Controlling ICMP generation during mitigation of UDP flooding attacks in Internet of Things

Dr. K.N.Venkata Ratna Kumar[1] D.Subba Rao[2] K.Srinivasa Rao[3]

[1]*Professor & Principal - Engineering, St. Mary's Group of Institutions Guntur, Guntur, Andhra Pradesh, India*

[2]*Associate Professor, Dept. of MCA, Narasaraopeta Engineering College, Narasaraopeta, Andhra Pradesh, India*

[3]*Associate Professor & Principal-Diploma, BRIG Engineering College, Opp. Ramoji Film City, Hyderabad, Telangana, India*

Abstract - For last few years, Internet of Things (IoT) has gained much attention due to its wide usage in almost all the avenues to make our lives easier with smart objects that can communicate with each other without much human intervention. However, in similar to other Networks, IoT networks bring new risks. These risks reaching tormenting levels cause some significant issues such as security, privacy, and energy in the network topology. The IPv6 Routing Protocol for Low-Power and Lossy Network (RPL) is a routing protocol for resource-constrained devices in IoT networks. When it transmits packets between nodes, the nodes can be exposed to a series of attacks. UDP Flooding attack is one of the most effective types of attacks against this protocol and negatively affects the energy level of the node and its limited processing capacities. Although many intrusion detection methods are used to detect attacks in IoT security, innovative and energy-saving methods are needed. In this paper, we propose a count-based rate limiting mechanism to mitigate UDP flooding attacks in IoT networks. The nodes are configured with a limit at which it sends ICMP error messages. The rate limit parameters will be set as part of the configuration of the node. This count-based mechanism says that if N is the rate limit value, then the victim will send one ICMP error message after overall N packets are dropped. Also, a timer is enabled to every IoT node to limit the number of UDP packets generation so that the total number of UDP packets are limited in every node. This will reduce the bulk generation of UDP packets in a short span of time. These combined measures effectively reduce the consumption of bandwidth and other IoT resources.

Keywords : *IoT, RPL, UDP Flooding attacks, Attack formation, Attack mitigation, ICMP.*

I. INTRODUCTION

The Internet of Things (IoT) is an emerging technology that envisages providing all physical objects a virtual presence on the Internet. The basic idea of IoT is to make physical objects as smart objects by embedding electronics, software, sensors, actuators, and network connectivity to them. Thus, IoT can be defined as a network of these smart objects that have the ability to collect and exchange data over the Internet. Like other immense technological shifts throughout history, the IoT is changing the way we work, play, learn and organize our societies. As per forecast by Gartner Inc., 8.4 billion connected things will be in use worldwide in 2017, up 31percent from 2016, and will reach 20.4 billion by 2020. Besides, the total spending on endpoints and services reached almost $2 trillion in 2017 itself [1]. Whether one is a technology enthusiast, a business leader, a lawmaker, or a consumer, IoT holds tremendous potential and opportunities for everyone. The advent of new protocols like IEEE 802.15.4[2], Routing over Low Power and Lossy Networks (RPL) [3], Internet Protocol version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) [4], Constrained Application Protocol (CoAP) [5], etc. developed specifically for constrained devices in order to ease the realization of IoT networks. IoT and IIoT applications are crucial for the support of services and sensitive data infrastructures. The amount of data generated will increase with applications for healthcare, household, and industrial use [6]. According to the authors [7], approximately 70% of the most frequently used IoT devices are vulnerable to several types of attacks. These attacks include eavesdropping, replay attacks, Denial of Service (DoS)/Distributed DoS (DDoS), sybil and blackhole attacks. For example, in 2016, the DNS provider that supported the internet services and platforms, including PayPal, VISA and Twitter, was attacked by DDoS through the vulnerabilities of IoT devices such as IP cameras, Printers and residential gateways that were infected by malware named Miria [8].

II. LITERATURE SURVEY

Traditionally, most DDoS attacks are analyzed in cloud servers. The literature [9] combines the features of different types of DDoS attacks to train and defend attacks from the source side in the cloud. In DNS attacks, they monitor the inbound and outbound traffic to calculate the inbound/outbound packets ratio to detect the DNS reflection attack. For ICMP flood, if there are a large number of ICMP

packets in a short time, it means that DDoS attacks have probably occurred. For the SYN flood, the author uses the SYN/ACK ratio as the SYN flood indicator. When the SYN/ACK ratio reaches high, it is abnormal. The authors [10] presented a faster and accurate DDoS attack detection system based on the C4.5 algorithm and signature detection techniques in the cloud computing environment.

For DDoS attacks detection in IoT, the authors [11] select stateless features, packet size, inter-packet interval, protocol, bandwidth, and the count of distinct destination IP addresses to detect DDoS attacks from IoT devices. The literature [12] proposes a multi-level DDoS mitigation framework and provides a solution to prevent and detect DDoS attacks for every layer. The authors [13] combine new features with old features for machine learning-based DDoS attacks to make an early detection. The paper [14] proposes a classification-based DDoS attack detection in IoT. The authors [15] propose deep learning models, including MLP (Multilayer Perceptron), CNN (Convolutional Neural Network), and LSTM (Long Short Term Memory), to detect whether the packet is anomalous or not in the IoT network. The literature [16] aims to analyze the botnet attacks through the SVM algorithm in IoT and focuses on the protocols, HTTP, TCP, and ICMP.

For DDoS attacks detection in SDN, the author [17] proposes SDNShield, an NFV-based defense framework that joins the strengths of software switches and a two-stage filtering algorithm to protect the centralized controller. The proposed model [18] devises a statistical solution that evaluates an entropy-based security scheme to enhance the SDN security and mitigates the DDoS attacks. The proposed framework [19] is a multi-layer framework that consists of a controller pool containing main SD-IoT controllers, SD-IoT switches integrated with an IoT gateway, and IoT devices. The framework uses the threshold value of the cosine similarity of the vectors to judge whether a DDoS attack has occurred and blocked the DDoS attack at the source site.

The machine learning techniques make the DDoS defense systems in SDN efficiently. The paper [20] proposes an authorization module to check whether the controller can send requests to the server or not and a machine learning based prediction module to detect potential DDoS attacks. If the learning model detects that the packet is abnormal, the controller will increase a new rule to SDN switches to block the attacker's IP address. In [21], the authors proposed a smart DDoS mitigation system, including two modules for information collection and DDoS mitigation in the application plane.

In [22], author provides a broad anatomy of IoT protocols and their inherent weaknesses that can enable attackers to launch successful DDoS attacks. One of the major contributions of this paper is the implementation and demonstration of UDP (User Datagram Protocol) flood attack in the Contiki operating system, an open-source operating system for the IoT. This attack has been implemented and demonstrated in Cooja simulator, an inherent feature of the Contiki operating system. Furthermore, in this paper, a rate limiting mechanism is proposed that must be incorporated in the Contiki OS to mitigate UDP flood attacks.

III. EXISTING SYSTEM

In this section, we propose a count-based rate limiting mechanism to mitigate UDP flooding attacks in IoT networks. A node in Contiki should be able to limit the rate at which it sends ICMP error messages. The rate limit parameters will be set as part of the configuration of the node. Our count based mechanism says that if N is the rate limit value then the victim will send one ICMP error message after overall N packets are dropped. This effectively reduces the consumption of bandwidth on the reverse path of already low power and lossy networks of the IoT. Another advantage of our mechanism is the reduced use of node's resources i.e. transmission and CPU processing power. We have used two counters*ctr1* and *ctr2* for counting the number of ICMP messages sent and the number of dropped packets respectively. We set the initial values of both counters as *zero* and then gradually increment them in either case of sending the ICMP messages or simply discarding the received packet. The algorithm ensures that only one ICMP error message is sent for every N dropped packets. Algorithm-I exemplifies the logic used in our mechanism.

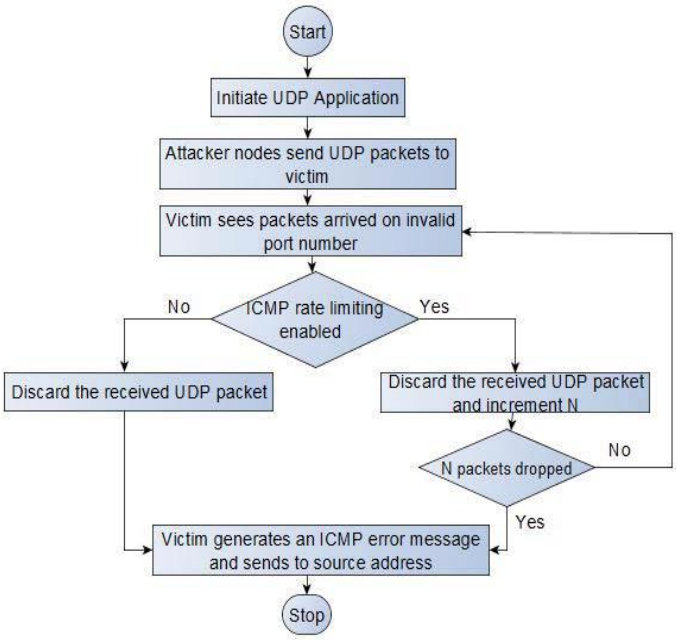

Figure-1: Flowchart of Existing Algorithm

IV. PROPOSED SYSTEM

Even though the existing algorithm provides necessary security measures to safeguard the network, it has few drawbacks which make the network vulnerable in few ways. The existing scheme generates limitless ICMP packets which extends the network overhead. This may result in increase of the traffic rate among the nodes due to countless ICMP generation. Also, no control mechanism available to control the generation of ICMP packets which again creates flooding-like situation in the network.

In this work, we propose a new solution that limits the generation of UDP & ICMP control packets. The proposed solution limits the flow of ICMP control packets when the attackers send flooding attack to the victim node. The proposed solution is a light-weight security mechanism works well against UDP flooding attacks. The main advantage of the proposed solution is it requires less transmission & processing power.

The objective of this proposal is to suggest a security mechanism against UDP flooding attacks with low overhead.

The aim of this proposal is to put forward a security mechanism to protect the IoT network against UDP flooding attacks with limited ICMP packet generation and reduced overhead.

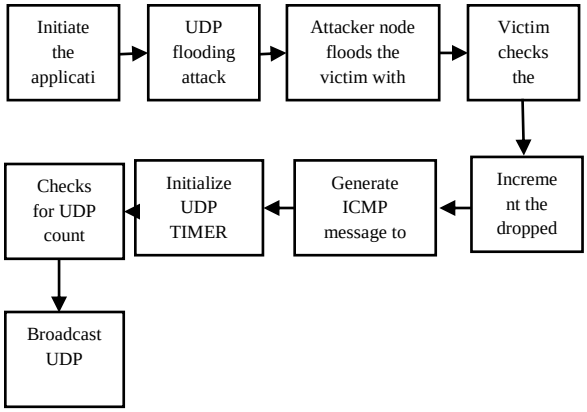

Figure-2: Block diagram of proposed system

Attacker node initiate the flooding attack into the network Attacker node broadcasts a bunch of UDP packets in a short period of time without any prior notice the participant nodes. Suddenly all the nodes become the victim as these nodes unable to handle the larger number of packets. Upon receiving the victim nodes initiate the ICMP and discard the received UDP packets and make a count of dropped packets. The victim nodes initiate the ICMP controller to generate and broadcast the ICMP packets. Also, timer is enabled to control the flooding of UDP packets in a short interval. So that the broadcast of UDP packets in a short interval is prevented and flood attack is controlled.

V. RESULT AND DISCUSSION

In this section, we simulate and evaluate our mitigation scheme on the basis of two parameters, the aggregate transmission power and the aggregate CPU processing power of the victim node. Contiki implements the uIP TCP/IP stack to provide communication abilities to resource constrained IoT devices. It is written in C language and only has the minimal set of features needed for a full TCP/IP stack. To implement UDP flooding attack in Contiki, we exploited and modified the existing rpl-udp example. We developed a UDP flooding program that was self-programmed on a number of client motes.

Parameter	**Value**
No. of motes	11
Malicious mote	Mote number 11
Server mote	Mote number 1
Mote deployment	Random position
Mote type	SKY mote

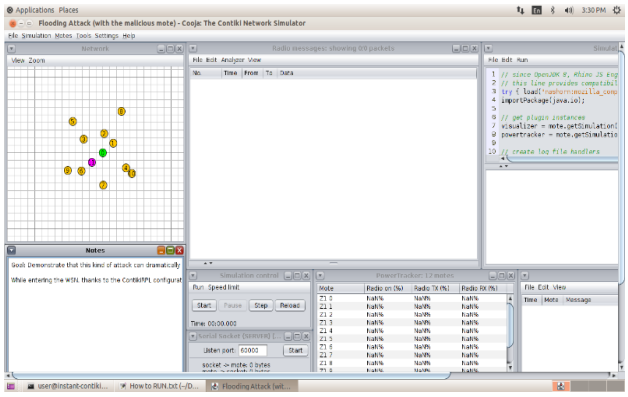

Figure-3: Motes deployment in Network Simulation

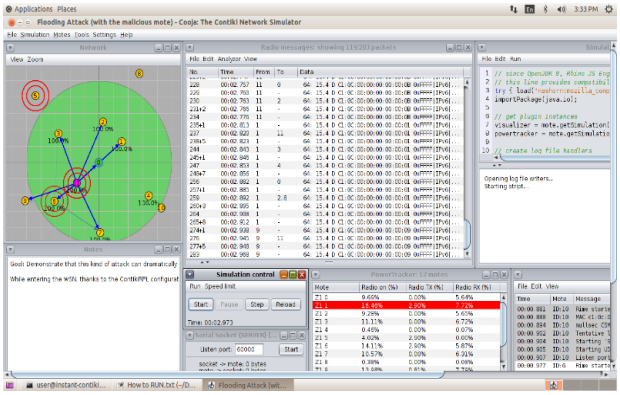

Figure-4: Simulation process initialization

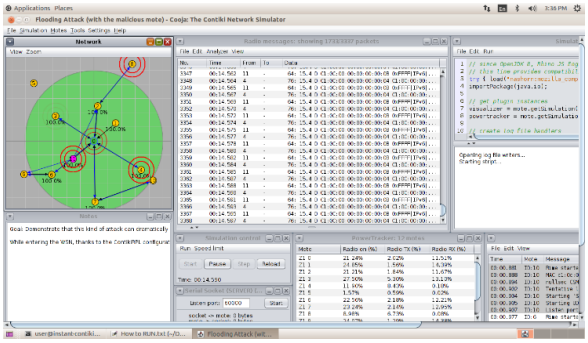

Figure-5: Initialization of server mote process

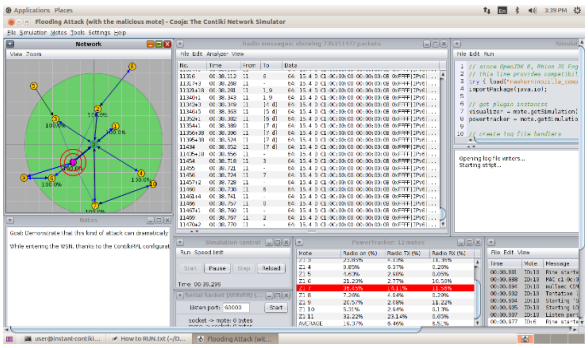

Figure-6: Communication starts from malicious mote

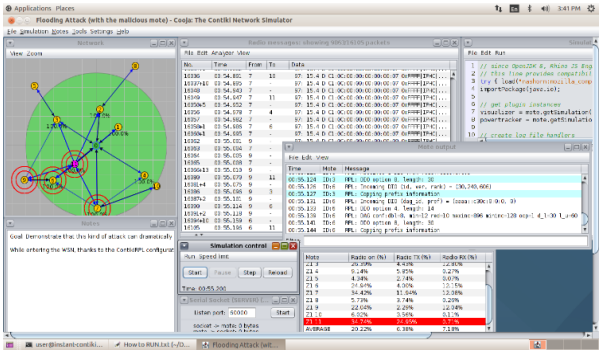

Figure-7: Radio messages starts and updated transmission process

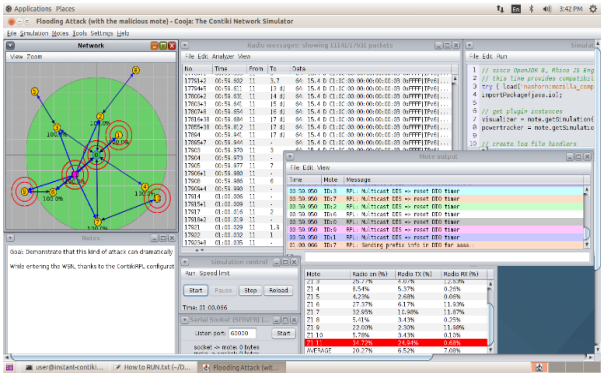

Figure-8: Mitigation of malicious mote communication

In network simulation, broadcasting and data communication process run as per time. Figures **3 to 8** represent the network initialization to simulation ending communication as per work duration. Here malicious activity starts and attacked on different motes available in network range. We added proposed mechanism to network communication, while malicious mote running on system, then our mechanism supports and mitigate the process of malicious activity.

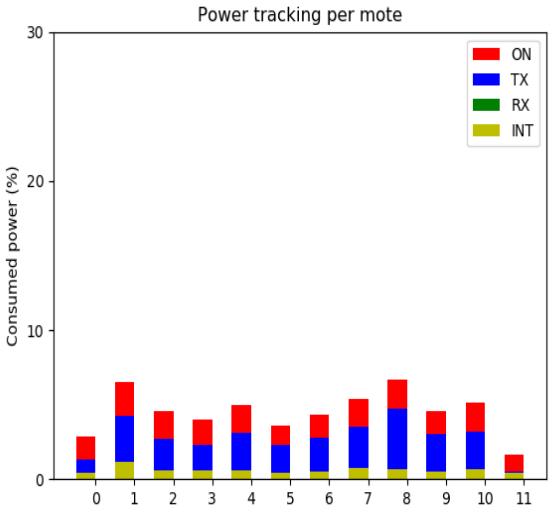

Figure-9: Graph analysis of Existing system

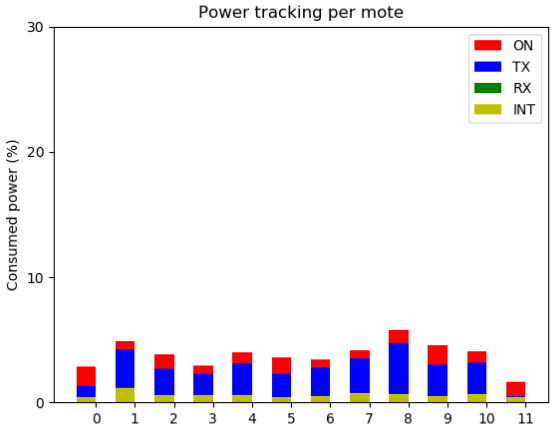

Figure-10: Graph analysis of proposed system

The above figures 9 and 10 depict the power consumption graphs of existing and proposed methods. The power consumption ratio of proposed method is a way higher than the power consumption of the existing method. We can notice that both initialization and transmission power of both comparisons are same but both differs in transmission power consumption rate. This was due to the limited generation of both UDP and ICMP generation with less overhead and processing power.

Power tracking: It means the power consumed in every IoT mote for the overall transaction

In graph, the power consumption during proposed method execution are denoted as:

INT –power consumption for initialization

RX - power consumption for receiving packets

TX - power consumption for transmitting packets

ON - power consumption in the mote until the end of running (red)

By comparing proposed Vs Extension graphs, we conclude that extension method consumes less resources due to the limitations set in UDP generation timer.

VI. CONCLUSION

In this work, UDP flooding attacks and its control measure is studied. In UDP flooding attack, the attacker node initiates the flooding attack and broadcasts a bunch of UDP packets in a short period of time without any prior notice to the participant nodes. The receiving nodes become the victim as these nodes are unable to handle the larger numbers of packets. In the proposed technique, the victim nodes initiate the ICMP controller to generate and broadcast the ICMP packets. Also, timer is configured with IoT nodes to control the generation of UDP packets in a short interval so that the broadcast of UDP packets in a short interval is prevented and flood attack is controlled. The comparative results proved that the proposed technique consumes less power and resources in IoT devices.

VII. REFERENCES

[1] Rob van der Meulen, "Gartner Says 6.4 Billion Connected Things WillBe in Use in 2016, Up 30 Percent From 2015", Nov 2015. Available : http://www.gartner.com/newsroom/id/3165317, accessed 2017/04/02

[2] IEEE Standard for Local and metropolitan area networks--Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment1: MAC sub layer, IEEE Std 802.15.4e-2012 (Amendment to IEEE Std802.15.4-2011), 2011, pp. 1-225.

[3] P. Thubert et al., "RPL: IPv6 Routing Protocol for Low-Power andLossy Networks," RFC 6550, 2012.

[4] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, "Transmission ofIPv6 Packets over IEEE 802.15.4 Networks," RFC 4944, 2007.

[5] Z. Shelby, K. Hartke, C. Bormann, "The Constrained ApplicationProtocol," RFC 7252, 2014.

[6] Lee, I.; Lee, K. The internet of things (iot): Applications, investments, and challenges for enterprises. Bus. Horizons **2015**,58, 431–440. [CrossRef]

[7] Hp News hp Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Available online: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676 (accessed on 15 April 2020).

[8] Flashpoint—Mirai Botnet Linked to Dyn DNS DDoS Attacks. Available online: https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/(accessed on 20 October 2020).

[9] Z. He, T. Zhang, and R.B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, July 2017

[10] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software Defined Networks," Proceedings of the IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, Sept. 2018.

[11] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," Proceedings of the IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, May 2018.

[12] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. Richard Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things," IEEE Communications Magazine, Feb. 2018.

[13] Y. Feng, H. Akiyama, L. Lu, and K. Sakurai, "Feature Selection for Machine Learning-Based Early Detection of Distributed Cyber Attacks," Proceedings of the IEEE 16th Intl Conf on DASC/PiCom/DataCom/CyberSciTech(DASC/PiCom/DataCom/CyberSciTech),Athens, Greece, Oct. 2018.

[14] V. Selis and A. Marshall, "A Classification-Based Algorithm to Detect Forged Embedded Machines in IoT Environments," IEEE Systems Journal, May 2018.

[15] M. Roopak, G. Y. Tian, and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, Mar. 2019

[16] K. Gurulakshmi and A. Nesarani, "Analysis of IoT Bots Against DDOS Attack Using Machine Learning Algorithm," Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, Dec. 2018.

[17] K. Chen, A. R. Junuthula, I. K. Siddhrau, Y. Xu, and H. J. Chao, " SDNShield: Towards More Comprehensive Defense against DDoS Attacks on SDN Control Plane," Proceedings of the IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, Feb. 2017.

[18] K. Kalkan, L. Altay, G. Gür, and F. Alagöz, "JESS: Joint EntropyBased DDoS Defense Scheme in SDN," IEEE Journal on Selected Areas in Communications, Sep. 2018.

[19] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," IEEE Access, Apr. 2018.

[20] S.S. Mohammed, R. Hussain, B. Bimaganbetov, and J. Lee, "A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network," Proceedings of the 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, Oct. 2018.

[21] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software Defined Networks," Proceedings of the IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, Sept. 2018.

[22] Malik, M. and Dutta, M., 2017, May. Contiki-based mitigation of UDP flooding attacks in the Internet of things. In *2017 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1296-1300). IEEE.