Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning

Nhu-Ngoc Dao, Trung V. Phan, Umar Sa'ad, Joongheon Kim, Thomas Bauschert, Dinh-Thuan Do, and Sungrae Cho

***Abstract*—The rapid increase of diverse Internet of things (IoT) services and devices has raised numerous challenges in terms of connectivity, interoperability, and security. The heterogeneity of the networks, devices, and services introduces serious vulnerabilities to security, especially distributed denial-of-service (DDoS) attacks, which exploit massive IoT devices to exhaust both network and victim resources. As such, this study proposes FOGshield, which is a localized DDoS prevention framework leveraging the federated computing power of the fog computing-based access networks to deploy multiple smart endpoint defenders at the border of relevant attack-source/destination networks. Cooperation among the smart endpoint defenders is supervised by a central orchestrator. The central orchestrator localizes each smart endpoint defender by feeding appropriate training parameters into its self-organizing map (SOM) component, based on the attacking behavior. Performance of the FOGshield framework is verified using three typical IoT traffic scenarios. Numerical results reveal that FOGshield outperforms existing solutions.**

***Index Terms*—heterogeneous IoT, defense framework, self-organizing map, DDoS attack**

I. Introduction

In a recent report by Gartner [1], approximate 5.8 billion Internet of things (IoT) devices are expected to be in use this year. These devices have become popular in whole market segments of the fifth generation (5G) mobile networks, including consumer applications, cross-industry business, and vertical-specific industry. This big IoT data paradigm faces a large variety of device vendors and network technologies, often called heterogeneous IoT (HIoT) systems [2], [3]. HIoT imposes several security challenges due to the heterogeneity and massiveness of HIoT traffic. In particular, lightweight HIoT devices, which are typically characterized by low computing power, may be exploited by attackers to generate promiscuous flooding traffic in distributed denial-of-service (DDoS) attacks [4]. For instance, a swarm of more than 400,000 vendor/technology-specific IoT devices, hijacked by Mirai malware, generated about 1 Tbps of DDoS traffic to a French webhost [5].

This research was supported in part by Korea Electric Power Corporation under Grant R20XO02-15 and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1G1A1008105).

N.-N. Dao is with the Department of Computer Science and Engineering, Sejong University, Seoul 05006, Republic of Korea (email: nndao@sejong.ac.kr).

T. V. Phan and T. Bauschert are with the Chair of Communication Networks, Technische Universität Chemnitz, Chemnitz 09126, Germany (email: trung.phan-van@etit.tu-chemnitz.de, thomas.bauschert@etit.tu-chemnitz.de).

U. Sa'ad and S. Cho are with the School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, Republic of Korea (email: umar@uclab.re.kr and srcho@cau.ac.kr).

J. Kim is with the School of Electrical Engineering, Korea University, Seoul 02841, Republic of Korea (email: joongheon@korea.ac.kr).

D.-T. Do is with the Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan (email: dodinhthuan@asia.edu.tw).

Corresponding author: S. Cho (srcho@cau.ac.kr)

A. Literature Review and Motivations

In order to countermeasure against the DDoS issues, literature review [6], [7] has recognized that 5G cloudization is beneficial for significantly strengthening DDoS prevention by enabling various learning techniques, especially for such IoT environments [8]. The cloudization extends computing capability from the cloud to the access tier realizing fog computing-based radio access networks [9]. As a result, cloudization provides IoT devices with intelligent DDoS prevention instead of a simple defense as in the past. Cloudization-based DDoS prevention solutions can be classified into either centralized or distributed approaches.

As an example of the centralized approach, a multi-level DDoS mitigation framework (MLDMF) [10] has been proposed using machine learning techniques. In the MLDMF, big IoT data, which is collected from multiple lightweight endpoint defenders, is used to train a central controller in the cloud. Based on the training results, the central controller generates a common policy, which is then dispatched to all endpoint defenders. Focusing the operational cost, Zheng *et al.* [11] proposed a low-cost DDoS solution, DynaShield working on the cloud infrastructure. DynaShield yields cost reduction by considering on-demand defense services with elastic resource allocation. To enhance the DDoS defense capability in a software defined networking (SDN)-based environment, Xu *et al.* [12] proposed a defense strategy based on traffic classification, namely DDTC. The DDTC mechanism is implemented as a virtualized network function to improve the flexibility and reduce the load of SDN against DDoS attacks. Nevertheless, it is observed that centralized approaches generally face bottleneck and reaction latency issues due to overload of the central controller, especially in the big IoT context.

To mitigate these issues, Phan *et al.* proposed a distributed DDoS prevention system (namely D-SOM) [13]. Unlike the centralized counterpart, training is cooperatively performed among the distributed controllers. Hereafter, the training results are collected in a central head in order to generate a common policy. Then, the central head dispatches its final policy to all endpoint defenders. In [14], Liu *et al.* proposed

a defense method in edge environment to handle large-scale and low-rate DDoS attacks. The solution exploits advantages of data locality by using deep convolution neural network to learn traffic features. Similarly, Jia *et al.* [15] presented the FlowGuard system for detection, identification, classification, and mitigation of IoT DDoS attacks at the edge. The proposed detection algorithms adapt to the traffic variances by using long short term memory networks.

Although distributed approaches might perform suitably in light and homogeneous IoT traffic in general, they may not do so for massive HIoT traffic since promiscuous big HIoT data is not easily classifiable. A mixture of data flows from various webcams, DVRs, and routers, generated by Mirai attacks, for instance, might be considered as normal traffic at first glance in central analysis even though they are collected from non-certified sources. To achieve better classification, existing approaches require comprehensive analysis and consume a significant amount of time [5]. Consequently, reaction latency and accuracy detection remain open challenges to protect the HIoT networks against DDoS attacks.

B. Paper Contributions

In this article, we propose a DDoS prevention framework called *FOGshield*. Distinguished from the above approaches, FOGshield exploits a federated learning model, which shifts the training function from a cloud-based orchestrator to every fogging-based smart endpoint defenders while the orchestrator performs defense policy orchestration at the central. In a nutshell, the contributions of this paper are as follows:

- A HIoT system was investigated to expose the vulnerabilities and resistances to DDoS attacks. Consequently, we analyzed the adversary model of two typical DDoS attack scenarios in such a HIoT system (i.e., volumetric and application layer attacks) in terms of the attack objectives, initial capabilities, and processes.
- We proposed the FOGshield framework, which exploits the federated learning model consisting of a cloud-based orchestrator and multiple fogging-based smart endpoint defenders to improve the attack detection performance. Empowered by fog computing technology, the smart endpoint defenders continuously train their own self-organizing map (SOM) components [16] by exploiting their local traffic to filter abnormal flows. A central orchestrator coordinates the training results among multiple smart endpoint defenders to generate appropriate filter policies (i.e., centralized controls).
- As a result, FOGshield prevents both ingress and egress malicious threats at the border of relevant attack-source/destination networks, respectively. These advantages of the FOGshield are demonstrated by conducting a security performance analysis among FOGshield, MLDMF [10], and D-SOM [13] in three typical IoT traffic scenarios extracted from reputable datasets such as CAIDA-attack-traffic [17], NSL-KDD [18], and DARPA Intrusion Detection [19]. The performance comparison consists of reaction latency, detection rate and accuracy, bottleneck handling, and resource consumption.

The rest of the paper is organized as follows. In Section II, we investigate the vulnerabilities and resistances of HIoT systems against DDoS attacks. Consequently, two typical attack scenarios are analyzed in Section III. We propose the FOGshield platform development and operations in Section IV. To validate security performance of the FOGshield, emulation and result analysis are discussed in Section V. Finally, the paper is concluded in Section VI.

II. Vulnerabilities and Resistances

This section describes the features of HIoT system for determining their vulnerabilities (*V1*, *V2*, and *V3*) and resistances (*R1*, *R2*, and *R3*) to DDoS attacks; see Fig. 1 for the reference model. Fogging-enabled HIoT networks consist of various homogeneous IoT networks distributed at the edge and interconnected via the networking infrastructure. The following features are derived from two distinguishing facets of the network: the heterogeneity of IoT devices, and in-network computation served by fog servers. Detailed description is as follows.

Power-constrained devices (V1): Although IoT does not exclude high-power devices, those with constrained power in terms of computing resources and memory typically occupy the dominant positions [2]. Owing to their lack of computational power, these IoT devices may not support complex and evolving security algorithms, such as effective encryption for data transfer and endpoint protection against local security attacks. Furthermore, the weak security implemented on these devices means exploiting and recruiting them into botnets and injecting different types of malware are trivial tasks for even unskilled attackers.

Massive connections (V2): Billions of connected IoT devices generate massive volumes of data. This is an important ingredient for effective DDoS attacks. The traffic is usually generated from many constrained HIoT devices. However, the same amount of traffic might also be generated from fewer powerful devices in other networks [7]. These factors make HIoT traffic containing malicious DDoS flows more difficult to handle than other network traffic.

Heterogeneous group-specific traffic (V3): HIoT traffic is considered heterogeneous from a macro perspective, but group-specific from the perspective of each local network [20]. In particular, IoT devices serving individual applications may be separately connected in different virtual local area networks. As such, behaviors of the generated traffic can be identified via a tuple of flow parameters such as protocols, ports, transmission rates, and port growth. From a security viewpoint, the aggregated traffic at the attack-destination site is classified into a heterogeneous category, while the egress traffic from the attack-source sites is divided into group-specific categories.

Mobile cloudization (R1): Fog computing technology provides cloudization capabilities at the access networks, where beneficial applications are from latency sensitive devices such as factory automation, autonomous driving, and remote surgery. The fog computing is characterized by low execution latency and context-aware computation. This environment

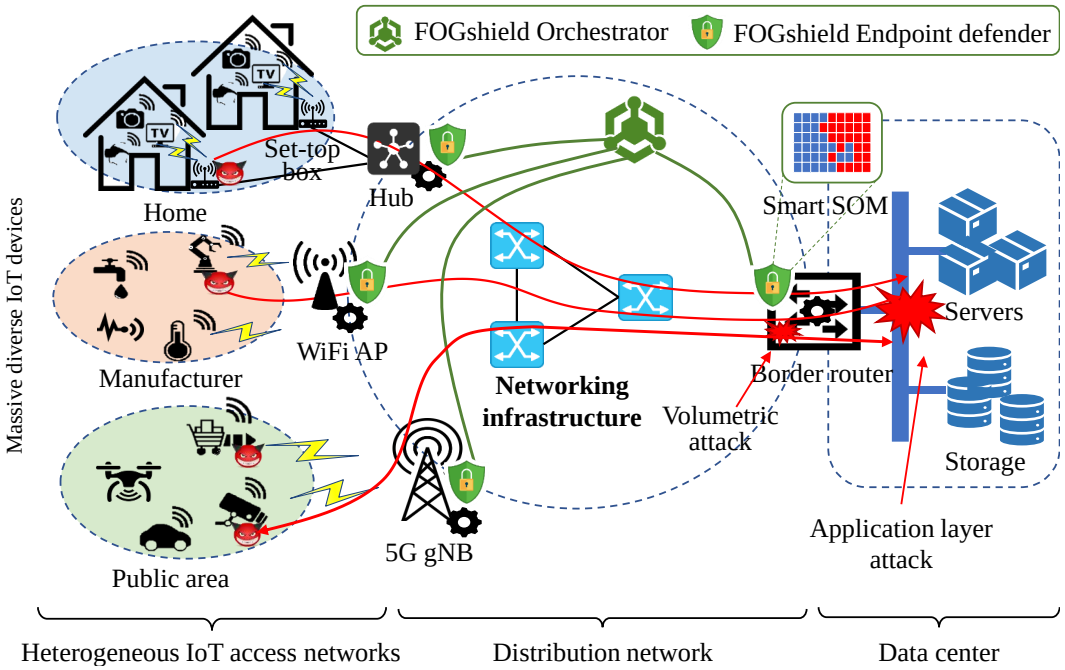

Fig. 1. FOGshield deployment to protect HIoT systems against DDoS attacks leveraging fog computing capability.

enables services such as resource scheduling, and security protection to be scalably deployed in proximity to the IoT devices. Therefore, comprehensive DDoS prevention, facilitated by the fog computing, can be implemented in collaboration with advanced techniques such as machine learning and big data mining in a local context.

Service execution offloading (R2): Mobile cloudization has enabled the increasingly popular service execution offloading in HIoT. While lightweight IoT devices lack the powerful computation capability necessary for the timely execution of complex services, the networks are equipped with sufficient computational resources to provide tailored service execution on demand. This trend has resulted in traffic behavior that prioritizes local processing at the access tier, rather than on Internet servers. Tracking this traffic behavior of each local network might help to detect security threats when abnormal traffic behavior occurs.

Contextual information fusion (R3): Although the traffic properties can be distinguished among local IoT networks, applications running at the access tier may need to merge contextual IoT data to obtain comprehensive information. The relationships among contextual IoT data can be considered a criterion for abnormal traffic detection when individual partners defect [21]. For instance, standard images are transferred from cameras to a surveillance system during the day, while thermographic images and motion detection signals are more useful at night. The traffic is considered abnormal when, for example, thermographic images are sent during the day, or standard images are sent at night.

III. Adversary Model Analysis

This section analyzes the adversary models of two DDoS attack scenarios (a volumetric DDoS attack and an application layer attack) in terms of the attack objectives, initial capabilities, and process.

Objective: The objectives of the scenarios are as follows:

(i) *Scenario 1* – A volumetric DDoS attack on the infrastructure between users and data centers. The objective is to send lots of bogus traffic generated from compromised HIoT devices, resulting in the total malicious traffic size exceeding the network capacity.

(ii) *Scenario 2* – An application layer DDoS attack generally focuses on servers as its victim. The objective is to flood the server with seemingly legitimate, but bogus requests in order to exhaust the ability of the application to serve legitimate users. This is a more sophisticated type of DDoS attack, and is difficult to detect because the attack traffic is not easily distinguishable from benign traffic.

Initial capabilities: In order to execute the attacks, we assume the adversary has the following capabilities:

- *Botnet:* Access to a group of compromised HIoT devices (HIoT botnet). The adversary may be the owner of the botnet (botmaster), or may have access to it through a third party (e.g., a DDoS-for-hire service).
- *Command and Control (C2):* A command and control infrastructure (C2), which is used to control the compromised devices and possibly recruit additional devices.
- *System Knowledge:* Some knowledge about the victim, such as IP addresses, domain names, existing vulnerabilities, and so on.
- *Amplifiers:* Poorly configured network services (e.g., Open DNS resolver), which the attacker can exploit to increase the volume of the generated botnet traffic. This capability is crucial for the attack in scenario 1.
- *IP Spoofing:* Ability to spoof the source IP address of the botnet traffic. This capability *reflects* the amplified

botnet traffic by sending it to the victim rather than the real source.

Attack process: The attack process in each scenario is described as follows:

(i) *Scenario 1:*
- *Botnet Activation:* The attacker uses a controller to send commands to the HIoT botnet. The instructions may include the victims IP address, attack rate, and target services.
- *Traffic Generation:* The botnet is used to generate traffic using the above parameters.
- *Amplification:* Some UDP-based network protocols have a high bandwidth amplification factor, which simply means they return very large responses for much smaller requests. For example, DNS has an amplification factor of 28 to 54, NTP has a factor of 556.9, and SSDP has a factor of 30.8 [22]. This property is exploited by attackers in volumetric DDoS attacks, in which a large HIoT botnet is used to send requests to these services in order to generate an enormous amount of traffic as a response.
- *Reflection:* The source IP address of the botnet packets is spoofed and replaced with the IP address of the victim. Therefore, the amplified traffic is sent to the victim rather than to the attacker.
- *Network Disruption/Degradation:* The network capacity is eventually exceeded by the amplified and reflected traffic, thereby degrading or disrupting the operations of the network.

(ii) *Scenario 2:*
- *Botnet Activation:* This process is the same as that in scenario 1.
- *Traffic Generation:* At this stage, traffic is generated from each compromised device in the HIoT botnet. The intent of the attacker is not easily discernible because the traffic conforms to all protocols.
- *Flooding:* At this stage, the attacker floods the server with requests from each compromised device in the HIoT botnet. There are three types of application layer flooding attacks: session flooding, where each device sends sessions at higher rates than those of non-malicious users; request flooding, where each attack session involves sending higher requests than those of non-malicious users; and an asymmetric attack, where each attack session contains requests with much higher workloads than those of non-malicious sessions.
- *Service Disruption/Degradation:* The capacity of the server to respond to user requests is eventually exceeded, thus making the server unavailable.

Feasible defense strategies: Based on the aforementioned behavior analysis, it is seen that source-based prevention could effectively mitigate and block bad traffic at proximity to the source of attack in the volumetric attack scenario. By contrast, the destination-based prevention strategy plays a key role in mitigating the impact of the application layer attack. In particular, the endpoint defender located at the front of the victim must deploy an adaptive policy to prioritize the IP reputation database while limiting, filtering, and rerouting the suspicious traffic. Moreover, additional utilization of source-based prevention and software-based techniques (e.g., the CAPTCHA test [23]) can supplement the defense performance.

IV. FOGshield Framework

On the basis of the previously mentioned adversary model analysis, we propose FOGshield, a novel DDoS prevention framework.

A. Design Rationale

The rationale behind the FOGshield framework design includes (i) utilizing *fog computing capability* to provide training-enabled endpoint defenders in front of the attack-source/destination sites; (ii) *well-adaptation* to local traffic of the smart SOM filter at each endpoint defender with the purpose of abnormal detection improvement; and (iii) *cooperation* among the endpoint defenders, supervised by a central orchestrator.

B. Self-Organizing Map Algorithm

The SOM algorithm is one of the most effective unsupervised learning solutions in artificial neural networks, which converts a higher-dimensional input space into a lower-dimensional representation called an SOM as illustrated on the left side of Figure 2. An SOM consists of $\mathcal{S}$ neurons arranged on a grid. Neuron j has a weight vector $\vec{w}_j$, which has the same size as the input training vector $\vec{x}_i$, i.e., $\vec{w}_j = [w_{j1}, w_{j2}, \ldots, w_{jm}]$ and $\vec{x}_j = [x_{i1}, x_{i2}, \ldots, x_{im}]$, where m is the input dimension. Let $\mathcal{R}$ is radius of the SOM map which is given as

$$\mathcal{R} = \frac{\max(MapWidth, MapHeight)}{2}. \tag{1}$$

Let $\sigma(t)$ represent the neighborhood radius of a winning neuron. At the iteration i of the training process, $\sigma(t)$ is defined as

$$\sigma(t) = \mathcal{R} \times e^{-\frac{t}{\lambda}}, \qquad t = 1, \ldots, k, \tag{2}$$

where k is the number of input vector and λ is calculated as

$$\lambda = \frac{k}{\lg(\mathcal{R})}. \tag{3}$$

It is observed that $\sigma(t)$ decreases by time during the training.

A pseudocode of the SOM algorithm is illustrated in Figure 2 as follows:

1) In the preparation stage, all neurons initiate their weight vectors adopting a common policy to ensure equality among neurons, i.e., $\vec{w}_j = [w_{j1}, w_{j2}, \ldots, w_{jm}]$, where $1 \le j \le \mathcal{S}$.
2) In the training stage, when an input vector is fed to the SOM map, a wining neuron w^* is elected. The wining neuron is the one with the smallest Euclidean distance from its weight vector to the input vector. That is,

$$w^* = \underset{j}{\operatorname{argmin}} \left\| \vec{x}_i - \vec{w}_j \right\|, \qquad \forall j. \tag{4}$$

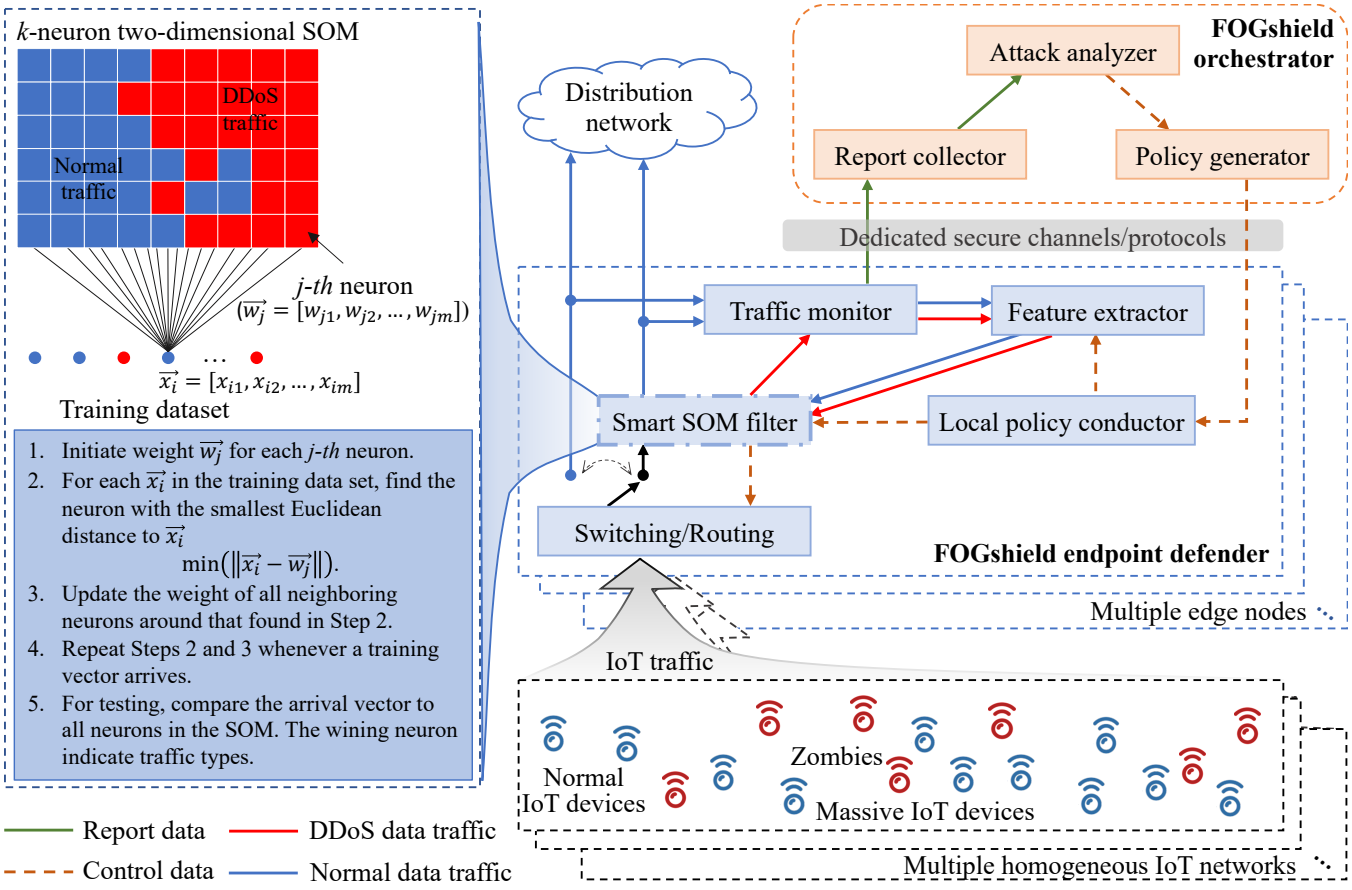

Fig. 2. FOGshield architecture design adopting the federated learning model and SOM algorithms.

Consequently, all neighboring neurons around the wining neuron w^* update their weights to represent relations to the input vector based on the following policy

$$\vec{w}_j \leftarrow \vec{w}_j + \alpha(t) \times \Theta(t) \times (\vec{x}_i - \vec{w}^*), \tag{5}$$

where $\alpha(t)$ is a learning rate function which decays over time and is expressed as

$$\alpha(t) = \alpha_0 \times e^{-\frac{t}{\lambda}}, \tag{6}$$

and $\Theta(t)$ is an influence function which is calculated by the distance between neurons j and w^* as follows

$$\Theta(t) = e^{-\frac{\|\vec{x}_i - \vec{w}_j\|^2}{2\sigma^2(t)}}. \tag{7}$$

This procedure is repeated until there is no more input vector fed into the SOM map.

3) In the testing stage, the SOM classifies a new input vector by comparing the input vector to all neurons on the map. The winning neuron indicates whether the input vector is normal traffic or DDoS traffic.

Theoretically, the complexity of this algorithm depends on step 2 operation. In particular, the argmin function in (4) results in a complexity $O(\mathcal{S}m)$. While (5) has a complexity $O(\mathcal{S}m^3)$ that is derived from (2), (6), and (7). Finally, the total complexity is given by $O(\mathcal{S}m + \mathcal{S}m^3)$. In practice, m is selected quite small. Especially, $m = 3$ and 5 in our proposed framework (see the Feature extractor description of the FOGshield endpoint defender in the next section).

C. FOGshield Framework

Figure 2 illustrates the proposed FOGshield framework. Logically, the FOGshield framework consists of a central orchestrator and multiple endpoint defenders located at the border of each homogeneous IoT system.

The feature distribution of the FOGshield framework adopts the federated learning model, wherein:

- The FOGshield endpoints: (*i*) Exploit local data to train their own SOM maps. By this way, the SOM map at each endpoint better represents specific traffic classification for the network sites protected by the endpoint. (*ii*) Frequently, send traffic statistics reports and SOM parameters to the FOGshield orchestrator.
- The FOGshield orchestrator: (*i*) Based on the traffic statistics reports, the orchestrator clusterizes the endpoints into two groups: (1) source-destination relationship and (2) traffic similarity. (*ii*) Among the endpoints which have traffic similarity, the orchestrator builds a SOM model using the collected SOM parameters. This SOM model is dispatched to these endpoints to update their local SOM models. (*iii*) Among the endpoints which have source-destination relationship, the orchestrator dispatches appropriate policy to the source (of attack) endpoints to

activate their source-site SOM maps for filter egress traffic. In addition, the orchestrator specifies prominent features in order to make a tuple of features for each input vector in the local SOM map training procedure at the source (of attack) endpoints.

The communication between the central orchestrator and the endpoint defenders is facilitated via secure channels/protocols supported by the networks (e.g., Openflow protocol). The physical positions of the FOGshield components are also depicted in Figure 1. Adopting the European telecommunications standards institute (ETSI) network functions virtualization management and orchestration (NFV-MANO) model, the FOGshield can be implemented as a virtualized network function of the 5G networks on the cloud. In contrast, FOGshield endpoint defenders are deployed at the 5G point of attachments (5GPoA) such as 5G NodeB (gNB), Wifi access point, and gateways of emerging IoT technologies [24].

FOGshield orchestrator: The main purpose of the central orchestrator is to cooperate training results and policies among the localized endpoint defenders. To this end, the FOGshield orchestrator is developed consisting of the following components:

- *Report collector:* This component gathers traffic reports from federated endpoint defenders, including traffic protocols, port ranges, volume or traffic flow quantity, source IP address ranges, and destination IP address(es). Adopting the requirements of the detection mechanism applied in the attack analyzer, the reported information is preprocessed and updated at the report collector before being transferred to the attack analyzer. For instance, to analyze the characteristics of a spoofed DDoS flooding attack, protocol, port range and volume are necessary for attack investigation.
- *Attack analyzer:* First, this component clusterizes the endpoint defenders into two groups by considering (i) source-destination relationship and (ii) traffic similarity, which can be derived from received information of the report collector. The source-destination relationship criterion identifies sources of attack if the attack is detected at the destination site. Appropriate DDoS attack detection techniques [6] are utilized to identify the attack symptoms based on the processed information from the report collector. For instance, multiple reports can indicate that their egress traffic intends to reach a specific destination, even if this destination has been reported as a victim of a volumetric attack (i.e., abnormal extreme ingress traffic statistics). Meanwhile, the traffic similarity criterion identifies endpoint defenders who have similar traffic patterns such as traffic types, protocols, and volume. The SOM parameters in these endpoint defenders can be collaborated to build an improved SOM map following the federated learning model. Iteratively, notifications of these analyses are sent to the policy generator to dispatch updated protection policies to corresponding endpoint defenders.
- *Policy generator:* As a result of the federated learning model, the improved SOM parameters are sent to the corresponding endpoint defenders to update their local SOM maps. On the other hand, once a DDoS attack is identified, primary policies are generated and forwarded to the corresponding endpoint defenders located at the borders of the source and destination sites of the attack. The policies contain an activation command to activate whether the destination-site or source-site SOM maps, respectively. In addition, desired features of the local traffic are specified accordingly. The feature information will be delivered to the feature extractor module via the local policy conductor in order to request the desired extraction, which is used in the SOM training and classification processes.

FOGshield endpoint defender: The primary purpose of the FOGshield endpoint defenders is training and classification of the DDoS traffic. The components of the FOGshield endpoint defenders are as follows:

- *Traffic monitor:* The main function supported by this component is to generate the traffic statistics report. It regularly records the statistics of ingress traffic, including traffic protocols, service ports, volumes and source/destination IP address ranges. A summary of the information is periodically delivered to the report collector in the central orchestrator. Depending on current situation, the time period can be dynamically set to reduce communication overhead on the link between the endpoint defenders and the orchestrator. In addition, ingress traffic is also forwarded to the feature extractor in order to make the SOM map's inputs.
- *Local policy conductor:* Based on the primary policy dispatched from the orchestrator, the local policy conductor informs the feature extractor about prominent features in order to make a tuple of features for each input vector in the SOM map training procedure. Moreover, the local policy conductor will send localized information to the smart SOM filter to apply appropriate policies for attack traffic classification. For example, a drop action should be given to TCP SYN flooding attack flows if the number of flows is huge and the packet per flow is tiny. Meanwhile, a blocking action should be applied for attack flows transferring a large amount of packet in a flow.
- *Feature extractor:* This component extracts the features of traffic delivered from the traffic monitor and generates tuples for the SOM training inputs based on the requirements of the local policy conductor. In case the source-site SOM map is activated, a tuple of traffic features including (*protocol, port_number, flow_number, packet/flow, growth of source port*) is extracted from the monitoring traffic. Meanwhile, in case the destination-site SOM map is activated, a tuple of (*protocol, port_number, flow_number*) is extracted instead. Then, these tuples are incorporated into the smart SOM for classification, respectively.
- *Smart SOM filter:* This component applies the SOM algorithm to classify ingress/egress traffic to/from the local network. First, the SOM is trained continuously by input vectors transferred from the feature extractor. Second,

when a vector of DDoS attack traffic is recognized at the SOM, the smart SOM filter notifies the switching/routing component. Consequently, the protection mode is activated and the egress traffic is switched using the filter. The protection mode is deactivated if the SOM does not receive an input vector from a DDoS attack within a predefined time length. This means that no DDoS attack occurs.
- *Switching/Routing:* This is a basic function of borders used to handle ingress/egress traffic.

D. Operational Workflow

Under normal conditions, the protection mode is deactivated; that is, egress traffic from IoT devices bypasses the smart SOM filter to improve the networking performance. In this case, the traffic is still captured by the traffic monitor to extract features for smart SOM training and for traffic statistics reports (brown lines in Fig. 2). Whenever a DDoS symptom is detected by the attack analyzer in the orchestrator or by the smart SOM filter in the federated endpoint defenders, the protection mode is activated.

In the DDoS attack condition, the egress traffic from IoT devices should go through the smart SOM filter. Depending on the classification provided by the filter, the detected DDoS traffic is dropped. The traffic monitor collects statistics on the DDoS traffic, which it then reports to the orchestrator. After identifying the attack targets and attack methods, the orchestrator dispatches primary policies to all endpoint defenders distributed at the border of the corresponding local networks. The local policy conductor in each FOGshield endpoint defender assigns requirements to the feature extractor to generate appropriate training vectors, and it also informs the smart SOM filter of possible mitigation policies to tackle the attack traffic flows. During the attack time, the smart SOM filter still transfers ingress attack traffic (red lines in Fig. 2) to the traffic monitor, eventually to generating statistics and training samples. The security performance of the proposed framework is achieved through two points of protection given by the FOGshield endpoint defenders at the attack-source and destination sites.

Regarding communication overhead, the endpoints frequently send traffic statistic reports (traffic protocols, service ports, volumes, and source/destination IP ranges) and SOM parameters to the central orchestrator. Because the data fields of the reports are fixed and the size of the SOM parameters is deterministic, it is observed that the communication overhead between the endpoint defenders and the orchestrator is constant over time. In the downlink from the orchestrator to the endpoint defenders, the primary policies have a constant size as the size of the SOM activation command and desired traffic features are fixed. In addition, these policies are only sent whenever a DDoS attack is detected. Regarding the improved SOM parameter updates, its size is deterministic. Therefore, the communication overhead is controlable by the FOGshield.

V. Security Performance Analysis

A. Experiment Preparation

Initially, the smart SOM filters are trained using data sets of DDoS attacks and normal traffic. The DDoS-attack training sets are obtained from three data sets: CAIDA-attack-traffic [17], NSL-KDD [18], and DARPA Intrusion Detection [19]. The normal-traffic training set is derived from CAIDA-normal-traffic [17]. The statistics of these data sets are provided in Table I.

Owing to the wide variety of HIoT devices, we generalize the types of traffic into three categories:

- *Sensor traffic*: This traffic is generated by sensor devices in a fixed period, with a low number of packets per flow.
- *Monitor traffic*: This involves real-time traffic, characterized by a small number of flows and a significant number of packets per flow.
- *Alarm traffic*: This traffic type is not easily discernible because alarm IoT devices only generate traffic when an abnormal event occurs. However, we assume the alarm traffic has both moderate flows and a moderate number of packets per flow.

Accordingly, 10,000 samples of the three categories are extracted from the data sets. Static cross-validations with rotated 7:3 ratio of the training and testing are conducted. Within a validation profile, each testing sample is continuously utilized for training after testing. In particular, a tuple (*protocol*, *port_number*, *flow_number*) is applied for SOM training in the FOGshield endpoint defenders at the destination-site; at the source-site, a tuple (*protocol*, *port_number*, *flow_number*, *packet/flow*, *growth of source port*) is used. Details of these features are as follows:

- *protocol*: this factor is crucial in recognizing the presence of different types of DDoS attacks, e.g., ICMP, TCP SYN, and UDP flood attacks.
- *port_number*: this presents the number of layer-4 ports, which can be significant under DDoS attacks that exploit the vulnerabilities of transmission protocol, e.g., a TCP SYN flood attack.
- *flow_number*: this is a critical attribute for common DDoS attacks, e.g., an ICMP flood attack has few flows, while a TCP SYN flood attack generates a large number of traffic flows.
- *packet/flow*: this feature represents how many packets are transferred in a traffic flow, which is a crucial factor for DDoS attack detection. For instance, a vast number of packets are generated in one traffic flow in case of an ICMP flood attack, while there are a few packets for a TCP SYN flood attack.
- *growth of source port*: during DDoS attacks, the change in the number of source ports is trivial in the case of attacks that aim to send a massive number of packets in a few flows, e.g., ICMP flood. Meanwhile, for attacks, e.g., TCP SYN and UDP flood, a client generates many service ports.

Under DDoS attacks, the destination-site victim (e.g., edge network devices) usually has to deal with a massive traffic volume sending from arbitrary networks where each source

TABLE I
STATISTICAL INFORMATION OF CAIDA, NSL-KDD AND DARPA DATA SETS

	Characteristics			
CAIDA	**Traffic state**	**TCP (%)**	**ICMP (%)**	**Others (%)**
	Normal (2015)	88.45	6.0	5.55
	Attack (2007)	7.58	91.25	1.17
NSL-KDD	**Attack type**	**#Training patterns**	**#Testing patterns**	**#Features**
	back, land, neptune, pod, smurf, and teardrop	45927	7458	41
DARPA	**Attack types**	**Attack source**	**Attack time**	**Data size**
	SYN flooding	100 different IPs	6 minutes	3 GB

(of attack) network only generates a portion of the total traffic. Therefore, to avoid resource exhaustion at the destination-site in extracting detailed features for every incoming IP address, a three-feature tuple for a destination-site SOM training is used. Meanwhile, a five-feature tuple is chosen for a source-site SOM training to exactly identify which IoT devices in the local network are sending the attack traffic to the victim. As a result, the malicious devices are prohibited from sending out the traffic during a predefined period. In addition, the learning rate is set 0.1 to ensure that the SOM map does not miss any local minimal in all emulated systems.

B. Emulation Setup

A SDNFV-enabled network consisting of four Openflow switches has been designed by using `Mininet` platform [25] to represent a FOGshield orchestrator and three FOGshield endpoint defenders directly connected to three IoT networks (sensor, monitor, and alarm). FOGshield endpoint defenders were implemented as a software-based box, including SOM, an OpenvSwitch agent, and operational modules. An SDN controller is placed in the same machine with the FOGshield orchestrator to control traffic going through OpenvSwitch agents (e.g., redirect traffic to the smart SOM filter). Applications in the servers are in charge of storing IoT traffic arrival and responding to the IoT devices with acknowledgement messages.

To analyze the security performance of FOGshield, we conducted a comparison with two competitive frameworks on the basis of SOM technique utilization, specifically MLDMF [10] and D-SOM [13]. Note that all solutions use the same training data sets. For each local homogeneous IoT network, we use the `BoNeSi` DDoS Simulator [26] to generate different levels of attack traffic (50, 100, 200, and 300 Mbps). The `BoNeSi` output was configured to adopt the traffic features of three generalized categories: *Sensor traffic*, *Monitor traffic*, and *Alarm traffic*.

C. Emulation Results and Analysis

To analyze the security performance of FOGshield, we conducted a comparison with two competitive frameworks on the basis of SOM technique utilization, specifically MLDMF [10] and D-SOM [13].

Reaction latency: The first criterion is the attack reaction latency at each endpoint defender, which shows how fast a policy is implemented by FOGshield endpoint defenders to mitigate malicious traffic flows since an attack is detected by the smart SOM filter. In this measurement, we record four different attack traffic levels, as depicted in Figure 3. These results can be explained as follows:

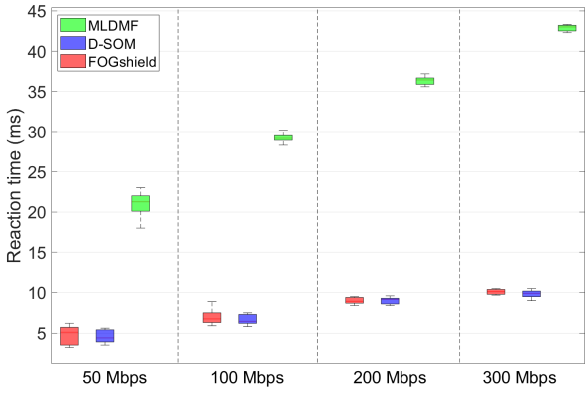

Fig. 3. Reaction latency to various attack levels.

- In the MLDMF, there is a considerable latency because all of the traffic is forwarded to the central controller from all endpoint defenders for attack investigation. Afterwards, a common policy is sent back to the endpoint defenders for traffic-handling operations. Moreover, the transmission time between the central controller and endpoint defenders supplement the overall reaction latency. Numerical results reveal a linear proportional dependence of reaction latency on the volume of traffic.
- In the other schemes, the attack investigation is performed by adopting a distributed model. Therefore, whenever an attack occurs, endpoint defenders immediately identify and prevent the attack from entering the network or reaching the victims. The data volume (and therefore, the data transmission time) reported to the central entities is inconsiderable. As a result, the reaction time of the FOGshield and the D-SOM solutions are lower for all traffic levels, e.g., 5 ms and 10 ms in the case of 50-Mbps and 300-Mbps traffic, respectively; see Figure 3.

Detection Rate and Accuracy: As a second criterion, we measure the detection rate and accuracy of three schemes during the whole experiment time. The detection rate and

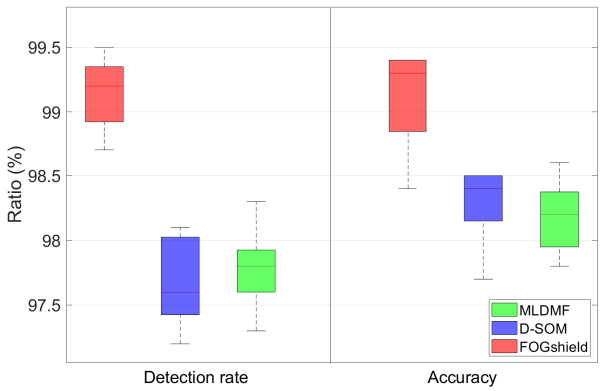

Fig. 4. Detection rate and accuracy in detecting abnormal traffic with the SOM map.

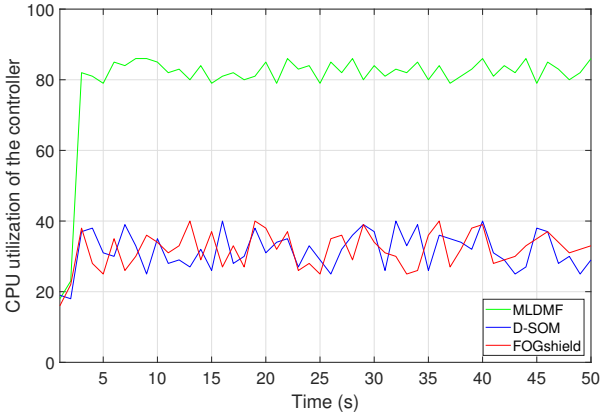

Fig. 5. CPU utilization under DDoS attacks in controller.

accuracy are defined respectively as follows:

$$\text{Detection rate} = \frac{TP}{TP + FN}, \tag{8}$$

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \tag{9}$$

where

- TP (i.e., true positive) indicates the number of correctly identified attack flows;
- TN (i.e., true negative) indicates the number of correctly identified normal flows;
- FP (i.e., false positive) indicates the number of normal flows that are incorrectly identified as attack flows;
- FN (i.e., false negative) indicates the number of attack flows that are incorrectly identified as normal flows.

Figure 4 presents the emulation results. In both criteria, FOGshield performed better than the other schemes, up to approximately a 99.3% detection rate and 99.4% accuracy. This is because SOM maps in the FOGshield endpoint defenders are separately trained (offline and online training) by local homogeneous IoT traffic. Hence, these filters find it easier to recognize patterns or in other words, they are well-adapted to local IoT traffic. Conversely, with a fixed and limited number of neurons in the common trained SOM, if there are many traffic types trained for a SOM map in the MLDMF case, or several merging times in the case of the D-SOM mechanism, the weights of each neuron in the SOM map will change considerably. This leads to degradation of both the detection rate and the accuracy of these schemes.

Bottleneck Handling: To assess the robustness of the schemes, we investigate the problem of bottlenecks occurring in the controller during our experiments. The results are shown in Figure 5. A major difference is observed between the distributed and centralized solutions. Both FOGshield and D-SOM show acceptable CPU usage of around 35%. On the other hand, the MLDMF mechanism shows a high usage of the controller's CPU (83%, on average). The reason is the traffic is always forwarded to the MLDMF central controller for processing, while the FOGshield and D-SOM process the traffic in a distributed manner.

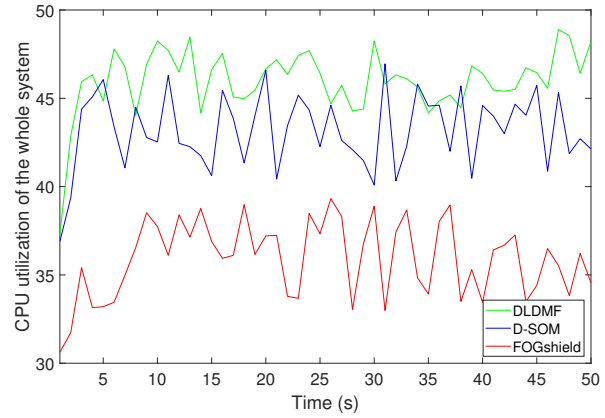

Fig. 6. CPU utilization under DDoS attacks in the whole protection system.

Resource Consumption: Finally, we assess the resource consumption issues; see Figure 6. We record the CPU usage of all machines and evaluate the average system resource consumption. The CPU usages of FOGshield, D-SOM, and MLDMF are 36%, 43%, and 46%, respectively. As discussed in Section IV-C, we consider the IP ranges of ingress traffic. Therefore, depending on the IP ranges, the FOGshield orchestrator can inform dedicated endpoint defenders to enable the SOM filter function in the case of attacks. As a result, the FOGshield framework can save resources because of the limited number of running SOM filters. In contrast, the D-SOM and MLDMF schemes always have to enable endpoint defenders at all time. Hence, the computing resources are consumed, even if there is no ingress traffic.

Remark: Based on the analysis, the benefits of FOGshield can be summarized into three main points:

- *Security improvement:* Detection accuracy is increased, while reaction latency is decreased. These achievements are obtained via two main development strategies in FOGshield. One is mitigation of the training functions from the cloud to the access tier in order to separately handle homogeneous IoT traffic. The other is cooperation between the attack source and destination to provide two protection points against malicious ingress and egress

traffic.

- *Traffic overhead reduction:* Since smart endpoint defenders are deployed in front of the attack source, malicious traffic generated by the HIoT devices is typically blocked at the border before traversing over the network. Moreover, large data collection for training purposes is unnecessary for delivery to the central controller. Instead, statistics reports are used for local traffic management.
- *System stabilization:* Since the training operation is performed locally for each individual IoT access network by using fog computing technology, FOGshield avoids the bottleneck problems experienced by the controller(s) typical in DDoS attacks.

VI. Conclusions and Future Research

In this study, we propose FOGshield, which is a DDoS prevention framework at the border of attack-source/destination in HIoT systems. FOGshield enables the network to defend against malicious traffic from HIoT devices by using smart SOM filters. Experimental results show that the detection rate and accuracy are improved because of the adaptation to local traffic at the SOM filters. Moreover, the federated architecture and control scheme of the FOGshield avoid the usual bottleneck occurring in DDoS attacks, saving around 10% resource consumption in terms of CPU usage compared to the distributed approaches. Finally, FOGshield introduces an efficient and feasible security framework for HIoT environments. Since the 5GPoA nodes are equipped with various computing capabilities and each local network is characterized by different IoT traffic volumes, a flexible filter training mechanism with optimal configurations should be considered in order to balance the workload among the endpoint defenders and central orchestrator as well as reducing unnecessary training efforts. In addition, other specific attack analysis is necessary for an efficient and comprehensive version of the intelligent FOGshield.

References

[1] "Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020," Technical Report, August 29, 2019. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

[2] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of things build our future: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2011–2027, 2018.

[3] N.-N. Dao, J. Kim, M. Park, and S. Cho, "Adaptive suspicious prevention for defending DoS attacks in SDN-based convergent networks," *PloS one*, vol. 11, no. 8, 2016.

[4] N.-N. Dao, Y. Kim, S. Jeong, M. Park, and S. Cho, "Achievable multi-security levels for lightweight IoT-enabled devices in infrastructureless peer-aware communications," *IEEE Access*, vol. 5, pp. 26 743–26 753, 2017.

[5] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *IEEE Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[6] B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3655–3682, 2017.

[7] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[8] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[9] N.-N. Dao, W. Na, and S. Cho, "Mobile cloudization storytelling: Current issues from an optimization perspective," *IEEE Internet Computing*, vol. 24, no. 1, pp. 39–47, Jan. 2020.

[10] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 30–36, 2018.

[11] S. Zheng and X. Yang, "Dynashield: reducing the cost of ddos defense using cloud services," in *11th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 19)*, July, 2019.

[12] C. Xu, H. Lin, Y. Wu, X. Guo, and W. Lin, "An SDNFV-based DDoS defense technology for smart cities," *IEEE Access*, vol. 7, pp. 137 856–137 874, 2019.

[13] T. V. Phan, N. K. Bao, and M. Park, "Distributed-SOM: A novel performance bottleneck handler for large-sized software-defined networks under flooding attacks," *Journal of Network and Computer Applications*, vol. 91, pp. 14–25, 2017.

[14] Z. Liu, X. Yin, and Y. Hu, "CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-learning," *IEEE Access*, vol. 8, pp. 42 120–42 130, 2020.

[15] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An intelligent edge defense mechanism against IoT DDoS attacks," *IEEE Internet of Things Journal*, 2020.

[16] T. Kohonen, "Essentials of the self-organizing map," *Neural networks*, vol. 37, pp. 52–65, 2013.

[17] CAIDA, "The CAIDA datasets of anonymized Internet traces and DDoS attack," (Accessed on Sep. 10, 2019). [Online]. Available: https://data.caida.org/datasets/

[18] NSL-KDD, "Data set for network-based intrusion detection systems," (Accessed on Sep. 10, 2019). [Online]. Available: https://data.caida.org/datasets/security/ddos-20070804/

[19] LANDER, "LANDER:DARPA DDoS attack-20091105," (Accessed on Sep. 10, 2019). [Online]. Available: https://ant.isi.edu/datasets/readmes/DARPA-2009-DDoS-attack-20091105.README.txt

[20] Z. Piao, M. Peng, Y. Liu, and M. Daneshmand, "Recent advances of edge cache in radio access networks for Internet of things: Techniques, performances, and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 1010–1028, 2018.

[21] A. Aleroud and G. Karabatis, "Contextual information fusion for intrusion detection: a survey and taxonomy," *Knowledge and Information Systems*, vol. 52, no. 3, pp. 563–619, 2017.

[22] E. Leverett and A. Kaplan, "Towards estimating the untapped potential: a global malicious DDoS mean capacity estimate," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 195–208, 2017.

[23] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, and M. Ma, "Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics," *IEEE Access*, vol. 7, pp. 158 481–158 491, 2019.

[24] Z. Zhao, C. Feng, H. H. Yang, and X. Luo, "Federated-learning-enabled intelligent fog radio access networks: Fundamental theory, key techniques, and future trends," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 22–28, 2020.

[25] Mininet Simulator, Accessed on August 27, 2020. [Online]. Available: http://mininet.org/

[26] BoNeSi DDoS Simulator, Accessed on August 27, 2020. [Online]. Available: https://github.com/Markus-Go/bonesi