Computers, Materials & Continua
DOI:10.32604/cmc.2022.017772
Article

Tech Science Press

SDN Based DDos Mitigating Approach Using Traffic Entropy for IoT Network

Muhammad Ibrahim[1], Muhammad Hanif[2], Shabir Ahmad[3], Faisal Jamil[1], Tayyaba Sehar[2] YunJung Lee[4] and DoHyeun Kim[1,*]

[1]Department of Computer Engineering, Jeju National University, Jeju-si, Jeju Special Self-Governing Province, 63243, Korea
[2]Virtual University Islamabad, Pakistan
[3]Department of IT Convergence Engineering, Gachon University, Sujeong-Gu, Seongnam-Si, Gyeonggi-Do, 461-701, Korea
[4]Department of Computer Science and Statistics, Jeju National University, Korea
[*]Corresponding Author: DoHyeun Kim. Email: kimdh@jejunu.ac.kr
Received: 10 February 2021; Accepted: 23 May 2021

Abstract: The Internet of Things (IoT) has been widely adopted in various domains including smart cities, healthcare, smart factories, etc. In the last few years, the fitness industry has been reshaped by the introduction of smart fitness solutions for individuals as well as fitness gyms. The IoT fitness devices collect trainee data that is being used for various decision-making. However, it will face numerous security and privacy issues towards its realization. This work focuses on IoT security, especially DoS/DDoS attacks. In this paper, we have proposed a novel blockchain-enabled protocol (BEP) that uses the notion of a self-exposing node (SEN) approach for securing fitness IoT applications. The blockchain and SDN architectures are employed to enhance IoT security by a highly preventive security monitoring, analysis and response system. The proposed approach helps in detecting the DoS/DDoS attacks on the IoT fitness system and then mitigating the attacks. The BEP is used for handling Blockchain-related activities and SEN could be a sensor or actuator node within the fitness IoT system. SEN provides information about the inbound and outbound traffic to the BEP which is used to analyze the DoS/DDoS attacks on the fitness IoT system. The SEN calculates the inbound and outbound traffic features' entropies and transmits them to the Blockchain in the form of transaction blocks. The BEP picks the whole mined blocks' transactions and transfers them to the SDN controller node. The controller node correlates the entropies data of SENs and decides about the DoS or DDoS attack. So, there are two decision points, one is SEN, and another is the controller. To evaluate the performance of our proposed system, several experiments are performed and results concerning the entropy values and attack detection rate are obtained. The proposed approach has outperformed the other two approaches concerning the attack detection rate by an increase of 11% and 18% against Approach 1 and Approach 2 respectively.

Keywords: SDN; control plane; load balancing; decision tree; CPU utilization

1 Introduction

In the future, the Internet will be a communication system for billions of interconnected smart devices embedded within the objects in the environment [1] that will be a revolution of data gathering and sharing among the smart devices. These devices will be carrying sensors generating a massive amount of data, gathered from these objects, and later analyzed for useful knowledge. Some examples of these smart devices carrying objects are traffic lights, appliances (fridge, Air conditioner), lampposts, irrigation outlets, medical equipment for monitoring and vehicles, etc. The Internet of things (IoT) [2,3] is the interaction of sensing and physical devices contained in buildings, vehicles, and other things connected through a network and offer services to accumulate data. It is the most extensive infrastructure running without human involvement. The IoT is permitted to sense, control distantly within the provided network structure. IoT has produced more openings for integrating the world into the systems created by the latest computing technologies. Due to these technological advancements, financial benefits are enlarged, efficiency is enhanced, and accuracy is peaked [3]. Each thing is individually identified and operated within internet infrastructure through an embedded computing system within IoT. By 2020, 30 billion objects are expected to be within the IoT system [4]. The technologies which play a pivotal role in enabling IoT are sensors, low-power electronics, connectivity, backbone connectivity, and hardware, to name a few.IoT gateways are vital for IoT and commonly consisted of small gateways. These gateways are capable of interconnecting wireless sensors that are distributed in the environment. These gateways form wireless sensor networks (WSN) and functioning internet gateway among the interconnected smart devices in the IoT. According to the requirements, it is a great challenge to impose the policies in such a complex and dynamic environment. Resource management and security gain immense importance in present-day networks that are still two important challenges in networks. Decoupling the networking data plane from network control logic is the main obstacle in these traditional networks [5]. SDN is possibly a revolutionized computer network and might be a 5th generation wireless network known as 5G. Since IoT is the future, the integration of IoT and SDN has a considerable advantage. SDN is a crucial enabler for the integration of IoT services with traditional services. SDN can transport large amount of data gathered from the machines, terminals, sensors, and nodes in the IoT. It can allocate storage and computing resources in the distributed data centers. By automatically configuring network devices, SDN gathers such data required for analysis. SDN is designed to authenticate users for security purposes by following the prescribed rules for accessing the data. This new networking paradigm permits a centralized system as software to control the whole network behavior by decoupling the forwarding layer from the routing decision-making plane [6]. A mechanism is required to enhance the communication between the control plane and the data plane. For this purpose, the OpenFlow system is utilized. The combination of SDN and OpenFlow permits us to implement high-level control programmed software system that provides the network components' behavior. Many new networking tasks are achieved through these programs including resource management, routing, and security. In the industry and academia, data transport and media requirements with the best quality are growing nowadays. Due to this growth of data requirements, the SDN could be used to tackle the challenge [7]. SDN and IoT are two technologies that are very much dependent on each other. Both of these technologies complement each other in bringing us a better and connected world. SDN technology can prepare a network for a robust and successful IoT. It provides elasticity and agility, which IoT demands. Furthermore, SDN offers application developers an environment to develop new software and tools connecting the IoT effectively [8]. Hackers have been performing DoS attacks for many years that increased exponentially over time.

Due to the internet bandwidth evolution, such attacks have enlarged from 400 Mbps to 600 Gbps by 2015. The purpose of DoS attacks includes financial blackmailing, hacking and state-sponsored attacks on enemies, DoS attacks on sensitive systems of banks disrupt its working [6,9]. The rest of the paper is organized as follows: Section 2 presents the state-of-the-art literature related to IoT, SDN, and Blockchain for IoT security solutions. The discussion about the proposed work is delineated in Section 3. In Section 4, the evaluation and results of the experiment are discussed. Finally, the conclusions and future work is presented in Section 5.

2 Related Work

In [10], the authors presented the challenges and opportunities in IoT. Data collection and brokerage, smart cities, aviation sector, automotive industry, energy sector, manufacturing, addressing and tagging, IoT applications are discussed, and opportunities and challenges associated with these areas are explained. The authors addressed the security issues in IoT [11]. They gave a brief overview of IoT applications in different fields like Industries, personal medical devices, smart homes, etc. IoT security requirements are briefly discussed, including resilience of attacks, client privacy, access control, and data authentication. IoT security threats are end-to-end data life cycle protection, secure things planning, visible/usable security, and privacy. The attacks are classified into low-level, medium-level, high-level, and extremely high-level attacks. The authors in [12] discussed the research directions for IoT. Five research communities of IoT are carrying the research: IoT, cyber-physical systems, wireless sensor networks, mobile computing, and pervasive computing. The study has been conducted in the areas of IoT. These areas are Massive Scaling of IoT devices embedded within objects operated in daily life, the architecture of IoT for correct operations and dependencies, and the issues faced during in the design and development of IoT systems; the robustness of underlying network during the communication of massive amount of data is another big issue; the openness of the IoT is an issue because sensor-based systems traditionally closed systems and it is challenging to give them a property of transparency; a big problem for the IoT is the security attacks due to low memory and processing power of devices being used within IoT; physically accessing the sensors, objects, actuators and openness of the systems; and Privacy of the information being obtained from IoT devices is another significant concern. The authors presented a comprehensive survey on the SDN technology and security for the IoT [13]. They compared several SDN architectures and presented their benefits and drawbacks. Furthermore, the discussion about role-based security controller for the SDN-IoT environment is also designed in their work. The authors in [14] presented a survey on the security and privacy issues of IoT. This work presented the evolution of IoT, architecture, and protocol stack of IoT for the IoT applications. IoT's primary security concerns are front-end sensors and equipments leads to unauthorized access to data, threats to the Internet, and DoS attacks. IoT privacy concerns are privacy in devices being used for data collection, privacy during communication of sensed data, privacy in data storage during data storage on physical devices, and privacy during data processing. In [15], the authors presented a simple approach based on statistical analysis for Intrusion Detection System (IDS). The authors employed a simple statistical process for modeling a new IDS. An argument is given that the necessary statistical methodology is still used if search space is not reduced. This argument is confirmed by the deployment of the exhaustive search method. The authors in [16] presented SDN as a solution to overcome security challenges in the IoT. Four layers architecture is presented that support smart devices integrated with the IoT system. These four layers are the smart object layer providing tools to the programmers. The Internet layer provides network protocols for communication between the smart devices within the Internet. The middleware layer provides management IoT, and the application layer provides applications used in the smart

devices. IoT-associated challenges are constraints on device resources, heterogeneous networks, and most importantly, the absence of common communication standards. Security issues in the IoT are trillion points of failure and vulnerabilities, integrating the people's data and trust, and most importantly the privacy of the collected data. The authors proposed a defense approach against a new flow attack in SDN-based IoT system [17]. A new Smart Security System (SSM) mechanism is presented in this work. SSM is a monitoring system and mitigation method. The monitoring system is low-cost that reuses the invocation of controller-to-switch messages and asynchronous messages. The mitigation method has used the function of redirection of suspicious flows. These flows are redirected to the security middleware in IoT, and the controller is informed about the result. The controller executes dynamic access control as the attacker access the SDN-based IoT switches. James Cannady (2016) compared the state-of-the-art Intrusion detection methods. The authors presented foundations of Intrusion detection systems (IDSs), development/evolution of IDSs, and approaches being used. These intrusion detection techniques are Next-Generation Intrusion Detection Expert System (NIDES), Distributed Intrusion Detection System (DIDS), State Transition Analysis Tool (STAT), USTAT, tripwire, Graph-based Intrusion Detection System (GrIDS), thumb printing and Cooperating Security Managers (CSM).

The authors in [18] presented a survey on securing the network using SDN. The primary security configuration using SDN is a key to secure the network. Security configuration using SDN is achieved by centralizing the control plane and implementing flexible security policies. Configuring the network to detect the DoS attack, traffic anomaly detection, etc., is an excellent method for a secured network. In SDN, having programmatic capabilities with dynamic responses is used for threat remediation. In SDN, network verification and consistency are straightforward and could be verified for consistent networks. SDN is used as a service to facilitate some new network security measures beyond protecting the network and enabling the new services such as anonymization which enhanced the trust and remote management. The authors in [15] argued that SDN brings many benefits by decoupling control and data plane. By this mechanism, SDN makes it easy to detect and react to DoS/DDoS attacks. In [19], the authors discussed the development of Blockchain-based systems.s. While reimagining the space with the Blockchain, highlighted various common challenges, drawbacks, and shortcomings that can occur. The authors in [6] presented a comprehensive framework of entropy to deduce the state of network flow rates and properties in probabilistic form. Network traffic uncertainty is symbolized by the joint probability function over its unknowns. Kornites et al. presented a comprehension dataset of the normal and malicious traffic of IoT. They developed a Bot-IoT dataset of the traffic. The authors also presented some statistical analysis of this dataset. The authorpresented Blockchain and IoT's integration called Blockchain of Things (Cot). His work presented IoT and Blockchain Technologies' union concerning architecture and security. The author claimed that IoT requires security features while Blockchain naturally has these features due to its broader use of cryptography and peer-to-peer consensus model. A holistic approach that presented attackers' motives for using IoT devices to launch DDoS attacks is proposed in [20]. Attack tools are defined for infecting IoT devices with botnet malware and initiating DDoS attacks on networks and servers. New and emerging attack patterns as multi-vector attacks are introduced along with a detailed taxonomy of attacks on IoT layers and Cloud layers. The authors discussed IoT and the Cloud environment, providing a complete view of DDoS attacks and defensive measures. The authors also presented a detailed description of DDoS attacks from the formation of a botnet of IoT devices to implement them as DDoS attack traffic sources. In [21], the authors described the IoT data aspects, categorized as heterogeneity, inaccuracy of sensed data, scalability, and semantics. IoT data management also provides support for offline analysis. Management systems need to support heterogeneous

devices that operates in heterogeneous networks in confined areas. Administrators can remotely control IoT devices that will reduce the costs associated with maintenance activities quickly. The authors presented an integrated research project between universities, government, and private sector companies in the USA and introduced IoT middleware [22]. The middle layer constrains mobile access like smartphones, single board computers like the Raspberry pi, and laptops act as a gateway. Both layers have access to the CloudCloud services. This IoT middleware solution is not simple and can be installed on the embedded devices such as edge or Cloud devices. Actor-based IoT middleware sensors may not have a final service. However, the character provides a storage service that can be downloaded from Cloud storage where needed. Calvin and Node-RED are examples of character-based IoT middlewares. In [23], the authors presented a complete list of significant challenges, including collaboration, distribution, rollout, infrastructure support, security, and privacy by investigating the IoT Middleware solutions. The authors also concluded that the Web semantic-based IoT Middleware solution is adaptable to these challenges without the persistence service's resilience. It is an effective solution for device support and service availability; however, IoT Middleware-based web service is heavy and is not ideal for downloading Middleware to Edge devices integrated with IoT applications. It has become more important to make a simple Middleware solution with the IoT network development and to distribute across both the Cloud or Edge devices as a function. Sensitive latency applications like autonomous driving may require Middleware to be applied to sensor nodes or edge devices. In contrast, applications that require advanced computing and analytics prefer Cloud-based Middleware solutions. In [24], the authors investigated that the device access management file for the IoT system is essential as critical details are important to understand different intelligent things. In [25], the authors proposed a device authentication approach for securing IoT communication networks. Various methods, such as dual authentication, PSO-AES, and authentication are used to authenticate the devices using the blockchain techniques. In [26], the authors proposed and implemented an efficient DDoS detection algorithm to maximize the detection rate with high efficiency. The detection approach integrates the PSD (Power Spectral Density) entropy method with the SVM (Support Vector Machine) for detecting the DDoS attacks from legitimate traffic. The proposed approach calculates the PSD-entropy first and then compares it against two pre-define adaptive thresholds values.

3 Proposed Model

The proposed BEP protocol comprises two components: SEN and SDN controller, as shown in Fig. 1.

The SEN module receives the inbound traffic using the packet capturing module. The packet processing and features distribution module process the inbound and outbound traffic and extract important features (i.e., 26 in this case as shown in Tab. 1) from the traffic which are used by the entropy calculation module. The entropy information and traffic features are stored in the local Blockchain and then correlation of the entropy information is performed against the history entropy information by the features entropy data module to confirm about the traffic legitimacy. The BEP transmits the entropies information to the miners for the development of the block.

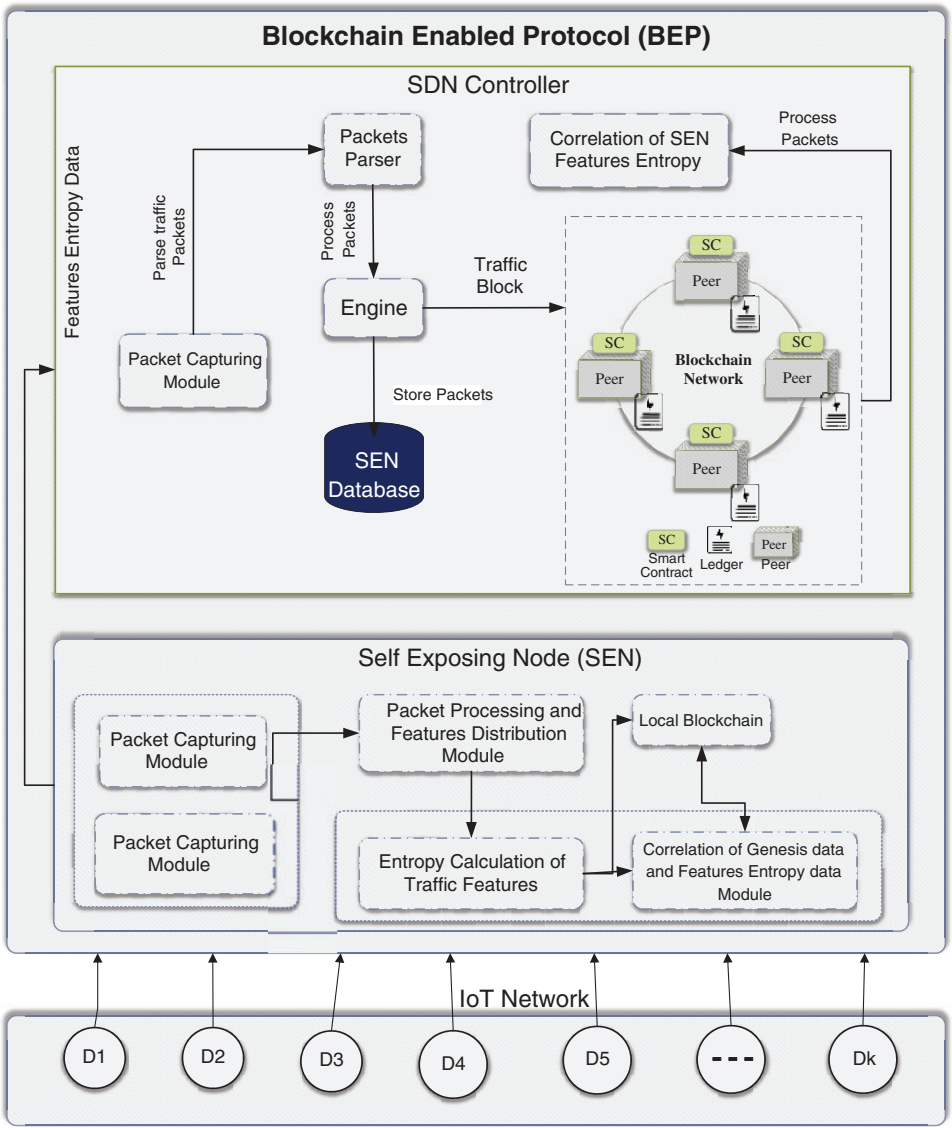

Figure 1: System Architecture of BEP protocol

The BEP is a proprietary protocol written in Python3 over Transport and Control Protocol (TCP) that provides a set of rules for transmission of transactions, blocks, data, and Blockchain between Controller node the Sens. BEP is an application layer protocol that is capable of transmitting Blockchain-related data that works as the client-server model. SEN captures the inbound and outbound traffic features and calculates its average joint entropies, and hand over to the Blockchain network. The miners mine this transaction and validate the transactions and put in the Blockchain as a block. On average, a block (the structure containing transaction) is mined every 10 s in the Blockchain and is transmitted to the controller by the BEP, where this block is mined into global Blockchain.

Table 1: Traffic features and descriptions

Sr. No.	Feature	Description	Average joint entropy
2	pkts_sent	Packets sent	0.761733
3	pkts_received	Packet received	0.961453
4	bytes_sent	Bytes sent	0.468683
5	byte_received	Bytes received	0.561783
6	pkts_count	Total count of packets in transactions	0.661783
7	Total_bytes	Total number of bytes in transaction	0.661768
8	scr_pkts	Source-to-destination packet count	0.661812
9	dst_pkts	Destination-to-source packet count	0.661718
10	scr_bytes	Source-to-destination byte count	0.661772
11	dst_bytes	Destination-to-source byte count	0.661718
12	pkts_per_sec	Total packets per second in transaction	0.664154
13	scr_dst_pkts_per_sec	Source-to-destination packets per second	0.661734
14	dst_ scr _pkts_per_sec	Destination-to-source packets per second	0.661720
15	tot_no_bytes_per_src_ip	Total Number of bytes per source IP	0.635689
16	tot_no_bytes_per_dst_ip	Total Number of bytes per destination IP	0.635674
17	tot_no_pkts_per_src_ip	Total Number of packets per source IP	0.635686
18	tot_no_pkts_per_dst_ip	Total Number of packets per destination IP	0.635701
19	tot_no_pkts_per_proto	Total Number of packets per protocol	0.636924
20	tot_no_pkts_per_dst_port	Total Number of packets per destination port	0.635630
21	avg_rate_per_proto_per_src_ip	Average rate per protocol per Source IP (packets/second)	0.636084
22	avg_rate_per_proto_per_dst_ip	Average rate per protocol per Destination IP	0.636399
23	no_inbound_conn_per_src_ip	Number of inbound connections per source IP	2.067795
24	no_inbound_conn_per_dst_ip	Number of inbound connections per destination IP	1.430813
25	avg_rate_per_proto_per_scr_port	Average rate per protocol per sport	0.636738
26	avg_rate_per_proto_per_dst_port	Average rate per protocol per dport	0.637848

For profiling the DoS/DDoS, we have used the Bot-IoT dataset to profile and twenty-six features are extracted from the dataset [24]. The average joint entropy is calculated for each feature and saved in the genesis block of the Blockchain by profiling from the Bot-IoT dataset and features of the traffic entropies of the DoS/DDoS attacks. Every SEN node detects the attack by correlating the genesis block's entropies with its calculated entropies and getting information about the compromised node by itself. Each SEN can detect the attack by correlating the inbound and outbound entropy values with the values in the genesis block. The Controller node of the SDN is also taking part in the overall process. This controller maintains a database of all the SENs in the network by extracting Blockchain blocks' entropy data. By analyzing and correlating each

entropy's data, the decisions are made about either SEN is a bot or not. If SEN is a bot/botnet, it is blocked by the SDN infrastructure, which mitigates the attack.

Finally, SEN calculates the entropies of the features of the inbound and outbound traffic and handover to the Blockchain as data of the block. Also, it correlates the entropies of the features to the dataset calculated entropies in the genesis block. The BEP picks the whole mined block and transmits it to the Controller node. The controller takes the block, extracts it, mines its information to the global Blockchain, and saves this information into the analysis database. The Controller node correlates the data of SENs and decides the DoS or DDoS attack. So, there are two decision points, one is SEN, and another is the controller. As SEN detects a botnet, the OFM will compose a flow entry and push it to the controller. The controller then updates the Voss's flow tables and block the interface from the Voss to which bot SEN is connected to the network. In this way, SEN is isolated, and the network resources are saved from DoS/DDoS attacks.

Profiling the network traffic features is an integral part of the SEN. The architecture of the profiler is shown in Fig. 2. The profiler's basic functionality is that it captures the traffic, distributes the traffic features, and calculates the entropy of the features, detection, and output. At first, already captured traffic files in the cap format of bots by different entities are provided to the profiler and generated a profile database of malicious traffic. This malicious traffic database gives us the basis for detecting DoS attacks by different bots of the botnet. The class and methods are given below class play reader and redcap ("file.pcap") [24]. The profile is developed from the Bot-IoT dataset (Koroniotis, 2019). The reasons behind using this dataset are because it uses realistic testbed configuration, realistic traffic, labeled data, IoT traces, diverse attack scenarios, total capture packets, and newly generated features. This dataset includes both attack traffic and regular traffic. This dataset has a size of 69.3 GB cap files.

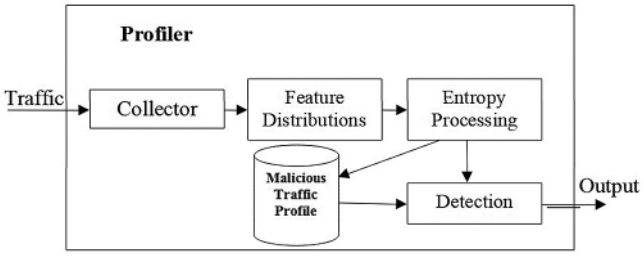

Figure 2: Workflow of traffic profiler

Several fitness IoT devices are used, and data is stored in the Cloud. The generated messages are transmitted to the Cloud using the MQTT protocol. The statistics of regular traffic included in the dataset are shown in Tab. 2.

The dataset used four Linux Virtual Machines to start cyber-attacks in parallel for implementing different botnet scenarios. The cyber-attacks and their tools considered in the Bot-IoT dataset are described in Tab. 3.

Table 2: Statistics of normal instances included in the Bot-IoT dataset

Protocol	Number
TCP	1750
UDP	7225
ARP	468
ICMP	9
IPV6-ICMP	88
IGMP	2
RARP	1
Total	**9543**

Table 3: Statistics of attacks in IoT-Bot dataset

Information gathered	Fingerprint	Protocols	Tools	Packets	Size(bytes)
Denial of Service	DDoS	TCP	hping3	19547603	11924037830
Denial of Service	DDoS	UDP	hping3	18965106	1242878221710
Denial of Service	DDoS	HTTP	golden eye	19771	15816800
Denial of Service	DoS	TCP	hping3	12315997	492639880
Denial of Service	DoS	UDP	hping3	20659491	1353919742685
Denial of Service	DoS	HTTP	golden eye	29706	23764800
Total				**71537674**	**2609254223705**

4 Experimental Setup and Evaluation

A testbed of SDN and IoT is developed in Mininet. Mininet is a network emulator that generates a network by the links, controllers, switches, and virtual hosts. It is highly flexible and customizable simulation tool that supports network testbeds and complex topology configurations. Mininet provides CLI that is OpenFlow- enabled and topology-aware for running and debugging network-wide tests. This tool also provides Python APIs for network application programming and experimentation. The tool runs real code and can be moved to a real system with minimal changes. Blockchain and BEP are developed in Python3. The core components of Blockchain network are nodes, transaction, block, chain, miners, and consensus algorithm. These all components are implemented in Python3. We have two scenarios in this simulation. Firstly, when the SEN is under DoS attacks and secondly, when the SEN performs the DoS attack after being compromised by the malware attack.

4.1 SEN Under Attack Scenario

The topology of the smart Fitness IoT network is shown in Fig. 3. The simulation is conducted on a system equipped with a CPU of 3 GHz, RAM 16 GB, and 150 GB of Hard drive, and for the simulation, the Mininet tool is installed and configured. Mininet is a powerful simulation tool to develop, share, and test OpenFlow and Software-Defined Networking systems. Open Daylight controller, OFM, OVS, and SEN are installed on the hosts. The results in Fig. 4 show the SEN node's traffic entropies when no attack is performed on the SEN node. The x-axis corresponds to the inbound traffic, and the y-axis's inter-arrival time representing the entropies of

traffic features. In this case, the entropy values follow a linear pattern that shows the SEN node's normal behavior.

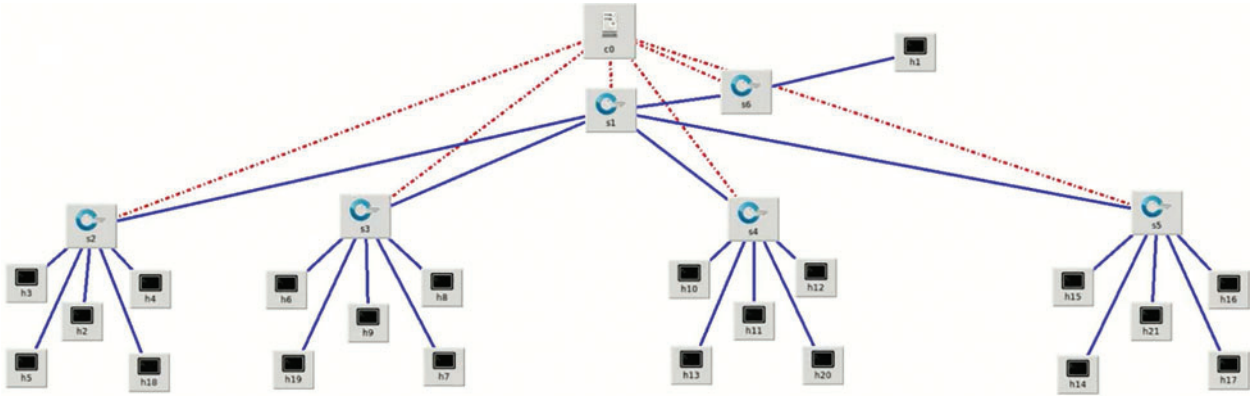

Figure 3: DoS attack

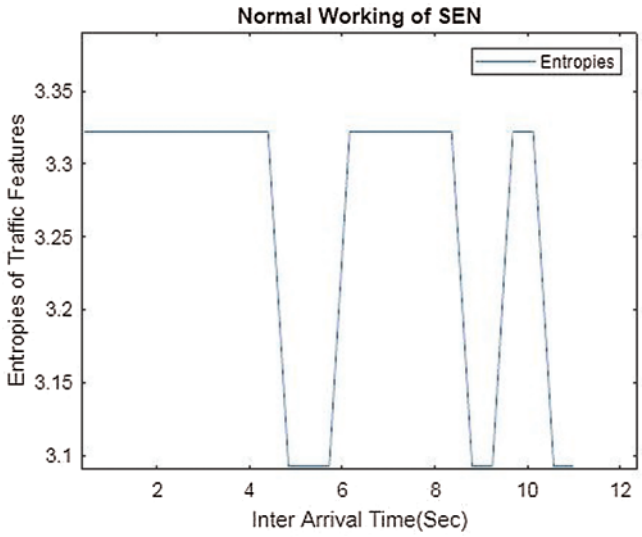

Figure 4: Traffic entropy of traffic features in normal scenario

The results are shown in Fig. 5a and present the SEN node's abnormal behavior due to a DoS attack. A DoS attack is just started, and the normal functioning of SEN is disturbed due to significant data traffic.

The shift from high entropy values to low entropy values can be seen in the results. This shows that SEN is sending/receiving a significant amount of data. This data inflow or outflow from the SEN monitors itself continuously and saves information about the inbound and outbound traffic in the Blockchain as shown in Fig. 5b. A significant shift in entropy is demonstrated at the period of 10th second. The huge surge of data shifts the SEN behavior, and SEN cannot send its sensed data for the IoT applications. In this case, SEN inbound traffic is observed and draws a graph

in the entropy time domain, as shown in Fig. 5c. The SEN behavior is changed from normal to attack, and inbound traffic is increasing tremendously. SENs and the decision algorithm's behavior with the observation of entropy of the traffic features and correlation of the traffic features like several packets inflow and outflow lead us to the final decision-making about the attacked/attacker SEN. The results are based on the entropy values of the traffic features correlation coefficient. We categorize the DoS/DDoS attacks strength concerning the correlation coefficient values as shown in Tab. 4.

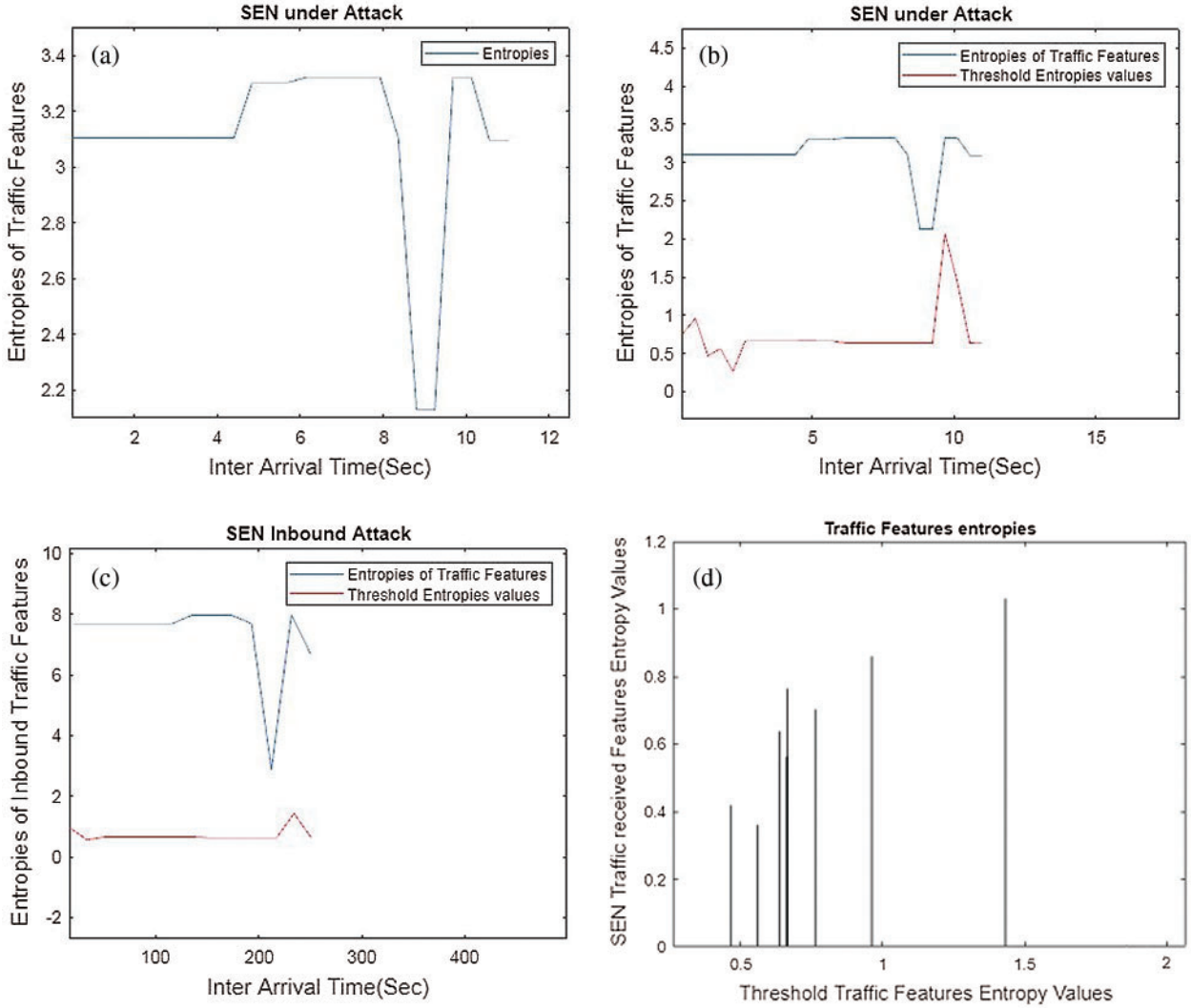

Figure 5: SEN attacks categories (a) Abnormal behavior of SEN (b) SEN under attack against threshold values (c) SEN under attack (d) SEN under attack scenario

The ideal correlation coefficient for both threshold values of entropy of dataset and SEN received traffic entropy values according to Tab. 3 values for a strong and powerful relationship. It is essential to mention that the simulation was executed for 26 simulated parameters, as given

in Tab. 1. Therefore, the conclusions and explanations are based strictly on simulation SEN traffic feature entropies and Threshold traffic features entropies shown in Fig. 5d. The simulations are executed multiple times, and the entropy values of traffic features are obtained. The next step is to calculate the correlation coefficient of test values of traffic features received on SEN with traffic features' threshold values. We got a correlation coefficient in the range of 0.600–0.799, which shows a strong relationship between SEN received traffic features entropy values and threshold traffic features entropy values that resulted from DoS/DDoS attack on the SEN.

Table 4: Correlation coefficient interpretation

Size of correlation	Interpretation
0.000–0.199	Very weak
0.200–0.399	Weak
0.400–0.599	Medium
0.600–0.799	Strong
0.800–1.000	Very strong

4.2 SEN Attacking Scenario

The obtained results are based on the entropy values of the traffic features correlation coefficient. The following simulation experiment corresponds to the scenario when SEN compromised and is performing the attack. In this case, SEN outbound traffic is observed and draws a graph in the entropy time domain, as shown in Fig. 6a. The SEN behavior is changed from normal to attack, and outbound traffic is increased tremendously. The simulation's primary purpose is to evaluate the SEN and detect the ideal correlation coefficient for both threshold values of entropy of dataset and SEN sent traffic entropy values according to Tab. 4 value for solid and powerful relationships. It is essential to mention that the simulation was realized for 26 simulated parameters, as shown in Tab. 1. Therefore, the conclusions and explanations are based strictly on the SEN traffic feature entropies and Threshold traffic features entropies shown in Fig. 6b.

A critical metric to quantify the performance of the DoS/DDoS detection approaches is the detection rate. Another set of experiments is carried out, and results concerning the proposed approach's detection rate and two compared contemporary methods are obtained and plotted in Fig. 7. *Approach 1* has shown a detection rate of 78% on the utilized dataset. A*pproach 2* has demonstrated an improvement of 6% against *Approach 1*. The proposed method has shown better entropy results and thus been able to improve the detection rate by 11% and 18.5% against *Approach 1* and *Approach 2,* respectively.

4.3 Results and Discussion

The proposed approach was evaluated using various SEN simulation experiments under attack and SEN as an attacker scenario. Several experiments were performed to test the performance of the proposed approach with different entropies settings. The value of the entropy was used as a measure to detect the DDoS attack occurrence. After performing various experiments, it was revealed that the proposed approach has been able to catch most of the DDoS attacks with a detection rate of 90 or more in each of the experiments. These results confirm that the proposed approach can significantly improve the detection of DDoS attacks for fitness IoT data.

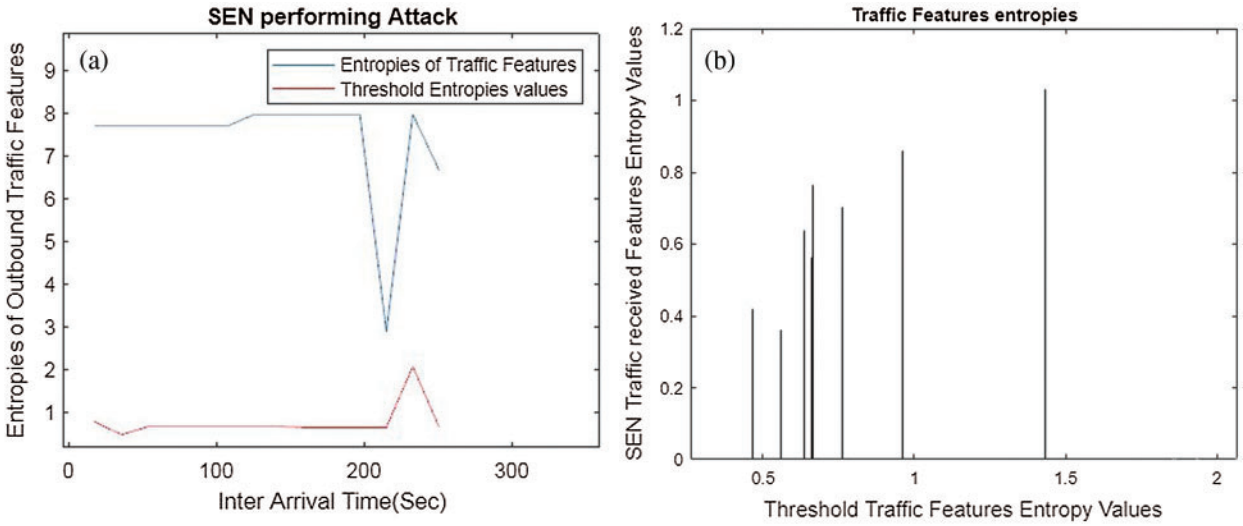

Figure 6: SEN performing different Scenarios. (a) SEN performing DoS attack (b) SEN attacking scenario

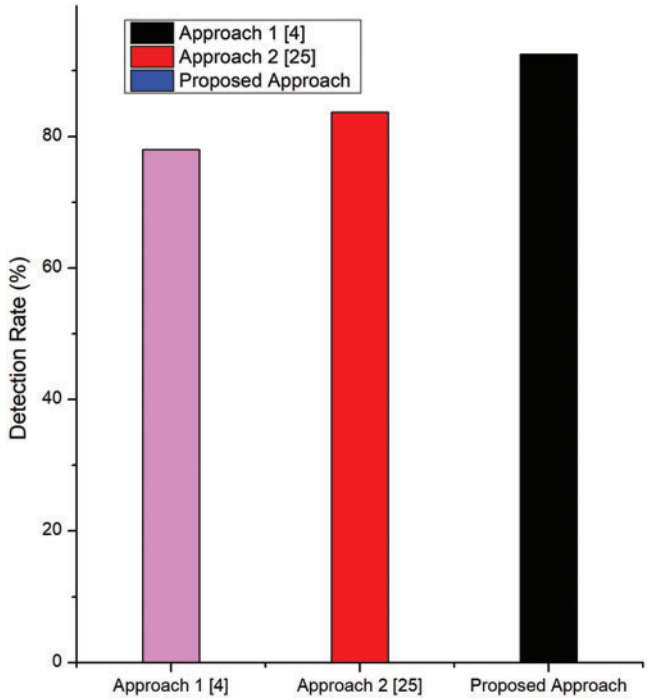

Figure 7: Detection rate comparison

5 Conclusions and Future Work

The simulation shows that the proposed approach has shown higher detection rate to counter DoS/DDoS attacks. In the current scenario, fitness data and access to the system are crucial due

to time restraints and resources availability. The DoS/DDoS attacks on the fitness IoT system block the traffic by heavy flooding of the packets on the specific machine, and the user of the fitness system cannot access the resources of IoT system SDN can counter this by dropping the machine's traffic by blocking the port on the OVS on which the attacking machine is connected. So, SDN has blocked the flooding traffic from the attacking machine and restored the fitness IoT system's normal working. SEN is able to detect and mitigate the DoS attacks at their origin. With the help of SDN, SEN strengthened the IoT security against the DoS attacks. In the future, we will carry on this work to detect the botnet and botnet controller. We will use current research work to trace the botnet which the controller controls. Our current research work can help trace the bots in botnet back and the botnets' controller responsible for DoS/DDoS attacks. A botnet is many Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed DDoS attacks, steal data, send spam, and allows the attacker to access the device and its connection.

Funding Statement: This research was supported by Energy Cloud R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT (2019M3F2A1073387), and this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2018R1D1A1A09082919), and this research was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2018-0-01456, AutoMaTa: Autonomous Management framework based on artificial intelligent Technology for adaptive and disposable IoT). Any correspondence related to this paper should be addressed to Do-hyeun Kim.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Ahmad, S. Malik, I. Ullah, M. Fayaz, D. H. Park *et al.*, "An adaptive approach based on resource-awareness towards power-efficient real-time periodic task modeling on embedded IoT devices," *Processes*, vol. 6, no. 7, pp. 90–116, 2018.

[2] S. Ahmad, S. Malik, I. Ullah, D. H. Park, K. Kim *et al.*, "Towards the design of a formal verification and evaluation tool of real-time tasks scheduling of IoT applications," *Sustainability*, vol. 11, no. 1, pp. 204–226, 2019.

[3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[4] S. Ahmad, L. Hang and D. Kim, "Design and implementation of cloud-centric configuration repository for DIY IoT applications," *Sensors*, vol. 18, no. 2, pp. 474–494, 2018.

[5] T. A. Tang, L. Mhamdi, D. McLernon, S. A. Zaidi, M. Ghogho *et al.*, "DeepIDS: Deep learning approach for intrusion detection in software defined networking," *Electronics*, vol. 9, no. 9, pp. 1533, 2020.

[6] A. Mubarakali and A. S. Alqahtani, "A survey: security threats and countermeasures in software defined networking," in *IEEE 2nd Int. Conf. on Information and Computer Technologies (ICICT)*, University of Hawaii Maui College, USA, pp. 180–185, 2019.

[7] H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li *et al.*, "A survey on security-aware measurement in SDN," *Security and Communication Networks*, vol. 2018, pp. 1–14, 2018.

[8] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Yau *et al.*, "Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1838–1853, 2018.

[9] N. M. Abd Elazim, M. A. Sobh and A. M. Bahaa-Eldin, "Software defined networking: attacks and countermeasures," in *2018 13th Int. Conf. on Computer Engineering and Systems (ICCES)*, Cairo, Egypt, pp. 555–567, 2018.

[10] T. Ninikrishna, S. Sarkar, R. Tengshe, M. K. Jha, L. Sharma *et al.*, "Software defined IoT: Issues and challenges," in *Int. Conf. on Computing Methodologies and Communication (ICCMC)*, Erode, India, pp. 723–726, 2017.

[11] M. A. Razzaq, S. H. Gill, M. A. Qureshi and S. Ullah, "Security issues in the internet of things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 383–388, 2017.

[12] I. A. Meshchikhin and S. S. Gavriushin, "The application of elements of information theory to the problem of rational choice of measuring instruments," in *Int. Conf. of Artificial Intelligence, Medical Engineering, Education*, Springer, Cham, Moscow, Russia, pp. 705–712, 2018.

[13] D. L. C. Dutra, M. Bagaa, T. Taleb and K. Samdanis, "Ensuring end-to-end QoS based on multi-paths routing using SDN technology," in *GLOBECOM, IEEE global communications conference*, *Singapore*, pp. 1–6, 2017.

[14] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[15] C. Ieracitano, A. Adeel, F. C. Morabito and A. Hussain, "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing*, vol. 387, pp. 51–62, 2020.

[16] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in *15th Learning and Technology Conf. (L&T)*, Effat University, Jeddah, KSA, pp. 112–119, 2018.

[17] M. P. Singh and A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Computer Communications*, vol. 154, pp. 509–527, 2020.

[18] N. Sultana, N. Chilamkurti, W. Peng and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.

[19] I. Weber, V. Gramoli, A. Ponomarev, M. Staples, R. Holz *et al.*, "On availability for blockchain-based systems," in *IEEE 36th Symp. on Reliable Distributed Systems (SRDS)*, Hong Kong, pp. 64–73, 2017.

[20] M. M. Salim, S. Rathore and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: A survey," *The Journal of Supercomputing*, vol. 76, pp. 5320–5363, 2019.

[21] B. Liu, X. L. Yu, S. Chen, X. Xu and L. Zhu, "Blockchain-based data integrity service framework for IoT data, in *IEEE Int. Conf. on Web Services (ICWS)*, Honolulu, HI, USA, pp. 468–475, 2017.

[22] C. Xie, B. Yu, Z. Zeng, Y. Yang and Q. Liu, "Multi-layer internet of things middleware based on knowledge graph," *IEEE Internet of Things Journal*, pp. 2635–2648, 2020.

[23] A. Palade, C. Cabrera, G. White, M. A. Razzaque and S. Clarke "Middleware for the internet of things: A quantitative evaluation in small scale," in *IEEE 18th Int. Symp. on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Macao, China, pp. 1–6, 2017.

[24] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT,", *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[25] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[26] N. Zhang, F. Jaafar and Y. Malik, "Low-rate dos attack detection using psd based entropy and machine learning," in *2019 6th IEEE Int. Conf. on Cyber Security and Cloud Computing (CSCloud)*, Paris, France, pp. 59–62, 2019.