom (6).

$$H(X|Y) = -\sum_{\mathrm{j}=1}^{m} P(y_j) \sum_{i=1}^{n} P(x_i|y_j) log_2(P(x_i|y_j)) \tag{6}$$

Gdje je:

$P(y_i)$ – vjerojatnost pojave vrijednosti y_j značajke *Y*

$P(x_i|y_j)$ – uvjetna vjerojatnost značajke *X* s obzirom na vrijednosti značajke *Y*

Informacijska dobit odražava iznos za koji se smanjuje neizvjesnost identifikacije pojedine vrijednosti zavisne značajke *X* (klase uređaja) s obzirom na vrijednosti promatrane nezavisne značajke *Y* prema izrazu (7).

$$IG = H(X) - H(X|Y) \tag{7}$$

S obzirom da zavisna značajka *X* može poprimiti samo četiri vrijednosti (četiri moguće klase), maksimalna vrijednost *IG* iznosi 2 ($log_2 X$). Prema tome, vrijednost dobivena za pojedinu nezavisnu značajku predstavlja količinu informacije nezavisne značajke, odnosno iznos za koji promatrana nezavisna značajka smanjuje entropiju (neizvjesnost) zavisne značajke. Tablicom 5.11 prikazane su značajke prometnog toka s izraženom vrijednošću *IG*. Iz prikazane tablice uočava se kako, primjerice, značajka z12 gotovo u potpunosti umanjuje entropiju zavisne značajke (*IG*=1,832) dok određene značajke (npr. z67, z39, z37) ne pridonose smanjenju entropije zavisne značajke (*IG*=0).

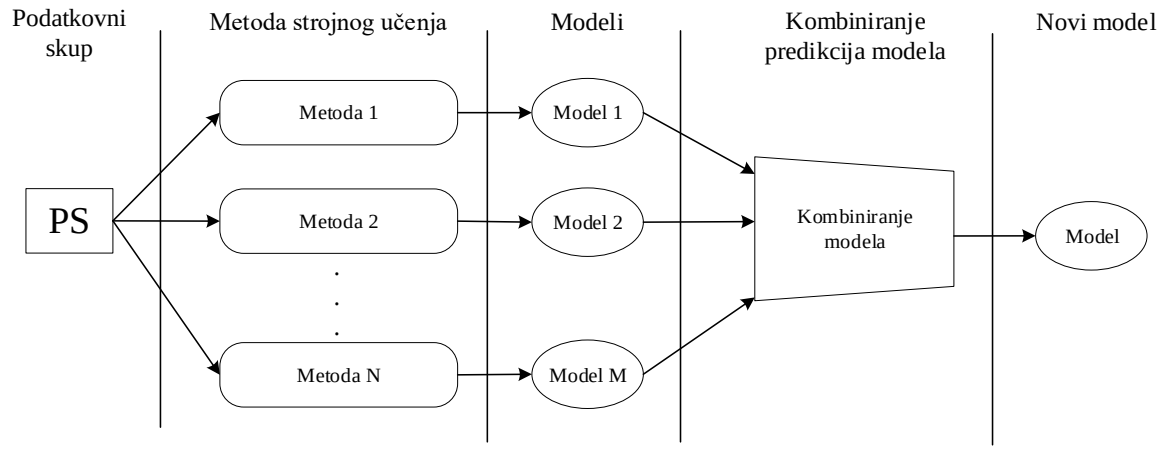
Tablica 5.11 Prikaz vrijednosti informacijske dobiti kao osnove za odabir podskupa relevantnih nezavisnih značajki

R.br.	IG vrijednost	Oznaka značajke	R.br.	IG vrijednost	Oznaka značajke	R.br.	IG vrijednost	Oznaka značajke
1.	1,831	z71	27.	1,2383	z27	53.	0,171	z51
2.	1,831	z12	28.	1,2116	z15	54.	0,1671	z54
3.	1,7287	z11	29.	1,2116	z60	55.	0,1101	z58
4.	1,7287	z69	30.	1,2021	z20	56.	0,1058	z53
5.	1,7279	z17	31.	1,2015	z80	57.	0,1058	z38
6.	1,7133	z46	32.	1,1743	z31	58.	0,0233	z50
7.	1,6839	z13	33.	1,1615	z29	59.	0	z66
8.	1,6836	z49	34.	1,1105	z83	60.	0	z37
9.	1,6178	z25	35.	1,1008	z36	61.	0	z52
10.	1,5472	z19	36.	1,0894	z26	62.	0	z39
11.	1,5472	z61	37.	1,0516	z42	63.	0	z55
12.	1,5247	z47	38.	1,0341	z41	64.	0	z40
13.	1,5182	z30	39.	0,997	z18	65.	0	z75
14.	1,5179	z35	40.	0,9598	z21	66.	0	z56
15.	1,501	z48	41.	0,9487	z79	67.	0	z65
16.	1,4204	z59	42.	0,726	z78	68.	0	z64
17.	1,374	z73	43.	0,6428	z68	69.	0	z67
18.	1,318	z23	44.	0,6428	z9	70.	0	z62
19.	1,3006	z16	45.	0,5977	z14	71.	0	z72
20.	1,29	z28	46.	0,5942	z45	72.	0	z57
21.	1,2837	z33	47.	0,5809	z74	73.	0	z63
22.	1,2761	z8	48.	0,4579	z70	74.	0	z81
23.	1,2727	z24	49.	0,4579	z10	75.	0	z77
24.	1,2675	z82	50.	0,4032	z22	76.	0	z76
25.	1,2488	z32	51.	0,3145	z44			
26.	1,2467	z34	52.	0,3103	z43			

Prema navedenome, skup od 76 dodatno je reduciran na 58 nezavisnih značajki. Pri tome su razmatrane one značajke koje zadovoljavaju uvjet $IG > 0$. Dobiveni podskup značajki ne može se smatrati konačnim budući da je u fazi razvoja modela klasifikacije SHIoT uređaja potrebno dodatno ispitati performanse modela ukoliko se uklone značajke s manjim IG vrijednostima. Cilj je koristiti minimalan skup značajki koji daje najbolje performanse modela klasifikacije u svrhu smanjenja vremena potrebnog za predviđanje klase, smanjenje kompleksnosti te smanjenje pojave pristranosti modela.

5.6 Razvoj modela klasifikacije SHIoT uređaja

U svrhu razvoja modela višeklasne klasifikacije SHIoT uređaja korištena je *logitboost* metoda. Korištena metoda pripada ansambl (engl. *ensemble*) skupini metoda strojnog učenja, a temelji se na statističkoj metodi logističke regresije. Ansambli kombiniraju veći broj modela, kako je prikazano slikom 5.6, pri čemu svaki model rješava izvorno postavljeni problem, a s ciljem dobivanja boljeg kompozitnog globalnog modela s boljim performansama nego kod primjene jednog modela [217].



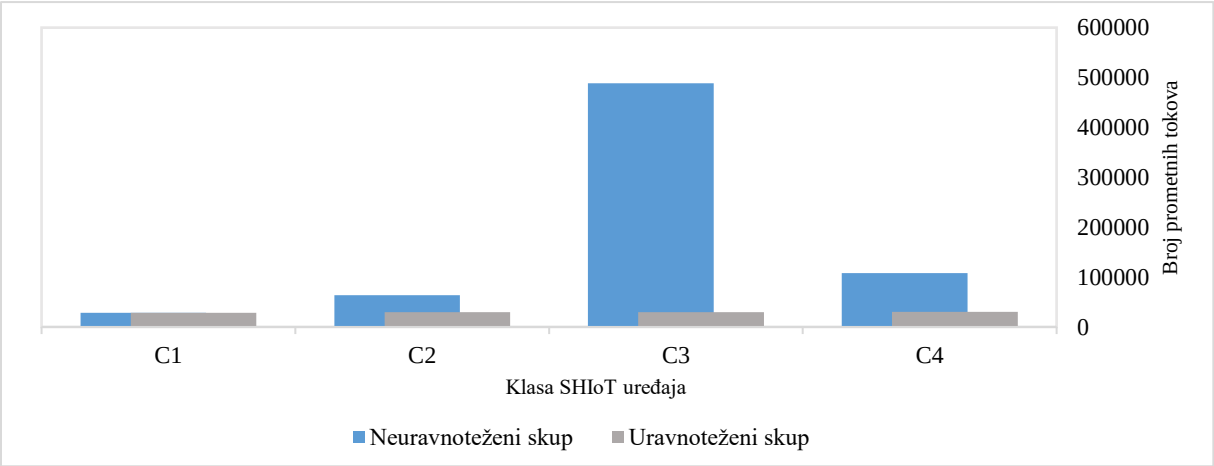
Slika 5.6 Poopćeni prikaz rada ansambl metoda strojnog učenja

Boosting pripada skupu ansambl metoda koje su u mogućnosti pretvoriti više „slabih“ klasifikatora (modela koji predviđaju ciljanu klasu u ovisnosti o vrijednostima značajki promatranih vektora značajki) u „snažne“ klasifikatore. Općenito, „slabi“ klasifikator je model čija je točnost predikcije klase neznatno bolja od nasumičnog pogađanja dok je snažan klasifikator karakteriziran performansama koje su blizu idealnih. *Boosting* metode pokazale su se kao prikladna klasifikacijska tehnika koja pruža dobre rezultate pri rješavanju problema iz različitih domena [218]. S obzirom na klasifikacijski problem koji se nastoji riješiti i na dokazanu učinkovitost *boosting* skupine metoda strojnog učenja, u ovom istraživanju korištena je *logitboost* metoda.

5.6.1 Podatkovni skup korišten pri razvoju modela klasifikacije SHIoT uređaja

Klasifikacijski model, kojemu je cilj utvrditi klasu kojoj uređaj pripada na temelju značajki prometnog toka koji generira, temeljen je na značajkama prometnih tokova prikupljenim u vremenskom periodu od 10 dana za svaki uređaj. Vektori značajki prometnih tokova ekstrahirani za SHIoT uređaje označeni su odgovarajućom klasom (tablica 5.10). Broj prometnih tokova generiranih u promatranom vremenskom periodu ovisan je o karakteristikama pojedinog SHIoT uređaja.

Grafikon 5.4 Distribucija prometnih tokova prema klasama SHIoT uređaja



Inicijalni podatkovni skup, prema prethodno navedenome, ima karakteristiku neuravnoteženoga podatkovnog skupa i sadrži ukupno 681684 vektora značajki distribuiranih u četiri klase prema grafikonu 5.4. Stoga je, prije razvoja klasifikacijskog modela, broj prometnih tokova u korištenom podatkovnom skupu uravnotežen (stratificiran) metodom poduzorkovanja (engl. *under-sampling)* većinski zastupljene klase uz uvažavanje zastupljenosti prometnih tokova pojedinog uređaja u inicijalnom podatkovnom skupu. Razlog za ovakav pristup je mogućnost pojave pristranosti modela onoj klasi koja sadrži najveći broj vektora značajki te je prema [219] nužno stratificirati klase prije razvoja modela. Nakon provedene stratifikacije, podatkovni skup sadrži 117 423 vektora značajki korištenih za daljnji razvoj klasifikacijskog modela.

5.6.2 Primjena metode aditivne logističke regresije za višeklasnu klasifikaciju SHIoT uređaja

Aditivna logistička regresija (*logitboost*) predstavlja metodu nadziranog strojnog učenja koju je moguće promatrati kao generalizaciju klasične statističke metode logističke regresije. *Logitboost* metoda razvijena je 2000. godine i predstavljena u istraživanju [220].

5.6.2.1 Metoda logističke regresije

Metoda logističke regresije modelira uvjetnu vjerojatnost pripadanja promatranog primjera određenoj klasi *Pr(G=j|X=x)* za *J* klasu, pri čemu je moguće odrediti klase nepoznatih primjera prema izrazu (8).

$$j = \underset{j}{\operatorname{argmax}}\, Pr(G = j|X = x) \tag{8}$$

Gdje je

j – *j*-ta klasa iz skupa klasa *G*

G – skup klasa (1,…,*J*)

x – nezavisna značajka iz skupa *X*

X – skup nezavisnih značajki

Logistička regresija modelira vjerojatnosti korištenjem linearnih funkcija u *x* dok istovremeno osigurava da njihov zbroj ostane u granicama [0,1]. Model je specificiran u uvjetima *J* – 1 *log-odds*[18] koji razdvajaju svaku klasu od „osnovne“ klase *J* prema izrazima (9)-(11).

$$log\,\frac{Pr[G = j|X = x]}{Pr[G = J|X = x]} = \beta_j^T x_i; j = 1,..,J-1 \tag{9}$$

Gdje je:

β_j – logistički koeficijent nezavisne značajke za klasu *j*

$$Pr(G = j|X = x) = \frac{e^{\beta_j^T x_i}}{1 + \sum_{l=1}^{J-1} e^{\beta_l^T x_i}}; j = 1,..,J-1 \tag{10}$$

$$Pr(G = J|X = x) = \frac{1}{1 + \sum_{l=1}^{J-1} e^{\beta_l^T x_i}} \tag{11}$$

U izrazu (9) podrazumijeva se višeklasni klasifikacijski model u kojemu je x_i *i*-ti vektor značajki, a *J* predstavlja klasu gdje je $j \in \{0,1,2,..,J-1\}$ uz uvjet da je $J \geq 3$. Ovakav model postavlja linearne granice između područja koja odgovaraju različitim klasama. Pa tako, primjeri (x_i) koji leže na granici između dvije klase (*j* i *J*) su oni za koje vrijedi *Pr(G=j|X=x)=Pr (G=J|X=x)* što je i ekvivalent *log odds*=0. Prilagodba modela logističke regresije

[18] Logaritam izgleda događaja

podrazumijeva procjenu parametra β_j pri čemu je standardna statistička procedura pronaći maksimum funkcije vjerodostojnosti (engl. *likelihood function*) [221].

5.6.2.2 Logitboost metoda

U modelima temeljenim na logističkoj regresiji ne postoji jedinstvena metoda procjene parametra β_j što bi rezultiralo maksimiziranjem funkcije vjerodostojnosti, već je potrebno koristiti optimizacijske metode. Na taj način do maksimuma funkcije vjerodostojnosti dolazi se iterativnim postupkom. *Logitboost* predstavlja jednu od takvih metoda koja je korištena u ovom istraživanju, a temelji se na metodi multinomne ordinalne logističke regresije zbog postojanja više od dvije zavisne značajke čije vrijednosti prate prirodan slijed. Općenito, *logitboost* poprima formu prikazanu izrazom (12).

$$Pr(G = j|X = x) = \frac{e^{F_j(x)}}{\sum_{k=1}^{J} e^{F_k(x)}}; \sum_{k=1}^{J} F_k(x) = 0 \qquad (12)$$

Gdje je:

$F_j(x)$ – funkcija nezavisne značajke (x)

Funkcije $F_j(x) = \sum_{m=1}^{M} f_{mj}(x)$ i f_{mj} funkcije nezavisnih značajki. U svakoj iteraciji m $(m \in \{1,2,\ldots, M\})$, primjeru ($x_i$) koji je pogrešno klasificiran, povećava se težinski koeficijent (w) dok se ispravno klasificiranom primjeru težinski koeficijent smanjuje. Na taj način m-ti „slabi“ klasifikator f_m usredotočuje se na primjere koji su u prethodnim iteracijama pogrešno klasificirani.

Logitboost metoda

1. Dodijeli početne težine primjerima $w_{i,j} = 1/N$, $i = 1,2,..,N$, $j = 0,1,..,J$, $F_j(x)=0$, $p_j(x) = 1/(J+1)$ $\forall j$.
2. Ponavljaj za m=1,2,..,M:
   - Ponavljaj za j=0,1,..,J:
     - Izračunaj radne odgovore i težine za klasu j

       $z_{ij} = \frac{y_{ij} - p_j(x_i)}{p_j(x_i)(1 - p_j(x_i))}$;

       $w_{ij} = p_j(x_i)\left(1 - p_j(x_i)\right)$.

     - Prilagodi funkciju $f_{mj}(x)$ s težinskom regresijom najmanjih kvadrata od z_{ij} za x_i uz težine w_{ij}
   - Postavi $f_{mj}(x) \leftarrow \frac{J-1}{J}\left(f_{mj}(x) - \frac{1}{J}\sum_{k=1}^{J} f_{mk}(x)\right)$,

$$F_j(x) \leftarrow F_j(x) + f_{mk}(x)$$

- Ažuriraj $p_j(x) = \frac{e^{F_j(x)}}{\sum_{k=1}^{J} e^{F_k(x)}}$

3. Izlazni klasifikacijski model $argmax_j F_j(x)$

Slika 5.7 Prikaz *logitboost* metode [218]

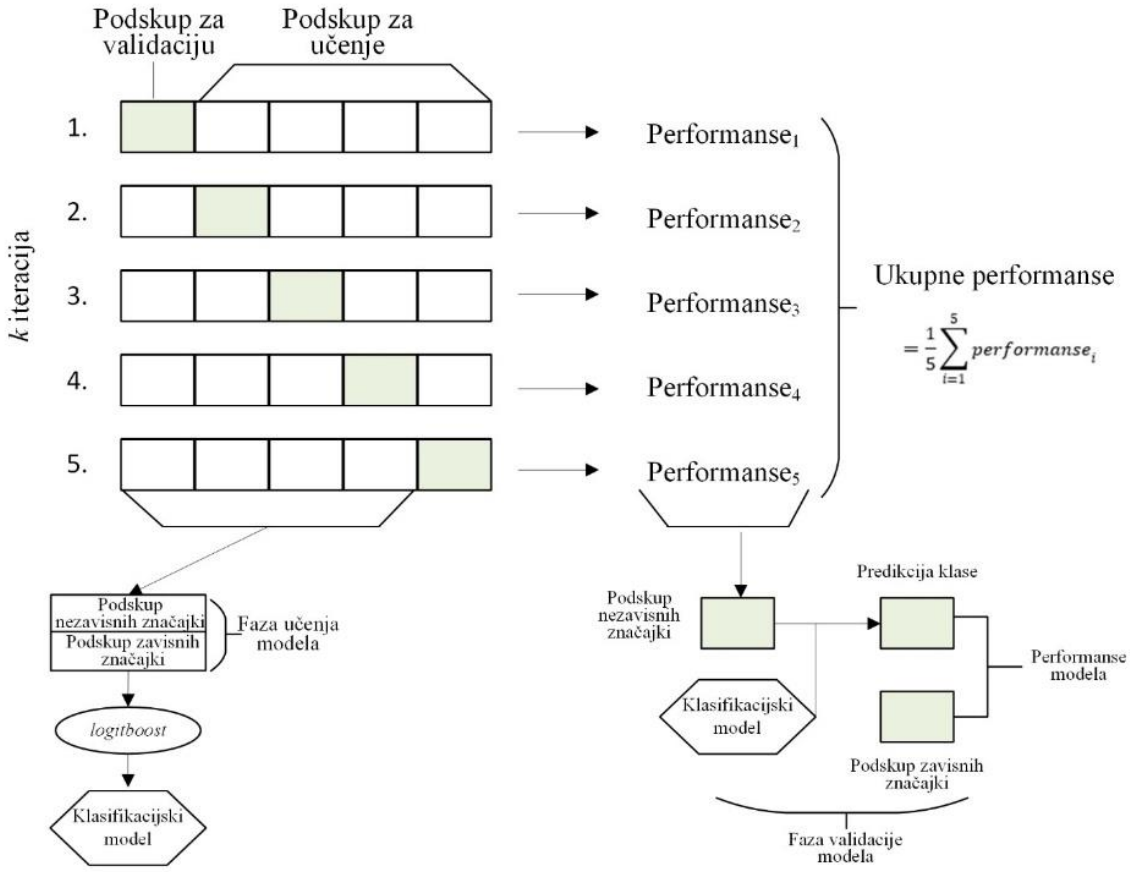
Izlaz *logitboost* metode predstavlja skup $J+1$ funkcija odgovora $\{F_j(x);\ j=0,1,\ldots,J\}$ kako je prikazano slikom 5.7. Pri tome je svaki $F_j(x)$ linearna kombinacija skupa „slabih" klasifikatora.

5.6.3 Analiza rezultata i ocjena performansi modela klasifikacije SHIoT uređaja

Razvoj, testiranje i validacija modela provedeni su korištenjem programskog alata WEKA uz potporu MS Excel 2016 tijekom pripreme podatkovnog skupa za razvoj modela. Budući da je u podpoglavlju 5.5 korištenjem metode informacijske dobiti odabrano ukupno 59 značajki, tijekom razvoja modela broj značajki je postepeno reduciran kada su uspoređene validacijske mjere za svaki model. Cilj ovog postupka je razvoj modela koji će koristiti najmanji mogući broj nezavisnih značajki koji neće značajno negativno utjecati na njegove performanse.

Svaki model je validiran *k*-strukom unakrsnom validacijom uz *k*=10. Princip rada *k*-struke unakrsne validacije za *k*=5 prikazan je slikom 5.8. Unakrsna validacija je statistička metoda namijenjena procjeni performansi modela strojnog učenja na novim, neviđenim podatcima. Ova metoda koristi se za procjenu ponašanja modela nad podatcima koji nisu korišteni u fazi učenja. Pri tome model se primjenjuje iterativno *k* puta nad podatkovnim skupom. U svakoj iteraciji podatkovni skup se dijeli na *k* dijelova. Jedan dio skupa koristi se za validaciju modela dok se preostalih *k*-1 dijelova skupa objedinjuje u podskup za učenje modela.

Tablicama 5.12 - 5.15 prikazane su performanse i rezultati validacijskih mjera za ukupno pet modela (M1,…,M5) uz različiti broj korištenih nezavisnih značajki (M1 - 59 značajki, M2 – 48 značajki, M3 – 33 značajki, M4 – 13 značajki i M5 – 8 značajki). Značajke su reducirane prema najmanjoj vrijednosti *IG* (tablica 5.11). Inicijalni podatkovni skup podijeljen je u omjeru 70/30 pri čemu je 70 % primjera u skupu korišteno za učenje modela dok je 30 % korišteno za testiranje modela. Ovakva podjela je uz 60/40 i 80/20 uobičajena u razvoju modela temeljenih na metodama strojnog učenja [222].



Slika 5.8 Prikaz *k*-struke unakrsne validacije uz *k*=5 [222]

Performanse klasifikacijskog modela temeljenog na strojnom učenju potrebno je izraziti kroz više različitih mjera, posebno kada je model višeklasni, s obzirom da svaka mjera ima prednosti i ograničenja [223]. Točnost je jedna od tih mjera koja predstavlja udio točno klasificiranih primjera u skupu svih primjera prema izrazu (13) gdje je *TP* (stvarno pozitivni primjeri), *TN* (stvarno negativni primjeri), *FP* (lažno pozitivni primjeri) i *FN* (lažno negativni primjeri).

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \tag{13}$$

Gdje je:

Acc – udio točno klasificiranih primjera u skupu svih primjera

TP – broj stvarno pozitivnih primjera

TN – broj stvarno negativnih primjera

FP – broj lažno pozitivnih primjera

FN – broj lažno negativnih primjera

Iz tablice 5.12 vidljivo je da svi modeli imaju približno jednaku točnost klasifikacije (≈ 99,8 %). Pad točnosti uočava se tek kod modela M5 koji koristi osam nezavisnih značajki. Pri tome točnost klasifikacije iznosi 99,71 %, odnosno 336 pogrešno klasificiranih primjera. Iz prikazane tablice uočava se neznatni pad točnosti klasifikacije za model M4 (99,7956 %) u odnosu na model M1 (99,8075 %) koji koristi svih 59 značajki.

Tablica 5.12 Prikaz performansi modela klasifikacije SHIoT uređaja

	M1 – 59	M2 – 48	M3 - 33	M4-13	M5 - 8
Točno klasificirani primjeri	117197 (99,8075 %)	117188 (99,7999 %)	117178 (99,7914 %)	117183 (99,7956 %)	117087 (99,7139 %)
Pogrešno klasificirani primjeri	226 (0,1933 %)	235 (0,2001 %)	245 (0,2086 %)	240 (0,2044 %)	336 (0,2861 %)
Kappa koeficijent (κ)	0,9974	0,9973	0,9972	0,9973	0,9962
Ukupno primjera	117423				

Kappa koeficijent (κ) izražava mjeru uspješnosti promatranog modela prema idealnom uz korekciju slučajnog izbora [224]. Vrijednosti *kappa* koeficijenta kreću se u intervalu [0,1] pri čemu je κ = 0 - 0,2 izrazito loš model, κ = 0,2 - 0,39 loš model, κ = 0,4 – 0,59 umjeren model, κ = 0,6 - 0,79 dobar model, κ = 0,8 - 0,9 vrlo dobar model o κ = 0,9 – 1 odličan model. Prema prikazanoj skali i rezultatima vidljivima u tablici 5.12, svi modeli pokazuju odlične karakteristike prema *kappa* koeficijentu pri čemu model M4 pokazuje minimalno odstupanje od modela M1 (0,0001) uz značajnu redukciju korištenih nezavisnih značajki.

Dodatne validacijske mjere izražene su kroz osjetljivost, odnosno stopu ili učestalost stvarno pozitivnih (engl. *True Positive Rate, TPR*) i stopu ili učestalost lažno pozitivnih primjera (engl. *False Positive Rate, FPR*) i prikazane su tablicom 5.13.

Tablica 5.13 Prikaz validacijskih mjera modela (*TPR* i *FPR*)

Klasa	**Stopa stvarno pozitivnih primjera (*TPR*)**					**Stopa lažno pozitivnih primjera (*FPR*)**				
	M1 - 59	**M2 – 48**	**M3 - 33**	**M4-13**	**M5 - 8**	**M1 - 59**	**M2 – 48**	**M3 - 33**	**M4-13**	**M5 - 8**
C1	0,998	0,998	0,997	0,997	0,997	0,001	0,001	0,001	0,001	0,001
C2	0,999	0,999	0,999	0,999	0,999	0	0	0	0	0,001
C3	0,998	0,998	0,998	0,998	0,997	0,001	0	0,001	0	0,001
C4	0,997	0,997	0,997	0,997	0,996	0,001	0,001	0,001	0,001	0,001

Stopa stvarno pozitivnih rezultata predstavlja točno klasificirane primjere klase u skupu svih primjera dodijeljenih toj klasi prema izrazu (14). Stopa lažno pozitivnih primjera predstavlja odnos pogrešno klasificiranih primjera klase u skupu svih primjera dodijeljenih toj klasi prema izrazu (15).

$$TPR = \frac{TP}{TP + FN} \tag{14}$$

Gdje je:

TPR – stopa stvarno pozitivnih rezultata

$$FPR = \frac{FP}{FP + TN} \tag{15}$$

Gdje je:

FPR – stopa lažno pozitivnih primjera

Iz tablice 5.13 uočava se da modeli M1 i M2 pružaju najbolje rezultate prema *TPR* mjeri za klasu C1, za klasu C2 svi promatrani modeli pružaju iste rezultate, dok za klase C3 i C4 model M5 pruža nešto lošije rezultate u odnosu na ostale. S aspekta *FPR* mjere modeli M2 i M4 pružaju bolje ili jednako dobre rezultate u odnosu na ostale modele pri čemu model M5 pruža najlošije rezultate.

Dodatne validacijske mjere koje pokazuju kvalitetu klasifikacijskog modela su preciznost ili vrijednost pozitivne predikcije (engl. *precision, Positive Predictive Value, STRV*) i F-mjera prikazani tablicom 5.14 te *ROC* (engl. *Reciver Operating Characteristics*) i *PRC* (engl. *Precision-Recall Curve*) krivulje čije su vrijednosti prikazane tablicom 5.15.

Tablica 5.14 Prikaz validacijskih mjera modela (*F*-mjera i preciznost)

Klasa	**Preciznost**					***F*-mjera (*F1* ocjena)**				
	M1 - 59	**M2 – 48**	**M3 - 33**	**M4-13**	**M5 - 8**	**M1 - 59**	**M2 – 48**	**M3 - 33**	**M4-13**	**M5 - 8**
C1	0,998	0,997	0,997	0,997	0,995	0,998	0,997	0,997	0,997	0,996
C2	0,999	0,999	0,999	0,999	0,998	0,999	0,999	0,999	0,999	0,999
C3	0,998	0,999	0,998	0,999	0,998	0,998	0,998	0,998	0,998	0,998
C4	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,997	0,996

Mjera preciznosti koristi se za iskazivanje broja ispravno klasificiranih primjera u odnosu na ukupan broj primjera koji pripadaju toj klasi prema izrazu (16).

$$PPV = \frac{TP}{TP + FP} \tag{16}$$

Gdje je:

STRV – vrijednost pozitivne predikcije

Prema vrijednostima izraženim tablicom 5.14 vidljivo je da za klasu C1 najbolje rezultate daje model M1 dok su najlošiji rezultati vidljivi kod modela M5. Za klase C2 i C4 uočavaju se jednako dobri rezultati za sve modele uz iznimku modela M5 za klasu C2 dok za klasu C3 najbolje rezultate pružaju modeli M2 i M4.

F-mjera ili *F1* ocjena predstavlja harmonijsku srednju vrijednost mjera preciznosti i *TPR* prema izrazu (17) [223]. Prema [225], harmonijska srednja vrijednost je intuitivnija nego klasična aritmetička srednja vrijednost za izračunavanje srednje vrijednosti odnosa.

$$F1 = \frac{2(PPV \cdot TPR)}{PPV + TPR} \tag{17}$$

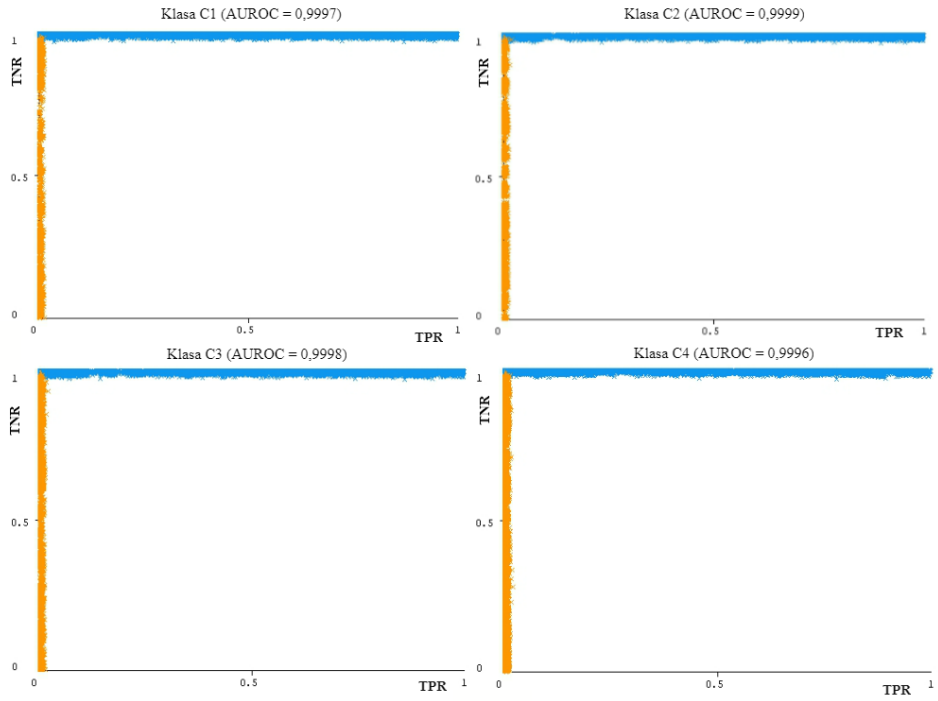
Izračunate vrijednosti F-mjere prikazane tablicom 5.14 ukazuju na model M5 kao najlošiji promatrano s aspekta klasa C1 i C4 dok ostali modeli pokazuju približno jednake rezultate.

Tablicom 5.15 prikazane su vrijednosti *ROC* i *PRC* validacijskih mjera. *ROC* krivulja, odnosno AUROC (engl. *Area Under The ROC Curve*) površina ispod *ROC* krivulje predstavlja jednu od najvažnijih i najčešće korištenih mjera koje pokazuju kvalitetu klasifikacijskog modela. ROC je, iako u ovom slučaju izražena tablično, grafička reprezentacija odnosa stope stvarno pozitivnih klasifikacija (*TPR*) i specifičnosti, odnosno stope stvarno negativnih klasifikacija (*TNR* = 1 - *FPR*). Primjer grafičkog prikaza *ROC* krivulje vidljiv je na slici 5.9 za model M4. Pri tome se površina ispod krivulje, *AUROC*, interpretira kao prosječna vrijednost *TPR* za sve vrijednosti *TNR* u intervalu [0,1]. Što je *AUROC* bliže vrijednosti 1, to su performanse klasifikacijskog modela bolje. Donja vrijednost 0,5 predstavlja performanse modela jednake slučajnom pogađanju [226]. Vrijednosti prikazane tablicom 5.15 ukazuju na izuzetno dobre performanse svih promatranih modela, odnosno gotovo sve *AUROC* vrijednosti su vrlo blizu vrijednosti 1.

Tablica 5.15 Prikaz validacijskih mjera modela (*ROC* i *PRC*)

Klasa	***ROC***					**PRC**				
	M1 - 59	**M2 – 48**	**M3 - 33**	**M4-13**	**M5 - 8**	**M1 - 59**	**M2 – 48**	**M3 - 33**	**M4-13**	**M5 - 8**
C1	0,9999	0,9999	0,9998	0,9997	0,9998	0,999	1	0,999	0,998	0,999
C2	1	1	1	0,9999	0,9998	1	1	1	1	1
C3	0,9997	0,9999	0,9999	0,9998	0,9998	1	1	1	1	1
C4	0,9998	0,9999	0,9998	0,9996	0,9997	1	1	0,999	0,999	0,999

Alternativnu mjeru *ROC* krivulji predstavlja *PRC* (engl. *Precision-Recall Curve*) krivulja koja se često koristi u slučajevima neuravnoteženih podatkovnih skupova pri čemu kod *ROC* mjere velika promjena u broju lažno pozitivno klasificiranih primjera može rezultirati malom promjenom stope lažno pozitivno klasificiranih primjera.



Slika 5.9 Prikaz ROC krivulje za klasifikacijski model M4

Zbog toga, budući da *PRC* koristi odnos *STRV* i *TPR*, tj. fokusira se na pozitivno klasificirane primjere (*TP* i *FP*), može bolje prikazati utjecaj velikog broja negativnih primjera na performanse modela. Budući da je u ovom istraživanju podatkovni skup stratificiran, *PRC* mjera daje gotovo jednake rezultate kao i *ROC* mjera za sve promatrane modele.

Provedenom analizom rezultata model M4 odabran je kao optimalan model klasifikacije SHIoT uređaja s obzirom da njegove performanse prema svim prikazanim mjerama ne odstupaju značajno od ostalih promatranih modela (*TPR* 0 – 0,001, *FPR* 0 – 0,001, *STRV* 0 – 0,001, *F1* 0 – 0,001, *ROC* 0,0001 – 0,0003 i *PRC* 0 – 0,002) uz značajnu redukciju korištenih nezavisnih značajki. Točnost modela u predviđanju klasa SHIoT uređaja prema značajkama prometnog toka dana je i matricom konfuzije prikazanom tablicom 5.16.

Tablica 5.16 Matrica konfuzije za klasifikacijski model M4

Predviđena pripadnost klasi					
C1	**C2**	**C3**	**C4**		
28068	7	16	54	**C1**	*Stvarna pripadnost klasi*
12	29831	3	7	**C2**	
18	3	29331	28	**C3**	
57	12	23	29953	**C4**	

U modelu M4 korišteno je ukupno 13 nezavisnih značajki u odnosu na inicijalnih 59 koje su prema *IG* vrijednosti imale određeni utjecaj na zavisnu značajku. Korištene nezavisne značajke prikazane su tablicom 5.17.

Tablica 5.17 Korištene nezavisne značajke u procesu razvoja klasifikacijskog modela

Podskup značajki	Broj značajki	Oznaka značajke
Inicijalni skup	83	z1, z2, z3, z4, z5, z6, z7, z8, z9, z10, z11, z12, z13, z14, z15, z16, z17, z18, z19, z20, z21, z22, z23, z24, z25, z26, z27, z28, z29, z30,z31, z32, z33, z34, z35, z36, z37, z38, z39, z40, z41, z42, z43, z44, z45, z46, z47, z48, z49, z50, z51, z52, z53, z54, z55, z56, z57, z58, z59, z60, z61, z62, z63, z64, z65, z66, z67, z68, z69, z70, z71, z72, z73, z74, z75, z76, z77, z78, z79, z80, z81, z82, z83
Informacijska dobit	59	z9, z10, z11, z12, z13, z14, z15, z16, z17, z18, z19, z20, z21, z22, z23, z24, z25, z26, z27, z28, z29, z30, z31, z32, z33, z34, z35, z36, z38, z41, z42, z43, z44, z45, z46, z47, z48, z49, z50, z51, z53, z54, z58, z59, z60, z61, z68, z69, z70, z71, z73, z74, z78, z79, z8, z80, z82, z83
Model M4	13	z11, z12, z13, z17, z19, z25, z30, z46, z47, z49, z61, z69, z71

Kako je iz tablice vidljivo, najrelevantnije značajke odnose se na informacije povezane s duljinom paketa u promatranom prometnom toku (z11 – ukupna duljina poslanih paketa u prometnom toku; z12 – ukupna duljina primljenih paketa; z13 – maksimalna duljina poslanih paketa; z17 – maksimalna duljina primljenih paketa; z19 – srednja vrijednost duljine primljenih paketa; z46 – maksimalna duljina paketa; z47 – srednja vrijednost duljine paketa; z49 – varijacija duljine paketa), zatim informacije o međudolaznim vremenima paketa u prometnom toku (z25 – maksimalno međudolazno vrijeme paketa u prometnom toku; z30 – maksimalno vrijeme između dva uzastopno poslana paketa u prometnom toku). Relevantnima su se pokazale i značajke koje pružaju informacije o segmentima u prometnom toku (z61 – prosječna veličina primljenog segmenta) kao i značajke koje pružaju informacije o količini podataka prenesenih u podtoku[19] (z60 – količina podataka poslana u podtoku; z71 – količina podataka primljena u podtoku).

5.7 Definiranje profila legitimnog prometa za klase SHIoT uređaja

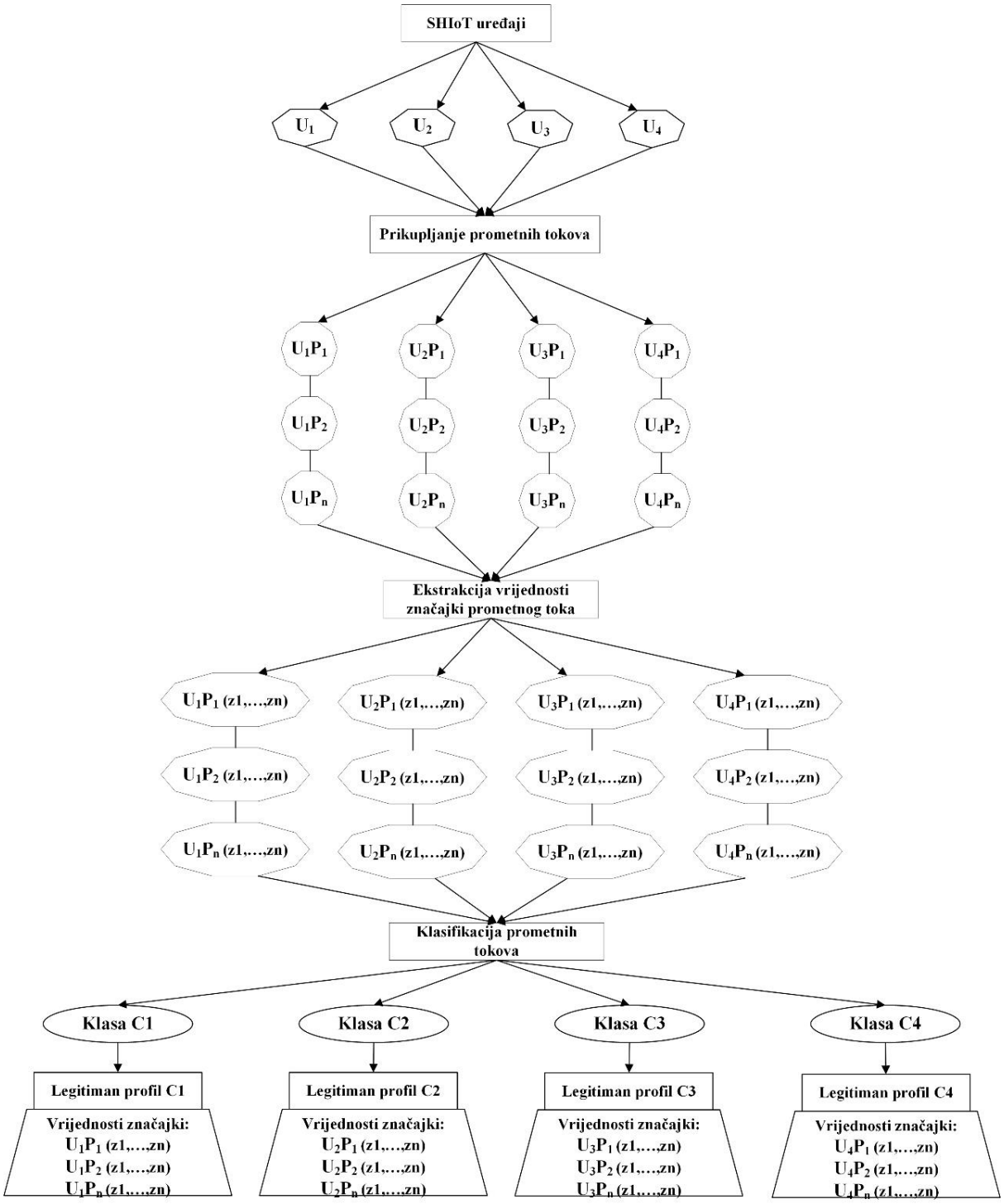
Problem brzorastućeg i sveprisutnog okruženja koje predstavlja IoT, a time i SHIoT kao podskupina IoT koncepta, ogleda se u kontinuiranosti pojave novih uređaja na tržištu koji posjeduju različite funkcionalnosti i nalaze primjenu u trenutno nepoznatim scenarijima. Prema tome, novi, nepoznati SHIoT uređaji mogu posjedovati funkcionalnosti različite od onih koje

[19] Podtok prometnog toka rezultat je *multipath* TCP veze koja se koristi za definiranje komunikacijskog puta između dva krajnja uređaja, a ne između dva komunikacijska sučelja, kao što je to slučaj kod standardne TCP veze. Standardna TCP veza omogućava samo jedan komunikacijski link temeljen na izvorišnoj i odredišnoj IP adresi i komunikacijskim portovima. *Multipath* TCP veza omogućava korištenje više komunikacijskih puteva i stvaranje TCP veze na svakom od njih [229]. Detaljan princip rada protokola objašnjen je u RFC 6824.

posjeduju trenutno dostupni SHIoT uređaji. Navedeno predstavlja izazov u identifikaciji takvih uređaja i poznavanju njihovog legitimnog ponašanja što čini osnovu za detekciju anomalija u ponašanju kao što je generiranje DDoS prometa.

U svrhu razvoja modela detekcija DDoS prometa na temelju prethodno definiranih klasa SHIoT uređaja, potrebno je definirati profil legitimnog prometa svake klase uređaja. Kod razvoja svakog modela detekcije anomalija temeljenog na nadziranim metodama strojnog učenja, potrebno je posjedovati skup podataka koji će predstavljati legitiman promet i skup podataka koji će predstavljati nelegitiman promet. Definirane klase SHIoT uređaja omogućuju uspostavu profila legitimnog prometa pojedine klase uređaja što je od važnosti u kasnijem razvoju modela detekcije anomalija. Pri tome vrijednosti značajki prometa SHIoT uređaja postaju dijelom legitimnog profila promatrane klase uređaja. Profil legitimnog prometa pojedine klase SHIoT uređaja definiran je vrijednostima značajki onih prometnih tokova koji su klasifikacijskim modelom dodijeljeni pojedinoj klasi SHIoT uređaja kako je prikazano slikom 5.10.

Neka je SHIoT uređaj predstavljen oznakom U_x, a prometni tok koji generira takav uređaj oznakom U_xPT_y. Svaki uređaj U_x predstavljen je kao skup prometnih tokova U_xPT_y, odnosno svaki uređaj sadrži skup prometnih tokova, $U_x = \{U_xPT_1,\ldots,U_xPT_y\}$. Tada je profil legitimnog prometa svake klase C definiran kao skup prometnih tokova koji su klasifikacijskim modelom identificirani kao dio klase C, odnosno $C_m=\{U_1PT_1,\ldots,U_xPT_y\}$; $m \in \{1,2,3,4\}$. *Ka*da je svaki prometni tok predstavljen svojim značajkama z, tada ga je moguće promatrati i kao skup vrijednosti značajki koje predstavljaju promatrani prometni tok, $U_xPT_y=\{z(U_xPT_y)_1, \ldots, z(U_xPT_y)_n\}$.



Slika 5.10 Prikaz procesa određivanja profila legitimnog prometa za klase SHIoT uređaja

Do sada prikazani rezultati istraživanja potvrđuju prvu hipotezu ovog doktorskog rada, odnosno da je na temelju vrijednosti značajki prometa koje generiraju SHIoT uređaji moguće definirati klase SHIoT uređaja i tako definirati profil legitimnog prometa pojedine klase. Uz to što je moguće definirati klase SHIoT uređaja, što je prikazano u podpoglavlju 5.4, moguće je i klasificirati uređaje, odnosno prometne tokove koje takvi uređaji generiraju korištenjem razvijenog klasifikacijskog modela i 13 značajki prometnog toka uz visoku točnost klasifikacije

(99,7956 %) što omogućava stvaranje profila legitimnog prometa pojedine klase SHIoT uređaja.

5.8 Razvoj modela detekcije nelegitimnog DDoS mrežnoga prometa

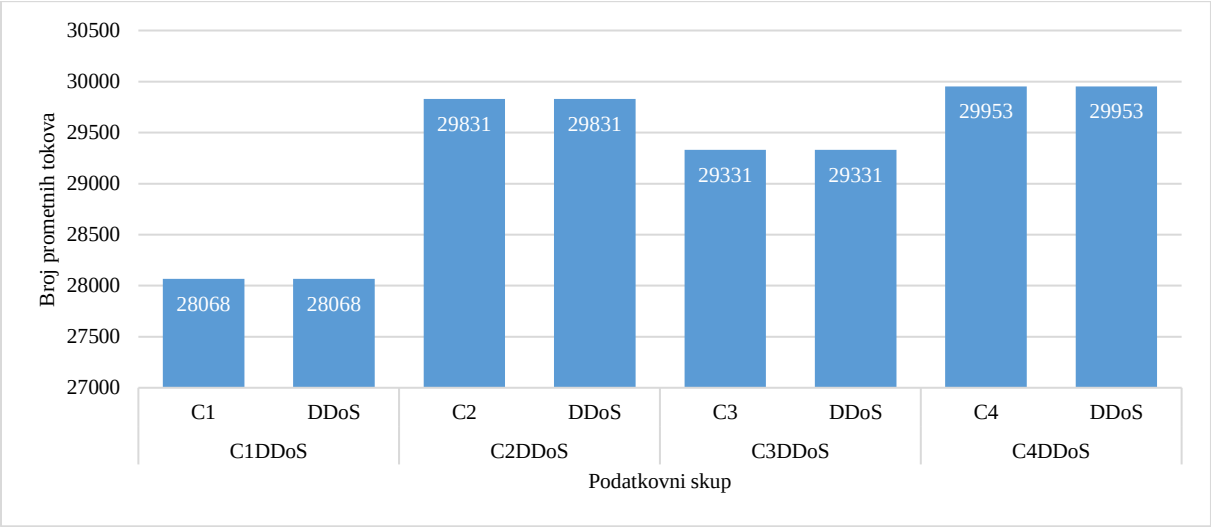
Prethodno realizirane i opisane aktivnosti u okviru ovog doktorskog istraživanja osnova su za razvoj modela detekcije anomalija mrežnoga prometa SHIoT uređaja koji se temelji na značajkama prometa i klasnoj pripadnosti uređaja. Klase SHIoT uređaja definirane istraživanjem omogućuju identifikaciju klasne pripadnosti uređaja na temelju prometnog toka koji uređaj generira. To ujedno omogućuje i stvaranje profila legitimnog prometa jer svaki prometni tok koji je klasifikacijskim modelom dodijeljen jednoj od četiri definirane klase postaje dijelom skupa koji predstavlja profil legitimnog prometa iste klase.

U svrhu razvoja modela detekcije nelegitimnog DDoS mrežnoga prometa korištena je metoda logističkih stabala odluke (engl. *Logistic Model Trees,* LMT). Za implementaciju metode i obradu podataka korišten je programski alat WEKA te podatkovni skupovi koji predstavljaju profile normalnog prometa proizašli kao rezultat modela klasifikacije SHIoT uređaja i podatkovni skupovi nelegitimnog DDoS prometa.

5.8.1 Podatkovni skupovi korišteni u razvoju modela detekcije anomalija

Za potrebe razvoja modela detekcije anomalija formirani su podatkovni skupovi koji sadrže združene vektore značajki profila legitimnog prometa svake klase SHIoT uređaja i DDoS prometa. Prema tome formirana su ukupno četiri podatkovna skupa (C1DDoS, C2DDoS, C3DDoS i C4DDoS). Inicijalno sva četiri skupa sadrže vrijednosti svih nezavisnih značajki prometnog toka (ukupno 83) navedenih u prilogu 3.

Grafikon 5.5 Broj i distribucija prometnih tokova korištenih u razvoju modela detekcije anomalija mrežnoga prometa



Broj i distribucija prometnih tokova u skupovima prikazana grafikonom 5.5 temelji se na skupu profila legitimnog prometa proizašlim iz klasifikacijskog modela SHIoT uređaja.

Kao i kod svakog razvoja modela strojnog učenja, cilj je koristiti one nezavisne značajke čija promjena ima najveći utjecaj na promjenu zavisne značajke. Isto tako važno je reducirati i one značajke koje mogu dovesti do pristranosti modela. Zato su, kao i kod razvoja modela klasifikacije SHIoT uređaja, iz inicijalnih podatkovnih skupova uklonjene nezavisne značajke od z1 do z7 koje predstavljaju identifikatore prometnog toka, a sadrže informacije o izvorišnim i odredišnim IP adresama, korištenim protokolima i vremenu generiranja prometnih tokova. Kao rezultat dobiven je skup od ukupno 76 nezavisnih značajki koje će biti promatrane u svrhu daljnjeg razvoja modela.

Tablica 5.18 Parcijalan prikaz podatkovnih skupova korištenih u razvoju modela detekcije anomalija mrežnoga prometa

R.br.	**z8**	**z9**	**z10**	**z11**	**z12**	**…**	**z23**	**…**	**z36**	**…**	**z83**	**Klasa**
							C1DDoS					
1.	110176901	5	4	372	648	…	13800000	…	113851	…	54900000	C1
2.	110117149	5	4	372	648	…	13800000	…	166655	…	54800000	C1
3.	110119161	5	4	372	648	…	13800000	…	104640	…	54900000	C1
4.	4307304	12	1	366	40	…	358942	…	0	…	0	C1
5.	55120696	3	3	186	494	…	11000000	…	100485	…	54900000	C1
6.	110105251	5	4	372	648	…	13800000	…	113492	…	54900000	C1
7.	110099556	5	4	372	648	…	13800000	…	106592	…	54900000	C1
8.	110204528	5	4	372	648	…	13800000	…	117421	…	54900000	C1
9.	105583649	10	2	0	0	…	9598510000000000	…	6549	…	5825650	DDoS
10.	114974487	13	1	0	0	…	8844190000000000	…	0	…	5402915	DDoS
							C2DDoS					

1.	32421069	12	12	2973	6626	…	1409612	…	76	…	0	C2
2.	119994320	8	5	724	913	…	9999527	…	214652	…	29800000	C2
3.	101213499	7	9	255	425	…	6747567	…	2704	…	7896986	C2
4.	32939864	12	12	2975	6626	…	1432168	…	91	…	0	C2
5.	62977269	1	3	32	794	…	21000000	…	14796	…	62900000	C2
6.	33378868	12	12	2978	6626	…	1451255	…	71	…	0	C2
7.	107438715	7	9	255	425	…	7162581	…	4731	…	11000000	C2
8.	33110147	12	12	2974	6626	…	1439572	…	79	…	0	C2
9.	119998748	9	5	724	915	…	9230673	…	30000000	…	29800000	C2
10.	63201982	1	3	32	794	…	21100000	…	18035	…	63200000	C2
							C3DDoS					
1.	91127887	3	3	33	95	…	18225577	…	120725	…	90875582	C3
2.	47780	5	5	84	474	…	5309	…	2	…	0	C3
3.	1787369	1	1	146	146	…	1787369	…	0	…	0	C3
4.	232794	2	4	157	371	…	46559	…	881	…	0	C3
5.	7218295	1	1	146	146	…	7218295	…	0	…	0	C3
6.	90623459	7	5	123	205	…	8238496	…	131264	…	30017272	C3
7.	23377840	5	7	146	1194	…	2125258	…	861	…	0	C3
8.	90620131	7	5	123	205	…	8238194	…	131116	…	30024178	C3
9.	91127406	3	3	33	95	…	18225481	…	124302	…	90869902	C3
10.	8725432	20	20	3829	5010	…	223729	…	1	…	5932015	C3
							C4DDoS					
1.	119436915	16	18	5158	527	…	3619300	…	136	…	6167447	C4
2.	119436449	16	18	5158	527	…	3619286	…	136	…	6138410	C4
3.	736266	8	12	904	3156	…	38751	…	92	…	0	C4
4.	119489464	18	20	5952	527	…	3229445	…	159	…	6208411	C4
5.	119435509	16	18	5158	527	…	3619258	…	130	…	5036095	C4
6.	70078432	11	13	3053	527	…	3046888	…	149	…	5005368	C4
7.	868401	9	13	1357	3866	…	41352	…	96	…	0	C4
8.	884067	9	13	1357	3866	…	42098	…	104	…	0	C4
9.	110665346	19	21	5589	527	…	2837573	…	128	…	9437527	C4
10.	111033283	15	17	4737	527	…	3581719	…	147	…	5976015	C4

Tablicom 5.18 parcijalno su prikazani skupovi korišteni u procesu razvoja modela detekcije anomalija mrežnoga prometa. Svaki skup sastoji se od vrijednosti nezavisnih značajki pojedinog prometnog toka i pridružene odgovarajuće zavisne značajke koja predstavlja klasu. Klasa je u ovom slučaju binarna, odnosno može poprimiti dvije vrijednosti (0,1) što označava prometni tok kao legitiman za promatranu klasu ili nelegitiman, tj. prometni tok nastao kao rezultat generiranja DDoS prometa. Ovakav pristup nužan je za daljnji razvoj modela uz primjenu metode nadziranog strojnog učenja.

5.8.2 Primjena metode logističkih stabala odluke pri razvoju modela detekcije anomalija

Metoda LMT je *boosting* metoda nadziranog strojnog učenja koja predstavlja fuziju dviju često korištenih klasifikacijskih metoda, logističke regresije i stabala odluke s ciljem njihove međusobne nadogradnje. Metoda je razvijena 2003. godine i opisana u istraživanju [227]. Osnovni princip rada metode sastoji se od stvaranja stabala odluke i formiranja modela logističke regresije na čvorovima stabla. Modeli logističke regresije međusobno se nadograđuju u jedan jedinstveni model. Na taj način metoda logističke regresije služi za procjenu vjerojatnosti pripadanja pojedinog vektora značajki definiranoj klasi.

Za numeričke značajke (kakve se i nalaze u predočenim podatkovnim skupovima) odabire se značajka koja predstavlja čvor u kojemu je podjela „najčišća“. To podrazumijeva da maksimalan broj vektora značajki pripada jednoj klasi kada je vrijednost odabrane značajke ispod definiranog praga vrijednosti i drugoj klasi ako se promatra odabrana značajka iznad definiranog praga vrijednosti. Formalizirano, LMT model sastoji se od strukture stabla odluke koje sadrži unutarnje čvorove *N* i skup terminalnih čvorova *T*. *S* predstavlja cjelokupan skup podatka sa svim značajkama [221]. Tada stablo odluke dijeli skup *S* u disjunktne podskupove (regije) S_t. Svaka regija prezentirana je terminalnim čvorom stabla kako je prikazano izrazom (18).

$$\mathrm{S} = \bigcup_{t \in T} S_t, \qquad S_t \cap S_{t'} = \emptyset \;\; za \; t \neq t' \tag{18}$$

Gdje je:

S – skup svih vektora značajki

S_t – disjunktni podskup vektora značajki

t – terminalni čvor iz skupa terminalnih čvorova *T*

Za razliku od klasičnog stabla odluke, kod LMT metode se terminalnim čvorovima $t \in T$ asociraju funkcije logističke regresije, f_t umjesto oznake klase. Pri tome logistička regresija u obzir uzima podskup $Z_t \subseteq Z$ svih nezavisnih značajki u skupu podataka i modelira vjerojatnost pripadanja klasi prema izrazima (19) i (20).

$$Pr(G = j|X = x) = \frac{e^{F_j(x)}}{\sum_{k=1}^{J} e^{F_k(x)}} \tag{19}$$

$$F_j(x) = \alpha_0^j + \sum_{k=1}^{m} \alpha_{z_k}^j \cdot z_k \tag{20}$$

Gdje je

α^j – koeficijent nezavisne značajke *z*

z_k – nezavisna značajka iz skupa nezavisnih značajki $Z = \{z_1, \ldots, z_m\}$

Konačan LMT model poprima oblik dan izrazom (21).

$$f(x) = \sum_{t \in T} f_t(x) \cdot I(x \in S_t), \qquad I(x \in S_t) \begin{cases} 1 \; ako \; vrijedi \; x \in S_t \\ 0 \qquad u \; suprotnom \end{cases} \tag{21}$$

Kako navode istraživači u [221], cilj metode je prilagodba podatcima tako da logističko stablo odluke bude poopćeno (engl. *pruned*) do razine jednog modela logističke regresije, odnosno do korijenskog čvora stabla odluke (engl. *root node*) ukoliko je to moguće s obzirom na podatkovni skup nad kojim se metoda primjenjuje.

Odabir relevantnih nezavisnih značajki iz skupa svih značajki kod korištenja LMT metode nije potrebno raditi zasebno budući da ova metoda prilagođava (engl. *fitting*) regresijsku funkciju svakoj nezavisnoj značajki korištenjem najmanje kvadratne pogreške. Prema tom kriteriju, u konačni model uvrštavaju se one značajke koje rezultiraju najmanjom kvadratnom pogreškom.

Korištenjem WEKA programskog okruženja implementirana je opisana LMT metoda nad četiri podatkovna skupa (C1DDoS, C2DDoS, C3DDoS i C4DDoS) s ciljem razvoja LMT modela za svaku klasu SHIoT uređaja.

5.8.2.1 LMT model za C1 klasu SHIoT uređaja

Implementacijom LMT metode korištenjem WEKA programskog okruženja odabrane su nezavisne značajke s najvećim utjecajem na zavisnu značajku te je razvijen jedan model logističke regresije s obzirom da je stablo odluke poopćeno do korijenskog čvora. Prema tome na korijenskom čvoru stabla odluke definiran je pripadajući LMT model prema izrazima (22) i (23).

$$Pr(G = \mathrm{C1} | X = x) = \frac{e^{F_{C1}(x)}}{e^{F_{C1}(x)} + e^{F_{DDoS}(x)}} \tag{22}$$

$$Pr(G = \mathrm{DDoS} | X = x) = \frac{e^{F_{DDoS}(x)}}{e^{F_{C1}(x)} + e^{F_{DDoS}(x)}} \tag{23}$$

Funkcije F_{C1} i F_{DDoS} korištene su za određivanje vjerojatnosti pripadanja klasi tako da modeliraju utjecaj nezavisnih značajki na zavisnu značajku. Za klasu C1 model logističke regresije poprima izgled prikazan izrazima (24) i (25).

$$F_{C1}(x) = -1{,}37 + 0{,}02 \cdot z14 + 0{,}01 \cdot z18 + 3{,}29 \cdot \mathrm{z38} + 0{,}01 \cdot \mathrm{z46} + (-3{,}72) \cdot \mathrm{z50} + (-1{,}08) \cdot \mathrm{z51} + (-0{,}2) \cdot \mathrm{z54} + 0{,}88 \cdot \mathrm{z58} + 0{,}57 \cdot \mathrm{z74} \quad (24)$$

$$F_{DDoS}(x) = -F_{C1}(x) = 1{,}37 + (-0{,}02) \cdot z14 + (-0{,}01) \cdot z18 + (-3{,}29) \cdot \mathrm{z38} + (-0{,}01) \cdot \mathrm{z46} + 3{,}72 \cdot \mathrm{z50} + 1{,}08 \cdot \mathrm{z51} + 0{,}2 \cdot \mathrm{z54} + (-0{,}88) \cdot \mathrm{z58} + (-0{,}57) \cdot \mathrm{z74} \quad (25)$$

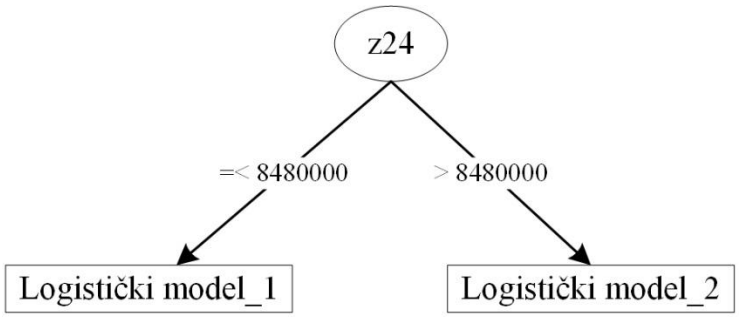
Modelom su obuhvaćene nezavisne značajke za koje je metodom najmanjeg kvadratnog odstupanja utvrđen najveći utjecaj na promjenu zavisne značajke. Svakoj značajki dodijeljeni su odgovarajući koeficijenti koji predstavljaju utjecaj nezavisnih na zavisnu značajku. Dodijeljeni koeficijent označava da će porast za jednu jedinicu nezavisne značajke promijeniti zavisnu značajku za iznos logaritma izgleda koeficijenata logističke regresije, dok će ostale nezavisne varijable ostati nepromijenjene.

Primjerice, koeficijent dodijeljen uz nezavisnu značajku z14 iznosi -0,02, a predstavlja procjenu promjene (povećanja ili smanjenja; što je određeno predznakom), u konkretnom slučaju smanjenje iznosa logaritma izgleda zavisne značajke ukoliko se nezavisna značajka z14 poveća za jednu jedinicu, a ostale nezavisne značajke u modelu ostanu nepromijenjene.

5.8.2.2 LMT model za C2 klasu SHIoT uređaja

LMT model detekcije anomalija mrežnoga prometa za klasu C2 SHIoT uređaja razvijen je na isti način kao i prethodno opisani model za klasu C1. Budući da različiti SHIoT uređaji pripadaju različitim klasama, intuitivno je jasno da se prometni tokovi koje generiraju SHIoT uređaji iz klase C2 prema vrijednostima značajki razlikuju od prometnih tokova SHIoT uređaja iz klase C1. Prema tome i model razvijen za ovu klasu uređaja, iako temeljen na istoj metodi, posjeduje određene različitosti. Prvenstveno se to odnosi na izgled stabla odluke, ali i na nezavisne značajke koje su uvrštene u model kao i koeficijenti pridodani tim značajkama. To znači da se nezavisne značajke koje utječu na promjenu zavisne značajke razlikuju od klase do klase SHIoT uređaja. S druge strane, moguće je da različite klase dijele iste relevantne

nezavisne značajke, ali s različitim stupnjem utjecaja pa imaju i dodijeljene različite koeficijente.



Slika 5.11 Primjer primjene LMT metode pri klasifikaciji vektora značajki

Za klasu C2 stablo odluke razlikuje se od onoga za klasu C1 jer na korijenskom čvoru nije moguće definirati modele logističke regresije koji bi pružili zadovoljavajuće performanse LMT modela. U ovom slučaju stablo odluke poopćeno je do razine tri čvora (jedan korijenski čvor i dva terminalna čvora) kako je i prikazano ranije na slici 5.11. Prema tome, na terminalnim čvorovima definirana su 2 logistička modela, LM1 prema izrazima (26) i (27) i LM2 prema izrazima (28) i (29) koji se primjenjuju ovisno o uvjetu koji je zadovoljen pri grananju stabla odluke.

$$F_{C2}(x) = -16{,}07 + 3{,}42 \cdot z10 + 4{,}35 \cdot z38 + 0{,}01 \cdot z41 + 0{,}01 \cdot z46 + (-2{,}06) \cdot z50 + (-0{,}39) \cdot z51 + 2{,}28 \cdot z54 + 0{,}97 \cdot z58 + 14{,}58 \cdot z74 \quad (26)$$

$$F_{DDoS}(x) = -F_{C2}(x) = 16{,}07 + (-3{,}42) \cdot z10 + (-4{,}35) \cdot z38 + (-0{,}01) \cdot z41 + (-0{,}01) \cdot z46 + 2{,}06 \cdot z50 + 0{,}39 \cdot z51 + (-2{,}28) \cdot z54 + (-0{,}97) \cdot z58 + (-14{,}58) \cdot z74 \quad (27)$$

$$F_{C2}(x) = -20{,}68 + 2{,}32 \cdot z38 + 0{,}01 \cdot z46 + (-2{,}06) \cdot z50 + (-0{,}39) \cdot z51 + 2{,}28 \cdot z54 + 0{,}84 \cdot z58 \quad (28)$$

$$F_{DDoS}(x) = -F_{C2}(x) = 20{,}68 + (-2{,}32) \cdot z38 + (-0{,}01) \cdot z46 + 2{,}06 \cdot z50 + 0{,}39 \cdot z51 + (-2{,}28) \cdot z54 + (-0{,}84) \cdot z58 \quad (29)$$

Uočava se kako se LMT model za detekciju anomalija mrežnoga prometa za SHIoT uređaje koji pripadaju klasi C2 sastoji od stabla odluke na čijim se terminalnim čvorovima

nalaze dva logistička modela i njihovo korištenje ovisi o tome koji uvjet zadovoljava promatrani vektor značajki s obzirom na vrijednost nezavisne značajke z24. O tom uvjetu ovisi i koje nezavisne značajke će biti uvrštene u logistički model kao i koeficijenti koji su pridruženi tim značajkama.

5.8.2.3 LMT model za C3 klasu SHIoT uređaja

Za klasu C3 SHIoT uređaja u svrhu detekcije anomalija mrežnoga prometa razvijen je LMT model na principu primijenjenom za klase C1 i C2. Jednako kao za klasu C1, stablo odluke poopćeno je do korijenskog čvora kojemu je pridružen jedan logistički model. Konačan oblik LMT modela, s najznačajnijim nezavisnim značajkama i njihovim koeficijentima za klasu C3 prikazan je izrazima (30) i (31).

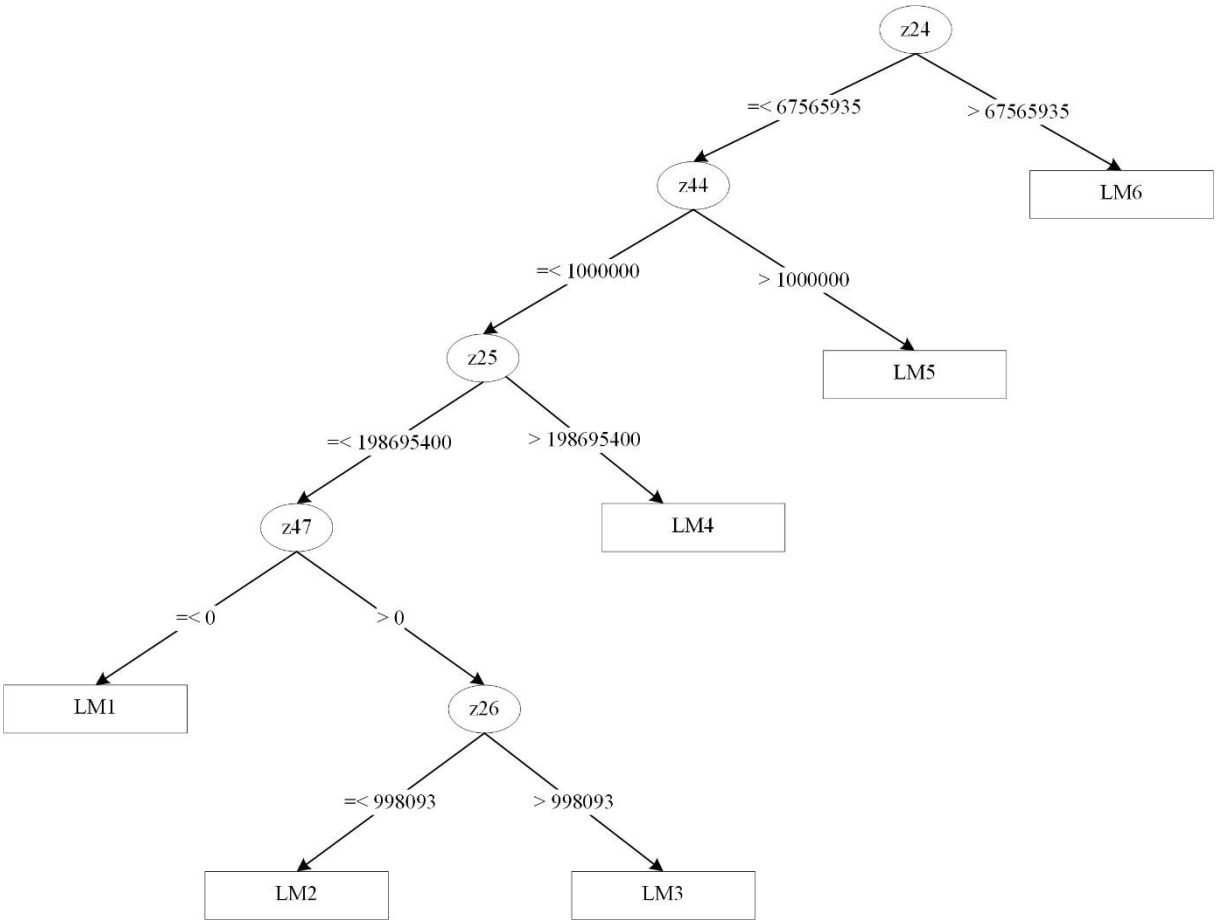
$$\begin{aligned} F_{C3}(x) = {} & -1{,}01 + 0{,}03 \cdot \mathrm{z14} + 2{,}91 \cdot z38 + 0{,}01 \cdot \mathrm{z45} + 0{,}02 \\ & \cdot \mathrm{z46} + (-2) \cdot \mathrm{z50} + (-1{,}82) \cdot \mathrm{z51} + 1{,}12 \cdot \mathrm{z54} \\ & + 0{,}87 \cdot \mathrm{z58} + 0{,}04 \cdot \mathrm{z74} \end{aligned} \tag{30}$$

$$\begin{aligned} F_{DDoS}(x) = {} & -F_{C3}(x) \\ & = 1{,}01 + (-0{,}03) \cdot \mathrm{z14} + (-2{,}91) \cdot z38 + (-0{,}01) \cdot \mathrm{z45} \\ & + (-0{,}02) \cdot \mathrm{z46} + 2 \cdot \mathrm{z50} + 1{,}82 \cdot \mathrm{z51} + (-1{,}12) \cdot \mathrm{z54} \\ & + (-0{,}87) \cdot \mathrm{z58} + (-0{,}04) \cdot \mathrm{z74} \end{aligned} \tag{31}$$

Modelom je obuhvaćeno ukupno devet nezavisnih (z14, z38, z45, z46, z50, z51, z54, z58, z74) značajki za koje je metodom najmanjih kvadrata utvrđeno da imaju najveći utjecaj na promjenu zavisne značajke.

5.8.2.4 LMT model za C4 klasu SHIoT uređaja

Uređaji klase C4, zbog većeg indeksa C_u, generiraju promet i prometne tokove čije karakteristike je teže razlikovati od anomalije mrežnoga prometa kao što je DDoS promet. Razlog je manja razina predvidivosti prometa uzrokovana načinom rada uređaja, poput visoke razine interakcije s korisnikom, reprodukcija audio/video sadržaja i slično. To rezultira i kompleksnijim LMT modelom kojeg nije moguće poopćiti do korijenskog čvora, već se on sastoji od ukupno 11 čvorova, odnosno 6 terminalnih čvorova. Na svakom grananju stabla odluke koje završava terminalnim čvorom definiran je model logističke regresije.



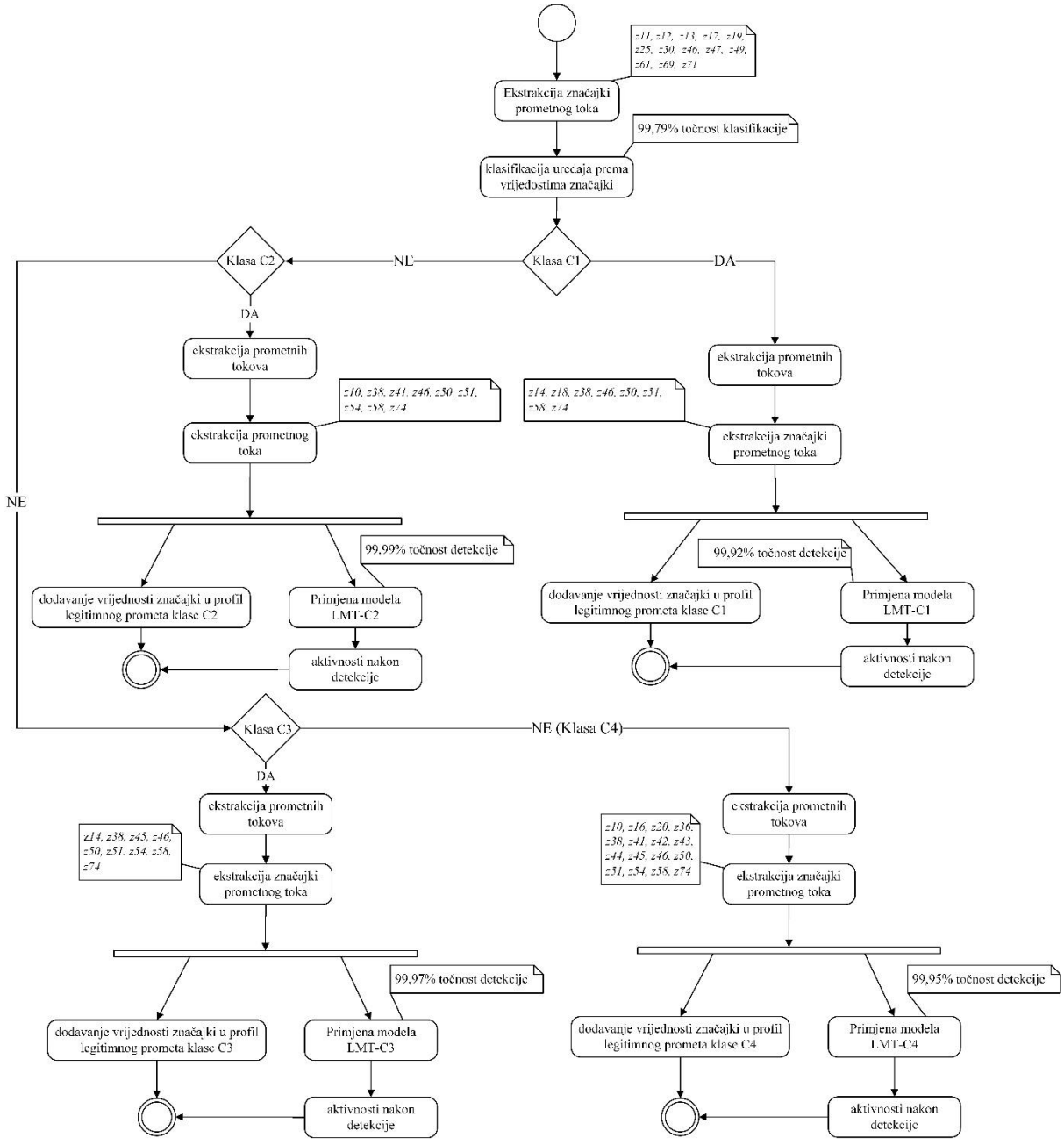
Slika 5.12 Prikaz LMT modela detekcije anomalija mrežnoga prometa za klasu C4

U konkretnom slučaju to znači da se LMT model sastoji od ukupno pet točaka grananja i šest modela logističke regresije kao što je prikazano slikom 5.12. LMT model koji sadrži stablo odluke i pripadajuće modele logističke regresije s odabranim relevantnim nezavisnim značajkama i pripadajućim koeficijentima, prikazan je prilogom 4 ovog rada.

5.8.3 Princip rada razvijenog modela detekcije nelegitimnog DDoS mrežnoga prometa

Rad razvijenog modela detekcije nelegitimnog DDoS prometa odvija se u dvije faze. Princip rada modela za pojedinačni SHIoT uređaj prikazan je UML dijagramom aktivnosti na slici 5.13. Prva faza čini preduvjet kasnije detekcije DDoS prometa u drugoj fazi rada, a podrazumijeva klasifikaciju SHIoT uređaja na temelju generiranog prometnog toka. Rezultati višeklasnog klasifikacijskog modela pokazuju kako je SHIoT uređaj moguće klasificirati u jednu od četiri preddefinirane klase s obzirom na prometne tokove koje generira točnošću od 99,79 %. Nakon što je uređaj uspješno klasificiran, novi generirani prometni tokovi provjeravaju se na temelju LMT modela detekcije nelegitimnog DDoS prometa pri čemu se utvrđuje pripadaju li ti prometni tokovi prepoznatoj klasi ili predstavljaju anomaliju mrežnoga

prometa. Osnovicu za razvoj modela detekcije DDoS prometa za pojedinu klasu predstavlja profil legitimnog prometa pojedine klase koji je rezultat rada višeklasnog klasifikacijskog modela u prvoj fazi.



Slika 5.13 Princip rada razvijenog modela detekcije nelegitimnog DDoS prometa za pojedinačni SHIoT uređaj

Pri tome vrijednosti značajki prometnih tokova klasificiranih u određene preddefinirane klase postaju i dijelom profila legitimnog prometa tih klasa. Ovisno o pripadajućoj klasi SHIoT uređaja, pojedini LMT model u mogućnosti je detektirati odstupanja ili anomalije od postojećeg profila normalnog prometa uz visoku točnost (LMT-C1 = 99,99 %, LMT-C2 = 99,92 %, LMT-

C3 = 99,97 % i LMT-C4 = 99,95 %) te uz korištenje različitih skupova nezavisnih značajki prometnog toka.

5.8.4 Analiza rezultata i ocjena performansi modela detekcije nelegitimnog DDoS prometa

Razvoj modela detekcije anomalija mrežnoga prometa temeljen na značajkama prometa i na klasnoj pripadnosti uređaja ukazuje na važnost prepoznavanja klase kojoj SHIoT uređaj pripada kao temeljnu aktivnost daljnjeg prepoznavanja anomalija u mrežnome prometu kao što je DDoS promet. Prema modelu prikazanom u prethodnom podpoglavlju, jasno je vidljivo da nisu sve nezavisne značajke jednako važne pri detekciji anomalija za pojedinu klasu. Isto tako, određene značajke u jednoj klasi mogu biti relevantne dok promatrano s aspekta druge klase ne moraju. Primjer je vidljiv u tablici 5.19 koja prikazuje LMT modelom procijenjene relevantne nezavisne značajke. Iz prikazanih podataka uočava se kako se LMT model za svaku klasu razlikuje prema broju relevantnih nezavisnih značajki, a isto tako vidljivo je da nisu iste značajke relevantne kod detekcije anomalija za svaku klasu.

Tablica 5.19 Prikaz nezavisnih značajki uključenih u LMT model pojedine klase SHIoT uređaja

LMT model									
LMT-C1	**LMT-C2**		**LMT-C3**	**LMT-C4**					
Logistički modeli									
LM1	**LM1**	**LM2**	**LM1**	**LM1**	**LM2**	**LM3**	**LM4**	**LM5**	**LM6**
z14	z10	z38	z14	z10	z10	z10	z10	z10	z10
z18	z38	z46	z38	z16	z16	z16	z16	z16	z38
z38	z41	z50	z45	z20	z20	z20	z20	z38	z50
z46	z46	z51	z46	z36	z36	z36	z38	z41	z51
z50	z50	z54	z50	z38	z38	z38	z41	z42	z54
z51	z51	z58	z51	z41	z41	z41	z42	z45	z58
z58	z54		z54	z42	z42	z42	z45	z50	z74
z74	z58		z58	z45	z43	z44	z50	z51	
	z74		z74	z50	z44	z45	z51	z54	
				z51	z45	z46	z54	z58	
				z54	z46	z50	z58	z74	
				z58	z50	z51	z74		
				z74	z51	z58			
					z54	z73			
					z58	z74			
					z74				

Nadalje, prag vrijednosti pojedine nezavisne značajke koji određuje grananje stabla odluke razlikuje se za pojedine klase. Kao što je vidljivo iz slike 5.11 i 5.12, grananje u stablu odluke odvija se na osnovi praga vrijednosti značajke z24 koja predstavlja standardnu devijaciju međudolaznih vremena paketa u promatranom prometnom toku izraženo u mikro sekundama (μs). Pri tome se koristi algoritam C4.5 koji odabire onaj prag vrijednosti nezavisne značajke

koji omogućuje „najčišću“ podjelu vektora značajki u skupu [228]. Tako se, primjerice, prag vrijednosti značajke z24 u LMT modelu za klasu C2 razlikuje od praga vrijednosti iste značajke za klasu C4.

Svaka inačica LMT modela validirana je metodom *k*-struke unakrsne validacije uz *k*=10 u svrhu procjene ponašanja modela nad podatcima koji nisu korišteni u fazi učenja, kako je i pojašnjeno u 5.6.3. Na osnovi provedene validacije izračunate su performanse modela uz korištenje metrika primijenjenih i u razvoju klasifikacijskog modela prikazanog u 5.6. Navedene metrike (točnost, *kappa* statistika, *TPR*, *FPR*, preciznost, *F*-mjera, *ROC* i *PRC*) su standardne i često korištene za razvoj klasifikacijskih modela primjenom metoda strojnog učenja.

5.8.4.1 Točnost razvijenih LMT klasifikacijskih modela

Jedna od osnovnih metrika koje ukazuju na performanse modela su točnost klasifikacije i *kappa* statistika. Prema točnosti klasifikacije, sva četiri modela pokazuju visoke performanse što znači da na temelju promatranog toka mogu s visokom točnošću utvrditi je li prometni tok rezultat legitimne komunikacije uređaja ili uređaj generira DDoS promet. Prema tablici 5.20 uočava se visoka točnost sve četiri inačice LMT modela razvijene za pojedinu klasu SHIoT uređaja. Pogreške u klasifikaciji sve četiri inačice LMT modela vizualizirane su i prikazane slikom 5.14

Tablica 5.20 Prikaz točnosti razvijenih modela i *kappa* koeficijenta

Model	**LMT-C1**		**LMT-C2**		**LMT-C3**		**LMT-C4**	
Točno klasificirani primjeri	56092	99,9216 %	59660	99,9966 %	58646	99,9744 %	59879	99,9583 %
Pogrešno klasificirani primjeri	44	0,0784 %	2	0,0034 %	15	0,0256 %	25	0,0417 %
***Kappa* koeficijent (κ)**	0,9984		0,9999		0,9995		0,9992	
Ukupno	56136		59662		58661		59904	

Tako LMT model za klasu uređaja C1 pokazuje točnost 99,9216 %, odnosno 56092 točno klasificiranih prometnih tokova, kao DDoS ili prometni tok koji legitimno pripada SHIoT uređaju iz klase C1. Pogrešno su klasificirana ukupno 44 prometna toka, odnosno 0,0784 % u ukupnom skupu od 56136. Od 44 pogrešno klasificirana prometna toka, za 41 je predviđena pripadnost legitimnom prometnom toku klase C1 dok su tri prometna toka klasificirana kao DDoS promet kako je i prikazano matricom konfuzije u tablici 5.21. Uz visoku točnost, LMT model za klasu uređaja C1 pokazuje i *kappa* koeficijent (κ = 0,9984) koji označava visoku uspješnost modela.

Tablica 5.21 Matrica konfuzije LMT modela za klase C1 i C2

Predviđena pripadnost klasi			
Klasa C1	**DDoS**		
28065	3	**Klasa C1**	*Stvarna pripadnost klasi*
41	28027	**DDoS**	
Predviđena pripadnost klasi			
Klasa C2	**DDoS**		
29830	1	**Klasa C2**	
1	29830	**DDoS**	

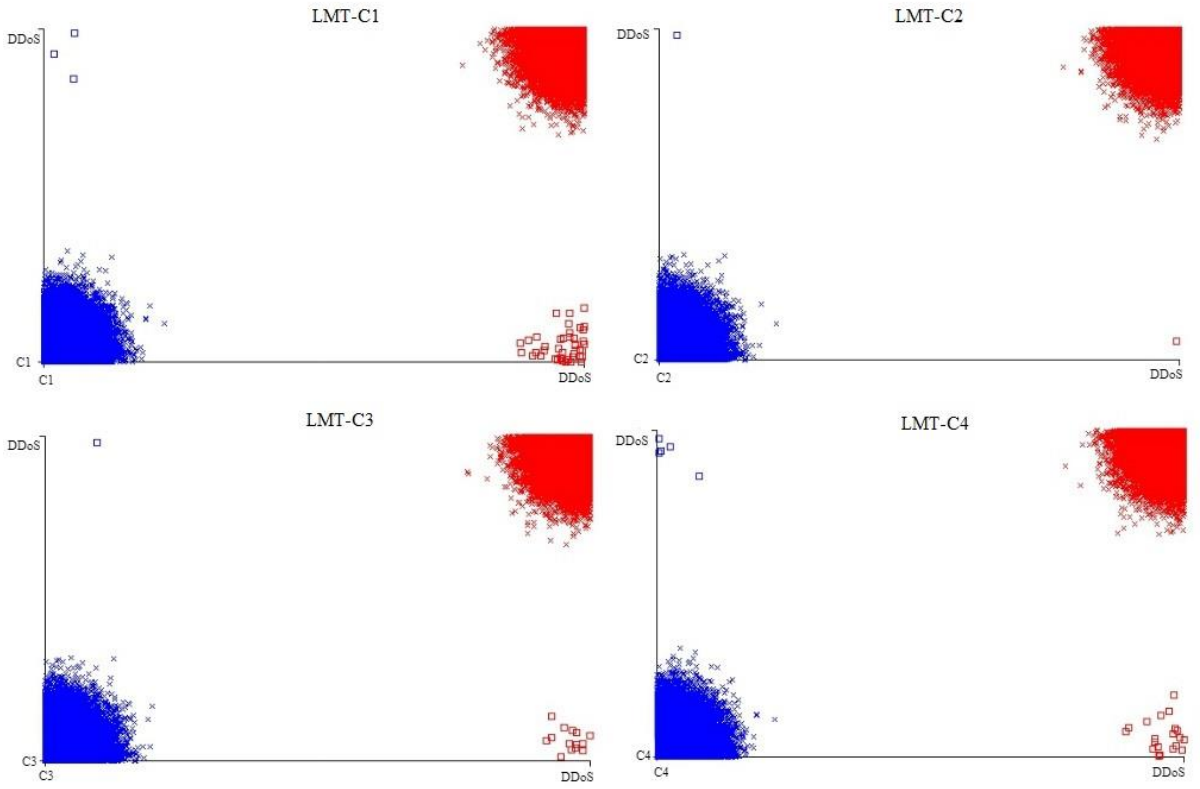
Inačica LMT modela razvijena za klasu C2 pokazuje visoku točnost (99,9966 %), prikazano tablicom 5.20. Navedeno podrazumijeva 59660 točno klasificiranih prometnih tokova u skupu kojeg čine 59662 prometna toka. Pogreška u klasifikaciji iznosi 0,0034 %, odnosno dva prometna toka, pri čemu je jedan pogrešno dodijeljen klasi C2, a drugi DDoS prometu što je i vidljivo iz tablice 5.21. Iznos *kappa* koeficijenta je 0,9999 što ukazuje na visoku uspješnost i ove inačice LMT modela.

LMT model klasifikacije razvijen za klasu C3 pruža točnost od 99,9744 % kako je prikazano tablicom 5.20. Prema tome, od ukupno 58661 prometnih tokova, njih 15 je pogrešno klasificirano, odnosno 0,0256 % dok ih je točno klasificirano 58646. Prema matrici konfuzije, prikazano tablicom 5.22, jedan prometni tok pogrešno je klasificiran kao DDoS promet dok je 14 prometnih tokova pogrešno klasificirano kao dio legitimnog prometa klase C3.

Tablica 5.22 Matrica konfuzije LMT modela za klase C3 i C4

Predviđena pripadnost klasi			
Klasa C3	**DDoS**		
29329	1	**Klasa C3**	*Stvarna pripadnost klasi*
14	29317	**DDoS**	
Predviđena pripadnost klasi			
Klasa C4	**DDoS**		
29947	5	**Klasa C4**	
20	29932	**DDoS**	

Iznos *kappa* koeficijenta od 0,9995, kao i kod prethodnih inačica LMT modela, ukazuje na njegovu visoku uspješnost. Posljednja inačica LMT modela, razvijena za klasu C4, pokazuje točnost od 99,9583 % što podrazumijeva 59879 ispravno klasificiranih prometnih tokova.



Slika 5.14 Vizualizacija pogreške LMT klasifikacijskih modela za pripadajuće klase

Prema tome, pogrešno je klasificirano ukupno 25 prometnih tokova i to pet kao DDoS promet i 20 kao legitiman promet klase C4, kako je prikazano matricom konfuzije u tablici 5.22. Uspješnost modela mjerena *kappa* koeficijentom iznosi 0,9992, vidljivo u tablici 5.20.

5.8.4.2 Analiza performansi temeljenih na pozitivnim i negativnim rezultatima modela

Daljnja analiza i ocjena performansi razvijenih LMT modela provedena je korištenjem metrika koje su temeljene na pozitivnim i negativnim rezultatima, sve mjere opisane su u 5.6.3. Prva takva mjera je stvarno pozitivna stopa (*TPR*). Iz tablice 5.23 vidljivi su rezultati *TPR* za sve inačice LMT modela pri čemu *TPR* za sve klase legitimnog prometa iznosi 1. Vrijednosti TPR za DDoS klasu za modele LMT-C2 i LMT-C3 iznosi 1 dok se za modele LMT-C1 i LMT-C4 uočava minimalan pad performansi pri čemu *TPR* iznosi 0,999.

Tablica 5.23 Prikaz validacijskih mjera LMT modela (*TPR* i *FPR*)

Klasa	**Stvarno pozitivna stopa primjera (*TPR*)**				**Lažno pozitivna stopa primjera (*FPR*)**			
	LMT-C1	**LMT-C2**	**LMT-C3**	**LMT-C4**	**LMT-C1**	**LMT-C2**	**LMT-C3**	**LMT-C4**
C1/C2/C3/C4	1	1	1	1	0,001	0	0	0,001
DDoS	0,999	1	1	0,999	0	0	0	0

Iduća važna mjera ocjene performansi je lažno pozitivna stopa primjera (FPR) prikazana istom tablicom. Prema ovoj mjeri svi modeli pokazuju dobre rezultate za klase legitimnog prometa i DDoS klasu.

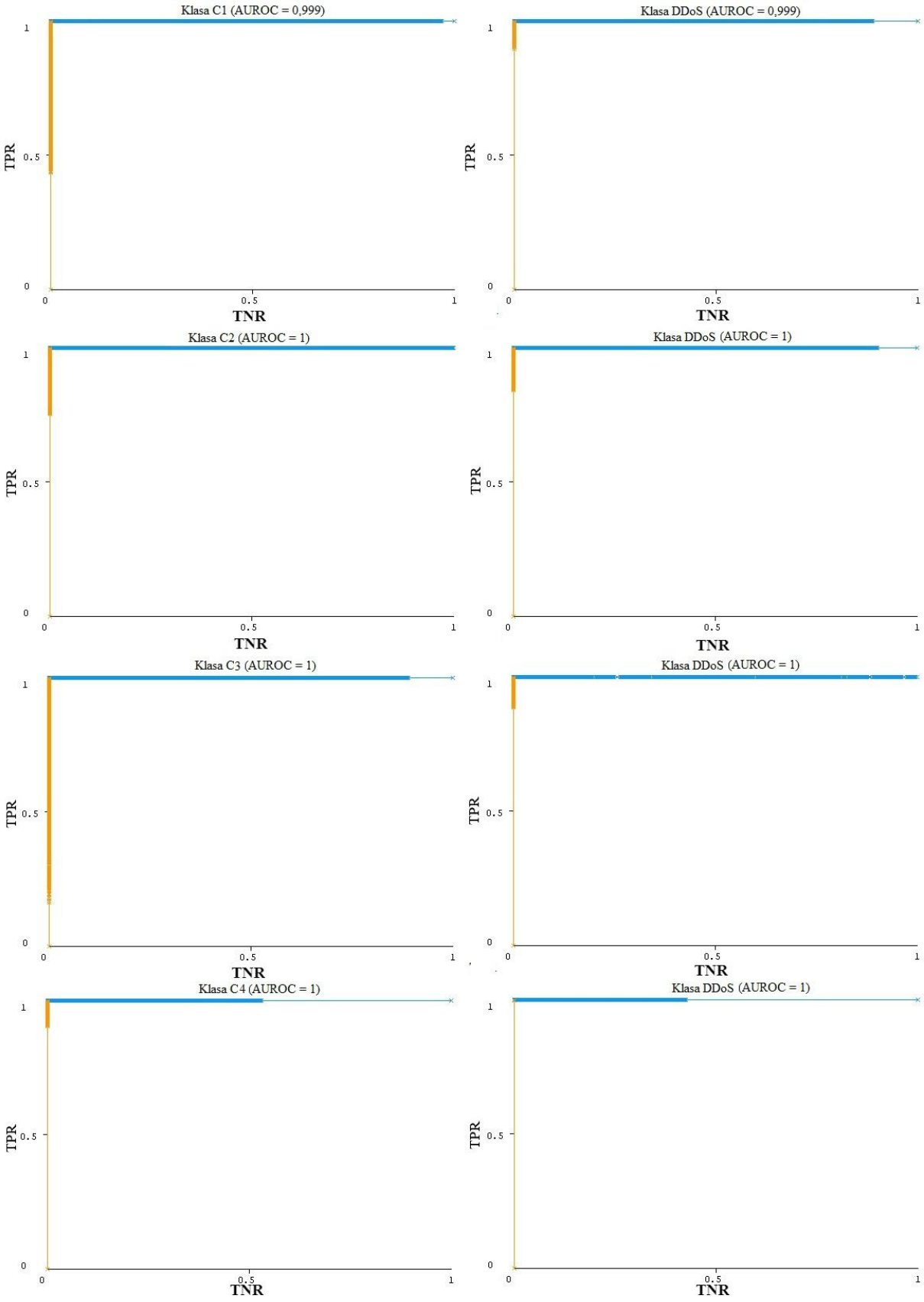
Minimalan pad performansi vidljiv je, kao i u slučaju TPR mjere, za modele LMT-C1 i LMT-C4 za klase legitimnog prometa (C1 i C4). Ovakvi rezultati TPR i FPR mjere pokazuju da razvijeni modeli imaju visoku stopu točno klasificiranih primjera i nisku stopu lažno pozitivno klasificiranih primjera.

Rezultati provedenih validacijskih mjera preciznosti i F1 ocjene prikazani su tablicom 5.24. Prema prikazanim vrijednostima, obje mjere ukazuju na visoke performanse svih inačica LMT modela. Minimalan pad performansi uočljiv je za LMT-C1 i LMT-C4 (0,999) za klase C1 i C4 kod mjere preciznosti te za LMT-C1 za klasu C1 i DDoS kod F1 ocjene (0,999).

Tablica 5.24 Prikaz validacijskih mjera LMT modela (Preciznost i F-mjera)

Klasa	**Preciznost**				**F-mjera (F1 ocjena)**			
	LMT-C1	**LMT-C2**	**LMT-C3**	**LMT-C4**	**LMT-C1**	**LMT-C2**	**LMT-C3**	**LMT-C4**
C1/C2/C3/C4	0,999	1	1	0,999	0,999	1	1	1
DDoS	1	1	1	1	0,999	1	1	1

Visoke performanse sve četiri inačice LMT modela vidljive su i iz provedenih ROC i PRC mjera čiji su rezultati vidljivi u tablici 5.25. Rezultati ROC mjere, kao jedne od najvažnijih i najčešće korištenih mjera koje pokazuju kvalitetu klasifikacijskog modela, ukazuju na visoku kvalitetu svih inačica razvijenih LMT modela. Dokaz tome je vrijednost odnosa stope TPR i TNR koja iznosi 1 za modele LMT-C2, LTM-C3 i LMT-C4, odnosno 0,999 za model LMT-C1. Dokaz tome je i AUROC, odnosno površina ispod krivulje prikazana slikom 5.15 iz koje je vidljivo da je AUROC=1 ili približno 1.



Slika 5.15 Vizualni prikaz ROC krivulja za LMT modele prema definiranim klasama (C1, C2, C3, C4)

S obzirom da su podatkovni skupovi stratificirani, *PRC* mjera, kao alternativa *ROC* mjeri, koja može bolje procijeniti utjecaj velikog broja negativnih primjera na performanse modela, daje gotovo jednake vrijednosti za sve promatrane LMT modele.

Tablica 5.25 Prikaz validacijskih mjera LMT modela (ROC i PRC)

Klasa	***ROC***				***PRC***			
	LMT-C1	**LMT-C2**	**LMT-C3**	**LMT-C4**	**LMT-C1**	**LMT-C2**	**LMT-C3**	**LMT-C4**
C1/C2/C3/C4	0,999	1	1	1	0,998	1	1	1
DDoS	0,999	1	1	1	0,999	1	1	1

Prikazani rezultati razvijenoga modela jasno potvrđuju drugu hipotezu ovog doktorskog istraživanja, odnosno da je na temelju definiranog profila legitimnog prometa pojedine klase IoT uređaja u okruženju pametnog doma moguće uz visoku točnost detektirati nelegitiman promet koji takvi uređaji generiraju.

5.9 Diskusija o rezultatima dobivenim istraživanjem

5.9.1 Značaj detekcije DDoS prometa temeljene na klasnoj pripadnosti uređaja

Model detekcije anomalija mrežnoga prometa prikazan u ovom doktorskom radu pruža novu percepciju detekcije anomalija mrežnoga prometa i ukazuje na originalnost rada s više aspekata. Dosadašnja istraživanja problema detekcije DDoS prometa pretežno su se temeljila na generiranju profila legitimnog prometa za koji se pretpostavljalo da je primjenjiv na sve terminalne uređaje. Takav pristup je logičan u okruženjima gdje su terminalni uređaji u mreži većinski bili konvencionalni uređaji koji podržavaju instalaciju velikog broja aplikacija i čije karakteristike generiranog prometa ovise upravo o radu instaliranih aplikacija i načinu na koji korisnik koristi takve uređaje.

Pojavom koncepta IoT sve su brojniji uređaji koji su u manjoj ili većoj mjeri ograničeni svojim funkcionalnostima što se odražava i na karakteristike prometa koji generiraju. I nakon pojave takvog novog okruženja na globalnoj razini, istraživači i dalje nastoje primijeniti postojeći pristup detekciji anomalija korišten u okruženju konvencionalnih uređaja. Drugi pristup koji istraživači koriste je detekcija anomalija koje generiraju pojedinačni uređaji. Problem prvog pristupa jest da se određeni uređaji u IoT okruženju ponašaju drugačije od drugih uređaja. Neki uređaji će generirati uvijek istu i približno istu količinu prometa, dok će kod drugih uređaja ta značajka varirati jer omogućuju veću interakciju s korisnikom koji može koristiti više različitih funkcionalnosti tog uređaja. Problem drugog pristupa jest da je trend

rasta broja uređaja u IoT okruženju eksponencijalan, a modeli koji se temelje na karakteristikama pojedinačnog uređaja zahtijevaju ponovno učenje ili čak ponovni razvoj modela za svaki novi uređaj koji se pojavljuje na tržištu. Takav pristup je izrazito kompleksan i nedovoljno generički kada se problem promatra s aspekta IoT okruženja te brojnosti i raznovrsnosti uređaja koje takvo okruženje podrazumijeva.

Pristup detekciji anomalija mrežnoga prometa temeljen na značajkama prometa i klasnoj pripadnosti uređaja značajan je upravo u kontekstu IoT okruženja. Ovakvim pristupom profil legitimnog prometa nije unificiran za sve uređaje koji egzistiraju na određenom području niti je ograničen na pojedinačne uređaje, već je stvoren za klase uređaja ovisno o karakteristikama prometa koji generiraju. Na taj način formira se profil legitimnog prometa za svaku klasu uređaja na temelju kojih su razvijeni modeli detekcije anomalija. Ovakav pristup ima potencijal klasificirati uređaje koji nisu obuhvaćeni istraživanjem na temelju značajki prometnog toka koji generiraju te naknadno utvrditi ponaša li se takav uređaj u legitimnim okvirima ili generira DDoS promet. Primjena klasa uređaja kao osnove za detekciju DDoS prometa donosi prednosti i s aspekta implementacije. Iako navedeno nije obuhvaćeno ovim istraživanjem, pretpostavka je da ovakav pristup smanjuje kompleksnost modela detekcije anomalija i omogućuje brži rad modela u praksi.

Istraživanjem je dokazano da je moguće definirati klase uređaja na temelju varijacije odnosa primljenog i poslanog prometa te je moguće klasificirati uređaje u definirane klase na temelju značajki prometnih tokova koje takvi uređaji generiraju. Konačno, ovisno o pripadnosti pojedinog uređaja definiranoj klasi, moguće je utvrditi predstavlja li prometni tok kojeg uređaj generira anomaliju u vidu DDoS prometa ili legitiman promet.

5.9.2 Praktična primjenjivost razvijenog modela

Česta je pretpostavka da je detekciju DDoS prometa nužno provoditi isključivo na odredištu, odnosno na cilju napada u svrhu očuvanja načela dostupnosti informacijsko-komunikacijskih resursa. Unatoč tome, ovim istraživanjem obuhvaćeni su uređaji iz okruženja pametnog doma koji prema statističkim pokazateljima bilježe najveću stopu rasta s aspekta primjene koncepta IoT. Isto tako, ovo istraživanje usmjereno je na detekciju DDoS prometa na izvorištu, odnosno na mrežu u kojoj se takav promet generira. DDoS promet nema negativan utjecaj isključivo na odredištu, već može prouzrokovati probleme na izvorišnom dijelu kao i u mreži pružatelja internetskih usluga.

Mogućnost primjene ovakvog rješenja u praksi vidljiv je s aspekta više dionika koje čine krajnji korisnik, pružatelj internetskih usluga (telekom operator) te proizvođač uređaja i pružatelj usluga u okruženju pametnog doma. S aspekta korisnika kao dionika okruženja pametnog doma ističe se potreba da uređaji u okruženju pametnog doma funkcioniraju onako kako predviđa proizvođač, odnosno da su sve funkcionalnosti uređaja dostupne u traženom vremenu. Generiranje DDoS prometa može uzrokovati i nepredvidivo ponašanje uređaja koji takav promet generira što može smanjiti njegove funkcionalnosti ili učiniti uređaj u potpunosti nedostupnim. Stoga je u interesu korisnika pravovremena detekcija neželjenog ponašanja uređaja što omogućuje aktivnosti koje slijede nakon detekcije.

Generiranje DDoS prometa posredstvom velikog broja IoT uređaja u okruženju pametnog doma može negativno utjecati i na mrežnu i poslužiteljsku infrastrukturu telekom operatora. S obzirom da su telekom operatori često i pružatelji usluge pametnog doma, zasigurno im je u interesu pravovremeno detektirati neovlašteno ponašanje uređaja da bi zaštitili vlastitu mrežnu infrastrukturu.

Konačno, proizvođači takvih uređaja moraju osigurati ispravan rad uređaja s ciljem povećanja zadovoljstva korisnika i tržišnog širenja. To će osigurati pravovremenom detekcijom neovlaštenog rada uređaja koja će im omogućiti reakciju na neželjene događaje i osiguranje željene razine korisničkog zadovoljstva.

5.9.3 Ograničenja i buduća istraživanja problemskog područja

Unatoč ostvarenim ciljevima koji su postavljeni pred istraživanje u okviru ovog doktorskog rada te potvrdi znanstvenih hipoteza, valja istaknuti i ograničenja istraživanja. Kao prvo ograničenje uočava se broj SHIoT uređaja obuhvaćenih istraživanjem. Iako, prema autorovom saznanju, ovo istraživanje uključuje najveći broj uređaja od svih analiziranih istraživanja u ovom i sličnim problemskim područjima, veći broj uređaja osigurao bi i kvalitetniji uvid u razlike u ponašanju uređaja kroz analizu prometa.

Sljedeće ograničenje ogleda se u prikupljenim podatcima. Dio podataka prikupljen je iz sekundarnog izvora pri čemu autor nije imao potpunu kontrolu nad uređajima iako je prema autorima podatkovnog skupa korištena ista metodologija prikupljanja podataka. Pretpostavka je da uređaji nisu neovlašteno mijenjani te da rade onako kako je definirao proizvođač. Da bi se osiguralo željeno stanje uređaja, u budućim istraživanjima potrebno je proširiti inicijalni skup SHIoT uređaja.

Uz otklanjanje uočenih ograničenja i nedostataka predmetnog istraživanja, budućim istraživanjima potrebno je obuhvatiti i aktivnosti koje slijede nakon detekcije DDoS prometa, odnosno reaktivne aktivnosti. Također, potrebno je usmjeriti istraživanja u provjeru primjenjivosti razvijenog modela u drugim primjenama koncepta IoT kao što je zdravstvo, transport ili industrija 4.0 s obzirom da su takva okruženja komparativna s okruženjem pametnog doma i primjena im je također u porastu.

Ovo istraživanje pod anomalijom mrežnoga prometa podrazumijeva DDoS promet. Uz DDoS promet, anomalijom se smatraju i drugi oblici prijetnji i neovlaštenih radnji koje se odvijaju u komunikacijskoj mreži. U budućim istraživanjima potrebno je obuhvatiti i druge oblike anomalija i utvrditi primjenjivost razvijenog modela u izvornom ili prilagođenom obliku.

6 Zaključak

Ovim poglavljem prikazana su zaključna razmatranja temeljena na dobivenim rezultatima istraživanja kojima su dokazane postavljene znanstvene hipoteze predmetnog istraživanja te su dani izvorni znanstveni doprinosi. Istaknuta je učinkovitost korištenog pristupa u razvoju modela detekcije anomalija mrežnoga prometa u IoT okruženju kao i učinkovitost primjene metoda strojnog učenja u promatranom problemskom području. Uz navedeno, dan je osvrt na potencijalne prednosti razvijenog modela u praksi.

Detekcija DDoS prometa predstavlja aktualno problemsko područje s obzirom na trend porasta broja i intenziteta DDoS napada. Razvoj i sve učestalija primjena koncepta IoT u različitim područjima čimbenik je koji uzrokuje dodatan porast ovakvih napada što čini ovo problemsko područje istraživački aktualnijim. Okruženje pametnog doma, kao jedno od najbrže rastućih područja primjene koncepta IoT, često je posrednik u generiranju DDoS prometa kroz SHIoT uređaje koji su se kroz veći broj istraživanja pokazali nezaštićenima. Zbog toga im je moguće neovlašteno udaljeno pristupiti i kontrolirati ih s ciljem izvršavanja raznovrsnih malicioznih aktivnosti.

Generiranje DDoS prometa posredstvom SHIoT uređaja nema nužno negativan utjecaj samo na odredište ili cilj napada, već i na uređaj koji takav promet generira, lokalnu mrežu i ostale SHIoT uređaje povezane na tu mrežu, ali i na pristupnu komunikacijsku infrastrukturu telekom operatora. Upravo iz navedenih razloga, pravovremena detekcija ovakvog prometa može imati pozitivan učinak na zadovoljstvo korisnika pametnog doma, pružatelje internetskih usluga, a svakako može pridonijeti u smanjenju broja i intenziteta provedbe DDoS napada na globalnoj razini.

Istraživanje prikazano u ovom doktorskom radu pruža novi pristup u detekciji DDoS prometa generiranog korištenjem terminalnih uređaja u okruženju pametnog doma. Cilj, koji je predmetnim istraživanjem i ostvaren, bio je razviti model detekcije nelegitimnog DDoS prometa generiranog IoT uređajima u okruženju pametnog doma koji se temelji na značajkama prometa i klasnoj pripadnosti IoT uređaja.

Osnova provedbe istraživanja i postizanja definiranog cilja su dvije postavljene znanstvene hipoteze:

- na temelju značajki prometa koji generiraju IoT uređaji u okruženju pametnog doma moguće je definirati klase IoT uređaja i pripadajuće profile legitimnog prometa te

- temeljem definiranog profila legitimnog prometa pojedine klase IoT uređaja u okruženju pametnog doma moguće je uz visoku točnost detektirati nelegitiman promet koji takvi uređaji generiraju.

Obje znanstvene hipoteze potvrđene su tijekom istraživanja. Prva hipoteza dokazana je definiranjem četiriju klasa uređaja na osnovi varijacije koeficijenta varijacije odnosa primljenog i poslanog prometa. Definirane klase uvjetovale su razvoj klasifikacijskog modela IoT uređaja čiji rad je omogućio stvaranje profila legitimnog prometa pojedine klase IoT uređaja. Definirani profili temelj su razvijenog modela detekcije anomalija mrežnoga prometa

temeljenog na LMT metodi strojnog učenja koji pokazuje visoku točnost detekcije anomalija prometa, čime je dokazana druga znanstvena hipoteza. Na osnovi prethodno dokazanih znanstvenih hipoteza, ostvareni su sljedeći, izvorni znanstveni doprinosi u polju tehnologije prometa i transporta:

- identificirane su značajke prometa na temelju kojih je moguće klasificirati IoT uređaje u okruženju pametnog doma u svrhu detekcije nelegitimnog DDoS prometa,

- definirani su profili legitimnog prometa za pojedinu klasu IoT uređaja u okruženju pametnog doma, i

- razvijen je model detekcije DDoS prometa temeljen na značajkama prometa i klasnoj pripadnosti IoT uređaja.

Doktorskim radom pojašnjeni su i analizirani svi elementi ključni za predmetno problemsko područje. Pojašnjen je koncept IoT te je prikazana njegova arhitektura kao i ključne tehnologije potrebne za funkcioniranje ovog koncepta poput senzorskih, aktuatorskih i komunikacijskih tehnologija. Analizirana su vertikalna područja primjene koncepta IoT te su analizirani statistički pokazatelji s ciljem utvrđivanja onih područja primjene čija je penetracija i razvoj u najvećem porastu.

Detaljno i sustavno je analizirano okruženje pametnog doma kao jedno od najbrže rastućih područja primjene koncepta IoT i fokusa ovog doktorskog rada. Prikazane su postojeće skupine uređaja, korištene komunikacijske tehnologije te arhitektura pametnog doma. S obzirom na već utvrđene nedostatke takvih uređaja, analizirani su njihovi nedostatci s aspekta sigurnosti kroz prijetnje kao što su prisluškivanje prometa, mogućnosti lažnog predstavljanja, iskorištavanja ranjivosti softvera te generiranja DDoS prometa.

Budući da je detekcija DDoS prometa problemsko područje koje je istraženo ovim doktorskim radom, sustavno je analiziran i pojašnjen problem anomalija mrežnoga prometa u vidu DDoS prometa s fokusom na DDoS promet generiran posredstvom SHIoT uređaja.

Doktorskim radom prikazan je razvoj modela detekcije anomalija mrežnoga prometa temeljen na značajkama prometa i klasnoj pripadnosti uređaja. U tu svrhu formirano je laboratorijsko okruženje sačinjeno od ukupno 41 SHIoT uređaja i popratne mrežne i hardversko-softverske infrastrukture namijenjeno prikupljanju prometa kojeg generiraju SHIoT uređaji. Uz navedeno, korišten je i BoNaSi programski alat za simulaciju DDoS prometa u svrhu stvaranja podatkovnog skupa nelegitimnog prometa, odnosno anomalije mrežnoga

prometa. Iz prikupljenog prometa ekstrahirane su ukupno 83 značajke prometnog toka koje su korištene u narednim fazama istraživanja.

Tijekom istraživanja uočeno je da se određeni SHIoT uređaji razlikuju prema koeficijentu varijacije odnosa primljenog i poslanog prometa. Spomenutom koeficijentu dodijeljen je naziv *indeks* C_u koji je odabran kao zavisna značajka korištena u svrhu definiranja ukupno četiri klase SHIoT uređaja primjenom metode klasifikacije koeficijenta varijacije. Na temelju definiranih klasa SHIoT uređaja razvijen je višeklasni klasifikacijski model temeljen na *boosting* metodi aditivne logističke regresije kao metode strojnog učenja koji prema svim validacijskim mjerama pokazuje visoke performanse uz točnost prepoznavanja pripadnosti SHIoT uređaja jednoj od definiranih klasa (99,79 %) na osnovi vrijednosti 13 nezavisnih značajki prometnog toka. Relevantne nezavisne značajke prometnog toka korištene u razvoju modela odabrane su primjenom metode informacijske dobiti. Razvijeni model omogućio je stvaranje profila legitimnog prometa svake klase SHIoT uređaja tako da nezavisne značajke svakog prometnog toka kojeg klasifikacijski model dodijeli određenoj klasi SHIoT uređaja ujedno postaje i dijelom profila legitimnog prometa te klase. Navedeno je predstavljalo ključnu važnosti za sljedeću fazu istraživanja jer su profili legitimnog prometa korišteni za razvoj modela detekcije DDoS prometa.

Model detekcije DDoS prometa temeljen je na metodi logističkih stabala odluke iz skupa metoda strojnog učenja. Problem detekcije DDoS prometa temeljenog na klasama uređaja sveden je na problem binarne klasifikacije pri čemu su za svaku klasu SHIoT uređaja razvijene različite inačice istog modela. To je razlog što promet svake klase SHIoT uređaja posjeduje različite karakteristike što je vidljivo i iz prikazanih inačica modela pri čemu se svaka razlikuje u broju korištenih nezavisnih značajki, veličini stabla odluke i pragovima vrijednosti njegovog grananja. Ovakav pristup pokazuje visoke performanse prema svim promatranim mjerama (točnost, TPR, FPR, F1 ocjena, preciznost, ROC i PRC) pri čemu točnost modela za klase iznosi redom C1=99,9216 %, C2=99,9966 %, C3=99,9744 % i C4=99,9583 %.

Istraživanje je dokazalo da je moguće uz visoku točnost detektirati nelegitiman promet na temelju svrstavanja uređaja u preddefinirane klase i stvaranjem profila legitimnog prometa za svaku klasu uz primjenu *boosting* metoda strojnog učenja. Uz navedeno, ovakav pristup odgovara na potrebe novonastalog IoT okruženja u kojemu broj uređaja eksponencijalno raste i nije moguće (ili isto zahtijeva velike resurse) poznavati profile legitimnog prometa za svaki uređaj, već je dovoljno prepoznati kojoj klasi uređaj pripada i na temelju toga utvrditi ponaša li se uređaj legitimno ili generira promet koji predstavlja anomaliju.

Model detekcije DDoS prometa razvijen u okviru ovog doktorskog rada ima potencijal primjene i na ostala IoT okruženja. Isto tako ima i potencijal praktične primjene koji bi bio od koristi brojnim dionicima ekosustav pametnog doma kao što su proizvođači SHIoT uređaja, pružatelji usluga u okruženju pametnog doma te pružatelji internetskih usluga. Uvođenje ovakvog modela u praksu pozitivno bi se odrazilo i na smanjenje broja i intenziteta DDoS napada na globalnoj razini.

Popis korištene literature

[1] **Bhattacharyya, D.K.**, **Kalita, J.K.**: *Network Anomaly Detection: A Machine Learning Perspective*, CRC Press, Boca Raton, USA, 2014

[2] **Husnjak, S.**, **Peraković, D.**, **Cvitić, I.**: Relevant Affect Factors of Smartphone Mobile Data Traffic, PROMET - Traffic&Transportation, Vol. 28, 2016, str. 435–444

[3] **Bidgoli, H.**: *Handbook of Information Security*, vol. 3, John Wiley & Sons Inc., New Jersey, USA, 2006

[4] **Tulloch, M.**: *Encyclopedia of Security*, Microsoft Press, Redmond, USA, 2003

[5] **Cvitić, I.**, **Peraković, D.**, **Periša, M.**, **Jerneić, B.**: *Availability Protection of IoT Concept Based Telematics System in Transport*, Challenge of Transport Telematics, Springer International Publishing, Katowite, Poland, 2016, str. 109–121

[6] **Hoque, N.**, **Bhuyan, M.H.**, **Baishya, R.C.**, **Bhattacharyya, D.K.**, **Kalita, J.K.**: Network attacks: Taxonomy, tools and systems, J. Netw. Comput. Astrl., Vol. 40, 2014, str. 307–324

[7] **Bhattacharyya, D.K.**, **Kalita, J.K.**: *DDoS Attacks: Evolution, Detection, Prevention, Reaction and Tolerance*, CRC Press, Boca Raton, USA, 2016

[8] **Erlang, A..**: The Theory of Probabilities and Telephone Conversations, Nyt Tidsskr. Mat., Vol. B, 1909

[9] **Begović, M.**: *Podvorbeni sustavi*, Fakultet prometnih znanosti, Zagreb, 2006

[10] **Bošnjak, I.**, **Badanjak, D.**: *Osnove prometnog inženjerstva*, Fakultet prometnih znanosti, Zagreb, 2005

[11] **Bauer, S.**, **Clark, D.**, **Lehr, W.**: The Evolution of Internet Congestion, The 37th Research Conference on Communication, Information, and Internet Policy, TPRC2009, 2009

[12] **Bošnjak, I.**: *Telekomunikacijski promet 2*, Fakultet prometnih znanosti, Zagreb, 2001

[13] **Chandola, V.**, **Banerjee, A.**, **Kumar, V.**: Anomaly detection, ACM Comput. Surv., Vol. 41, 2009, str. 1–58

[14] **Thottan, M.**: Anomaly detection in IP networks, IEEE Trans. Signal Process., Vol. 51, 2003, str. 2191–2204

[15] **Tan, Z.**, **Jamdagni, A.**, **He, X.**, **Member, S.**, **Nanda, P.**, **Member, S.**, **Liu, R.P.**, **Member, S.**, **Hu, J.**: Detection of Denial-of-Service Attacks Based on Computer Vision Techniques, IEEE Trans. Comput., Vol. 64, 2015, str. 1–14

[16] **Deka, R.K.**, **Bhattacharyya, D.K.**: Self-similarity based DDoS attack detection using Hurst parameter, Secur. Commun. Networks, Vol. 9, 2016, str. 4468–4481

[17] **Kizza, J.**, **Migga Kizza, F.**: *Intrusion Detection and Prevention Systems*, Securing the Information Infrastructure, IGI Global, 2008, str. 239–258

[18] **David, J.**, **Thomas, C.**: DDoS Attack Detection Using Fast Entropy Astrroach on Flow- Based Network Traffic, Procedia Comput. Sci., Vol. 50, 2015, str. 30–36

[19] **Mirkovic, J.**, **Reiher, P.**: A taxonomy of DDoS attack and DDoS defense mechanisms,

ACM SIGCOMM Comput. Commun. Rev., Vol. 34, 2004, str. 39

[20] **Bhuyan, M.H.**, **Bhattacharyya, D.K.**, **Kalita, J.K.**: Network Anomaly Detection: Methods, Systems and Tools, IEEE Commun. Surv. Tutorials, Vol. 16, 2014, str. 303–336

[21] **Zeb, K.**, **AsSadhan, B.**, **Al-Muhtadi, J.**, **Alshebeili, S.**: Anomaly detection using Wavelet-based estimation of LRD in packet and byte count of control traffic, Proceedings of 7th International Conference on Information and Communication Systems (ICICS), 2016

[22] **Xiang, Y.**, **Li, K.**, **Zhou, W.**: Low-rate DDoS attacks detection and traceback by using new information metrics, IEEE Trans. Inf. Forensics Secur., Vol. 6, 2011, str. 426–437

[23] **Zargar, S.T.**, **Joshi, J.**, **Tistrer, D.**: A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks, IEEE Commun. Surv. Tutorials, Vol. 15, 2013, str. 2046–2069

[24] **Bhuyan, M.H.**, **Kashyap, H.J.**, **Bhattacharyya, D.K.**, **Kalita, J.K.**: Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions, Comput. J., Vol. 57, 2014, str. 537–556

[25] **Zeb, K.**, **AsSadhan, B.**, **Al-Muhtadi, J.**, **Alshebeili, S.**, **Bashaiwth, A.**: Volume based anomaly detection using LRD analysis of decomposed network traffic, Proceedings of 4th International Conference on the Innovative Computing Technology (INTECH 2014), 2014

[26] **Kaur, G.**, **Saxena, V.**, **Gupta, J.P.**: Detection of TCP targeted high bandwidth attacks using self-similarity, J. King Saud Univ. - Comput. Inf. Sci., Vol. 32, 2017, str. 35–49

[27] **Johnson Singh, K.**, **Thongam, K.**, **De, T.**: Entropy-Based Astrlication Layer DDoS Attack Detection Using Artificial Neural Networks, Entropy, Vol. 18, 2016, str. 350

[28] **David, J.**, **Thomas, C.**: DDoS Attack Detection Using Fast Entropy Astrroach on Flow- Based Network Traffic, Procedia Comput. Sci., Vol. 50, 2015, str. 30–36

[29] **Feinstein, L.**, **Schnackenberg, D.**, **Balupari, R.**, **Kindred, D.**: Statistical astrroaches to DDoS attack detection and response, Proceedings of DARPA Information Survivability Conference and Exposition, 2003

[30] **Oshima, S.**, **Nakashima, T.**, **Sueyoshi, T.**: A Statistical DoS/DDoS Detection Method Using the Window of the Constant Packet Number, Proceedings of 2nd International Conference on Computer Science and its Astrlications, 2009

[31] **Hoque, N.**, **Bhattacharyya, D.K.**, **Kalita, J.K.**: FFSc: a novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis, Secur. Commun. Networks, Vol. 9, 2016, str. 2032–2041

[32] **Hoque, N.**, **Bhattacharyya, D.K.**, **Kalita, J.K.**: Denial of Service Attack Detection using Multivariate Correlation Analysis, Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS ’16, 2016

[33] **Tan, Z.**, **Jamdagni, A.**, **He, X.**, **Nanda, P.**, **Liu, R.P.**: A system for denial-of-service attack detection based on multivariate correlation analysis, IEEE Trans. Parallel Distrib. Syst., Vol. 25, 2014, str. 447–456

[34] **Sharma, N.**, **Mahajan, A.**, **Mansotra, V.**: Machine Learning Techniques Used in Detection of DOS Attacks : A Literature Review, Int. J. Adv. Res. Comput. Sci. Softw. Eng., Vol. 6, 2016, str. 100–105

[35] **Hamid, Y.**, **Sugumaran, M.**, **Journaux, L.**: Machine Learning Techniques for Intrusion Detection, Proceedings of the International Conference on Informatics and Analytics - ICIA-16, 2016

[36] **Balkanli, E.**, **Alves, J.**, **Zincir-Heywood, A.N.**: Supervised learning to detect DDoS attacks, 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2014

[37] **Osanaiye, O.**, **Choo, K.-K.R.**, **Dlodlo, M.**: Analysing Feature Selection and Classification Techniques for DDoS Detection in Cloud, Southern Africa Telecommunication Networks and Astrlications Conference (SATNAC) 2016, 2016

[38] **Singh, M.**, **Jain, S.K.**: *Evaluating Machine Learning Algorithms for Detecting DDoS Attacks*, Communications in Computer and Information Science, vol. 196, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, str. 608–621

[39] **Jia, B.**, **Huang, X.**, **Liu, R.**, **Ma, Y.**: A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning, J. Electr. Comput. Eng., Vol. 2017, 2017, str. 1–9

[40] **Jalili, R.**, **Imani-Mehr, F.**, **Amini, M.**, **Shahriari, H.R.**: *Detection of Distributed Denial of Service Attacks Using Statistical Pre-processor and Unsupervised Neural Networks*, Information Security Practice and Experience. ISPEC 2005, Springer, Berlin, Heidelberg, Singapore, 2005, str. 192–203

[41] **Saied, A.**, **Overill, R.E.**, **Radzik, T.**: Detection of known and unknown DDoS attacks using Artificial Neural Networks, Neurocomputing, Vol. 172, 2016, str. 385–393

[42] **Perakovic, D.**, **Perisa, M.**, **Cvitic, I.**, **Husnjak, S.**: Artificial neuron network implementation in detection and classification of DDoS traffic, Proceedings of 24th Telecommunications Forum (TELFOR), 2016

[43] **Tuncer, T.**, **Tatar, Y.**: Detection SYN Flooding Attacks Using Fuzzy Logic, 2008 International Conference on Information Security and Assurance (isa 2008), 2008

[44] **Xia, Z.**, **Lu, S.**, **Li, J.**, **Tang, J.**: Enhancing DDoS flood attack detection via intelligent fuzzy logic, Informatica, Vol. 34, 2010, str. 497–507

[45] **Statista**: *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*, 2018, [Online], Dostupno na: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, [Datum pristupa: 24.6.2018].

[46] **Statista**: *The Internet of Things (IoT)* units installed base by category from 2014 to 2020 (in billions)*, 2018, [Online], Dostupno na: https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/, [Datum pristupa: 24.6.2018].

[47] **Cvitić**, **I.**, **Vujic, M.**, **Husnjak, S.**: Classification of Security Risks in the IoT Environment, Proceedings of the 26th DAAAM International Symposium, 2016

[48] **Ali, B.**, **Awad, A.**: Cyber and Physical Security Vulnerability Assessment for IoT-

Based Smart Homes, Sensors, Vol. 18, 2018, str. 817

[49] **Al-Shammari, B.K.J.**, **Al-Aboody, N.**, **Al-Raweshidy, H.S.**: IoT Traffic Management and Integration in the QoS Sustrorted Network, IEEE Internet Things J., Vol. 5, 2018, str. 352–370

[50] **Laner, M.**, **Svoboda, P.**, **Nikaein, N.**, **Rustr, M.**: Traffic models for machine type communications, 10th IEEE International Symposium on Wireless Communication Systems 2013, ISWCS 2013, vol. 9, 2013

[51] **Meidan, Y.**, **Bohadana, M.**, **Mathov, Y.**, **Mirsky, Y.**, **Breitenbacher, D.**, **Shabtai, A.**, **Elovici, Y.**: N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders, IEEE Pervasive Comput., Vol. 13, 2018, str. 1–8

[52] **Sivanathan, A.**, **Sherratt, D.**, **Gharakheili, H.H.**, **Radford, A.**, **Wijenayake, C.**, **Vishwanath, A.**, **Sivaraman, V.**: Characterizing and classifying IoT traffic in smart cities and campuses, 2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017, 2017

[53] **Sivanathan, A.**, **Gharakheili, H.H.**, **Loi, F.**, **Radford, A.**, **Wijenayake, C.**, **Vishwanath, A.**, **Sivaraman, V.**: Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics, IEEE Trans. Mob. Comput., Vol. 18, 2019, str. 1745–1759

[54] **Shafiq, M.Z.**, **Ji, L.**, **Liu, A.X.**, **Pang, J.**, **Wang, J.**: Large-scale measurement and characterization of cellular machine-to-machine traffic, IEEE/ACM Trans. Netw., Vol. 21, 2013, str. 1960–1973

[55] **Hallman, R.**, **Bryan, J.**, **Palavicini, G.**, **Divita, J.**, **Romero-Mariona, J.**: IoDDoS — The Internet of Distributed Denial of Sevice Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets, Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, 2017

[56] **Summerville, D.H.**, **Zach, K.M.**, **Chen, Y.**: Ultra-lightweight deep packet anomaly detection for Internet of Things devices, Proceedings of 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), 2015

[57] **Doshi, R.**, **Apthorpe, N.**, **Feamster, N.**: Machine Learning DDoS Detection for Consumer Internet of Things Devices, 2018 IEEE Security and Privacy Workshops (SPW), 2018

[58] **Ozcelik, M.**, **Chalabianloo, N.**, **Gur, G.**: Software-Defined Edge Defense Against IoT-Based DDoS, Proceedings of 2017 IEEE International Conference on Computer and Information Technology (CIT), 2017

[59] **Peraković, D.**, **Periša, M.**, **Cvitić, I.**: Analysis of the IoT impact on volume of DDoS attacks, Zbornik XXXIII Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2015, 2015

[60] **Vlajic, N.**, **Zhou, D.**: IoT as a Land of Ostrortunity for DDoS Hackers, Computer (Long. Beach. Calif)., Vol. 51, 2018, str. 26–34

[61] **Costa Gondim, J.**, **de Oliveira Albuquerque, R.**, **Clayton Alves Nascimento, A.**, **García Villalba, L.**, **Kim, T.-H.**: A Methodological Astrroach for Assessing Amplified Reflection Distributed Denial of Service on the Internet of Things, Sensors, Vol. 16, 2016, str. 1855

[62] **Madakam, S.**, **Ramaswamy, R.**, **Tripathi, S.**: Internet of Things (IoT): A Literature Review, J. Comput. Commun., Vol. 03, 2015, str. 164–173

[63] **Patel, K.**, **Patel, S.**: Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, astrlication & future challenges, Int. J. Eng. Sci. Comput., Vol. 6, 2016, str. 6122–6131

[64] **Sarma, S.**, **Brock, D.L.**, **Ashton, K.**: *The Networked Physical World Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identificatio*, SAD, 2000

[65] **Minerva, R.**, **Biru, A.**, **Rotondi, D.**: *Towards a definition of the Internet of Things (IoT)*, Torino, Italija, 2015

[66] **ETSI**: *Machine-to-Machine communications (M2M)-Functional architecture*, Francuska, 2007

[67] **Reddi, V.J.**, **Kim, H.**: On the Internet of Things, IEEE Micro, Vol. 36, 2016, str. 5–7

[68] **Wortmann, F.**, **Flüchter, K.**: Internet of Things, Bus. Inf. Syst. Eng., Vol. 57, 2015, str. 221–224

[69] **European Research Cluster on the Internet of Things**: *Internet of Things - Position Paper on Standardization for IoT Technologies*, Brussels, 2015

[70] **Evans, D.**: *The Internet of Things - How the Next Evolution of the Internet is Changing Everything*, San Francisco, SAD, 2011

[71] **GSM Association**: *Understanding the Internet of Things (IoT)*, 2014

[72] **De Saint-Exupery, A.**: *Internet of Things: Strategic Research Roadmap*, European Commission - Information Society and Media, 2009

[73] **Atzori, L.**, **Iera, A.**, **Morabito, G.**: Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm, Ad Hoc Networks, Vol. 56, 2017, str. 122–140

[74] **Sethi, P.**, **Sarangi, S.R.**: Internet of Things: Architectures, Protocols, and Astrlications, J. Electr. Comput. Eng., Vol. 1, 2017, str. 1–25

[75] **Yun, M.**, **Yuxin, B.**: Research on the architecture and key technology of Internet of Things (IoT) astrlied on smart grid, 2010 International Conference on Advances in Energy Engineering, ICAEE 2010, 2010

[76] **Mashal, I.**, **Alsaryrah, O.**, **Chung, T.-Y.**, **Yang, C.-Z.**, **Kuo, W.-H.**, **Agrawal, D.P.**: Choices for interaction with things on Internet and underlying issues, Ad Hoc Networks, Vol. 28, 2015, str. 68–90

[77] **Furdík, K.**, **Lukac, G.**, **Sabol, T.**, **Kostelnik, P.**: The Network Architecture Designed for an Adaptable IoT-based Smart Office Solution, Int. J. Comput. Networks Commun. Secur., Vol. 1, 2013, str. 216–224

[78] **Munir, A.**, **Kansakar, P.**, **Khan, S.U.**: IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things, arXiv, 2017, str. 1–9

[79] **Goleva, R.I.**, **Garcia, N.M.**, **Mavromoustakis, C.X.**, **Dobre, C.**, **Mastorakis, G.**, **Stainov, R.**, **Chorbev, I.**, **Trajkovik, V.**: *AAL and ELE Platform Architecture*,

Ambient Assisted Living and Enhanced Living Environments, Elsevier, 2017, str. 171–209

[80] **Al-Fuqaha, A.**, **Guizani, M.**, **Mohammadi, M.**, **Aledhari, M.**, **Ayyash, M.**: Internet of Things: A Survey on Enabling Technologies, Protocols, and Astrlications, IEEE Commun. Surv. Tutorials, Vol. 17, 2015, str. 2347–2376

[81] **Lin, J.**, **Yu, W.**, **Zhang, N.**, **Yang, X.**, **Zhang, H.**, **Zhao, W.**: A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Astrlications, IEEE Internet Things J., Vol. 4, 2017, str. 1125–1142

[82] **Bandyopadhyay, D.**, **Sen, J.**: Internet of Things: Astrlications and Challenges in Technology and Standardization, 2011

[83] **Sikder, A.K.**, **Petracca, G.**, **Aksu, H.**, **Jaeger, T.**, **Uluagac, A.S.**: A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Astrlications, arXiv, 2018

[84] **Yole Development**: *Ostrortunities for sensors in the IoT astrlications : What are the real growth drivers ?*, SAD, 2015

[85] **SCME**: *Introduction to Transducers, Sensors, and Actuators, Southwest Center for Microsystems Education (SCME) University of New Mexico*, 2014, [Online], Dostupno na: http://engtech.weebly.com/uploads/5/1/0/6/5106995/more_on_transducers_sensors_actuators.pdf, [Datum pristupa: 20.05.2018].

[86] **Ahmed, E.**, **Yaqoob, I.**, **Gani, A.**, **Imran, M.**, **Guizani, M.**: Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges, IEEE Wirel. Commun., Vol. 23, 2016, str. 10–16

[87] **Rawat, P.**, **Singh, K.D.**, **Chaouchi, H.**, **Bonnin, J.M.**: Wireless sensor networks: A survey on recent developments and potential synergies, J. Supercomput., Vol. 68, 2014, str. 1–48

[88] **Mocnej, J.**, **Pekar, A.**, **Seah, W.K.G.**, **Zolotova, I.**: *Network Traffic Characteristics of the IoT Astrlication Use Cases*, 2017, [Online], Dostupno na: https://ecs.victoria.ac.nz/foswiki/pub/Main/TechnicalReportSeries/IoT_network_technologies_embfonts.pdf, [Datum pristupa: 20.06.2018].

[89] **Alam, M.M.**, **Malik, H.**, **Khan, M.I.**, **Pardy, T.**, **Kuusik, A.**, **Le Moullec, Y.**: A survey on the roles of communication technologies in IoT-Based personalized healthcare astrlications, IEEE Access, Vol. 6, 2018, str. 36611–36631

[90] **Vermesan, O.**, **Harrison, M.**, **Vogt, H.**, **Kalaboukas, K.**, **Tomasella, M.**, **Wouters, K.**, **Gusmeroli, S.**, **Haller, S.**: *Cluster of European Research Projects on the Internet of Things: Vision and Challenges for Realising the Internet of Things*, no. March, Publications Office of the European Union, Brussels, 2010

[91] **Vermesan, B.O.**, **Friess, P.**, **Woysch, G.**, **Guillemin, P.**, **Gusmeroli, S.**, **Sundmaeker, H.**, **Bassi, A.**, **Eisenhauer, M.**, **Moessner, K.**: Europe's IoT Strategic Resea, 2012, str. 22–117

[92] **Lobaccaro, G.**, **Carlucci, S.**, **Löfström, E.**: A review of systems and technologies for smart homes and smart grids, Energies, Vol. 9, 2016, str. 1–33

[93] **Patel, K.**, **Khosla, A.**: Home energy management systems in future Smart Grid networks : A systematic review, 2015 1st International Conference on Next Generation Computing Technologies (NGCT), 2015

[94] **Electric, S.**: *Get Connected : Smart Buildings and the Internet of Things*, Andover, SAD, 2018

[95] **Kejriwal, S.**, **Mahajan, S.**: *Smart buildings: How IoT technology aims to add value for real estate companies*, 2016

[96] **Microsoft**: *Transforming buildings with the Internet of Things*, Baltimore, 2016

[97] **Meulen van der, R.**: *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, [Online], Dostupno na: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016, [Datum pristupa: 12.02.2019].

[98] **Ericsson**: Ericsson Mobility Report - November 2013, 2013

[99] **Digicert**: *State of IoT Security Survey 2018*, SAD, 2018

[100] **Vodafone**: *Your IoT-driven future*, 2019

[101] **IHS**: The Internet of Things : a movement , not a market Start revolutionizing the competitive landscape, IHS Markit, 2017

[102] *Smart Home - worldwide | Statista Market Forecast*, [Online], Dostupno na: https://www.statista.com/outlook/279/100/smart-home/worldwide, [Datum pristupa: 09.03.2019].

[103] **Blumtritt, C.**: *Smart Home Report 2019 – Control and Connectivity*, Hamburg, 2019

[104] **Blumtritt, C.**: *Smart Home Report 2019 – Comfort and Lighting*, Hamburg, 2019

[105] **Kaspersky Lab**: *Press Releases & News | Kaspersky Lab*, [Online], Dostupno na: https://www.kaspersky.com/about/press-releases/2017_63-connected-devices-24-people-and-03-pets-per-home-in-the-new-household-20-era, [Datum pristupa: 11.03.2019].

[106] **Meena, S.**, **Gillett, F.E.**: *Forrester Data: Smart Home Devices Forecast, 2017 To 2022 (US)*, 2017, [Online], Dostupno na: https://www.forrester.com/report/Forrester+Data+Smart+Home+Devices+Forecast+2017+To+2022+US/-/E-RES140374, [Datum pristupa: 14.03.2019].

[107] **Statista**: *Unit sales of smart devices worldwide by category worldwide from 2013 to 2020 (in millions)*, 2019, [Online], Dostupno na: https://www.statista.com/statistics/671053/smart-devices-unit-sales-worldwide/, [Datum pristupa: 14.03.2019].

[108] **Telsyte**: *INTERNET OF THINGS @ HOME*, [Online], Dostupno na: https://www.telsyte.com.au/research#/iot-home/, [Datum pristupa: 11.03.2019].

[109] **Cisco**: *Cisco Visual Networking Index (VNI): Forecast and Methodology*, 2019

[110] *Smart Home - Croatia | Statista Market Forecast*, [Online], Dostupno na: https://www.statista.com/outlook/279/131/smart-home/croatia, [Datum pristupa:

09.03.2019].

[111] **Alam, M.R.**, **Reaz, M.B.I.**, **Ali, M.A.M.**: A review of smart homes - Past, present, and future, IEEE Trans. Syst. Man Cybern. Part C Astrl. Rev., Vol. 42, 2012, str. 1190–1203

[112] **Bugeja, J.**, **Jacobsson, A.**, **Davidsson, P.**: On Privacy and Security Challenges in Smart Connected Homes, 2016 European Intelligence and Security Informatics Conference, 2016

[113] **Yang, H.**, **Lee, W.**, **Lee, H.**: IoT Smart Home Adoption: The Importance of Proper Level Automation, J. Sensors, Vol. 2018, 2018, str. 1–11

[114] **De Silva, L.C.**, **Morikawa, C.**, **Petra, I.M.**: State of the art of smart homes, Eng. Astrl. Artif. Intell., Vol. 25, 2012, str. 1313–1321

[115] **Mendes, T.**, **Godina, R.**, **Rodrigues, E.**, **Matias, J.**, **Catalão, J.**: Smart Home Communication Technologies and Astrlications: Wireless Protocol Assessment for Home Area Network Resources, Energies, Vol. 8, 2015, str. 7279–7311

[116] **Li, M.**, **Gu, W.**, **Chen, W.**, **He, Y.**, **Wu, Y.**, **Zhang, Y.**: Smart Home: Architecture, Technologies and Systems, Procedia Comput. Sci., Vol. 131, 2018, str. 393–400

[117] **Amar, Y.**, **Haddadi, H.**, **Mortier, R.**, **Brown, A.**, **Colley, J.**, **Crabtree, A.**: An Analysis of Home IoT Network Traffic and Behaviour, arXiv:1803.05368, 2018

[118] **Statista**: *Smart Home Report 2019*, Hamburg, 2019

[119] **Hamernik, P.**, **Tanuska, P.**, **Mudroncik, d.**: Classification of Functions in Smart Home, Int. J. Inf. Educ. Technol., Vol. 2, 2013, str. 149–155

[120] **Cvitić, I.**, **Peraković, D.**, **Periša, M.**, **Botica, M.**: Smart Home IoT Traffic Characteristics as a Basis for DDoS Traffic Detection, Proceedings of the 3rd EAI International Conference on Management of Manufacturing Systems, 2018

[121] **IHS Markit**: *Connectivity Technologies*, 2017

[122] **Meng, Y.**, **Zhang, W.**, **Zhu, H.**, **Shen, X.S.**: Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures, IEEE Wirel. Commun., Vol. 25, 2018, str. 53–59

[123] **Nikaein, N.**, **Laner, M.**, **Zhou, K.**, **Svoboda, P.**, **Drajic, D.**, **Popovic, M.**, **Krco, S.**: Simple traffic modeling framework for machine type communication, 10th IEEE International Symposium on Wireless Communication Systems 2013, ISWCS 2013, 2013

[124] **Laya, A.**, **Alonso, L.**, **Alonso-Zarate, J.**: Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives, IEEE Commun. Surv. Tutorials, Vol. 16, 2014, str. 4–16

[125] **Laner, M.**, **Nikaein, N.**, **Svoboda, P.**, **Popovic, M.**, **Drajic, D.**, **Krco, S.**: *Traffic models for machine-to-machine (M2M) communications*, Machine-to-machine (M2M) Communications, vol. 43, no. 7, Elsevier, 2015, str. 133–154

[126] **Thomsen, H.**, **Manchon, C.N.**, **Fleury, B.H.**: A traffic model for machine-type communications using spatial point processes, 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017

[127] **Ali, M.S.**, **Hossain, E.**, **Kim, D.I.**: LTE/LTE-A Random Access for Massive Machine-Type Communications in Smart Cities, IEEE Commun. Mag., Vol. 55, 2017, str. 76–83

[128] **Moon, J.**, **Lim, Y.**: A Reinforcement Learning Astrroach to Access Management in Wireless Cellular Networks, Wirel. Commun. Mob. Comput., Vol. 2017, 2017, str. 1–7

[129] **Wang, Y.**, **Cao, K.**, **Elloumi, O.**, **Song, J.**, **Ghamri-doudane, Y.**, **Leung, V.C.M.**, **Miorandi, D.**, **Sicari, S.**, **De Pellegrini, F.**, **Chlamtac, I.**, **Anisetti, M.**, **Bellandi, V.**, **Chehri, A.**, **Qian, Y.**, **Jeon, G.**, **Lee, S.-H.S.**, **Jeong, J.**, **Park, J.**, **Yang, W.**, **Lee, S.-H.S.**, **Zhu, J.Y.**, **Hwang, H.-T.**, **Paper, E.W.**, **Welbourne, E.**, **Battle, L.**, **Cole, G.**, **Gould, K.**, **Rector, K.**, **Raymer, S.**, **Balazinska, M.**, **Gu, Y.**, **Liu, Q.**, **Bonetto, R.**, **Bui, N.**, **Lakkundi, V.**, **Olivereau, A.**, **Serbanati, A.**, **Rossi, M.**, **Balestrini, M.**, **Diez, T.**, **Marshall, P.**, **Gluhak, A.**, **Rogers, Y.**, **Lee, W.H.**, **Tseng, S.S.**, **Shieh, W.Y.**, **Anand, T.M.**, **Ma, X.**, **Yu, H.**: Development of Web-based Collaborative Framework for the Simulation of Embedded Systems, Inf. Sci. (Ny)., Vol. 2014, 2015, str. 8–9

[130] **Jing, Q.**, **Vasilakos, A. V.**, **Wan, J.**, **Lu, J.**, **Qiu, D.**: Security of the Internet of Things: perspectives and challenges, Wirel. Networks, Vol. 20, 2014, str. 2481–2501

[131] **Čolaković, A.**, **Hadzialic, M.**: Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues, Comput. Networks, Vol. 144, 2018, str. 17–39

[132] **Pishva, D.**: Internet of Things: Security and privacy issues and possible solution, International Conference on Advanced Communication Technology, ICACT, no. December, 2017

[133] **Polk, T.**, **Turner, S.**: Security Challenges For the Internet Of Things, Work. Interconnecting Smart Objects with …, 2014, str. 638–643

[134] **Cherdantseva, Y.**, **Hilton, J.**: A Reference Model of Information Assurance, 2013 International Conference on Availability, Reliability and Security, 2013

[135] **Stouffer, K.**, **Falco, J.**, **Scarfone, K.**: *Guide to Industrial Control Systems (ICS) Security : Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)*, Gaithersburg, MD, 2013

[136] **Dahiya, M.**: Issues and Countermeasures for Smart Home Security Research in Engineering Issues and Countermeasures for Smart Home Security, 2017

[137] **Lin, H.**, **Bergmann, N.**: IoT Privacy and Security Challenges for Smart Home Environments, Information, Vol. 7, 2016, str. 44

[138] **Sanatinia, A.**, **Narain, S.**, **Noubir, G.**: Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study, 2013 IEEE Conf. Commun. Netw. Secur. CNS 2013, Vol. 2011, 2013, str. 430–437

[139] **Geneiatakis, D.**, **Kounelis, I.**, **Neisse, R.**, **Nai-Fovino, I.**, **Steri, G.**, **Baldini, G.**: Security and privacy issues for an IoT based smart home, 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017

[140] **Desai, D.**, **Upadhyay, H.**: Security and Privacy Consideration for Internet of Things in Smart Home Environments, Int. J. Eng. Res. Dev., Vol. 10, 2014, str. 73–83

[141] **Apthorpe, N.**, **Reisman, D.**, **Sundaresan, S.**, **Narayanan, A.**, **Feamster, N.**: Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic, 2017

[142] **Akram, H.**, **Konstantas, D.**, **Mahyoub, M.**: A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model, Int. J. Adv. Comput. Sci. Astrl., Vol. 9, 2018

[143] **Zhou, W.**, **Jia, Y.**, **Peng, A.**, **Zhang, Y.**, **Liu, P.**: The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, IEEE Internet Things J., 2018, str. 1–1

[144] **Copos, B.**, **Levitt, K.**, **Bishop, M.**, **Rowe, J.**: Is Anybody Home? Inferring Activity from Smart Home Network Traffic, Proc. - 2016 IEEE Symp. Secur. Priv. Work. SPW 2016, 2016, str. 245–251

[145] **Bitdefender**: *The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018*, 2018

[146] **Schiefer, M.**: Smart Home Definition and Security Threats, 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, 2015

[147] **De Donno, M.**, **Dragoni, N.**, **Giaretta, A.**, **Spognardi, A.**: DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation, Secur. Commun. Networks, Vol. 2018, 2018, str. 1–30

[148] **Sivaraman, V.**, **Chan, D.**, **Earl, D.**, **Boreli, R.**: Smart-Phones Attacking Smart-Homes, Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '16, no. 11, 2016

[149] **Aggarwal, C.C.**: Outlier Analysis, Artif. Intell. Rev., Vol. 24, 2017, str. 379–384

[150] **Hayward, C.**, **Madill, A.**: A Survey of Outlier Detection Methodologies, Artif. Intell. Rev., Vol. 22, 2004, str. 85–126

[151] **Ahmed, M.**, **Naser Mahmood, A.**, **Hu, J.**: A survey of network anomaly detection techniques, J. Netw. Comput. Astrl., Vol. 60, 2016, str. 19–31

[152] **Baddar, S.H.A.**, **Merlo, A.**, **Migliardi, M.**: Anomaly detection in computer networks: A state-of-the-art review, J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Astrl., Vol. 5, 2014, str. 29–64

[153] **Xiong, L.**, **Póczos, B.**, **Schneider, J.**: Group anomaly detection using Flexible Genre Models, Proceedings of the 24th International Conference on Neural Information Processing Systems, 2011

[154] **Difallah, D.E.**, **Cudre-Mauroux, P.**, **McKenna, S.A.**: Scalable anomaly detection for smart city infrastructure networks, IEEE Internet Comput., Vol. 17, 2013, str. 39–47

[155] **Bhardwaj, K.**, **Miranda, J.C.**, **Gavrilovska, A.**: *Towards IoT-DDoS Prevention Using Edge Computing*, *USENIX Workshop on Hot Topics in Edge Computing (HotEdge 18)*, 2018, [Online], Dostupno na: https://www.usenix.org/biblio-1765, [Datum pristupa: 15.03.2019].

[156] **Tripathi, N.**, **Mehtre, B.**: DoS and DDos Attacks: Impact, Analysis and Countermeasures, Natl. Conf. Adv. Comput. Netw. Secur., 2013, str. 1–6

[157] **Hussain, A.**, **Heidemann, J.**, **Papadopoulos, C.**: A framework for classifying denial

of service attacks, Proceedings of the 2003 conference on Astrlications, technologies, architectures, and protocols for computer communications - SIGCOMM ’03, 2003

[158] **De Donno, M.**, **Giaretta, A.**, **Dragoni, N.**, **Spognardi, A.**: A taxonomy of distributed denial of service attacks, 2017 International Conference on Information Society (i-Society), vol. 2018, 2017

[159] **Douligeris, C.**, **Mitrokotsa, A.**: DDoS attacks and defense mechanisms: Classification and state-of-the-art, Comput. Networks, Vol. 44, 2004, str. 643–666

[160] **Cvitić, I.**, **Peraković, D.**, **Periša, M.**, **Husnjak, S.**: An Overview of Distributed Denial of Service Traffic Detection Astrroaches, PROMET - Traffic&Transportation, Vol. 31, 2019, str. 453–464

[161] **Akamai**: *Akamai’s State of the Internet - Security (Q4-2015)*, Massachusetts, USA, 2015

[162] **Akamai**: *Akamai’s State of the Internet - Security (Q4-2016)*, Massachusetts, USA, 2016

[163] **Somani, G.**, **Gaur, M.S.**, **Sanghi, D.**, **Conti, M.**, **Buyya, R.**: DDoS attacks in cloud computing: Issues, taxonomy, and future directions, Comput. Commun., Vol. 107, 2017, str. 30–48

[164] **Asosheh, A.**, **Ramezani, N.**: A comprehensive taxonomy of DDoS attacks and defense mechanism astrlying in a smart classification, WSEAS Trans. Comput., Vol. 7, 2008, str. 281–290

[165] **Specht, S.**, **Lee, R.**: Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures, Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004

[166] **Gupta, B.B.**, **Joshi, R.C.**, **Misra, M.**: Defending against distributed denial of service attacks: Issues and challenges, Inf. Secur. J., Vol. 18, 2009, str. 224–247

[167] **Mahjabin, T.**, **Xiao, Y.**, **Sun, G.**, **Jiang, W.**: A survey of distributed denial-of-service attack, prevention, and mitigation techniques, Int. J. Distrib. Sens. Networks, Vol. 13, 2017, str. 1–32

[168] **Chang, R.K.C.**: Defending against flooding-based distributed denial-of-service attacks: a tutorial, J. IEEE Commun. Mag., Vol. 40, 2002, str. 42–51

[169] **Scarfone, K.**, **Soustraya, M.**, **Cody, A.**, **Orebaugh, A.**: *Technical Guide to Information Security Testing and Assessment*, 2008

[170] **Patrikakis, C.**, **Masikos, M.**, **Zouraraki, O.**: Distributed Denial of Service Attacks, Internet Protoc. J., Vol. 7, 2004, str. 13–36

[171] **Fachkha, C.**, **Bou-Harb, E.**, **Debbabi, M.**: Inferring distributed reflection denial of service attacks from darknet, Comput. Commun., Vol. 62, 2015, str. 59–71

[172] **Prolexic**: *Prolexic Quarterly Global DDoS Attack Report (Q1-2013)*, Prolexic Technologies, Inc., 2014

[173] **Antonakakis, M.**, **April, T.**, **Bailey, M.**: Understanding the Mirai Botnet, Proceedings of the 26th USENIX Security Symposium, 2017

[174] **Xu, Y.**: *Backbone Network DRDoS Attack Monitoring and Analysis*, 2017, [Online], Dostupno na: https://cybatk.com/2017/01/15/FloCon-2017/BackboneNetworkDRDoSAttackMonitoringAndAnalysis.pdf, [Datum pristupa: 18.05.2019].

[175] **Abliz, M.**: Internet Denial of Service Attacks and Defense Mechanisms, Univ. Pittsbg., 2011, str. 50

[176] **Kenig, R.**, **Manor, D.**, **Gadot, Z.**, **Trauner, D.**: *DDoS Survival Handbook*, Radware, 2013

[177] **Zargar, T.S.**: *Towards Coordinated , Network-Wide Traffic Monitoring for Early Detection of DDoS Flooding Attacks*, University of Pittsburgh, School of Information Sciences, 2015

[178] **Alomari, E.**, **Manickam, S.**, **B. Gupta, B.**, **Karustrayah, S.**, **Alfaris, R.**: Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art, Int. J. Comput. Astrl., Vol. 49, 2012, str. 24–32

[179] **NSFOCUS**: *Common DDoS Attacks*, 2019, [Online], Dostupno na: https://www.infosecurityeurope.com/__novadocuments/58389?v=635430220684370000, [Datum pristupa: 10.03.2019].

[180] **Alexandru, G.**, **Raj, S.**, **Marc, R.**: Classification of UDP Traffic for DDoS Detection, LEET'12 Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, 2012

[181] **Trabelsi, Z.**, **Alketbi, L.**: Using network packet generators and snort rules for teaching denial of service attacks, Proceedings of the 18th ACM conference on Innovation and technology in computer science education - ITiCSE '13, 2013

[182] **Bitdefender**: *78% of Malware Activity in 2018 Driven by IoT Botnets*, [Online], Dostupno na: https://www.bitdefender.com/box/blog/iot-news/78-malware-activity-2018-driven-iot-botnets-nokia-finds/, [Datum pristupa: 01.04.2019].

[183] **Angrishi, K.**: Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets, Mind Lang., Vol. 19, 2017, str. 113–146

[184] **Kolias, C.**, **Kambourakis, G.**, **Stavrou, A.**, **Voas, J.**: DDoS in the IoT: Mirai and Other Botnets, Computer (Long. Beach. Calif)., Vol. 50, 2017, str. 80–84

[185] **Bertino, E.**, **Islam, N.**: Botnets and Internet of Things Security, Computer (Long. Beach. Calif)., Vol. 50, 2017, str. 76–79

[186] **Spognardi, A.**, **Donno, M. De**, **Dragoni, N.**, **Giaretta, A.**: Analysis of DDoS-Capable IoT Malwares, Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, vol. 11, 2017

[187] **Lopez-Martin, M.**, **Carro, B.**, **Sanchez-Esguevillas, A.**, **Lloret, J.**: Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things, IEEE Access, Vol. 5, 2017, str. 18042–18050

[188] **Bekerman, D.**, **Shapira, B.**, **Rokach, L.**, **Bar, A.**: Unknown malware detection using network traffic classification, 2015 IEEE Conference on Communications and Network Security (CNS), 2015

[189] **Bai, L.**, **Yao, L.**, **Kanhere, S.S.**, **Wang, X.**, **Yang, Z.**: Automatic Device

Classification from Network Traffic Streams of Internet of Things, arXiv, 2018

[190] **Meidan, Y.**, **Bohadana, M.**, **Shabtai, A.**, **Ochoa, M.**, **Tistrenhauer, N.O.**, **Guarnizo, J.D.**, **Elovici, Y.**: Detection of Unauthorized IoT Devices Using Machine Learning Techniques, arXiv, 2017

[191] **Miettinen, M.**, **Marchal, S.**, **Hafeez, I.**, **Asokan, N.**, **Sadeghi, A.-R.**, **Tarkoma, S.**: IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT, 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017

[192] **Bezawada, B.**, **Bachani, M.**, **Peterson, J.**, **Shirazi, H.**, **Ray, I.**, **Ray, I.**: Behavioral Fingerprinting of IoT Devices, Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security - ASHES '18, 2018

[193] **Bereziński, P.**, **Jasiul, B.**, **Szpyrka, M.**: An Entropy-Based Network Anomaly Detection Method, Entropy, Vol. 17, 2015, str. 2367–2408

[194] **Bhuyan, M.H.**, **Bhattacharyya, D.K.**, **Kalita, J.K.**: Towards generating real-life datasets for network intrusion detection, Int. J. Netw. Secur., Vol. 17, 2015, str. 683–701

[195] **Hamza, A.**, **Ranathunga, D.**, **Gharakheili, H.H.**, **Roughan, M.**, **Sivaraman, V.**: Clear as MUD, Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18, 2018

[196] **Hamza, A.**, **Gharakheili, H.H.**, **Sivaraman, V.**: Combining MUD Policies with SDN for IoT Intrusion Detection, Proceedings of the 2018 Workshop on IoT Security and Privacy - IoT S&P '18, 2018

[197] *Iskon smarthome*, [Online], Dostupno na: https://smarthome.iskon.hr/static/pdf/Upute_basic_paket_SH31_5_B.pdf, [Datum pristupa: 30.09.2019].

[198] *Smart home uređaji | A1 Hrvatska*, [Online], Dostupno na: https://www.a1.hr/privatni/promocije/smarthome/uredaji, [Datum pristupa: 30-Sep-2019].

[199] **Karimi, A.M.**, **Niyaz, Q.**, **Weiqing Sun**, **Javaid, A.Y.**, **Devabhaktuni, V.K.**: Distributed network traffic feature extraction for a real-time IDS, 2016 IEEE International Conference on Electro Information Technology (EIT), 2016

[200] *GitHub - Markus-Go/bonesi: BoNeSi - the DDoS Botnet Simulator*, [Online], Dostupno na: https://github.com/Markus-Go/bonesi, [Datum pristupa: 07.08.2019].

[201] **Aghaei-Foroushani, V.**, **Zincir-Heywood, A.N.**: A Proxy Identifier Based on Patterns in Traffic Flows, 2015 IEEE 16th International Symposium on High Assurance Systems Engineering, 2015

[202] **Habibi Lashkari, A.**, **Draper Gil, G.**, **Mamun, M.S.I.**, **Ghorbani, A.A.**: Characterization of Tor Traffic using Time based Features, Proceedings of the 3rd International Conference on Information Systems Security and Privacy, no. Cic, 2017

[203] **Doshi, R.**, **Apthorpe, N.**, **Feamster, N.**: Machine Learning DDoS Detection for Consumer Internet of Things Devices, 2018 IEEE Security and Privacy Workshops (SPW), 2018

[204] **az, M.A.B.**, **Pacheco, P.S.**, **Seidel, E.J.**, **Ansuj, A.P.**: Classification of the coefficient of variation to variables in beef cattle experiments, Ciência Rural, Vol. 47, 2017, str. 9–12

[205] **Couto, M.F.**, **Peternelli, L.A.**, **Barbosa, M.H.P.**: Classification of the coefficients of variation for sugarcane crops, Ciência Rural, Vol. 43, 2017, str. 957–961

[206] **Romano, F.L.**, **Ambrosano, G.M.B.**, **Magnani, M.B.B. de A.**, **Nouer, D.F.**: Analysis of the coefficient of variation in shear and tensile bond strength tests., J. Astrl. oral Sci., Vol. 13, 2005, str. 243–6

[207] **Ferreira, A.A.S.N. de C.**, **Dourado, L.R.B.**, **Biagiotti, D.**, **Santos, N.P. da S.**, **Nascimento, D.C.N.**, **Sousa, K.R.S.**: Methods for classifying coefficients of variation in experimentation with poultrys, Comun. Sci., Vol. 9, 2019, str. 565–574

[208] **Ernst, P.A.**, **Thompson, J.R.**, **Miao, Y.**: Tukey's transformational ladder for portfolio management, Financ. Mark. Portf. Manag., Vol. 31, 2017, str. 317–355

[209] **Hanusz, Z.**, **Tarasińska, J.**: Normalization of the Kolmogorov–Smirnov and Shapiro–Wilk tests of normality, Biometrical Lett., Vol. 52, 2015, str. 85–93

[210] **Egea, S.**, **Rego Manez, A.**, **Carro, B.**, **Sanchez-Esguevillas, A.**, **Lloret, J.**: Intelligent IoT Traffic Classification Using Novel Search Strategy for Fast-Based-Correlation Feature Selection in Industrial Environments, IEEE Internet Things J., Vol. 5, 2018, str. 1616–1624

[211] **Zainal, A.**, **Maarof, M.A.**, **Shamsuddin, S.M.**: Feature Selection Using Rough Set in Intrusion Detection, TENCON 2006 - 2006 IEEE Region 10 Conference, vol. 1, no. 10, 2006

[212] **Forman, G.**: An Extensive Empirical Study of Feature Selection Metrics for Text Classification, J. Mach. Learn. Res., Vol. 3, 2003, str. 1289–1305

[213] **Inza, I.**, **Larrañaga, P.**, **Blanco, R.**, **Cerrolaza, A.J.**: Filter versus wrastrer gene selection astrroaches in DNA microarray domains, Artif. Intell. Med., Vol. 31, 2004, str. 91–103

[214] **Jovic, A.**, **Brkic, K.**, **Bogunovic, N.**: A review of feature selection methods with astrlications, 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015

[215] **Osanaiye, O.**, **Choo, K.-K.R.**, **Dlodlo, M.**: Analysing Feature Selection and Classification Techniques for DDoS Detection in Cloud, Southern Africa Telecommunication Networks and Astrlications Conference (SATNAC) 2016, 2016

[216] **Yu, L.**, **Liu, H.**: Feature Selection for High-Dimensional Data: A Fast Correlation-Based Filter Solution, Proceedings of the Twentieth International Conference on Machine Learning (ICML-2003), 2003

[217] **Rokach, L.**: *Ensemble Methods for Classifiers*, Data Mining and Knowledge Discovery Handbook, Springer-Verlag, New York, 2006, str. 957–980

[218] **Zhou, S.K.**, **Park, J.H.**, **Georgescu, B.**, **Comaniciu, D.**, **Simopoulos, C.**, **Otsuki, J.**: Image-Based Multiclass Boosting and Echocardiographic View Classification, 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Volume 2 (CVPR'06), vol. 2, 2006

[219] **Longadge, R.**, **Dongre, S.**: Class Imbalance Problem in Data Mining Review, Eur. J. Intern. Med., Vol. 24, 2013, str. 256

[220] **Friedman, J.**, **Hastie, T.**, **Tibshirani, R.**: Additive logistic regression: a statistical view of boosting (With discussion and a rejoinder by the authors), Ann. Stat., Vol. 28, 2000, str. 337–407

[221] **Landwehr, N.**, **Hall, M.**, **Frank, E.**: Logistic Model Trees, Mach. Learn., Vol. 59, 2005, str. 161–205

[222] **Raschka, S.**: Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning, arXiv, 2018

[223] **Hossin, M.**, **Sulaiman, M.N.**: A Review on Evaluation Metrics for Data Classification Evaluations, Int. J. Data Min. Knowl. Manag. Process, Vol. 5, 2015, str. 01–11

[224] **Seletković, A.**, **Pernar, R.**, **Jazbec, A.**, **Ančić, M.**: Točnost klasifikacije satelitske snimke visoke prostorne rezolucije IKONOS za potrebe šumarstva, Šumarski List, Vol. 588, 2008, str. 393–404

[225] **Sasaki, Y.**: *The truth of the F-measure*, 2007, [Online], Dostupno na: https://www.cs.odu.edu/~mukka/cs795sum09dm/Lecturenotes/Day3/F-measure-YS-26Oct07.pdf, [Datum pristupa: 13.06.2019].

[226] **Park, S.H.**, **Goo, J.M.**, **Jo, C.-H.**: Receiver Operating Characteristic (ROC) Curve: Practical Review for Radiologists, Korean J. Radiol., Vol. 5, 2004, str. 11

[227] **Landwehr, N.**, **Hall, M.**, **Frank, E.**: Logistic model trees, Lect. Notes Artif. Intell. (Subseries Lect. Notes Comput. Sci., Vol. 2837, 2003, str. 241–252

[228] **HSSINA, B.**, **MERBOUHA, A.**, **EZZIKOURI, H.**, **ERRITALI, M.**: A comparative study of decision tree ID3 and C4.5, Int. J. Adv. Comput. Sci. Astrl., Vol. 4, 2014, str. 13–19

[229] **Rojas, J.S.**, **Gallón, Á.R.**, **Corrales, J.C.**: *Personalized Service Degradation Policies on OTT Astrlications Based on the Consumption Behavior of Users*, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, str. 543–557

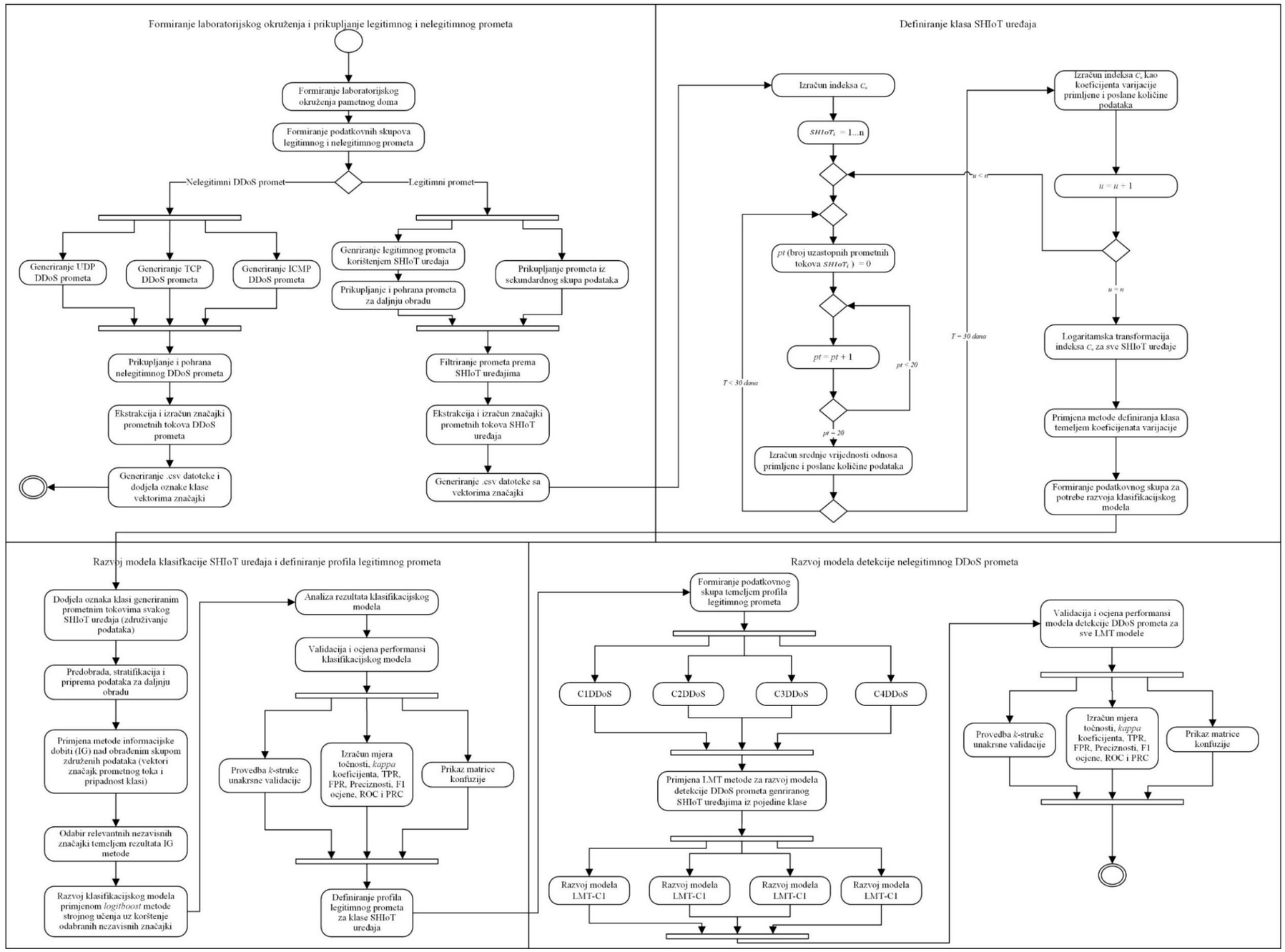
Popis slika

Popis grafikona

Popis tablica

Prilog 1

UML dijagram toka razvoja modela detekcije nelegitimnog DDoS prometa



Prilog 2

Primarni, sekundarni i DDoS podatkovni skup prikupljenog prometa SHIoT uređaja

R.br.	Naziv datoteke	Početak prikupljanja	Završetak prikupljanja	Broj prikupljenih paketa	Veličina datoteke (Byte)	Količina prikupljenih podataka (Byte)	Vremenski period prikupljanja (sekunde)	Prosječna brzina prijenosa podataka (B/s)	Prosječna brzina prijenosa paketa (paketa/s)	Prosječna veličina paketa (Byte)
1.	20000_15_10_2018	15.10.18. 2:00	16.10.2018 2:00	1127061	392238949	374205949	86400,12	4331,08	13,04	332,02
2.	20000_16_10_2018	16.10.18. 2:00	17.10.2018 2:00	1508918	795188049	771045337	86398,88	8924,25	17,46	510,99
3.	20000_17_10_2018	17.10.18. 2:00	18.10.2018 2:00	1617566	895190256	869309176	86399,21	10061,54	18,72	537,42
4.	20000_18_10_2018	18.10.18. 2:00	19.10.2018 2:00	1174870	411633936	392835992	86400,31	4546,70	13,60	334,37
5.	10000_22_11_2018	15.11.18. 18:14	16.11.2018 18:14	1903890	1286509419	1256047155	86399,67	14537,64	22,04	659,73
6.	10000_24_11_2018	24.11.18. 1:00	25.11.2018 0:59	1511253	661217311	637037239	86398,80	7373,22	17,49	421,53
7.	10000_25_11_2018	25.11.18. 1:00	26.11.2018 1:00	3059946	1901226990	1852267830	86399,25	21438,47	35,42	605,33
8.	10000_26_11_2018	26.11.18. 1:00	27.11.2018 1:00	2424369	1249754811	1210964883	86399,57	14015,87	28,06	499,50
9.	10000_27_11_2018	27.11.18. 1:00	28.11.2018 0:59	3636836	2185868991	2127679591	86399,05	24626,19	42,09	585,04
10.	10000_28_11_2018	28.11.18. 1:00	29.11.2018 1:00	2386044	1179684899	1141508171	86399,90	13211,92	27,62	478,41
11.	10000_29_11_2018	29.11.18. 1:00	30.11.2018 1:00	1979119	1174942658	1143276730	86400,11	13232,35	22,91	577,67
12.	10000_30_11_2018	30.11.18. 1:00	1.12.2018 1:00	3835838	2876031956	2814658524	86399,58	32577,23	44,40	733,78
13.	10000_1_12_2018	1.12.18. 1:00	2.12.2018 1:00	3712770	2814770790	2755366446	86400,06	31890,79	42,97	742,13
14.	10000_2_12_2018	2.12.18. 1:00	3.12.2018 1:00	4886026	4048446609	3970270169	86399,93	45952,24	56,55	812,58
15.	10000_3_12_2018	3.12.18. 1:00	4.12.2018 1:00	1933008	916427488	885499336	86399,65	10248,88	22,37	458,09
16.	10000_4_12_2018	4.12.18. 1:00	5.12.2018 1:00	1019339	288056862	271747414	86400,47	3145,21	11,80	266,59
17.	10000_5_12_2018	5.12.18. 1:00	6.12.2018 1:00	1022508	297227474	280867322	86399,52	3250,80	11,83	274,68
18.	10000_6_12_2018	6.12.18. 1:00	7.12.2018 1:00	1294608	544439444	523725692	86400,31	6061,62	14,98	404,54
19.	10000_7_12_2018	7.12.18. 1:00	8.12.2018 1:00	1846672	1079713640	1050166864	86399,71	12154,75	21,37	568,68
20.	10000_17_12_2018	17.12.18. 1:00	18.12.2018 1:00	2275314	1346592060	1310187012	86400,00	15164,20	26,33	575,83
21.	10000_18_12_2018	18.12.18. 1:00	19.12.2018 0:59	4487922	3302382487	3230575711	86398,67	37391,50	51,94	719,84
22.	10000_19_12_2018	19.12.18. 1:00	20.12.2018 1:00	4998914	3863585644	3783602996	86400,40	43791,50	57,86	756,88
23.	10000_20_12_2018	20.12.18. 1:00	21.12.2018 1:00	5006625	4176748870	4096642846	86399,48	47415,13	57,95	818,24
24.	10000_21_12_2018	21.12.18. 1:00	22.12.2018 1:00	3093352	2079965317	2030471661	86399,87	23500,87	35,80	656,40
25.	10000_22_12_2018	22.12.18. 1:00	23.12.2018 0:59	5775398	4840180468	4747774076	86395,49	54953,96	66,85	822,07
26.	10442_23_12_2018	23.12.18. 0:59	24.12.2018 1:00	6377327	5171149959	5069112703	86404,14	58667,47	73,81	794,86
27.	10000_27_12_2018	27.12.18. 1:00	28.12.2018 1:00	1332176	404742310	383427470	86399,71	4437,83	15,42	287,82
28.	10000_28_12_2018	28.12.18. 1:00	29.12.2018 1:00	1154745	315855138	297379194	86399,39	3441,91	13,37	257,53
29.	10000_29_12_2018	29.12.18. 1:00	30.12.2018 1:00	1131742	303873628	285765732	86399,96	3307,48	13,10	252,50
30.	10000_31_12_2018	31.12.18. 1:00	1.1.2019 1:00	6687296	6090938825	5983942065	86399,98	69258,60	77,40	894,82
31.	10000_1_1_2019	1.1.2019 1:00	2.1.2019 1:00	7455754	6630145986	6510853898	86399,97	75357,14	86,29	873,27
32.	10000_2_1_2019	2.1.2019 1:00	3.1.2019 1:00	2909079	1804161208	1757615920	86399,89	20342,80	33,67	604,18
33.	10000_3_1_2019	3.1.2019 1:00	4.1.2019 1:00	5339112	4383892980	4298467164	86399,92	49750,82	61,80	805,09
34.	10000_4_1_2019	4.1.2019 1:00	5.1.2019 1:00	8035771	6812427999	6683855639	86399,95	77359,48	93,01	831,76
35.	10000_5_1_2019	5.1.2019 1:00	6.1.2019 1:00	7349329	6054444387	5936855099	86400,04	68713,57	85,06	807,81
36.	10000_6_1_2019	6.1.2019 1:00	7.1.2019 1:00	10447146	8521885260	8354730900	86399,67	96698,65	120,92	799,71
37.	10000_7_1_2019	7.1.2019 1:00	8.1.2019 0:59	1839711	768772795	739337395	86399,53	8557,19	21,29	401,88
38.	10000_8_1_2019	8.1.2019 1:00	9.1.2019 1:00	3010604	2073785576	2025615888	86399,76	23444,69	34,85	672,83

39.	10000_9_1_2019	9.1.2019 1:00	10.1.2019 1:00	1520462	638968162	614640746	86399,67	7113,93	17,60	404,25
40.	10000_10_1_2019	10.1.2019 1:00	11.1.2019 1:00	4906740	3766013571	3687505707	86400,06	42679,44	56,79	751,52
41.	10003_11_1_2019	11.1.2019 1:00	12.1.2019 0:59	3326651	2499008464	2445782024	86398,92	28308,02	38,50	735,21
42.	10000_12_1_2019	12.1.2019 1:00	13.1.2019 1:00	1804171	756173211	727306451	86399,98	8417,90	20,88	403,13
43.	10000_13_1_2019	13.1.2019 1:00	14.1.2019 1:00	3392490	2003771504	1949491640	86399,90	22563,59	39,26	574,65
44.	10000_14_1_2019	14.1.2019 1:00	15.1.2019 1:00	7590730	6505508101	6384056397	86399,64	73889,85	87,86	841,03
45.	10009_15_1_2019	15.1.2019 1:00	16.1.2019 1:00	4073428	3276682633	3211507761	86399,80	37170,31	47,15	788,40
46.	10001_16_1_2019	16.1.2019 1:00	17.1.2019 1:00	4577307	3578039011	3504802075	86399,74	40564,96	52,98	765,69
47.	10000_17_1_2019	17.1.2019 1:00	18.1.2019 1:00	2400555	1515611017	1477202113	86400,11	17097,23	27,78	615,36
48.	10000_18_1_2019	18.1.2019 1:00	19.1.2019 1:00	3698220	2610137101	2550965557	86399,38	29525,27	42,80	689,78
49.	10000_19_1_2019	19.1.2019 1:00	20.1.2019 1:00	4749288	3614591586	3538602954	86399,78	40956,16	54,97	745,08
50.	10028_20_1_2019	20.1.2019 1:00	21.1.2019 1:00	6232739	5178140438	5078416590	86399,82	58778,09	72,14	814,80
51.	10000_21_1_2019	21.1.2019 1:00	22.1.2019 1:00	3340803	2267676987	2214224115	86400,33	25627,50	38,67	662,78
52.	10000_23_1_2019	23.1.2019 1:00	24.1.2019 1:00	4726719	3655674777	3580047249	86399,49	41435,98	54,71	757,41
53.	10000_24_1_2019	24.1.2019 1:00	25.1.2019 1:00	4393245	3513225338	3442933394	86400,13	39848,71	50,85	783,69
54.	10000_25_1_2019	25.1.2019 1:00	26.1.2019 1:00	2785631	1861475164	1816905044	86400,12	21028,96	32,24	652,24
55.	10000_26_1_2019	26.1.2019 1:00	27.1.2019 1:00	5545282	4772782421	4684057885	86399,44	54213,98	64,18	844,69
56.	10000_27_1_2019	27.1.2019 1:00	28.1.2019 1:00	3308361	2358529439	2305595639	86400,57	26684,96	38,29	696,90
57.	10000_28_1_2019	28.1.2019 1:00	29.1.2019 1:00	4255308	1612648592	1544563640	86399,31	17877,04	49,25	362,97
58.	10000_29_1_2019	29.1.2019 1:00	30.1.2019 1:00	2371696	1742108833	1704161673	86400,08	19724,07	27,45	718,54
59.	10000_30_1_2019	30.1.2019 1:00	31.1.2019 1:00	5210301	4451202370	4367837530	86400,27	50553,52	60,30	838,31
60.	10000_1_2_2019	1.2.2019 1:00	2.2.2019 1:00	7294254	5849241056	5732532968	86399,56	66349,10	84,42	785,90
61.	10004_2_2_2019	2.2.2019 1:00	3.2.2019 1:00	4992031	3881412013	3801539493	86399,76	43999,42	57,78	761,52
62.	10048_3_2_2019	3.2.2019 1:00	4.2.2019 1:00	10169612	9138103522	8975389706	86400,01	103881,82	117,70	882,57
63.	10000_4_2_2019	4.2.2019 1:00	5.2.2019 1:00	5591490	4534241078	4444777214	86400,09	51444,13	64,72	794,92
64.	10000_5_2_2019	5.2.2019 1:00	6.2.2019 1:00	3136197	2278013846	2227834670	86399,72	25785,21	36,30	710,36
65.	10000_6_2_2019	6.2.2019 1:00	7.2.2019 1:00	3334642	1845007103	1791652807	86399,19	20736,92	38,60	537,28
66.	10000_7_2_2019	7.2.2019 1:00	8.2.2019 1:00	3360055	2363337686	2309576782	86399,50	26731,37	38,89	687,36
67.	10000_8_2_2019	8.2.2019 1:00	9.2.2019 1:00	2506412	1976584887	1936482271	86400,54	22412,85	29,01	772,61
68.	10000_9_2_2019	9.2.2019 1:00	10.2.2019 1:00	1921541	1213718999	1182974319	86399,54	13691,91	22,24	615,64
69.	10000_10_2_2019	10.2.2019 1:00	11.2.2019 1:00	1694663	1000114218	972999586	86399,61	11261,62	19,61	574,16
70.	10000_11_2_2019	11.2.2019 1:00	12.2.2019 1:00	2925503	2328092860	2281284788	86400,02	26403,75	33,86	779,79
71.	10000_12_2_2019	12.2.2019 1:00	13.2.2019 1:00	4687408	3963805304	3888806752	86398,69	45010,02	54,25	829,63
72.	10000_13_2_2019	13.2.2019 1:00	14.2.2019 1:00	1246008	433488746	413552594	86399,77	4786,50	14,42	331,90
73.	10000_15_2_2019	15.2.2019 1:00	16.2.2019 1:00	3948710	2942758763	2879579379	86399,58	33328,63	45,70	729,25
74.	10000_28_2_2019	28.2.2019 1:00	1.3.2019 1:00	3108328	2225861424	2176128152	86399,20	25186,90	35,98	700,10
75.	10000_1_3_2019	1.3.2019 1:00	2.3.2019 1:00	7884147	5869441329	5743294953	86399,65	66473,59	91,25	728,46
76.	10000_2_3_2019	2.3.2019 1:00	3.3.2019 0:59	7816823	6425564268	6300495076	86398,48	72923,68	90,47	806,02
77.	10314_3_3_2019	3.3.2019 0:59	4.3.2019 1:00	3469817	2641944114	2586427018	86401,63	29934,93	40,16	745,41
78.	10000_4_3_2019	4.3.2019 1:00	5.3.2019 1:00	1253126	538436599	518386559	86399,61	5999,87	14,50	413,67
79.	10000_6_3_2019	6.3.2019 1:00	7.3.2019 1:00	3914427	2956066905	2893436049	86400,51	33488,64	45,31	739,17
80.	10000_7_3_2019	7.3.2019 1:00	8.3.2019 0:59	3312060	2381681524	2328688540	86399,21	26952,66	38,33	703,09
81.	10000_8_3_2019	8.3.2019 1:00	9.3.2019 1:00	7423337	6246525341	6127751925	86400,05	70923,01	85,92	825,47
82.	10000_9_3_2019	9.3.2019 1:00	10.3.2019 0:59	7833888	6931998361	6806656129	86391,89	78788,14	90,68	868,87
83.	10000_10_3_2019	10.3.2019 0:59	11.3.2019 1:00	8283385	6987500478	6854966294	86407,46	79333,04	95,86	827,56
84.	10002_11_3_2019	11.3.2019 1:00	12.3.2019 1:00	4889120	4407369174	4329143230	86399,13	50106,33	56,59	885,46

85.	10000_12_3_2019	12.3.2019 1:00	13.3.2019 1:00	3847093	2855959976	2794406464	86400,08	32342,64	44,53	726,37
86.	10000_14_3_2019	14.3.2019 1:00	15.3.2019 1:00	3048100	2188856913	2140087289	86400,09	24769,50	35,28	702,11
87.	10000_15_3_2019	15.3.2019 1:00	16.3.2019 1:00	6319472	5514153333	5413041757	86399,54	62651,28	73,14	856,57
88.	10000_16_3_2019	16.3.2019 1:00	17.3.2019 0:59	9399614	8370736333	8220342485	86398,10	95144,94	108,79	874,54
89.	10002_17_3_2019	17.3.2019 0:59	18.3.2019 1:00	5289130	4077311869	3992685765	86402,00	46210,57	61,22	754,89
90.	10000_18_3_2019	18.3.2019 1:00	19.3.2019 1:00	4947902	3997033364	3917866908	86399,43	45345,98	57,27	791,82
91.	10000_19_3_2019	19.3.2019 1:00	20.3.2019 1:00	3111587	1204275590	1154490174	86399,45	13362,24	36,01	371,03
92.	10000_20_3_2019	20.3.2019 1:00	21.3.2019 1:00	7216082	5253673395	5138216059	86399,26	59470,60	83,52	712,05
93.	10000_22_3_2019	22.3.2019 1:00	23.3.2019 1:00	5649729	4877796645	4787400957	86399,41	55410,11	65,39	847,37
94.	10000_23_3_2019	23.3.2019 1:00	24.3.2019 1:01	7431611	6260781528	6141875728	86461,24	71036,17	85,95	826,45
95.	10000_24_3_2019	24.3.2019 1:01	25.3.2019 1:01	9792724	8832994896	8676311288	86399,92	100420,36	113,34	886,00
96.	10000_25_3_2019	25.3.2019 1:01	26.3.2019 1:01	4788338	3779664649	3703051217	86399,96	42859,41	55,42	773,35
97.	10000_26_3_2019	26.3.2019 1:01	27.3.2019 1:01	10142911	8639556175	8477269575	86400,12	98116,41	117,39	835,78
98.	10000_29_3_2019	29.3.2019 1:00	30.3.2019 1:00	8329209	7302559218	7169291850	86399,52	82978,38	96,40	860,74
99.	10000_30_3_2019	30.3.2019 1:00	31.3.2019 1:00	6144234	5172766582	5074458814	86399,91	58732,22	71,11	825,89
100.	10000_31_3_2019	31.3.2019 1:00	1.4.2019 1:59	14815959	13562522315	13325466947	86398,39	154232,81	171,48	899,40
101.	20001_1_4_2019	1.4.2019 1:59	2.4.2019 2:00	3750484	2826412291	2766404523	86401,07	32018,18	43,41	737,61
102.	20000_2_4_2019	2.4.2019 2:00	3.4.2019 2:00	8141980	7296105672	7165833968	86400,36	82937,55	94,24	880,11
103.	20000_3_4_2019	3.4.2019 2:00	4.4.2019 2:00	3213373	2398679415	2347265423	86399,67	27167,53	37,19	730,47
104.	16-10-09	8.10.2016 15:00	9.10.2016 15:00	559444	101397620	82620960	86398,66065	956,28	147,68	6,48
105.	16-10-10	9.10.2016 15:00	10.10.2016 14:59	580488	104278784	84793564	86399,79486	981,41	146,07	6,72
106.	16-10-11	10.10.2016 15:00	11.10.2016 15:00	2073339	1159708764	1090301806	86399,25394	12619,34	525,87	24
107.	16-10-12	11.10.2016 15:00	12.10.2016 5:12	3591404	3201544192	3079686041	51167,36735	60188,48	857,52	70,19
108.	16-09-23	22.9.2016 16:00	23.9.2016 16:00	947072	369972064	338334998	86397,72875	3916,02	357,24	10,96
109.	16-09-24	23.9.2016 16:00	24.9.2016 16:00	799235	338676808	311747136	86396,99523	3608,31	390,06	9,25
110.	16-09-25	24.9.2016 16:00	25.9.2016 16:00	537650	102157816	84121469	86397,32215	973,66	156,46	6,22
111.	16-09-26	25.9.2016 16:00	26.9.2016 15:59	573848	114428448	95175244	86398,74894	1101,58	165,85	6,64
112.	16-09-27	26.9.2016 16:00	27.9.2016 16:00	527035	89615024	71959664	86399,49063	832,87	136,54	6,1
113.	16-09-28	27.9.2016 16:00	28.9.2016 16:00	2019000	1201784320	1133829781	86398,74056	13123,22	561,58	23,37
114.	16-09-29	28.9.2016 16:00	29.9.2016 16:00	738906	156105220	131269731	86397,97449	1519,36	177,65	8,55
115.	16-09-30	29.9.2016 16:00	30.9.2016 16:00	802226	194626836	167654532	86397,99434	1940,49	208,99	9,29
116.	16-10-01	30.9.2016 16:00	1.10.2016 16:00	736136	145294352	120552481	86397,62107	1395,32	163,76	8,52
117.	16-10-02	1.10.2016 16:00	2.10.2016 15:00	607202	105318708	84929427	82797,92716	1025,74	139,87	7,33
118.	16-10-03	2.10.2016 15:00	3.10.2016 15:00	670160	118963924	96458421	86397,976	1116,44	143,93	7,76
119.	16-10-04	3.10.2016 15:00	4.10.2016 15:00	2344991	2214665280	2135249966	86396,83762	24714,45	910,56	27,14
120.	16-10-05	4.10.2016 15:00	5.10.2016 15:00	1655879	652995052	597273748	86398,92406	6912,98	360,7	19,17
121.	16-10-06	5.10.2016 15:00	6.10.2016 14:59	719243	171410936	147259537	86397,35383	1704,44	204,74	8,32
122.	16-10-07	6.10.2016 15:00	7.10.2016 15:00	1362858	685917088	640012867	86398,73832	7407,66	469,61	15,77
123.	16-10-08	7.10.2016 15:00	8.10.2016 15:00	612210	114590784	94027793	86397,4278	1088,32	153,59	7,09
124.	18-10-28	27.10.2018 15:00	28.10.2018 13:59	7720905	1324274300	1073244828	86397,54828	12422,17	139,01	89,36
125.	18-10-29	28.10.2018 14:00	29.10.2018 13:59	1921098	732190340	667406075	86397,93182	7724,79	347,41	22,24
126.	18-05-29	29.5.2018 2:00	30.5.2018 2:00	4775591	3483660828	3322027939	86398,29081	38450,16	695,63	55,27
127.	18-05-31	31.5.2018 2:00	31.5.2018 15:23	2942043	2208591936	2108967124	48204,86766	43750,09	716,84	61,03
128.	18-06-10	10.6.2018 2:00	11.6.2018 2:00	2136429	749758868	677607698	86398,67227	7842,8	317,17	24,73
129.	18-06-12	12.6.2018 1:59	13.6.2018 1:59	2299052	893914480	816233687	86399,39216	9447,22	355,03	26,61

130.	18-06-14	14.6.2018 2:00	15.6.2018 1:59	3106106	1449139244	1344239966	86398,13736	15558,67	432,77	35,95
131.	18-06-16	16.6.2018 2:00	17.6.2018 2:00	2127853	739321464	667452100	86388,91842	7726,13	313,67	24,63
132.	18-06-17	17.6.2018 2:00	18.6.2018 1:59	2147648	744210312	671684180	86395,88868	7774,49	312,75	24,86
133.	18-06-18	18.6.2018 1:59	19.6.2018 1:59	2274782	842238620	765429656	86399,02193	8859,24	336,48	26,33
134.	18-06-19	19.6.2018 2:00	20.6.2018 1:59	2232749	802371976	726987984	86398,00667	8414,41	325,6	25,84
135.	18-10-10	9.10.2018 15:00	10.10.2018 15:00	4082069	1479073008	1341876999	86398,12047	15531,32	328,72	47,25
136.	18-10-11	10.10.2018 14:59	11.10.2018 15:00	3732304	1367147188	1241613260	86401,2084	14370,32	332,67	43,2
137.	18-10-12	11.10.2018 15:00	12.10.2018 14:56	4434330	1735065868	1585917318	86171,56988	18404,18	357,65	51,46
138.	18-10-13	12.10.2018 15:00	13.10.2018 15:00	3778146	1229538948	1102445083	86388,61496	12761,46	291,8	43,73
139.	18-10-14	13.10.2018 15:00	14.10.2018 15:00	4564069	1285881560	1132568242	86398,96456	13108,59	248,15	52,83
140.	18-10-15	14.10.2018 15:00	15.10.2018 15:00	5215518	1390161420	1214974409	86400,12212	14062,18	232,95	60,36
141.	18-10-16	15.10.2018 14:59	16.10.2018 15:00	4845398	1638535252	1475428711	86400,55871	17076,61	304,5	56,08
142.	18-10-17	16.10.2018 15:00	17.10.2018 15:00	3160761	1162741752	1055980020	86399,76189	12222,02	334,09	36,58
143.	18-10-18	17.10.2018 15:00	18.10.2018 14:59	3111097	1235245116	1130095577	86397,6309	13080,17	363,25	36,01
144.	18-10-19	18.10.2018 14:59	19.10.2018 14:56	3054441	1214069844	1110839493	86173,9929	12890,66	363,68	35,45

Prilog 3

Značajke prometnog toka korištene u istraživanju

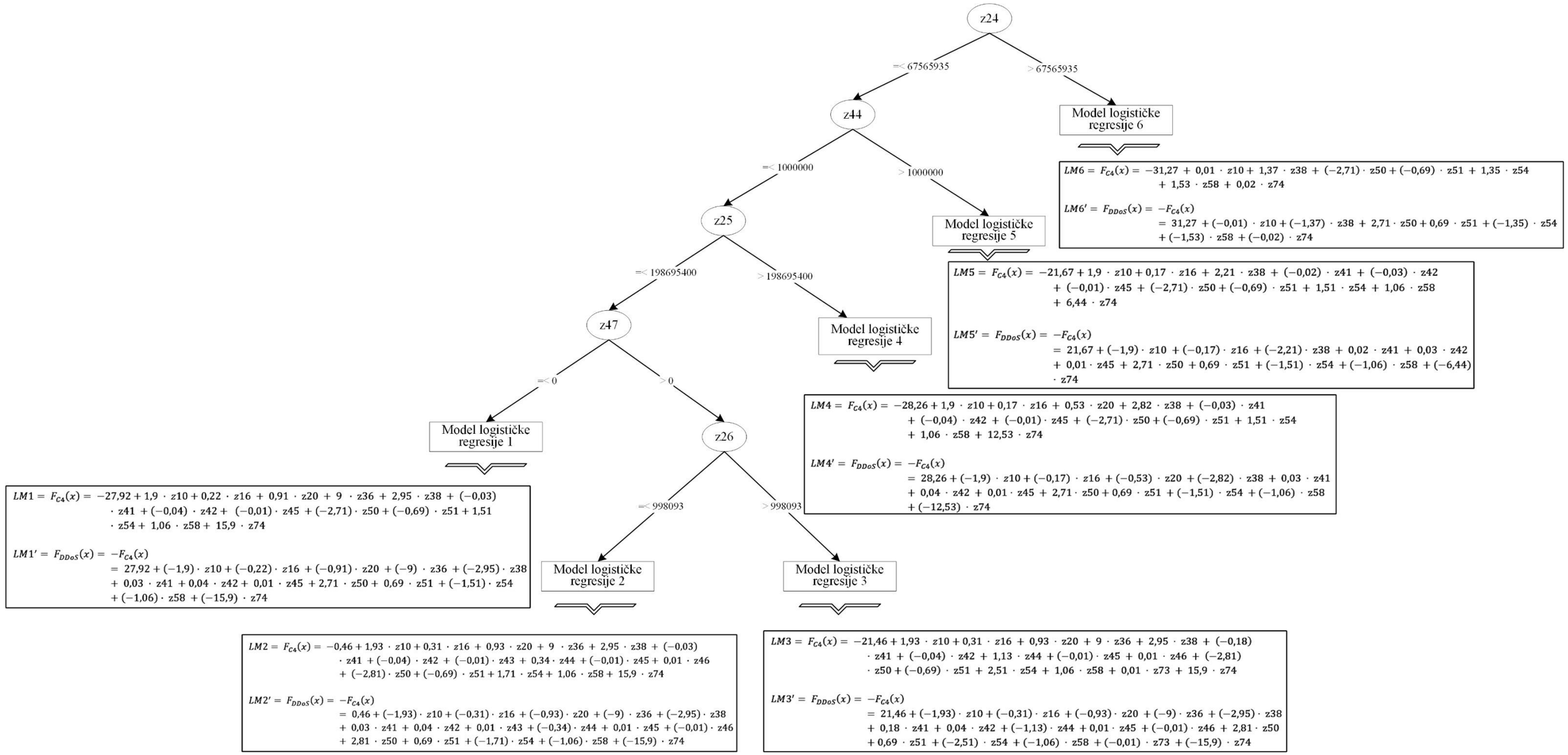
r.br.	Naziv značajke	Oznaka značajke	Opis značajke	Skupina značajki	Vrsta značajke
1.	Flow ID	z1	jedinstvena oznaka prometnog toka	Identifikatori prometnog toka	Značajke koje pružaju informacije povezane s izvorištem i odredištem prometnog toka
2.	Src IP	z2	izvorišna adresa prometnog toka		
3.	Src Port	z3	izvorišni komunikacijski port prometnog toka		
4.	Dst IP	z4	odredišna IP adresa prometnog toka		
5.	Dst Port	z5	odredišni komunikacijski port prometnog toka		
6.	Protocol	z6	korišteni komunikacijski protokol u prometnom toku		
7.	Timestamp	z7	datum i vrijeme početka prometnog toka		
8.	Flow Duration	z8	trajanje toka u milisekundama	Deskriptori prometnog toka	Značajke koje pružaju informacije povezane s karakteristikama prometnog toka
9.	Tot Fwd Pkts	z9	ukupan broj poslanih paketa		
10.	Tot Bwd Pkts	z10	ukupan broj primljenih paketa		
11.	TotLen Fwd Pkts	z11	ukupna duljina poslanih paketa		
12.	TotLen Bwd Pkts	z12	ukupna duljina primljenih paketa		
13.	Fwd Pkt Len Max	z13	maksimalna duljina poslanih paketa		
14.	Fwd Pkt Len Min	z14	Minimalna veličina poslanih paketa		
15.	Fwd Pkt Len Mean	z15	srednja vrijednost duljine poslanih paketa		
16.	Fwd Pkt Len Std	z16	standardna devijacija duljine poslanih paketa		
17.	Bwd Pkt Len Max	z17	maksimalna duljina primljenih paketa		
18.	Bwd Pkt Len Min	z18	minimalna veličina primljenih paketa		
19.	Bwd Pkt Len Mean	z19	srednja vrijednost duljine primljenih paketa		
20.	Bwd Pkt Len Std	z20	standardna devijacija duljine primljenih paketa		
21.	Flow Byts/s	z21	brzina prijenosa podataka za vrijeme trajanja prometnog toka		
22.	Flow Pkts/s	z22	brzina prijenosa paketa za vrijeme trajanja prometnog toka		
23.	Fwd Pkts/s	z43	brzina slanja paketa		
24.	Bwd Pkts/s	z44	brzina primanja paketa		
25.	Pkt Len Min	z45	minimalna duljina paketa		
26.	Pkt Len Max	z46	maksimalna duljina paketa		
27.	Pkt Len Mean	z47	srednja vrijednost duljine paketa		
28.	Pkt Len Std	z48	standardna devijacija duljine paketa		
29.	Pkt Len Var	z49	varijacija duljine paketa		
30.	Down/Up Ratio	z58	odnos primljenog i poslanog prometa		
31.	Fwd Seg Size Avg	z60	prosječna veličina poslanog segmenta		
32.	Fwd Seg Size Min	z75	minimalno vrijeme neaktivnosti prometnog toka		
33.	Bwd Seg Size Avg	z61	prosječna veličina primljenog segmenta		
34.	Fwd Byts/b Avg	z62	prosječno poslano byta po skupnom prijenosu podataka		
35.	Fwd Pkts/b Avg	z63	prosječno poslano paketa po skupnom prijenosu podataka		
36.	Fwd Blk Rate Avg	z64	prosječna brzina slanja pri skupnom prijenosu podataka		

37.	Bwd Byts/b Avg	z65	prosječno primljeno byta po skupnom prijenosu podataka		
38.	Bwd Pkts/b Avg	z66	prosječno primljeno paketa po skupnom prijenosu podataka		
39.	Bwd Blk Rate Avg	z67	prosječna brzina preuzimanja pri skupnom prijenosu podataka		
40.	Flow IAT Mean	z23	srednja vrijednost međudolaznog vremena paketa	Međudolazna vremena paketa	Značajke koje pružaju informacije o međudolaznim vremenima paketa pojedinog prometnog toka u odlaznom i dolaznom smjeru
41.	Flow IAT Std	z24	standardna devijacija međudolaznog vremena paketa		
42.	Flow IAT Max	z25	maksimalno međudolazno vrijeme paketa		
43.	Flow IAT Min	z26	minimalno međudolazno vrijeme paketa		
44.	Fwd IAT Tot	z27	ukupno vrijeme između dva uzastopno poslana paketa		
45.	Fwd IAT Mean	z28	srednje vrijeme između dva poslana paketa		
46.	Fwd IAT Std	z29	standardna devijacija vremena između dva poslana paketa		
47.	Fwd IAT Max	z30	maksimalno vrijeme između dva uzastopno poslana paketa		
48.	Fwd IAT Min	z31	minimalno vrijeme između dva uzastopno poslana paketa		
49.	Bwd IAT Tot	z32	ukupno vrijeme između dva uzastopno primljena paketa		
50.	Bwd IAT Mean	z33	srednje vrijeme između dva primljena paketa		
51.	Bwd IAT Std	z34	standardna devijacija vremena između dva primljena paketa		
52.	Bwd IAT Max	z35	maksimalno vrijeme između dva uzastopno primljena paketa		
53.	Bwd IAT Min	z36	minimalno vrijeme između dva uzastopno primljena paketa		
54.	Fwd PSH Flags	z37	broj PSH oznaka u poslanim paketima	*Flag* oznake	Značajke koje pružaju informacije o *flag* oznakama sadržanim u zaglavlju paketa prenesenih za vrijeme trajanja prometnog toka
55.	Bwd PSH Flags	z38	broj PSH oznaka u primljenim paketima		
56.	Fwd URG Flags	z39	broj URG oznaka u poslanim paketima		
57.	Bwd URG Flags	z40	broj URG oznaka u primljenim paketima		
58.	FIN Flag Cnt	z50	broj paketa sa FIN oznakom		
59.	SYN Flag Cnt	z51	broj paketa sa SYN oznakom		
60.	RST Flag Cnt	z52	broj paketa sa RST oznakom		
61.	PSH Flag Cnt	z53	broj paketa sa PUSH oznakom		
62.	ACK Flag Cnt	z54	broj paketa sa ACK oznakom		
63.	URG Flag Cnt	z55	broj paketa sa URG oznakom		
64.	CWE Flag Count	z56	broj paketa sa CWE oznakom		
65.	ECE Flag Cnt	z57	broj paketa sa ECE oznakom		
66.	Subflow Fwd Pkts	z68	poslano paketa u podtoku	Deskriptori podtoka	Značajke koje pružaju informacije o prometnom podtoku ukoliko on postoji
67.	Subflow Fwd Byts	z69	poslano byta u podtoku		
68.	Subflow Bwd Pkts	z70	primljeno paketa u podtoku		
69.	Subflow Bwd Byts	z71	primljeno byta u podtoku		
70.	Init Fwd Win Byts	z72	byte-a u inicijalnom poslanom TCP prozoru	Deskriptori zaglavlja paketa	Značajke koje pružaju informacije o zaglavlju paketa
71.	Init Bwd Win Byts	z73	byte-a u inicijalnom primljenom TCP prozoru		
72.	Fwd Act Data Pkts	z74	standardna devijacija vremena aktivnosti prometnog toka		
73.	Pkt Size Avg	z59	prosječna veličina paketa		
74.	Fwd Header Len	z41	duljina zaglavlja poslanih paketa		
75.	Bwd Header Len	z42	duljina zaglavlja primljenih paketa		

76.	Active Mean	z76	srednje vrijeme aktivnosti prometnog toka	Brojači vremena prometnog toka	Značajke koje pružaju informacije vezane uz vrijeme aktivnosti i neaktivnosti pojedinog prometnog toka
77.	Active Std	z77	standardna devijacija vremena aktivnosti prometnog toka		
78.	Active Max	z78	maksimalno vrijeme aktivnosti prometnog toka		
79.	Active Min	z79	minimalno vrijeme aktivnosti prometnog toka		
80.	Idle Mean	z80	srednje vrijeme neaktivnosti prometnog toka		
81.	Idle Std	z81	standardna devijacija vremena neaktivnosti prometnog toka		
82.	Idle Max	z82	maksimalno vrijeme neaktivnosti prometnog toka		
83.	Idle Min	z83	minimalno vrijeme neaktivnosti prometnog toka		
84.	Klasa	z84	oznaka klase uređaja temeljena na koeficijentu varijacija odnosa primljenih i poslanih podataka po prometnom toku u vremenskom periodu od 30 uzastopnih dana		

Prilog 4

Prikaz modela detekcije anomalija mrežnog prometa za klasu SHIoT uređaja C4



$LM6 = F_{C4}(x) = -31{,}27 + 0{,}01 \cdot z10 + 1{,}37 \cdot z38 + (-2{,}71) \cdot z50 + (-0{,}69) \cdot z51 + 1{,}35 \cdot z54 + 1{,}53 \cdot z58 + 0{,}02 \cdot z74$

$LM6' = F_{DDoS}(x) = -F_{C4}(x) = 31{,}27 + (-0{,}01) \cdot z10 + (-1{,}37) \cdot z38 + 2{,}71 \cdot z50 + 0{,}69 \cdot z51 + (-1{,}35) \cdot z54 + (-1{,}53) \cdot z58 + (-0{,}02) \cdot z74$

$LM5 = F_{C4}(x) = -21{,}67 + 1{,}9 \cdot z10 + 0{,}17 \cdot z16 + 2{,}21 \cdot z38 + (-0{,}02) \cdot z41 + (-0{,}03) \cdot z42 + (-0{,}01) \cdot z45 + (-2{,}71) \cdot z50 + (-0{,}69) \cdot z51 + 1{,}51 \cdot z54 + 1{,}06 \cdot z58 + 6{,}44 \cdot z74$

$LM5' = F_{DDoS}(x) = -F_{C4}(x) = 21{,}67 + (-1{,}9) \cdot z10 + (-0{,}17) \cdot z16 + (-2{,}21) \cdot z38 + 0{,}02 \cdot z41 + 0{,}03 \cdot z42 + 0{,}01 \cdot z45 + 2{,}71 \cdot z50 + 0{,}69 \cdot z51 + (-1{,}51) \cdot z54 + (-1{,}06) \cdot z58 + (-6{,}44) \cdot z74$

$LM4 = F_{C4}(x) = -28{,}26 + 1{,}9 \cdot z10 + 0{,}17 \cdot z16 + 0{,}53 \cdot z20 + 2{,}82 \cdot z38 + (-0{,}03) \cdot z41 + (-0{,}04) \cdot z42 + (-0{,}01) \cdot z45 + (-2{,}71) \cdot z50 + (-0{,}69) \cdot z51 + 1{,}51 \cdot z54 + 1{,}06 \cdot z58 + 12{,}53 \cdot z74$

$LM4' = F_{DDoS}(x) = -F_{C4}(x) = 28{,}26 + (-1{,}9) \cdot z10 + (-0{,}17) \cdot z16 + (-0{,}53) \cdot z20 + (-2{,}82) \cdot z38 + 0{,}03 \cdot z41 + 0{,}04 \cdot z42 + 0{,}01 \cdot z45 + 2{,}71 \cdot z50 + 0{,}69 \cdot z51 + (-1{,}51) \cdot z54 + (-1{,}06) \cdot z58 + (-12{,}53) \cdot z74$

$LM1 = F_{C4}(x) = -27{,}92 + 1{,}9 \cdot z10 + 0{,}22 \cdot z16 + 0{,}91 \cdot z20 + 9 \cdot z36 + 2{,}95 \cdot z38 + (-0{,}03) \cdot z41 + (-0{,}04) \cdot z42 + (-0{,}01) \cdot z45 + (-2{,}71) \cdot z50 + (-0{,}69) \cdot z51 + 1{,}51 \cdot z54 + 1{,}06 \cdot z58 + 15{,}9 \cdot z74$

$LM1' = F_{DDoS}(x) = -F_{C4}(x) = 27{,}92 + (-1{,}9) \cdot z10 + (-0{,}22) \cdot z16 + (-0{,}91) \cdot z20 + (-9) \cdot z36 + (-2{,}95) \cdot z38 + 0{,}03 \cdot z41 + 0{,}04 \cdot z42 + 0{,}01 \cdot z45 + 2{,}71 \cdot z50 + 0{,}69 \cdot z51 + (-1{,}51) \cdot z54 + (-1{,}06) \cdot z58 + (-15{,}9) \cdot z74$

$LM2 = F_{C4}(x) = -0{,}46 + 1{,}93 \cdot z10 + 0{,}31 \cdot z16 + 0{,}93 \cdot z20 + 9 \cdot z36 + 2{,}95 \cdot z38 + (-0{,}03) \cdot z41 + (-0{,}04) \cdot z42 + (-0{,}01) \cdot z43 + 0{,}34 \cdot z44 + (-0{,}01) \cdot z45 + 0{,}01 \cdot z46 + (-2{,}81) \cdot z50 + (-0{,}69) \cdot z51 + 1{,}71 \cdot z54 + 1{,}06 \cdot z58 + 15{,}9 \cdot z74$

$LM2' = F_{DDoS}(x) = -F_{C4}(x) = 0{,}46 + (-1{,}93) \cdot z10 + (-0{,}31) \cdot z16 + (-0{,}93) \cdot z20 + (-9) \cdot z36 + (-2{,}95) \cdot z38 + 0{,}03 \cdot z41 + 0{,}04 \cdot z42 + 0{,}01 \cdot z43 + (-0{,}34) \cdot z44 + 0{,}01 \cdot z45 + (-0{,}01) \cdot z46 + 2{,}81 \cdot z50 + 0{,}69 \cdot z51 + (-1{,}71) \cdot z54 + (-1{,}06) \cdot z58 + (-15{,}9) \cdot z74$

$LM3 = F_{C4}(x) = -21{,}46 + 1{,}93 \cdot z10 + 0{,}31 \cdot z16 + 0{,}93 \cdot z20 + 9 \cdot z36 + 2{,}95 \cdot z38 + (-0{,}18) \cdot z41 + (-0{,}04) \cdot z42 + 1{,}13 \cdot z44 + (-0{,}01) \cdot z45 + 0{,}01 \cdot z46 + (-2{,}81) \cdot z50 + (-0{,}69) \cdot z51 + 2{,}51 \cdot z54 + 1{,}06 \cdot z58 + 0{,}01 \cdot z73 + 15{,}9 \cdot z74$

$LM3' = F_{DDoS}(x) = -F_{C4}(x) = 21{,}46 + (-1{,}93) \cdot z10 + (-0{,}31) \cdot z16 + (-0{,}93) \cdot z20 + (-9) \cdot z36 + (-2{,}95) \cdot z38 + 0{,}18 \cdot z41 + 0{,}04 \cdot z42 + (-1{,}13) \cdot z44 + 0{,}01 \cdot z45 + (-0{,}01) \cdot z46 + 2{,}81 \cdot z50 + 0{,}69 \cdot z51 + (-2{,}51) \cdot z54 + (-1{,}06) \cdot z58 + (-0{,}01) \cdot z73 + (-15{,}9) \cdot z74$

Životopis autora

Ivan Cvitić rođen je 18.12.1986. u Zagrebu. Srednje obrazovanje stekao je u prirodoslovno-matematičkoj gimnaziji „Matija Antun Reljković“ u Vinkovcima. Na Fakultetu prometnih znanosti, Sveučilišta u Zagrebu završava preddiplomski (2011.) i diplomski studij (2013.) studij prometa, smjer informacijsko komunikacijski promet. Godine 2014. zapošljava se u suradničko zvanje asistent na Zavodu za informacijsko komunikacijski promet, Fakulteta prometnih znanosti, Sveučilišta u Zagrebu. Iste godine upisuje poslijediplomski doktorski studij pri istoj instituciji. Aktivno se bavi znanstveno-istraživačkim radom u domeni informacijsko-komunikacijskog prometa sa fokusom na istraživanje sigurnosti te dostupnosti informacijsko-komunikacijskih usluga i resursa. U autorstvu i koautorstvu objavio je ukupno 41 znanstveni rad u znanstvenim časopisima indeksiranima u CC (*Current Content*), SCI (*Social Citation Index),* SCI-E (*Science Citation Index – Expanded*) i Scopus bazama, te zbornicima međunarodnih znanstvenih konferencija i znanstvenim knjigama.

Godine 2013. dodijeljena mu je Dekanova nagrada za studentski rad naslova Razvoj sustava za upravljanje repom studentske službe Fakulteta prometnih znanosti. Na temelju kvalitete znanstvenog rada *Classification of Security Risks in IoT Environment* 2015. godine dodijeljena mu je FESTO stipendija u svrhu pohađanja četvrte Međunarodne doktorske škole DAAAM (*Danube Adria Association for Automation and Manufacturing*). Iste godine dobio je priznanje međunarodne znanstvene konferencije DAAAM 2015 za najbolju prezentaciju prethodno spomenutog rada.

Suradnik je u Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava pri Zavodu za informacijsko komunikacijski promet Fakulteta prometnih znanosti. Uz sigurnosne aspekte, aktivno istražuje i mogućnosti primjene postupaka digitalne forenzičke analize mrežnog segmenta informacijsko komunikacijskog sustava. Kao suradnik sudjelovao je na više znanstvenih i stručnih projekata.

Popis radova autora

1. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**; Zorić, Petra. Internet of Things Concept for Informing Visually Impaired Persons in Smart Factory Environments. // Industry 4.0: Trends in Management of Intelligent Manufacturing Systems / Knapčíková, Lucia ; Balog, Michal (ur.). Cham: Springer, 2019. str. 69-86 doi:10.1007/978-3-030-14011-3_7
2. Vagaš, Marek; Galajdová, Alena; Šimšík, Dušan; **Cvitić, Ivan** Proposal of an Algorithm for Data Collection and Processing Via RFID Technology. // Research Papers Faculty of Materials Science and Technology Slovak University of Technology, 27 (2019), 45; 19-25 doi:10.2478/rput-2019-0021 (međunarodna recenzija, članak, ostalo)
3. Rákay, Róbert; Galajdová, Alena; Šeminský, Jaroslav; **Cvitić, Ivan** Seleceted Wireless Communication Protocols and their Properties for Use in IoT Systems. // Research Papers Faculty of Materials Science and Technology Slovak University of Technology, 27 (2019), 45; 26-32 doi:10.2478/rput-2019-0022 (međunarodna recenzija, članak, ostalo)
4. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Husnjak, Siniša. An Overview of Distributed Denial of Service Traffic Detection Astrroaches. // Promet - Traffic & Transportation, 31 (2019), 4; 453-464 doi:10.7307/ptt.v31i4.3082 (međunarodna recenzija, članak, znanstveni)
5. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Botica, Mate. Novel astrroach for detection of IoT generated DDoS traffic. // Wireless networks, 25 (2019), 1-14 doi:10.1007/s11276-019-02043-1 (međunarodna recenzija, članak, znanstveni)
6. Forenbacher, Ivan; Husnjak, Siniša; **Cvitić, Ivan**; Jovović, Ivan. Determinants of mobile phone ownership in Nigeria. // Telecommunications policy, 43 (2019), 7; 101812, 12 doi:10.1016/j.telpol.2019.03.001 (međunarodna recenzija, članak, znanstveni)
7. Periša, Marko; Kuljanić, Tibor Mijo; **Cvitić, Ivan**; Kolarovszki, Peter. Conceptual model for informing user with innovative smart wearable device in industry 4.0. // Wireless networks, 25 (2019), 1-12 doi:10.1007/s11276-019-02057-9 (međunarodna recenzija, članak, znanstveni)
8. Periša, Marko; **Cvitić, Ivan**; Peraković, Dragan; Husnjak, Siniša. Beacon Technology for Real-Time Informing the Traffic Network Users about the Environment. // Transport, 34 (2019), 3; 373-382 doi:10.3846/transport.2019.10402 (međunarodna recenzija, članak, znanstveni)
9. **Cvitić, Ivan**; Zorić, Petra; Kuljanić, Tibor Mijo; Musa, Mario Analysis of Network Traffic Features Generated by IoT Devices. // XXXVII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2019 / Radojičić, Valentina ; Bojović, Nebojša ; Marković, Dejan ; Marković, Goran (ur.). Beograd, Srbija: Univerzitet u Beogradu - Saobraćajni fakultet, 2019. str. 193-200 (pozvano predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

10. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Botica, Mate. Smart Home IoT Traffic Characteristics as a Basis for DDoS Traffic Detection. // Proceedings of 3rd EAI International Conference on Management of Manufacturing Systems / Knapčíková, Lucia ; Peraković, Dragan ; Balog, Michal ; Periša, Marko (ur.). Dubrovnik, Hrvatska: EAI, 2018. str. 1-10 doi:10.4108/eai.6-11-2018.2279336 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
11. Husnjak, Siniša; Jovović, Ivan; **Cvitić, Ivan**; Štefanac, Josip. Overview: Operating Systems of Modern Terminal Devices. // RCITD 2018 - Proceedings in Research Conference in Technical Disciplines / Mokrys, Michal ; Badura, Stefan ; Peraković, Dragan (ur.). Žilina, Slovak Republic: EDIS - Publishing Institution of the University of Žilina, 2019. str. 8-13 doi:10.18638/rcitd.2018.6.1.124 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
12. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**. Analysis of the possible astrlication of assistive technology in the concept of Industry 4.0. // PosTel 2018 – XXXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju / Radojičić, Valentina ; Bojović, Nebojša ; Marković, Dejan ; Marković, Goran (ur.). Beograd, Srbija: Univerzitet u Beogradu - Saobraćajni fakultet, 2018. str. 175-184 (pozvano predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
13. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**; Brletić, Luka. Internet of things concept for informing visually impaired persons in indoor environments. // MMS Conference 2017 Proceedings / Balog, Michal ; Knapcikova, Lucia (ur.). Starý Smokovec, Slovakia: EAI, ACM, 2018. str. 1-12 doi:10.4108/eai.22-11-2017.2274670 (plenarno, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
14. Peraković, Dragan; **Cvitić, Ivan**; Kuljanić, Tibor Mijo; Brletić, Luka. Analysis of Wireless Routers Vulnerabilities Astrlied in the Contemporary Networks. // Proceedings of The 6th International Virtual Research Conference in Technical Disciplines (RCITD-2018) / Mokrys, Michal ; Badura, Stefan ; Peraković, Dragan (ur.). Zilina: Publishing Society, 2018. str. 31-37 doi:10.18638/rcitd.2018.6.1.123 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
15. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Husnjak, Siniša. Astrlication Possibilities of Digital Forensic Procedures in Vehicle Telematics Systems. // Proceedings on 18th Internation Conference Transport System Telematics TST'18 / Mikulski, Jerzy (ur.).
16. Peraković, Dragan; Zorić, Petra; Sente, Rosana Elizabeta; **Cvitić, Ivan**. Aktivnosti i rezultati provođenja projekta Utjecaj korištenja mobilnih uređaja na ponašanje vozača tijekom vožnje. // Ceste 2018. Rovinj, Hrvatska, 2018. str. 1-12. (https://www.bib.irb.hr/938524) (ostalo, recenziran, cjeloviti rad (in extenso), stručni)
17. Periša, Marko; Sente, Elizabeta, Rosana; **Cvitić, Ivan**; Kolarovszki, Peter. Astrlication of innovative smart wearable device in industry 4.0. // 3rd EAI International Conference on Management of Manufacturing Systems - MMS 2018 / Knapčíková, Lucia ; Peraković, Dragan ; Balog, Michal ; PEriša, Marko (ur.). Dubrovnik: EAI, 2018. str. 1-10

doi:10.4108/eai.6-11-2018.2279105 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

18. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Husnjak, Siniša. Astrlication Possibilities of Digital Forensic Procedures in Vehicle Telematics Systems. // Zeszyty Naukowe Wyższej Szkoły Technicznej w Katowicach, 1 (2018), 10; 133-144 (međunarodna recenzija, članak, znanstveni)
19. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**; Brletić, Luka. Innovative services for informing visually impaired persons in indoor environments. // EAI Endorsed Transactions on Internet of Things, 4 (2018), 15; e4, 9 doi:10.4108/eai.5-3-2019.156720 (međunarodna recenzija, članak, znanstveni)
20. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**; Husnjak, Siniša. Model for Detection and Classification of DDoS Traffic Based on Artificial Neural Network. // Telfor Journal, 9 (2017), 1; 26-31 doi:10.5937/telfor1701026P (recenziran, članak, znanstveni)
21. Periša, Marko; **Cvitić, Ivan**; Kolarovszki, Peter. Challenges of Information and Communication Technologies Usage in E-Business Systems. // E-Business - State of the Art of ICT Based Challenges and Solutions / Peraković, Dragan (ur.). Rijeka: InTech, 2017. str. 1-19. (https://www.bib.irb.hr/856363)
22. Forenbacher, Ivan; Husnjak, Siniša; **Cvitić, Ivan**. Exploring Digital Divide in Mobile Phone Ownership: Evidence from Nigeria. // Proceedings of The 5th International Virtual Research Conference in Technical Disciplines (RCITD-2017) / Mokrys, Michal ; Badura, Stefan ; Peraković, Dragan (ur.). Žilina, Slovak Republic: EDIS - Publishing Institution of the University of Žilina, 2017. str. 32-37 doi:http://www.dx..org/10.18638/rcitd.2017.5.1.102 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
23. Periša, Marko; **Cvitić, Ivan**; Sente, Rosana Elizabeta. IoT usluge u svrhu povećanja pokretljivosti korisnika u Smart City okruženju. // 37. skup o prometnim sustavima s međunarodnim sudjelovanjem "Automatizacija u prometu 2017" / Šakić, Željko (ur.). Zagreb: KoREMA, 2017. str. 147-151 (predavanje, domaća recenzija, cjeloviti rad (in extenso), stručni)
24. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Botica, Mate. An Overview of the Cyber Security Strategic Management in Republic of Croatia. // RCITD - Proceedings in Research Conference in Technical Disciplines / Mokrys, Michal ; Badura, Stefan ; Peraković, Dragan (ur.). Zilina, Slovakia: EDIS - Publishing Institution of the University of Zilina, 2017. str. 13-18 doi:10.18638/rcitd.2017.5.1 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
25. **Cvitić, Ivan**; Peraković, Dragan; Kuljanić, Tibor Mijo. Availability Factors in Delivery of Information and Communication Resources to Traffic System Users. // 17th International Conference on Transport Systems (TST 2017) Telematics Smart Solutions in Today's Transpor : proceedings , / Mikulski, Jerzy (ur.). Katowice-Ustroń: Springer International Publishing, 2017. str. 28-41 doi:10.1007/978-3-319-66251-0_3 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

26. Periša, Marko; **Cvitić, Ivan**; Sente, Rosana Elizabeta. Comparative Analysis of Mobile Phone Astrlication Solutions Accessibility for informing Visually Impaired Persons in Traffic Environment. // 25th International Symposium on Electronics in Traffic (ISEP 2017) / Rijavec, Robert ; Hernavs, Boštjan ; Godec, Andrej ; Štern, Andrej ; Gostiša, Blaž ; Gorup, Savin ; Anžek, Mario ; Kos, Serđo ; Meše, Pavel (ur.). Ljubljana, Slovenija: Electrotechnical Association of Slovenia, ITS Slovenia, 2017.. (https://www.bib.irb.hr/875278) (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

27. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Musa, Mario. Network Parameters Astrlicable in Detection of Infrastructure Level DDoS Attacks. // Proceedings of papers 25th Telecommunications Forum (TELFOR) 2017, Belgrade, Serbia: TELECOMMUNICATIONS SOCIETY - Belgrade, 2017. 4.22, 4 doi:10.1109/TELFOR.2017.8249347 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

28. Peraković, Dragan; Grgurević, Ivan; Šarić, Željko; Forenbacher, Ivan; Husnjak, Siniša; Jovović, Ivan; **Cvitić, Ivan**; Kordić, Gordana; Sente, Rosana Elizabeta; Zorić, Petra. Using mobile devices while driving in Croatia – preliminary analysis. // Proceedings of The 5th International Virtual Research Conference in Technical Disciplines (RCITD-2017) / Mokrys, Michal ; Badura, Stefan ; Peraković, Dragan (ur.). Žilina, Slovak Republic: EDIS - Publishing Institution of the University of Zilina, 2017. str. 56-61 doi:10.18638/rcitd.2017.5.1.109 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

29. **Cvitić, Ivan**; Peraković, Dragan; Periša, Marko; Jerneić Branimir. Availability Protection of IoT Concept Based Telematics System in Transport. // Challenge of Transport Telematics / Jerzy Mikulski (ur.). Katowice-Ustroń, Poland: Springer International Publishing, 2016. str. 109-121

30. Husnjak, Siniša; Peraković, Dragan; **Cvitić, Ivan**. Relevant Affect Factors of Smartphone Mobile Data Traffic. // Promet – Traffic&Transportation, 28 (2016), 4; 435-444 doi:10.7307/ptt.v28i4.2091 (međunarodna recenzija, članak, znanstveni)

31. Husnjak, Siniša; Peraković, Dragan; **Cvitić, Ivan**. Smartphone Data Traffic Measurement. // 24th International Symposium on Electronics in Transport - ISEP 2016, Ljubljana: Electrotechnical Association of Slovenia, ITS Slovenia, 2016. str. 1-10. (https://www.bib.irb.hr/808052) (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

32. Periša, Marko; **Cvitić, Ivan**; Senete, Rosana Elizabeta. Social Network Customer Requirements Analysis for Visually Impaired People. // RCITD 2016 - Proceedings in Research Conference in Technical Disciplines / Mokrys , Michal ; Badura, Stefan ; Peraković, Dragan (ur.). Zilina, Slovak Republic: EDIS - Publishing Institution of the University of Zilina, 2016. str. 36-44 doi:10.18638/rcitd.2016.4.1 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

33. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**; Husnjak, Siniša. Artificial Neuron Network Implementation in Detection and Classification of DDoS Traffic. // Proceedings of papers 24nd Telecommunications Forum (TELFOR) 2016, Belgrade, Serbia: TELECOMMUNICATIONS SOCIETY - Belgrade, 2016. str. 332-336. (https://www.bib.irb.hr/847519) (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
34. **Cvitić, Ivan**; Vujić, Miroslav; Husnjak, Siniša. Classification of Security Risks in the IoT Environment. // Proceedings of the 26th International DAAAM Symposium "Intelligent Manufacturing & Automation" / Katalinic, B. (ur.). Vienna, Austria: DAAAM International, 2016. str. 731-740 (poster, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
35. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**. Analysis of the IoT impact on volume of DDoS attacks. // 33. Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju - PosTel 2015 / Bakmaz, Miodrag ; Bojović, Nebojša ; Marković, Dejan ; Marković, Goran ; Radojičić, Valentina (ur.). Beograd: Saobraćajni fakultet, Univerziteta u Beogradu, 2015. str. 295-304 (pozvano predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
36. Peraković, Dragan; Periša, Marko; **Cvitić, Ivan**; Sente, Rosana Elizabeta; Radošević, Maja; Zorić, Petra Web 2.0 services for informing elderly people: Web for Health. // RCITD - Proceedings in Research Conference in Technical Disciplines 2015 / Mokrys, Michal ; Badura, Stefan(ur.). Zilina: EDIS - Publishing Institution of the University of Zilina, 2015. str. 65-70 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
37. Periša, Marko; **Cvitić, Ivan**; Križan, Josip Analysis of the Astrlication of Information and Communication Technologies in Product Promotion and Sales. // MODEL SURADNJE ZNANSTVENO NASTAVNIH INSTITUCIJA I GOSPODARSTVA / Ščukanec, Anđelko ; Babić, Darko (ur.). Zagreb: Fakultet prometnih znanosti, 2015. str. 163-174 (poster, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
38. Peraković, Dragan; Husnjak, Siniša; **Cvitić, Ivan**. IoT Infrastructure as a Basis for New Information Services in the ITS Environment. // 22nd Telecommunications Forum (TELFOR) 2014 - Proceeding of Papers Belgrade: Telecommunications Society, Academic Mind, 2014. str. 39-42 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
39. Peraković, Dragan; Husnjak, Siniša; **Cvitić, Ivan**. Comparative Analysis of Enterprise Mobility Management Systems in BYOD Environment. // RCITD 2014 - Proceedings in Research Conference in Technical Disciplines / Ing. Michal Mokrys ; Ing. Stefan Badura, Ph.D. (ur.). Žilina: EDIS - Publishing Institution of the University of Zilina, 2014. str. 76-81 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)
40. Peraković, Dragan; **Cvitić, Ivan**; Remenar, Vladimir. Designing Secure Information and Communication Infrastructure of Faculty of Transport and Traffic Sc iences. // Research Conference in Technical Disciplines / Mokrys, M. ; Badura, S. ; Lieskovsky, A. (ur.).

Zilina, Slovak Republic: EDIS - Publishing Institution of the University of Zilina, 2013. str. 131-136. (https://www.bib.irb.hr/680539) (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)

41. Ćavar, Ivana; Kavran, Zvonko; Jolić, Natalija; Anđelović, Neven; **Cvitić, Ivan**; Gović, Marko. Content-based Recommender System for Textual Documents Written in Croatian. // DATA ANALYTICS 2013, The Second International Conference on Data Analytics / Friedrich Laux, Reutlingen University, Germany (ur.). Porto, Portugal: IARIA, 2013. str. 25-29 (predavanje, međunarodna recenzija, cjeloviti rad (in extenso), znanstveni)