Smart Home IoT Traffic Characteristics as a Basis for DDoS Traffic Detection

Ivan Cvitić[1], Dragan Peraković[2], Marko Periša[3], Mate Botica[4]
{ivan.cvitic@fpz.hr[1], dragan.perakovic@fpz.hr[2], marko.perisa@fpz.hr[3], mate.botica@oiv.hr[4]}

University of Zagreb, Faculty of Transport and Traffic Sciences, Vukelićeva 4, 1000 Zagreb, Croatia[1,2,3], OiV Transmitters and Communications Ltd.[4]

Abstract. Distributed denial of Service (DDoS) attack is a continuous threat to the availability of information and communication resources. The development and growth of acceptance and the continuous increase in the number of devices within the IoT concept provides the platform for the implementation of DDoS attacks of significantly greater traffic intensity than is currently possible. Numerous botnet networks, where the most prominent representative is Mirai botnet, use the inadequate protection of IoT devices in the smart home environment for generating illegitimate DDoS traffic. To further development of the timely DDoS traffic detection generated in the aforementioned environment, this research seeks to establish the diversity of traffic generated by IoT devices in a smart home environment with respect to the traffic generated through human type communication. Research results will represent base for the future development of new models aimed at detecting this specific DDoS traffic type.

Keywords: MTC, HTC, Payload Exchange traffic, Event Driven traffic, Periodic Update traffic, SHIoT

1 Introduction and previous research

The rapid development of hardware, software and communication technologies enabled the development of the IoT (Internet of Things) concept. The IoT concept extends the existing Internet network and implies pervasive network-connected devices that represent the link between the digital and physical environment. Digital environment interacting with the physical through a variety of sensors and actuators that have the function to uniquely represent and manage objects from the physical environment. The sensors and actuators contain resources for communication, processing and storage of data, and enable detection and eventual change of a object state. According to the above-mentioned concept, IoT represents the agglomeration of various technologies that are interrelated with the aim of providing innovative services [1].

The security of a smart home IoT (SHIoT) device is a subject of numerous research. Paper [2] shows the first fundamental empirical analysis of the smart home platform security. Applications developed on the Samsung SmartThings platform have been analyzed and vulnerabilities of such applications to numerous security threats were identified such as access rights escalation, unauthorized access to pin code devices, unauthorized device configuration modifications, and so on. Numerous studies have identified the security challenges of a smart home environment associated with unauthorized data modification, inserting malicious code

MMS 2018, November 06-08, Dubrovnik, Croatia

DOI 10.4108/eai.6-11-2018.2279336

[3], unauthorized remote device management, eavesdropping [1], unauthorized routing [4] and others. Authors of paper [5] conducted a vulnerability assessment of SHIoT devices. The research involved a considerable number of vulnerabilities and related threats whose implementation could have a negative impact on user privacy, user data, traffic content, and disabling resource access as a result of DDoS attacks.

Due to numerous limitations, IoT devices are a potential target or source of various cyber-attacks. The availability of information and communication resources in a smart home environment is a key security challenge and can often be hindered by DDoS attacks. In addition to be the target of attack, devices in the smart home environment are ever more frequent sources of DDoS attacks, or generators of illegal DDoS traffic through unprotected IoT devices associated with the botnet network. An example of such botnet through which many DDoS attacks are performed is the Mirai botnet. Mirai has controlled more than 100,000 inadequately protected SHIoT devices and thus generated illegitimate network traffic (DDoS traffic) to the desired destinations. The problem of DDoS attacks generated by inadequately protected SHIoT devices is the motivation of this research in view of the increase in the number of such devices which can potentially result in more frequent and more intense attacks of this kind in the future. There are currently very few researches dealing with the problem.

This research will identify the differences in the characteristics of the traffic generated by SHIoT devices in relation to traffic generated by the HTC (Human Type Communication) and so far methods used in the detection of this specific form of DDoS traffic will be analyzed. The results of the research will provide a solid basis for further research for the development of detection and management model for DDoS traffic generated through the SHIoT device.

2 Classification of SHIoT devices

The concept of smart home implies automation of processes that take place within a household. For this purpose, network of interconnected mechanical and digital device is applied that can communicate with each other and with the user to create interactive space [6]. This goal can be achieved in two ways [7]:

- identifying user activity as a basis for increasing the degree of automation in the household or
- Applying remote household control to increase comfort levels, increase safety, monitor and reduce energy consumption, and reduce harmful gas emissions and environmental pollution.

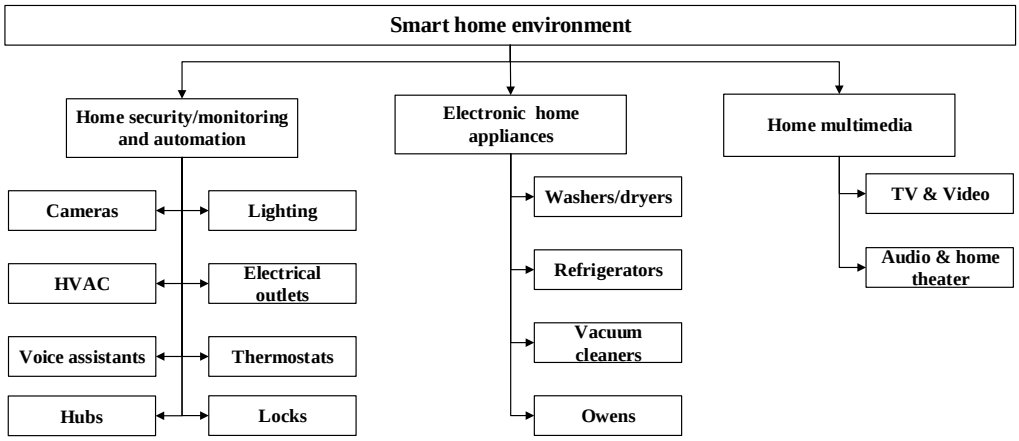

Fig. 1. Classification of SHIoT devices.

Number of research by the smart home environment also include personal computers, smart mobile devices, tablets, and related customer terminals that generate HTC traffic [8]. In the context of this research will be to observe IoT devices applicable in the smart home environment that generates only MTC (Machine Type Communication) traffic and are connected to the Internet network.

SHIoT devices can be categorized into three generic groups, Home security / monitoring and automation, Electric home appliances and Home and multimedia, as shown in Figure 1. Additionally, according to [5] based on the type of the smart home environment management IoT devices can be classified into locally managed devices and remote managed devices. Remote-controlled devices mean that they are connected to the Internet, and locally managed devices are only available within the local communications network to which the devices are connected.

2.1. Smart home architecture

Smart home environment can be observed through a layered architecture that is characteristic for the IoT concept that consists of four basic layers (perception, network, middleware and application) [9], shown in Figure 2. The perception layer includes sensors, actuators and communication technology that allows data transmission to the IoT concentrator located in the network layer. The concentrator in the shown architecture has the role of the gateway. Sensors and actuators use energy-efficient communication technology because of energy requirements (extension of autonomy). The most commonly used in the smart home environment are short-range technologies such as IEEE 802.15.4 ZigBee, ITU-T G.9959 Z-Wave or Bluetooth Low Energy (BLE) [10]. IoT concentrator enables mutual communication of the perception layer device and connection of the perception layer with the access network for transmitting the data to the middleware layer.

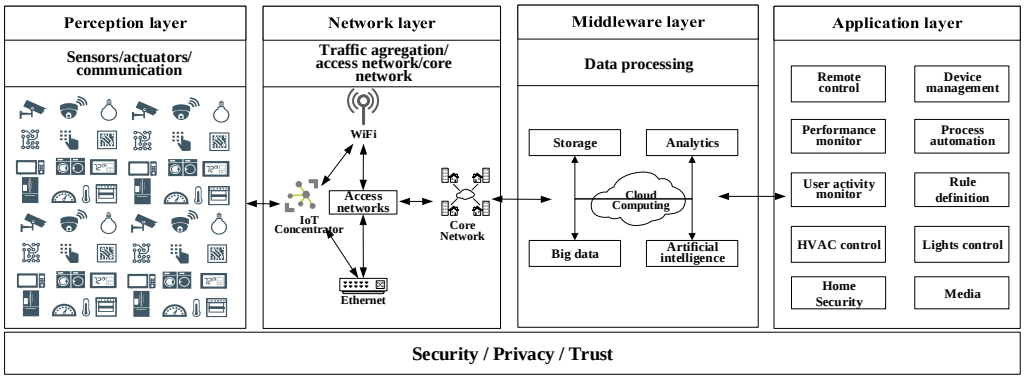

Fig 2. Architecture of smart home environment

Conventional access technologies such as xDSL, fiber optics, mobile data networks (3G, 4G, future 5G) and similar are used to transfer data from a network to a middleware layer. The middleware layer is based on the Cloud Computing concept, and it contains resources and processing elements for dana generated in the middleware layer for converting it into useful information. The middleware layer has three basic functions:

1) remote connectivity of users with SHIoT devices for remote management,
2) automation of SHIoT devices management based on the information obtained without user mediation, and
3) transfer of information to user terminal devices for providing information.

The application layer enables the provision of diverse services as well as remote management of devices by using different applications. Security, privacy and trust in such environments is horizontally oriented and must cover all vertically-oriented layers.

2.2. Penetration of SHIoT devices

According to forecasts, by 2020 the total number of devices that IoT concept combines will be approximately 31 billion, and by 2025 about 75 billion, as presented in Figure 2 [11].

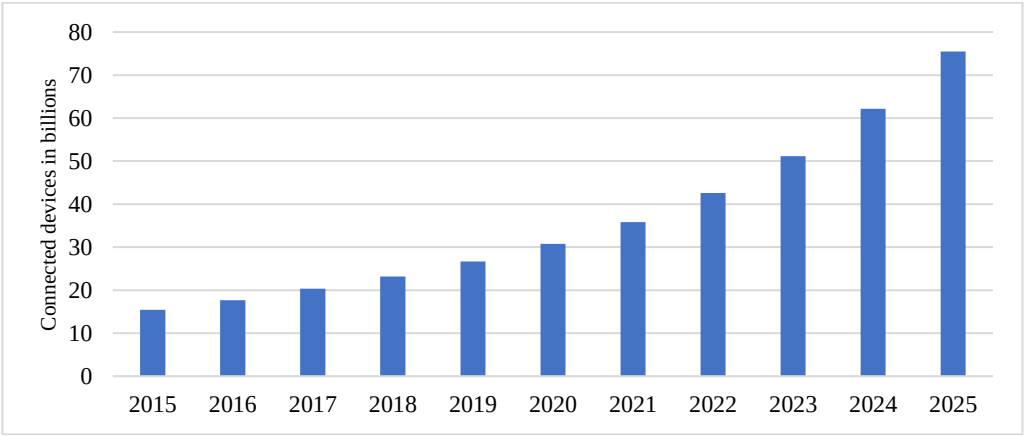

Fig 2. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [11]

Figure 3 shows the number of IoT devices in certain economic segments. There is a significant increase in the number of IoT devices in the consumer sector (SHIoT) compared to other business sectors.

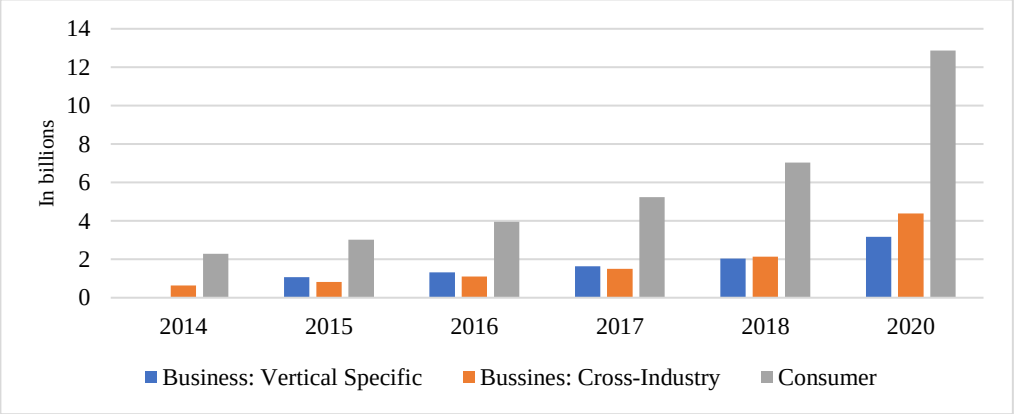

Fig 3. IoT devices installed by category from 2014 – 2020 [12]

Extrapolation of the SHIoT devices growth trend indicates 12,86 billion devices by 2020. According to [13] in 2008. the average household was 2.4 SHIoT devices, in 2015 there were 8.6 SHIoT units in the average household, and in 2022 the average household would contain more than 500 SHIoT devices.

According to the statistical data presented, it can be concluded that the increase in the number of SHIoT devices will also affect the increase of the DDoS traffic intensity generated by such devices [14]. The above indicates an increase in the need for detection methods and DDoS traffic management generated in the smart home environment.

3. Characteristics of MTC traffic

Understanding the nature and characteristics of the traffic generated by SHIoT device is necessary for detection and protection against DDoS attacks generated by such devices. According to the author's knowledge, there are no research aimed at identifying characteristics of exclusively MTC traffic that generate SHIoT devices but generic traffic generating IoT devices in a variety of application areas. Therefore, this research implies applicability of investigated MTC traffic characteristics in the smart home environment.

3.1. Differences between MTC and HTC traffic

Research like [15], [16] i [17] differentiate human-type traffic (HTC) and traffic generated by IoT devices (Machine Type Communication, MTC). The MTC represents the form of data communication between end devices and / or devices and servers that do not necessarily require human interaction [17]. The MTC traffic stream flows from the sensor node (SN) in the perception layer to the packet data network in the network layer. It is dominated by data transfer in uplink. The HTC traffic flow depends on the type of service used and its QoS (Quality of Service) requirements.

Research [17] and [18] identified the following MTC characteristics as compared to HTC traffic:

- the number of packages being transmitted is less than HTC traffic,
- an extended period of time between data transfer (long duty-cycle traffic patterns),
- traffic patterns of a device with similar statistical characteristics,
- domination of outgoing traffic,
- periodic traffic and traffic dependent on events,
- aggregated traffic (combined traffic from multiple sources specific to network nodes such as a gateway).

An important feature of MTC traffic is its homogeneity. All devices that have the same function generate traffic of similar characteristics as opposed to HTC traffic that is heterogeneous in nature [18]. The reason for HTC's heterogeneous nature is the numerous applications running on HTC and the many servers that one HTC device can access. Research [19] found that MTC devices communicate on average with less than 10 servers over a 24-hour time period, while HTC devices communicate with more than 500 different servers over a period of 2 hour.

3.2. Patterns of MTC traffic

Research [20] and [21] identify two samples of MTC traffic, periodic update (PU), and event driven (ED), while research [17] and [18] also define the third pattern, payload exchange (PE).

Periodic update represents the pattern of traffic caused by the transmission of the terminal devices updated value to a central device (e.g. IoT concentrator). This form of transport is not real-time and is characterized by regular time intervals of data transfer and a constant amount of data during each transfer [18].

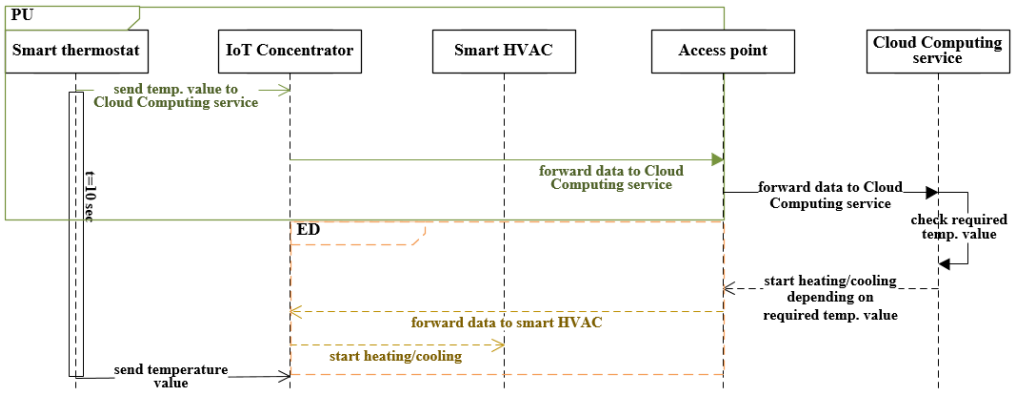

Fig 4. Sequence UML diagram of communication process in which PU and ED traffic patterns are generated

Figure 4 (green box), using the sequential UML diagram, shows the communication process where the PU traffic sample is generated. The smart thermostat periodically transmits the value of the temperature sensor to IoT concentrator to which it is connected and which through the Access Point passes the received data to the Cloud Computing (CC) service for further processing and decision making.

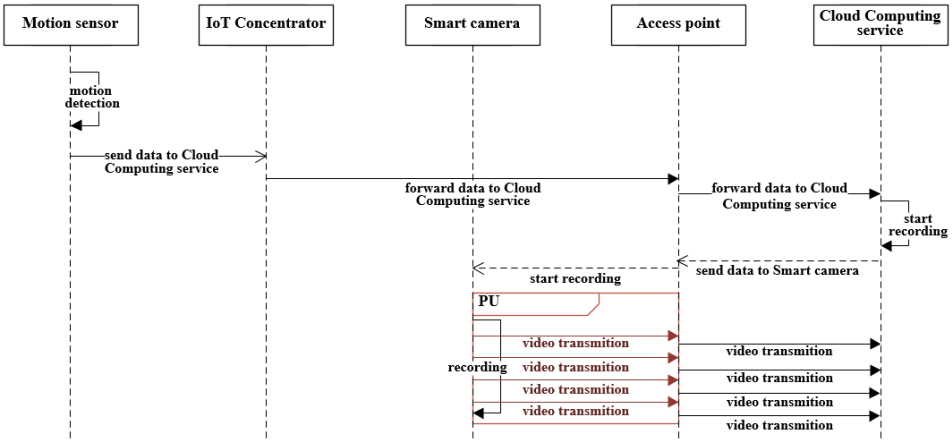

Fig 5. Sequence UML diagram of communication process in which PE traffic pattern is generated

Event-driven (ED) is a traffic pattern that occurs when an event triggers an actuator. The trigger may be a measured value sensor (smart thermostat) or command which is forwarded to the central unit (IoT concentrator) to control an actuator, as shown in Figure 4 (yellow box). The ED traffic pattern is most often real-time, with the variable data sending time. In specific cases, such as traffic that contains configuration data or device software update, the time period for sending data may be constant [17].

The third traffic sample is referred to as payload exchange (PE), and is the consequence of previous traffic patterns (PD and EU). It is understood the transfer of large quantities of data between end IoT devices and servers. This pattern is characterized by the dominance of outbound traffic whose intensity can be constant (when transmitting telemetry data) or variables when transmitting images or videos [18]. Figure 5, using a sequential UML diagram, shows a communication process between end devices (motion sensor and smart camera) communicating via IoT concentrator, access point and CC service. The shown diagram shows an example of generating a PE traffic pattern (red box) when transferring the data traffic generated by a smart camera.

4. Detection of IoT generated DDoS traffic

The characteristics of IoT traffic were used to solve various problems in the IoT network. Paper [15] uses the characteristics of MTC traffic for the purpose of its integration with HTC traffic into the LTE telecommunication network, with the aim of observing the impact of MTC traffic on QoS. Research [22] analyzes MTC traffic for the purpose of determining the characteristics and behavior patterns of IoT devices in a smart city and smart campus environment. Based on the attributes extracted from the collected traffic, the authors have been able to detect MTC from HTC traffic with 95% accuracy and identify specific IoT

devices. The research demonstrated by work [23] seeks to determine whether the MTC will cause new demands and challenges in design and management of the mobile telecommunications network.

IoT environment and MTC traffic is becoming more and more problematic in terms of design and management of telecommunication network (mobile or static) as well as from QoS aspect and mutual integration with HTC traffic. Contrary to researching the problem of detecting and managing the DDoS traffic that such devices can generate are very rare (especially in the smart home environment), Table 1 shows examples of the detection of DDoS traffic in the IoT environment. There have been researches on protection the IoT environment from DDoS attacks as shown in [23] and [24].

One of the first researches of detection DDoS traffic generated through the SHIoT device is [25]. The research is based on the differences between MTC and HTC traffic. The SHIoT device that generates MTC traffic can receive a fixed number of states and accordingly MTC traffic is deterministic and structured. Five methods of machine learning (KNN, SVM, DT, Random Forest and Artificial Neural Networks) were used to detect DDoS traffic, with detection accuracy of 91% to 99%. The lack of the present study is only reflected in the three SHIoT devices used and the 10-minute collection time. Research [26] developed a DDoS traffic detection model generated using SHIoT devices. The model is based on the Deep Autoencoding method, and the experiment has been proven to detect 100% DDoS traffic instances.

Table 1. Examples of IoT DDoS detection research.

Paper	**IoT environment**	**Type of problem**	**Used methods**	**No. of IoT devices for data collection**	**Accuracy**
[27]	General IoT	DDoS traffic detection at source	Software Defined Network	N/A	N/A
[25]	Smart home	DDoS traffic detection at source	k-Nearest Neighbor, Support Vector Machines with Linear Kernel, Decision Tree with Gini impurity scores, Artificial Neural Network	3 SHIoT devices	0,91 - 0,99
[28]	General IoT	Network traffic classification in IoT network for management and administration	Convolutional Neural Network, Recurrent Neural Network	N/A; 266,160 traffic flows	>98%
[26]	Smart home	DDoS traffic detection at source	Deep Autoencoders	9 SHIoT devices	≈100%

Future research needs to focus on the development of new methods of detecting DDoS traffic generated by SHIoT devices due to the increase in the number of such devices in households and their ever-increasing exploitation for creating IoT botnets. The MTC traffic generated by such devices possesses the characteristic features that make the SHIoT devices distinctly distinct from the devices that generate HTC traffic. Likewise, the characteristics of the MTC traffic and the final status of the device may be used to detect anomalies in traffic such as DDoS traffic.

Conclusion

This research shows an overview of MTC traffic characteristics that generate IoT devices. As shown, there are clear differences between MTC and HTC traffic (eg, domination of outbound, periodic, and event-related traffic). In addition, MTC traffic-specific (PU, ED and PE) specimens are notable. Motivation of this research is reflected in the increasing number of SHIoT devices, resulting in the creation of IoT botnet networks by using such devices. SHIoT devices often have limited resources for processing and storing data, so the implemented protection methods are often not adequate. This makes them vulnerable to numerous security threats, and one of their major exploitation is to generate DDoS traffic to number of destinations. The displayed characteristics of MTC traffic and differences in relation to HTC traffic provide the basis for the development of new DDoS traffic detection methods that generate SHIoT devices, which will be based on a limited number of states in which the devices may be contained, as well as on the predictability of traffic generated by such devices at the observed moment.

References

[1] J. Bugeja, A. Jacobsson, and P. Davidsson, “On Privacy and Security Challenges in Smart Connected Homes,” in 2016 European Intelligence and Security Informatics Conference, pp. 172–175 (2016)

[2] E. Fernandes, J. Jung, and A. Prakash, “Security Analysis of Emerging Smart Home Applications,” in IEEE Symposium on Security and Privacy 2016, pp. 636–654 (2016)

[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142 (2017)

[4] A. C. Jose and R. Malekian, “Improving Smart Home Security: Integrating Logical Sensing into Smart Home,” IEEE Sens. J., vol. 17, no. 13, pp. 4269–4286 (2017)

[5] B. Ali and A. Awad, “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes,” Sensors, vol. 18, no. 3, p. 817 (2018)

[6] G. Lobaccaro, S. Carlucci, and E. Löfström, “A review of systems and technologies for smart homes and smart grids,” Energies, vol. 9, no. 5, pp. 1–33 (2016)

[7] A. Saad al-sumaiti, M. H. Ahmed, and M. M. A. Salama, “Smart Home Activities: A Literature Review,” Electr. Power Components Syst., vol. 42, no. 3–4, pp. 294–305 (2014)

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

[9] I. Cvitić, M. Vujić, and S. Husnjak, “Classification of Security Risks in the IoT Environment,” in 26-th Daaam International Symposium on Intelligent Manufacturing and Automation, pp. 0731–0740 (2016)

[10] J. Mocnej, A. Pekar, W. K. G. Seah, and I. Zolotova, “Network Traffic Characteristics of the IoT Application Use Cases,” 2017. [Online]. Available: https://ecs.victoria.ac.nz/foswiki/pub/Main/TechnicalReportSeries/IoT_network_technologies_embfonts.pdf. [Accessed: 20-Jun-2018].
[11] Statista, “Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions),” 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed: 24-Jun-2018].
[12] Statista, “The Internet of Things (IoT)* units installed base by category from 2014 to 2020 (in billions),” 2018. [Online]. Available: https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/. [Accessed: 24-Jun-2018].
[13] T. Rockmann, J. Carter, and J. Kiessling, “Market Analysis Report: How to Create Growth From The Connected Home,” Bonn, Germany (2016)
[14] D. Peraković, M. Periša, and I. Cvitić, “Analysis of the IoT impact on volume of DDoS attacks,” in XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2015, pp. 295-304 (2015)
[15] B. K. J. Al-Shammari, N. Al-Aboody, and H. S. Al-Raweshidy, “IoT Traffic Management and Integration in the QoS Supported Network,” IEEE Internet Things J., vol. 5, no. 1, pp. 352–370 (2018)
[16] K. M. Koumadi, B. Park, and N. Myoung, “Introducing the Latest 3GPP Specifications and their Potential for Future AMI Applications,” J. Electr. Power Energy, vol. 2, no. 2, pp. 245–251 (2016)
[17] N. Nikaein et al., “Simple traffic modeling framework for machine type communication,” in 10th IEEE International Symposium on Wireless Communication Systems 2013, ISWCS 2013, pp. 783–787 (2013)
[18] M. Laner, N. Nikaein, P. Svoboda, M. Popovic, D. Drajic, and S. Krco, “Traffic models for machine-to-machine (M2M) communications,” in Machine-to-machine (M2M) Communications, Elsevier, pp. 133–154 (2015)
[19] A. Sivanathan et al., “Characterizing and classifying IoT traffic in smart cities and campuses,” in 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 559–564 (2017)
[20] M. S. Ali, E. Hossain, and D. I. Kim, “LTE/LTE-A Random Access for Massive Machine-Type Communications in Smart Cities,” IEEE Commun. Mag., vol. 55, no. 1, pp. 76–83 (2017)
[21] J. Moon and Y. Lim, “A Reinforcement Learning Approach to Access Management in Wireless Cellular Networks,” Wirel. Commun. Mob. Comput., vol. 2017, pp. 1–7 (2017)
[22] A. Sivanathan et al., “Characterizing and classifying IoT traffic in smart cities and campuses,” in 2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017, pp. 559–564 (2017)
[23] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, “Large-Scale Measurement and Characterization of Cellular Machine-to-Machine Traffic,” IEEE/ACM Trans. Netw., vol. 21, no. 6, pp. 1960–1973 (2013)
[24] A. P. Abidoye and I. C. Obagbuwa, “DDoS attacks in WSNs: detection and countermeasures,” IET Wirel. Sens. Syst., vol. 8, no. 2, pp. 52–59 (2018)
[25] R. Doshi, N. Apthorpe, and N. Feamster, “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” CoRR, abs/1804.04159 (2018)
[26] Y. Meidan et al., “N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders,” IEEE Pervasive Comput., vol. 13, no. 9, pp. 1–8 (2018)
[27] M. Ozcelik, N. Chalabianloo, and G. Gur, “Software-Defined Edge Defense Against IoT-Based DDoS,” IEEE CIT 2017 - 17th IEEE Int. Conf. Comput. Inf. Technol., pp. 308–313 (2017)
[28] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, “Network Traffic Classifier with Convolutional and Recurrent Neural Networks for Internet of Things,” IEEE Access, vol. 5, pp. 18042–18050 (2017)