International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Improving Security for Internet of Things Devices using Software Defined Networking

D. Prasad

Abstract*: *This theory has recently been expanded to IEEE 802.15.4 wireless networks, which constitute a key element of the Internet of Things (IoT). Nonetheless, the various patterns of traffic needed for SDN management make it difficult to adapt this method to these extremely demanding situations. Software-Defined Networking (SDN) key contribution of this work is the solution to network with IoT devices that enables network because of better functionalities in case of providing interfacesfor the layers. SDN enables significant advantages of applications to be created on the basis of interaction with traffic networks, trustable authentication, or service eminence. This report suggests the use of a SDN gateway as a decentralized platform to track traffic from IoT gadgets. The configured SDN gateway capable of detection the possible abnormal behaviors and provide it particularly valuable applicability for (obstructive, transmission or application of providing best services to the system).

Index Terms*: *IoT, SDN, Security,* Cyber *Physical Systems

I. INTRODUCTION

In recent years the fast growth in the field of internet its usage with relevance to Internet of Things (IoT) contributes to a rise in the number of innovative applications and services that could be powered by today's Internet. What is even worse is the heterogeneous systems serving such applications and the different applications specifications from various points of view, such as quality of service, security and privacy, as well as software and shop tools. Edge computing has been suggested as a supplementary approach to cloud computing to meet these persistent needs. Even so may researchers are carried work on the recent challenges and issues faced by the industries in the field of edge computing[1]-[3], previous supported work in various domains primarily on engineering, the availability as well controlling mechanismsof resources, software applications, etc. In addition, the latest current networking technology for software-defined networking (SDN) and related technologies does not provide the networking viewpoint.The recent progress achieved by IoT, capable of integrates enormous heterogeneous gadgets such as the product type, configuration, vendor and interaction protocol, requires new network structures which tackle a range of new problems, including the difficulty of handling heterogeneous devices, protocols and network resources and the proliferation of generators. We talk about the promising technologies from the networkpoint of view, SDN and NFV, to provide the scalability, versatility and safety essential to IoT services. On the other side, the convergence of SDN and IoT has been apparent. Below, we discuss the recent research attempts to exploit SDN to resolve the various challenges.

Management, allocation of assets and assurance of security/ privacy.In specific, we examine how SDN can be used to gain effective and efficient monitoring of equipment and network. Software Defined Networking (SDN) should be the main enabler for make it possible of 5G (5th generation of wireless networks) networks in the next decade that will have to combine the two IoT technologies along with existing functionalities for the gateway of the network. These are some of the greatest challenges for IoT administrators is to be able to collect and analyze data to generate positive user experience. SDN can automatically redirect traffic if necessary, significantly improving IoT applications. Virtual network arrangement, processing and computational services are supported for data analysis and immediately distributed.

It is more important to connect only the trustable devices to the network with proper installation for safeguarding the devices otherwise it leads to network security concerns may emerge. By this way the devices connected to the network provides wide range of security-enhancing resolutions. This article presents reliable controlling framework for resisting the incoming attacks from the network with the assistance of the SDN gateway for IoT devices. This adaptive process conducts a simple analysis test pattern for checking the data flow in the layers of the network to get the information of whether they are attacked or not maliciously or are the object of external use.

The main contributions and organization of this paper are summarized as follows: In section 2 we describe background details of SDN intrusion prevention systems. Section 3 discusses the proposed work. Section 4 deliberates results and discussions. Finally, in section 5, we concluded the paper.

II. BACKGROUND WORKS

In [4] used IPS in the controller but only the POX module. The work discussed in [5] merge intruder detection with that of network switches, makes evaluations and conversation results regarding granular latency and transmission delay were not presented. In [6] the researchers implemented SDN intrusion prevention systems based on the Internet. Referring to the recent trends occurring in the specifications and configuration of OpenFlow versions they used flow table features.

Revised Manuscript Received on December 30, 2019.

* Correspondence Author
D Prasad*, Professor, Department of ECE, Sasi institute of Technology & Engineering, Andhra Pradesh,India.

The research describes the basic things of structurenamed "CloudWatcher"[7], which is a protocol document that redirects network packages to existing risk detection systems. In [8], researchers explored the compatibility of OpenStack and Open Daylight controllers to SDN solution, which is more robust for certain type of SDN controllers. The framework in [9] identified improvements that were taken place in the OpenStack

As stated in[10], the researchers performed an extensive study on DDoS prevention using SDN capability and addressed some of the main weaknesses and drawbacks of the SDN channel command. In [11] authors showed a cloud firewall based on SDN. Threat detection and security protocols are introduced in control plane software and an API is provided for the administration to implement the firewall's data security policy. Nonetheless, they only offer a general model without test outcomes and interpretation of performance. The MAC / IP IDS filter system has but limitations on handling dynamic traffic with malicious payload. The goal of the (SDN), with brief explanation in [11], is to cope with the process of combining both the control as well data planes for suitable, so that machines dependent on code can be controlled, as shown in the Fig.1.

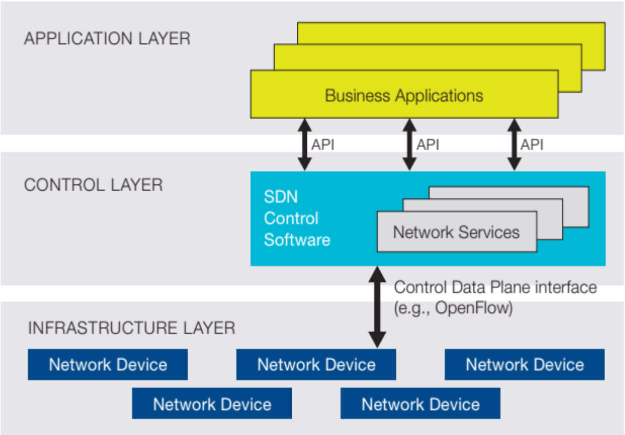

Fig. 1. Overview of Software Network layers [12]

To show the functionality of architecture at higher levels of SDN as [12], entails three main contributions to be considered, they are as follows:

1) Integration of control as well data planes
2) Logically hierarchical control
3) Access for external implementations to theoretical networking tools.

The condition of the network such concepts function together to promote the management and set-up via particular relevance elements that are most required for network formation, a logically centralized controller allows the overall network performance to be monitored and the set-up adjusted.

III. SYSTEM MODEL

Fig. 2 shows the machine structure suggested. Moving functionalities that were done at the computing edge of the devicescould visible as related to the initial concept of centrally controlled SDN devices, but it is essential here to meet the recitalneeds that are more desirable to make the security argumentmore rapidlytowards the corresponding IoT nodes. It is more relevant especially relevant for a network of SDNs that transfer OpenFlow messages to the controller so that attacks based on DoS can spread their effects across the network.

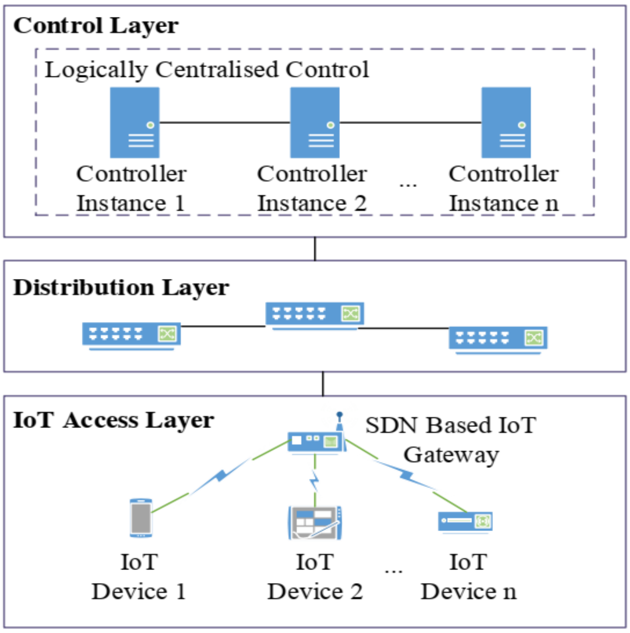

Fig. 2. Integration of IoT with Distribution layer for IoT SDN

SDN controller to detect and mitigate the attacks required. This has been built with the OpenFlow and Pox controller versions 1.3. There are three main components in the integrated controller: the primary switcher (forwarding, etc.), the numerical administrator and a number of preventive behavior.The statistics manager is required to collect data based on the present and previous data held at the network for all the layers. It was restricted to the output of the data rate transmission period. Nonetheless, thedevelopments may use testing of simple pattern analysis for data flow consistence in the network. The proposed mechanism executes an appropriate mitigation action after detection of an anomalous flow (as shown in Fig.3). Block, forward, or apply QoS are the three possible actions.

Blocking a flow: It lists the device effectively from getting the data from the source node to the destination node in the network of IoT gadgets. Uncertainty that was an existing origin computer, it should be wise to block access to the source system besides change the main section of the system and try torestrict the flow of date (internal or external) to the source. If the network itself is breached, traffic can be diverted from the computer conveyedto the main core section (to search for physical vulnerabilities or to upgrade software required, etc.).

Forwarding of a data flow: The isolated section of the system is could be inspected more thoroughly before a decision could be made on how a device should be treated.

Where decisions cannot be clarified or a single source not blocked, the use of Service Quality to limit the effects of any attack (i.e. by restricting the channel data rate for finding the flow from / to a device) can help to limit the effect of an attack.

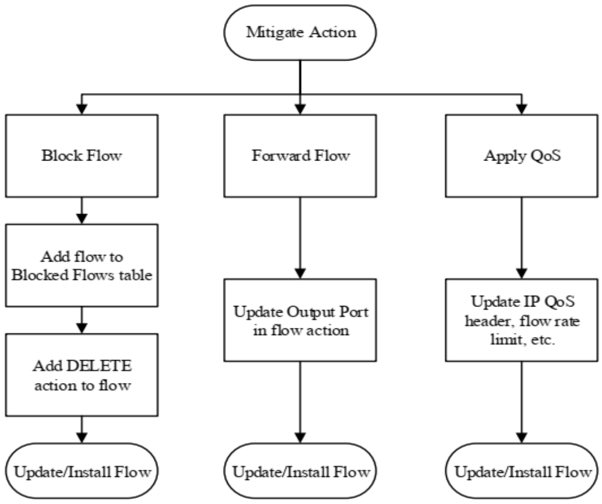
Mitigate Action
Block Flow
Forward Flow
Apply QoS
Add flow to Blocked Flows table
Update Output Port in flow action
Update IP QoS header, flow rate limit, etc.
Add DELETE action to flow
Update/Install Flow
Update/Install Flow
Update/Install Flow

Fig. 3. Mitigate Action

At this point, the choice between mitigation measures is to consider the time required for implementation and suitable decision making. Nonetheless, there is construction of process that is maintaining more quickly, provided that new threats were identified and analyzed based on reactions to similar attacks.

IV. RESULTS AND DISCUSSION

Experiments focused on the use of tools that are configured for simulation of environment in [13] for TCP floods and ICMP attacks to validate corresponding network layers derived toolsfor security operation and its ability to countermeasures to minimize this kind of attacks. The effect on true traffic from the device was demonstrated by a 1.5Mb/s TCP stream from the IoT model towards the end node. The network designed for simulating resource restricted connections with a peak bandwidth of 1.5Mbps.

Table 1.Parameters for TCP floodAttack

Time (sec)	GTCP Throughput (Mbps)	ATCP Throughput (Mbps)
0	0.4	0
5	1.5	2
10	0.8	2
15	1.6	0
20	1.6	0.1
25	1.6	0

TCP flood attack: The attacker primarily sends TCP link requests quicker than the goal computer can handle them through SYN flood DDoS, triggering network overload. The attacker sends repeated SYN packets in a SYN flood attack to each port on the targeted server, often using the fake IP address. Unconscious of the attack, the server receives multiple, apparently legitimate communication requests. It answers every attempt from every open port with a SYN-ACK packet. Either the malicious client does not send the anticipated ACK or if the IP address is broken, the SYN-ACK will never be received first. In any event, the database under attack must wait for some time for acknowledgment of its SYN-ACK packet, as shown in Fig.4.

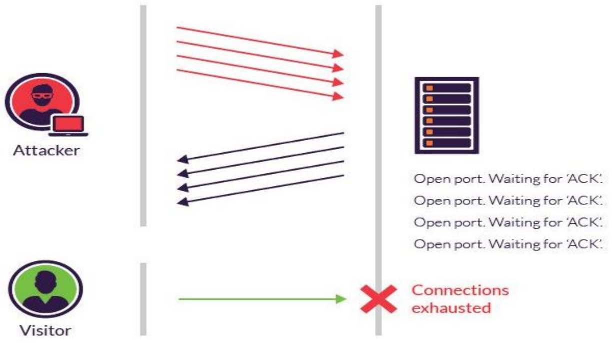
Attacker
Visitor
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Connections exhausted

Fig. 4. TCP SYN flood attack progression

The server cannot close the connection by sending an RST packet during this time, and the connection is open. Another SYN packet will arrive before the connection can time out. This leaves an increasing number of semi-open links–and SYN flood attacks are also called semi-open attacks.

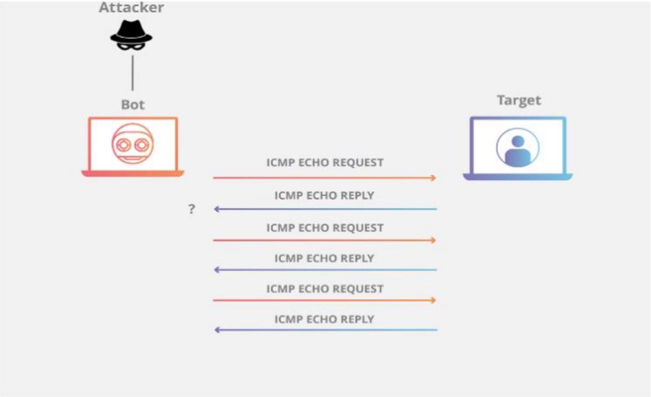

Fig. 5. ICMP attack progression

In order to process and send a response, an ICMP request needs some server resources. The query needs bandwidth for both incoming (echo-request) and outgoing (echo-reply) communications. The Ping Flood attack aims to overcome the ability of the targeted device to answer the many requests and / or to overload the network connection with falsified traffic, as shown in the Fig. 5. The attack traffic is substantially increased by many devices in a botnet targeting the same Internet property or infrastructure component as ICMP requests, potentially resulting in an interruption of normal network activity.

Table 2.Parameters for ICMPAttack

Time(sec)	GTCP Throughput (Mbps)	ATCP Throughput (Mbps)
0	1.4	0
5	1.5	3.2
10	0.9	3.1
15	1.5	0
20	1.6	0
25	1.6	0

Fig. 6 illustrates the attacker's TCP Flood attack on the gadgets that are supposed to in IoT. The actual traffic was transmitted via TCP at approx.

1.5 Mbps (link capacity). The results of this attack in this scenario. At 5 seconds, the attack was launched and the attack was mitigated by blocking the flow at around 10 seconds. The real traffic flow is restored and its optimum transition begins.

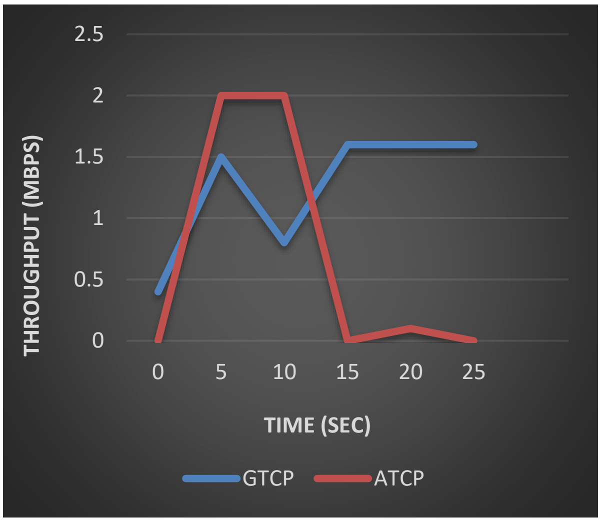

Fig. 6. Performance of the TCP floodAttack

Fig. 7 follows a similar pattern, which transmits an authentication of data for corresponding TCP at about 1,5Mbps as related to ICMP-based attack is launched on the IoT device at 5 seconds (Fig. 6). That can be seen to adversely affect the genuine traffic stream until the attack is blocked successfully at approximately 9 seconds and the TCP stream begins to recover.

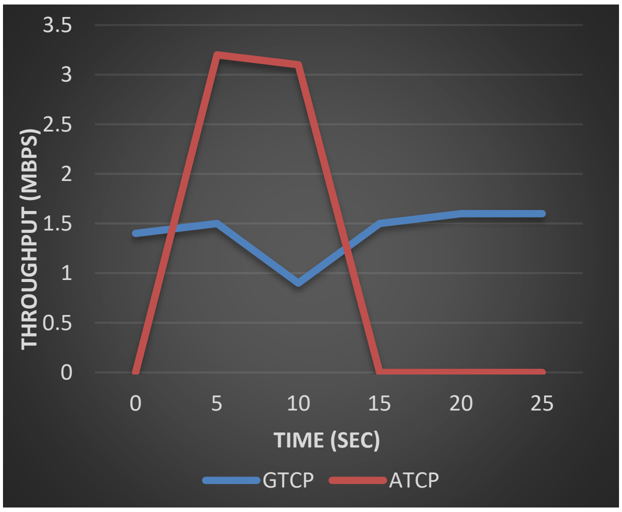

Fig. 7. Performance of the ICMP Attack

V. CONCLUSION

We have shown that a security system allowed by SDN is feasible and have introduced a security infrastructure for IoT devices, focused on SDN concepts. The Pox controller possess more robust towards security in case of IoT devices in the networking applications. It is used to resist a fixed amount of attacks is the network, the approach has been validated successfully and a platform has been created for further expansion. Further IoT security research needs to be carried out, but the powerful SDN framework has shown itself to be a useful weapon against security threads.

REFERENCES

1. W. Shi and S. Dustdar, "The promise of edgecomputing," *Computer*, vol. 49, no. 5, pp. 78–81,2016.
2. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edgecomputing: Vision and challenges," *IEEE InternetThings J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
3. Q. Zhang, Z. Yu, W. Shi, and H. Zhong, "Demoabstract: EVAPs: Edge video analysis for publicsafety," in *Proc. IEEE/ACM Symp. Edge Comput.(SEC)*, Oct. 2016, pp. 121–122.
4. Xing, T., Xiong, Z., Huang, D., Medhi, D.: "SDNIPS: Enabling Software-Defined Networking based intrusion prevention system in clouds", 10th International Conference on Networks and Service Management (CNSM) and Workshop. 1–4 (2014).
5. R. C. Diovu and J. T. Agee, "A cloud-based openflow firewall for mitigation against DDOS attacks in smart grid AMI networks," in Power Africa, 2017 IEEE PES, 2017.
6. P. Rengaraju, S. S. Kumar, and C. H. Lung, "Investigation of security and QOS on SDN firewall using mac filtering," in International Conference on Computer Communication and Informatics, 2017, pp. 1–5.
7. Kumar S et al. "Open flow switch with intrusion detection system", International Journal of Scientific Research Engineering & Technology, 2012, 1(7):1-4.
8. Chi, Y., Jiang, T., Li, X., Gao, C.: "Design and implementation of cloud platform intrusion prevention system based on SDN" 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA) (1–6 (2017).
9. Shin, S., Gu, G.: "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)." 2012 20th IEEE International Conference on Network Protocols (ICNP). 1–6 (2012).
10. Tkachova, O., Salim, M.J., Yahya, A.R.: "An analysis of SDN-OpenStack integration", Second International Scientific-Practical Conference Problems of Info communications Science and Technology (PIC S&T). 1–3 (2015).
11. F. Foresta, et al.:"Improving OpenStack Networking: Advantages and Performance of Native SDN Integration", 2018 IEEE International Conference on Communications (ICC).
12. Open Networking Foundation, "SDN Architecture Overview version1.1," Tech. Rep., 2014.
13. Praetox, "Low Orbit Ion Cannon," 2014. [Online]. Available:https://sourceforge.net/projects/loic/.

AUTHOR'S PROFILE

D. Prasad, currently working as Professor in ECE Dept. Sasi Institute of Technology and Engineering, Andhra Pradesh, India. He is having total teaching experience of 15 years.