ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Smart Home IoT Traffic Characteristics Based on DDoS Traffic Detection Using Edge Computing

Mohammed Ubaid Ur Rahman, Dr.A Bhavani Sankar

Research Scholar, Dept. of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences, Sehore, M.P, India

Associate Professor, Dept. of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences, Sehore, M.P, India

ABSTRACT: The heterogeneity of the networks, devices, and services introduces serious vulnerabilities to security attacks, especially distributed denial-of service (DDoS) attacks, which exploit massive IoT devices to exhaust both network and victim resources. This paper proposes a new approach which leverages mobile edge computing (MEC) to deploy edge functions in the smart home environment for generating illegitimate DDoS traffic. MEC gather information about incoming traffic and communicate that information via a fast-path with a nearby detection service. To further development of the timely DDoS traffic detection generated in the aforementioned environment, this research seeks to establish the diversity of traffic generated by IoT devices in a smart home environment with respect to the traffic generated through human type communication. As such, this study proposes MEC shield, a localized DDoS prevention framework leveraging MEC power to deploy multiple smart filters at the edge of relevant attack-source/destination networks. The numerical results reveal that MEC shield outperforms existing solutions. Preliminary investigation shows promise for up to 10x faster detection that reduces up to 82% of the Internet traffic due to IoT-DDoS.

KEYWORDS: distributed denial-of service (DDoS) attacks, mobile edge computing (MEC), smart home environment.

I. INTRODUCTION

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

Consequently, networking infrastructures are evolving into heterogeneous IoT (H-IoT) networks, which are characterized by diverse IoT devices, multiple access technologies, and powerful computation provided at the edge tier, referred to as mobile edge computing (MEC). Along with the software capability of emerging technologies, such as software-defined network function virtualization (SDNFV), MEC-enabled H-IoT networks support a promising framework for H-IoT security. Security-as-a-service (SaaS) can be deployed with the support of MEC technology to prevent internal/external attacks from/to the H-IoT networks [4].

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

The availability of information and communication resources in a smart home environment is a key security challenge and can often be hindered by DDoS attacks [6]. In addition to be the target of attack, devices in the smart home environment are ever more frequent sources of DDoS attacks, or generators of illegal DDoS traffic through unprotected IoT devices associated with the botnet network. An example of such botnet through which many DDoS attacks are performed is the ShadowNet and it can be described that a possible outcome is accelerated detection and response to an attack, potentially even before it reaches the target. Concretely, encouraging preliminary results are presented from experiments and carried out on an initial ShadowNet prototype. This research will identify the differences in the characteristics of the traffic generated by Smart home IoT devices in relation to traffic generated by the HTC (Human Type Communication) and so far methods used in the detection of this specific form of DDoS traffic will be analyzed. This also demonstrated that ShadowNet can detect an impending IoT DDoS attack up to 10x faster than the best case detection at victim, and prevents injection of up to 82% of the traffic in the Internet infrastructure by compromised IoT devices. In that sense, ShadowNet represents a major contribution towards defenses against IoT-DDoS attacks.

II. LITERATURE SURVEY

The security of a smart home IoT (SHIoT) device is a subject of numerous research. Paper [6] shows the first fundamental empirical analysis of the smart home platform security. Applications developed on the Samsung Smart Things platform have been analyzed and vulnerabilities of such applications to numerous security threats were identified such as access rights escalation, unauthorized access to pin code devices, unauthorized device configuration modifications, and so on. Numerous studies have identified the security challenges of a smart home environment associated with unauthorized data modification, inserting malicious cod, unauthorized remote device management, eavesdropping, unauthorized routing and others. Authors of paper [2] conducted a vulnerability assessment of SHIoT devices. The research involved a considerable number of vulnerabilities and related threats whose implementation could have a negative impact on user privacy, user data, traffic content, and disabling resource access as a result of DDoS attacks.

Cloud computing offers an efficient method to access the actual remote computing through the Internet. But its security vulnerabilities have been a major and continuous risk element for both the clients and the cloud service providers. There has been research discussion on the security threats associated with cloud computing and cloud service delivery models. The third party involvement in data processing is another security threat for the service availability and integrity and confidentiality of information in cloud computing. Distributed Denial of Service (DDoS) has been a major threat for cloud services. DDoS attacks often target cloud services with overwhelming floods of requests that result in service down time for legitimate users [7].

Various techniques have been proposed to enhance cloud computing security measures against DDoS attacks. However, these techniques are not able to resolve the sophisticated and distributed nature of the DDoS vector attacks, and the attacks are still compromising and shutting down the victims (cloud computing services) at an alarming rate. In 2004, Furnel [8] discussed the insider user attack in an IT organization. He categorized the insider attackers into three types: masqueraders, clandestine users and misfeasors. He argued that the installation of Misuse Based Intrusion Detection System and Anomaly Based Intrusion Detection System can mitigate the insider user attacks. Though, he did not propose any model to protect the cloud from insider attacks.

III. PROPOSED SYSTEM

A. Smart home architecture

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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

IoT concentrator enables mutual communication of the perception layer device and connection of the perception layer with the access network for transmitting the data to the middleware layer. Conventional access technologies such as xDSL, fiber optics, mobile data networks (3G, 4G, future 5G) and similar are used to transfer data from a network to a middleware layer. The middleware layer is based on the Cloud Computing concept, and it contains resources and processing elements for dana generated in the middleware layer for converting it into useful information. The middleware layer has three basic functions:
1) Remote connectivity of users with SHIoT devices for remote management,
2) Automation of SHIoT devices management based on the information obtained without user mediation, and
3) Transfer of information to user terminal devices for providing information.

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

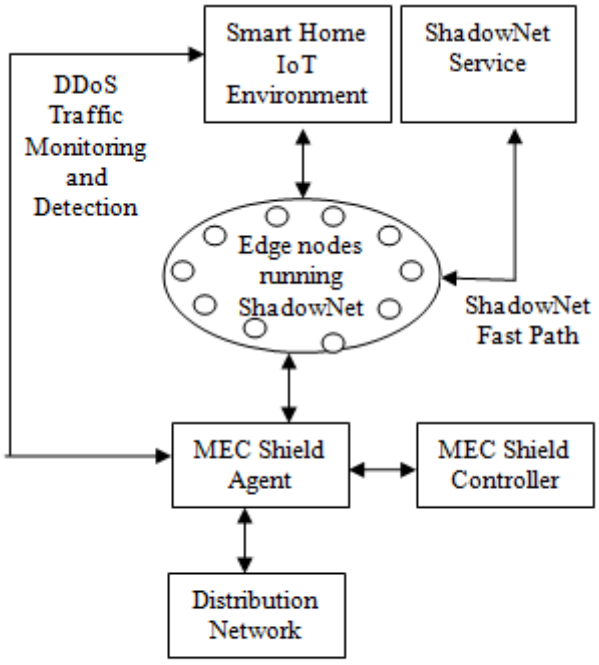

Fig. 1: FRAMEWORK OF SMART HOME DDOS TRAFFIC DETECTION USING MEC

B. ShadowNet

ShadowNet – an architecture that makes the edge the first line of defense against IoT-DDoS. It achieves its goals in the following manner. First, appropriate edge functions are deployed on the distributed edge infrastructure, on behalf of a backend IoT application seeking protection. The role of these edge functions are to sketch the profiles of IoT traffic streaming from a given edge location. Second, the edge function establishes a fast path between itself and a special ShadowNet web service. The edge function uses the fast path to send small shadow-packets with locally-derived information about IoT traffic to the ShadowNet web service. ShadowNet can then aggregate that information about the IoT traffic distributed across a number of edge nodes, detect an imminent IoT-DDoS attack, and respond with some proactive defensive action. The approach assumes that an edge function and web service can mutually attest each other to establish trust between them.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

C. MECshield Framework

Figure 2 illustrates the proposed MECshield framework. Logically, the MECshield framework consists of a central controller and multiple agents located at the edge of each local network. The communication between the central controller and the distributed agents is facilitated via secure channels/protocols supported by the H-IoT networks (e.g., Openflow protocol on secure management channels in SDNFV technology).

1. MECshield controller: The main purpose of the central controller is to orchestrate operations among the distributed agents. A local network might act as the source or destinationof DDoS attacks. Therefore, each local network requires a different smart Self organizing map filtering strategy, based on its position in the attack scenario. Alternatively, the source site(s) of the attack should be more concerned with features of its outgoing traffic for individual sources, such as the protocol, port number, flow number, packet number per flow, and transmission contiguity. Thus, only the attack-source sites participate in DDoS defense. Therefore, cooperation among the distributed local agents is crucial for an effective defense. The components of the MECshield controller are described as follows:

Report collector: This component gathers traffic reports from distributed agents including traffic protocols, port ranges, volume or traffic flow quantity, source IP address ranges, and destination IP address(es).

Attack analyzer: First, DDoS attack detection techniques are utilized to identify the attack symptom based on the processed information from the report collector. Once the attack is identified, further information is then considered to recognize attack targets, attack methods

Policy generator: Once the DDoS attack is identified, primary policies are generated and forwarded to the MECshield agents located at the edges of the source and destination sites of the attack.

2. MECshield agent

The primary purpose of MECshield agents is to mitigate the DDoS traffic and the components of MECshield agent are as follows:

Traffic monitor: The main function supported by this component is to make the traffic statistics report. This information is delivered to the report collector in the central controller. In addition, incoming 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 controller, 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 classification procedure. Moreover, the local policy conductor will send mitigation information to the smart SOM filter agent to apply appropriate policies for attack traffic.

Feature extractor: This component extracts the features of traffic delivered from the traffic monitor and make tuples for the SOM inputs based on requirements of the local policy conductor. Then, it forwards these tuples to the smart filter agent for classifying and training.

Smart SOM filter: 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, a protection mode is activated and the outgoing traffic is switched through the filter. The protection mode is deactivated if the SOM does not receive a training vector of a DDoS attack within a pre-defined duration. Finally, mitigating the DDoS attack by dropping the traffic is classified by the SOM as malicious.

Switching/Routing: This is a basic function of edges used to handle incoming/outgoing traffic.

IV. RESULT

The MECshield performed better than the other schemes. This is because SOM maps in the MECshield agents are separately trained by different local IoT traffic. Hence, these filters find it easier to recognize patterns or they are well-adapted to local IoT traffic in other word. Figure (2) presents the detection rate and accuracy of the three approaches.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

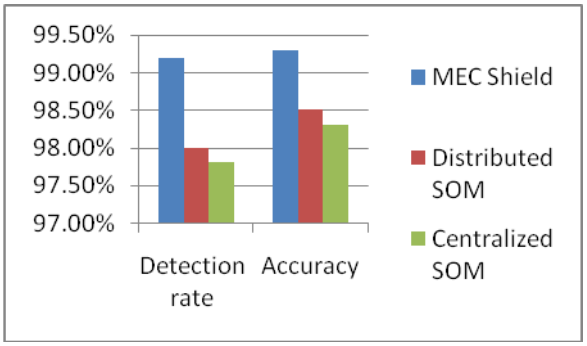

Fig. 2: DETECTION RATE AND ACCURACY IN CLASSIFYING DDOS TRAFFIC WITH THE SOM MAP

Conversely, with a fixed and limited number of neurons in a smart SOM agent, if there are many traffic types trained for a SOM map (Centralized-SOM case), or several merging times in the case of a Distributed-SOM mechanism, the weights of each neuron in the SOM map will change considerably. This leads to the degradation of both the detection rate and the accuracy of these schemes.

Table 1: COMPARISION OF TWO IOT ENVIRONMENTS BASED ON DDOS TRAFFIC DETECTION

IoT environment	Used methods	Accuracy	Detection rate
General IoT	CNN and RNN	>98%	93%
Smart home IoT	MEC and ShadowNet	≈100%	98%

Table (1) shows comparison of DDoS traffic detection in the General IoT and proposed smart home IoT environments. General IoT environment developed a DDoS traffic detection model generated using Convolutional Neural Network (CNN), Recurrent Neural Network (RNN). The experiment has been proven to detect 100% DDoS traffic instances in the proposed smart home IoT using mobile edge computing infrastructure with ShadowNet framework.

V. CONCLUSION

A smart home IoT characteristics based on DDoS traffic detection using edge computing is presented in this paper. Motivation of this research is reflected in increasing number of SHIoT devices, resulting in the creation of IoT botnet networks. IoT botnet network of ShadowNet approach is used to prevent application level IoT-DDoS attacks by leveraging the emerging mobile edge computing infrastructure. In this study, MECshield and a DDoS prevention framework are proposed that leverages MEC power to deploy multiple smart filters at the edge of attack-source/destination networks. MECshield enables the network to defend against malicious traffic from smart home IoT devices through smart SOM filters deployed in front of the attack source. Experimental results show that the detection rate 10 times faster than existing approaches and prevents 82% traffic to enter the Internet infrastructure. Finally, MECshield introduces an efficient and feasible security framework for a smart home IoT environment.

REFERENCES

[1] D'Cruze, H., Wang, P., Sbeit, R.O., & Ray, A. (2018). A software-defined networking (SDN) approach to mitigating DDoS attacks. In S. Latifi (Eds.) Information Technology- New Generations, Advances in Intelligent Systems and Computing, vol 558 (pp.141 145), Springer, Cham.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

[2] B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," Sensors, vol. 18, no. 3, p. 817 (2018)
[3] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. K. R. Choo, and M. Dlodlo, "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," IEEE Access, vol. 5. pp. 8284–8300, 2017.
[4] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the Internet of things," IEEE Communications Magazine, vol. 54, no. 12, pp. 22–29,
2016.
[5] V. Prokhorenko, K. K. R. Choo, and H.
Ashman, "Intent-Based Extensible Real-Time PHP Supervision Framework," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 10, pp. 2215–2226, 2016.
[6] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in IEEE Symposium on Security and Privacy 2016, pp. 636–654 (2016)
[7] Girma, A., & Garuba, M., & Goel, R. (2014). Cloud computing vulnerability: DDoS as its main security threat, and analysis of IDS as solution model. Proceedings of the 11th International Conference on Information
Technology: New Generations (ITNG 2014), 307-312.
[8] S. Furnell, "Enemies within: The problem of insider attacks," Computer Fraud and Security, vol. 2004, no. 7. pp. 6–11, 2004.
[9] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," in IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 2003, pp. 60–67.
[10] E. E. Schultz, "A framework for understanding and predicting insider attacks," Comput. Secur., vol. 21, no. 6, pp. 526–531, 2002.