Analyzing Threats of IoT Networks Using SDN Based Intrusion Detection System (SDIoT-IDS)

Azka Wani(✉) and S. Revathi

Crescent B. S. Abdur Rahman University, Vandalur, Chennai 600048, India
graceazka@gmail.com

Abstract. Internet of things (IoT) is developing and has become popular among individuals as well as industry. The IoT has revolutionized the technological aspect by making ordinary mundane devices smart and automatic. However, it is susceptible to various security threats. This paper highlights major security threats of IoT and uses a Software Defined Networking (SDN) based Intrusion Detection System (IDS) as a countermeasure towards such threats. Software Define Network (SDN) decouples the data and control planes resulting in programmable network architecture with centralized control. SDN based Intrusion Detection System (IDS) for IoT can rectify abnormal activity in an IoT network by examining network traffic in real time. The programmability feature of SDN makes IDS flexible and does not burden the forwarding devices. The SDN based IDS mechanism is run on a simulated IoT network. The experimental results exhibit 99% accuracy and can efficiently detect various attacks in an IoT environment.

Keywords: Internet of things · Software Defined Networks
Intrusion Detection System

1 Introduction

The Internet of Things (IoT) is a heterogeneous network consisting of sensor nodes, smart phones, switches/routers, servers, and software. IoT has been designed in a way that activities or movements are sensed and processed in real-time. IoT constitutes a means of communication between internet and physical world of ordinary things. The concept of IoT has led to improvement in production, processing and consumption of data.

The number of devices connected through internet has already exceeded the world population and is estimated to increase by large in a decade [1]. Since devices with very limited resources are participating in IoT, hence threats and vulnerabilities have amplified significantly. The proper analysis of the recorded data, over a period of time, in IoT environment can help to predict threats and detect them at an early stage. IDS are able to rectify malicious behavior in a network by analyzing the IoT traffic in real-time. On detecting an attack IDS takes the measures to protect the system from damage. SDN is a naïve way of networking that decouples the control plane and packet forwarding plane. SDN allows centralized control and a global view of the network.

P. Bhattacharyya et al. (Eds.): NGCT 2017, CCIS 828, pp. 536–542, 2018.
https://doi.org/10.1007/978-981-10-8660-1_41

A lot of research has been done regarding intrusion detection systems in traditional networks, and limited research focuses on detection of malicious behavior in IoT. The concept of intrusion detection system based on software define network technology is new particularly in the area of IoT. This paper discusses major security threats of the IoT and presents a brief survey of various research efforts put towards the development of intrusion detection system in IoT. Section 1 provides a brief introduction, Sect. 2 introduces the various threats in IoT network, Sect. 3 gives an overview of the SDN technology, Sect. 4 the discusses various types of IDS so far introduced in the area of IoT. The proposed SDN-based solution for IoT is discussed in Sect. 5. Finally, conclusions and future work are presented in Sect. 6.

2 Major Threats to the IoT

With limited resources it is difficult to provide a complete security mechanism in IoT devices and hence the attacks on Internet are on a rise; IoT attacks can be classified into following four types [2]:

(1) Distributed Denial of Service (DDoS) – This makes resources unavailable to user by keeping network busy with meaningless traffic. The volume of DDoS attacks has increased with more and more IoT devices participating in Internet.
(2) Botnets – Network of systems which are run by botnet operators. Such networks are joined for distributing malware and controlling network devices. Increasing number of networking objects and devices has led to formation of thingbots (botnet containing independent connected things).
(3) Virus or Malware – Some malicious code is executed to infect the devices on the IoT network. Such code can be used to steal sensitive information, or gain unauthorized access to the devices. The attacker can also control the devices after executing malware and can uses those devices to launch attacks.
(4) Data Theft – Confidential and crucial information is retrieved from the network because of poorly protected IoT devices. Spoofing or Phishing can be used to retrieve such information.

3 Overview of Software Defined Network (SDN)

In traditional networks the control mechanism and data forwarding capability is present in network devices i.e. switches or routers. The concept of Software Defined Network (SDN) makes networks programmable; it decouples the data and control planes. The switches or routers are just forwarding devices while as the control mechanism is shifted to a centralized controller. Software Define Network (SDN) manages the network with abstraction of lower level functionality and maintains an Application Programmable Interface (API) for delegating control to the lower level devices.

SDN controllers have a global view of the network and hence configuration of network has become an easy task. Moreover if there are any changes to be incorporated in a network, the programmability feature of SDN makes that quite simple. The

security mechanism or other additional features can also be programmed via API and implemented in the network through flow rules. The flow rules are governed by OpenFlow protocol. The programmability feature makes networks more flexible, if any changes are to be made in the network; those are to be included in the control plane instead of reconfiguring each network device [3] separately. A simple logical representation of SDN architecture is shown in figure (Fig. 1).

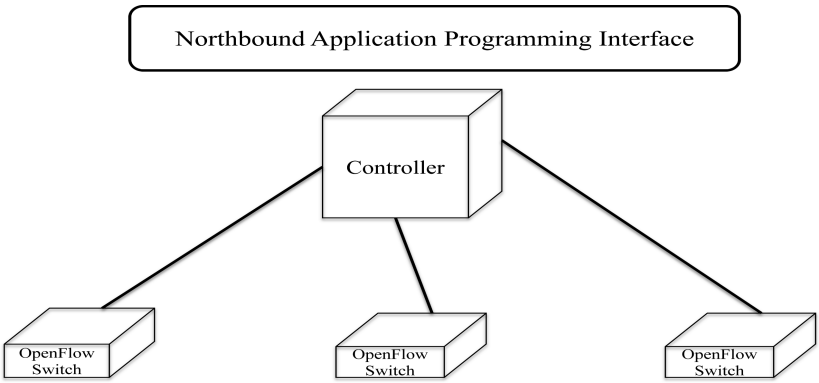

Fig. 1. Separation of data and control planes in SDN

Network control or logic is shifted to centralized SDN controllers for better management of the networks and infrastructure contains mere forwarding devices. The medium between the network infrastructure and the controller is known as southbound interface while as the API and controller communicate through northbound interface.

4 Related Work

In order to improve the security in IoT a lot of research work has been conducted. This section discusses various intrusion detection systems which have been proposed for improvement of security in IoT [4].

Thanigaivelan et al. [5] proposed IDS for internal anomaly detection in IoT. The system records the normal behavior of the network by analyzing the traffic. It looks for abnormalities by monitoring the packet length and frequency of packets for the nodes which are at a distance of one hop.

Pongle and Chavan [6] proposed IDS for wormhole attacks in IoT devices. It is simulated on Contiki OS using Cooja simulator. Using the symptoms of wormhole attack, for example, increase in control packets, anomalies are detected in IoT. The authors have used three algorithms for detection and achieved a better true positive rate for attack detection. Power and memory consumption for the proposed system are lesser and hence suitable for constrained environment of IoT.

Raza et al. [7] presented an intrusion detection system in IoT called as SVELTE which is implemented on Contiki OS and is a real-time mechanism to identify threats in

IoT. The system comprises of three major components kept at 6LoWPAN Border Router. The first component is called Mapper and it gathers information about the RPL protocol. The second component detects the intrusion by monitoring the information gathered by Mapper. The third element is filters the abnormal traffic.

Sforzin et al. [8] proposed an IDS architecture called RPIDS which is a portable device, with an inbuilt IDS. The setup of the proposed system contains a Raspberry Pi equipped with Snort which is a complete IDS mechanism. The devices perform intrusion detection locally or request traffic data from nearby devices in order to carry out intrusion detection more effectively.

Kasinathan et al. [9] presented an IDS for detection of DoS attacks. The proposed mechanism is designed to analyze 6LoWPAN traffic and the architecture is built on ebbits network framework. The major module of the system handles the DoS protection manager which raises alarm upon sensing some abnormality in network.

5 SDN Based Intrusion Detection System for IoT (SDIoT-IDS)

The paper proposes a system SDIoT-IDS to detect security attacks against IoT devices and starts a mitigation mechanism to defend such attacks. In this proposed system, SDN technology is used to provide security services and protect smart things in an IoT from top level. The traditional security features cannot be included in smart things individually since these are constrained. The proposed system is incorporated in SDN controller for better delegation of security policies and more control over the activities of network. The traffic is routed into an IoT network via SDN gateway. The gateway redirects new messages to the controller which generates flow rules based on the type of traffic it encounters. The working of SDIoT-IDS is depicted in following figure (Fig. 2).

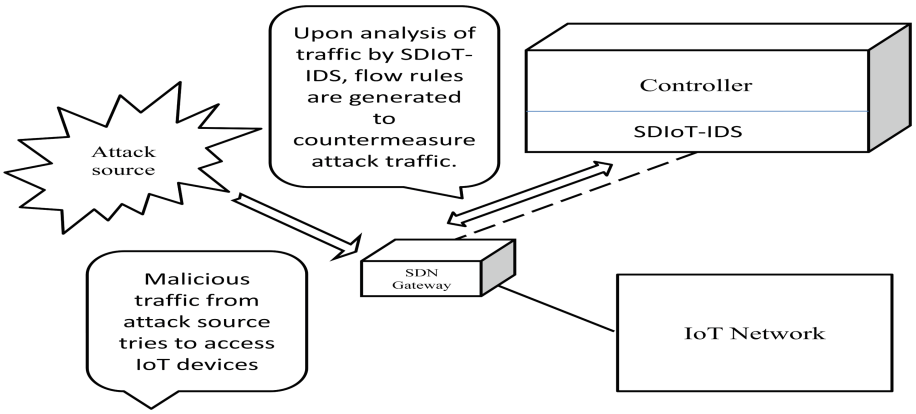

Fig. 2. Working of SDIoT-IDS

SDIoT-IDS consists of following major components:

Activity Monitor: This component monitors the traffic through IoT domain. It is primarily used to collect data for extracting flow statistics which helps in detecting the suspicious behavior. Activity monitor is placed at the IoT gateway which is an Openflow switch. It keeps record of sent and received packets through the IoT network.

Activity Analyzer: The Activity Analyzer is one of the major components of SDIoT-IDS. Here a machine learning algorithm is used to detect the specific type of network attack. Back propagation neural network (BPNN) has been used for detection purpose in this component of the system. First the BPNN is trained to detect different kinds of attacks. The back-propagation neural network used in this work has three layers of nodes (input, hidden, and output). All nodes from the input and hidden layers are connected to each of the nodes in the output layer. Each node from hidden layer is directed to one output. Then output O from the node in consideration can be calculated as below (f is an activation function such as sigmoid) [10] (Fig. 3):

$$O = f(a1 * w1 + a2 * w2 + a3 * w3)$$

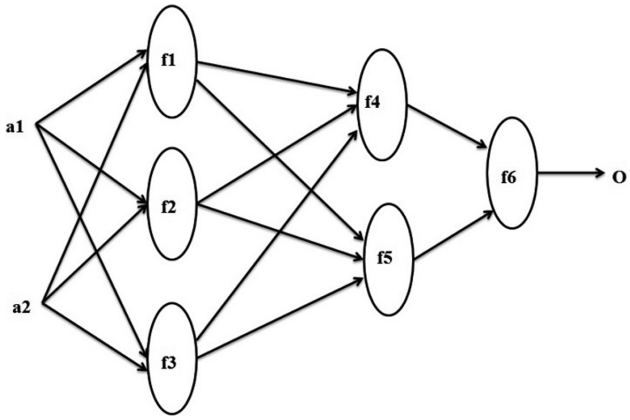

Fig. 3. Feed-forward mechanism in BPNN

Where a1, a2, a3 are inputs at various levels, w1, w2, w3 are the weights and f () is the activation function. The training is performed using NSL-KDD dataset [11]. The signature analysis is also carried out to understand the possible nature of known IoT attacks, before supplying the data to classifier. The accuracy of detection by algorithm is evaluated and improved [12].

Classifier and Alert Mechanism: This component classifies the data or information from the activity monitor as malicious or benign. It also identifies the specific attack that is might hit the network. Once the classification of information is done and it detects any attack, the alert is raised and control is shifted towards mitigation strategy.

The proposed mechanism is implemented using Mininet2.0. The controller used for the set up is the RYU controller, customized to incorporate SDIoT-IDS. The experimentation setup has used attacks like TCP flood and ICMP based attacks. The attacks simulations show ability of system against various attacks.

A flood attack from the attacker to the IoT Device was launched with 2.5 Mps rate and benign traffic was sent at a rate of 1 Mbps (the capacity of the link). As seen from the figure (Fig. 4) the attack which started at 7 s was successfully controlled by SDIoT-IDS by blocking the flood traffic at 11 s. The benign traffic which had been halted during the traffic is resumed after mitigation of attack.

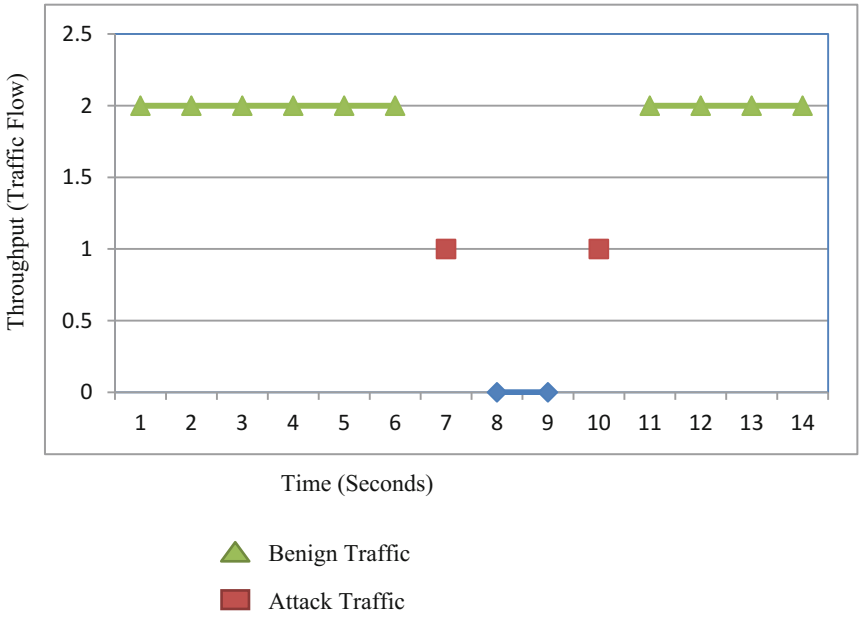

Fig. 4. Flood attack mitigation by SDIoT-IDS

6 Conclusion and Future Work

This paper introduces a new intrusion detection solution for IoT which is based on SDN. SDIoT-IDS can rectify attacks of several types unlike other security mechanism which focus on a single attack. The analysis portion of the system is developed in a way that it can identify several attacks threatening IoT networks currently. As future work, the proposed solution can be enhanced to countermeasure more IoT based attacks, and improve upon the detection capacity. The proposed solution can then be experimented on a real IoT scenario.

References

1. Kolias, C., Stavrou, A., Voas, J., Bojanova, I., Kuhn, R.: Learning internet-of-things Security "hands-on". IEEE Secur. Priv. 2–11 (2016). https://doi.org/10.1109/msp.2016.4
2. Wani, A., Revathi, S.: Protocols for secure internet of things. Int. J. Educ. Manag. Eng. (IJEME) **7**(2), 20–29 (2017). https://doi.org/10.5815/ijeme.2017.02.03
3. Wani, A., Revathi, S., Geetha, A.: A survey of applications and security issues in software defined networking. Int. J. Comput. Netw. Inf. Secur. (IJCNIS) **3**, 21–28 (2017). https://doi.org/10.5815/ijcnis.2017.03.03
4. Zarpelão, B.B., Mianib, R.S., Kawakania, C.T., de Alvarenga, S.C.: A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. **17**, 1–46 (2017)
5. Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J.: Distributed internal anomaly detection system for internet-of-things. In: 13th IEEE Annual Consumer Communications Networking Conference (CCNC), pp. 319–320 (2016)
6. Pongle, P., Chavan, G.: Real time intrusion and wormhole attack detection in Internet of Things. Int. J. Comput. Appl. **121**(9), 1–9 (2015)
7. Raza, S., Wallgren, L., Voigt, T.: SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw. **11**, 2661–2674 (2013)
8. Sforzin, A., Conti, M., Marmol, F.G., Bohli, J.-M.: RPiDS: raspberry Pi IDS a fruitful intrusion detection system for IoT. In: International IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, pp. 440–448 (2016)
9. Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., Spirito, M.A.: DEMO: an IDS framework for internet of things empowered by 6LoWPAN, pp. 1337–1339 (2013)
10. http://home.agh.edu.pl/∼vlsi/AI/backp_t_en/backprop.html
11. http://www.unb.ca/cic/research/datasets/nsl.html
12. Van, N.T.T., Thinh, T.N.: Accelerating anomaly-based IDS using neural network on GPU. In: International Conference on Advanced Computing and Applications (ACOMP), pp. 67–74 (2015)