A Survey of Distributed Denial Service Attacks Detection & Prevention in SDN-Internet of Things

Shubham Kumar Madhup[1] Manish Gurjar[2] Anshul Awasthi[3]
[1,2,3]Technocrats Institute of Technology-Advance, Bhopal, (M.P.), India

Abstract— The fundamental idea of IoT is the pervasive existence of an array of objects or things such as actuators, Radio-frequency Identification (RFID) tags, mobile phones, sensors, and so forth. The Smart Security Mechanism uses the standard northbound and southbound interfaces of SDN, and it contents a low-cost technique that monitors the DDoS based attack by reusing the asynchronous communication on the control link. Software-defined networking (SDN) provides a latest method to achieve secure, reliable and cheap idea of IoT. In IoT traditional IP networking unsuitable when dealing with various IoT scenarios. It should be noted that, the flexible and effective SDN based IoT also inherits the security issue of the SDN architecture. The prevention and detection of DoS attack in an IoT is challenging task for the researchers. DoS attacks usually flood IoT networks and increases massive traffic in order to overthrow the target resources and make impossible or difficult for valid IoT users to use services. This paper provides the survey of SDN based DDoS attack detection and prevention techniques in IoT.

Key words: Software Defined Networking, Internet of Things, Security, DDoS Attacks, Smart Security Mechanism

I. INTRODUCTION

In IoT[1] traditional IP networking unsuitable when dealing with various IoT scenarios. In order to connect IoT scenarios effectively, different communication protocols are proposed in physical and network layers however, due to the vendor-driven property of traditional IP networking[2], these proposals are not widely deployed. It should be noted that, the flexible and effective SDN[3] based IoT also inherits the security issue of the SDN architecture. In the SDN routing system, the switches request the controller to assign routing rules actively and cache routing rules passively through the control link. However, the control link bandwidth and the cache space that are regulated by the southbound interface have been proved to be limited. That provokes cyber attackers to find better solutions to attack the public network, such as the infrastructure layer DDoS attack [4], controller-switch communication flooding and switch flow table flooding attacks. These cyber-attacks can cut off the bridge between IoT devices and IoT servers in SDN-based IoT.

In cyber-attacks belong to the new-flow attack, because the attackers must send lots of unmatched packets to the SDN-enable switch. These unmatched packets are treated as new flows by the SDN routing system and lead to a series of subsequent processes in both the data plane and the control plane. The limited resources in both the data plane and the control plane make SDN vulnerable to the new-flow attack, which can cut off the communication between IoT devices and IoT servers in SDN-based IoT. The attackers aim to exhaust either the SDN-enabled switch or the controller with intensive new flows. According to the valuable suggestions [5], to defend against such an new-flow attack that targets the data plane and the control plane, attack detection and access control are promising approaches. IoT security middleware is considered as a promising way to deal with suspicious flows. However, because of its physical location and the absence of unified interface, it is hard for the security middleware to intercept the attack flows at their access switch actively.

The prevention and detection of DDoS attack in an IoT network is challenging task for the researchers. DDoS attacks frequently flood IoT networks, or IoT devices with immense traffic in order to take over the target object resources and make impossible or difficult for valid users to use services. The IoT network must be prevented and detected when DDoS attacks are launched unexpectedly. Although it is very tough to recognize DDoS attacks from standard traffic due to very high data rate property. DoS attacks are more difficult to recover, identify or prevent. A denial-of-service attack is a safety event that take place when an attacker takings action that avoids appropriate users from retrieving under attack computer network resources, devices, or systems. The DoS attacks almost crashes the node and blocks most of the path of the network. DOS attacks degrades the network performance and drop the packet delivery ratio.

The attack is distributed so the exact point of attack is problematical to recognize because of the uninformed delivery of attacking networks. The actual attacking IoT device is more challenging to diagnose, because they are masquerading behind various or archetypally compromised nodes. The attack can influence the higher volume[6] of IoT systems and to implement an enormously troublemaking attack. It is more challenging to shut down various IoT nodes than one. Paper is organized as follows. Section II provides background of IoT, SDN architecture and DDoS attacks. Section III provides literature survey and related work of the SDN and DDoS attacks. Section IV concludes the paper.

II. BACKGROUND

The Internet of Things (IoT) is considered as one future networking paradigm because of its promise that people and things can be connected at anytime and anyplace. To fulfill this promise, heterogeneous communication technologies such as wireless sensor networks (WSNs), radio frequency identification (RFID), and machine-to-machine (M2M)[7] are integrated in the IoT As a result, much more users with different service requirements are connected to the forwarding devices in the public network.

Recently, software-defined networking (SDN) provides a new way to achieve the idea of IoT. The combination of IoT and SDN definitely brings tremendous advantage in network resources visualization and network management simplification. The main difference between SDN and traditional IP networking is the decoupling of the data plane and the control plane. In the SDN architecture, the control logic is decoupled from the underlying switches and centralized in the network controller. Therefore, the switches are free from routing calculation and focused on packet forwarding, the controller can decide the routing path of a flow according to its communication context. That makes

SDN become custom-driven and show great advantage in routing and management for zillions of devices in the IoT

In the SDN architecture, the control logic is decoupled from the underlying switches and centralized in the network controller. Therefore, the switches are free from routing calculation and focused on packet forwarding, the controller can decide the routing path of a flow according to its communication context. That makes SDN become custom-driven and show great advantage in routing and management for zillions of devices in the IoT.

The SDN network comprises of three planes[8] upper layer is application, middle layer is control and lower layer is data plane. The data plane is infrastructure layer is in the bottom plane and is made up of SDN-enabled switches.

The control plane also control layer provides network services to the IoT network. The SDN-enabled switches direct routing requirements to the control plane. The routing requests instead of computing routing guidelines by themselves as soon as they accept new flows. The control plane computes paths for the incoming requests and allocates the routing instructions in acquiescence with the applications for the top application plane.

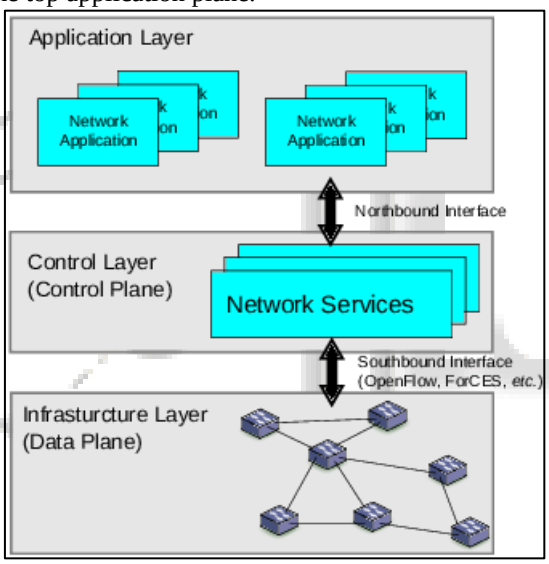

Fig. 1: SDN architecture

The upper application layer also network application is upper layer of the SDN architecture.

Every routing requests as of the data plane and the switch arrangements from the control plane are communicated from end to end with the help of southbound interface. The equivalent messages on the control link be there controlled by the southbound technique such as OpenFlow. Every controller arrangements are directed through the northbound interface. Then the equivalent messages are controlled by the northbound techniques like REST[9].

A. DDoS

A distributed denial-of-service attack is an event that take place when an attacker takings action that avoids appropriate users from retrieving under attack IoT network resources, and devices. DDoS attack prevents users from accessing the IoT services. In DDoS attack node sends excessive messages to block the IOT network, devices and services. DDoS makes the IoT network resources unavailable. In DDoS attacks the incoming traffic from IoT network flooding the devices from many different sources. DDoS assaults are very challenging to identify, recover and prevent. The DDoS occurrences very nearly crashes the IoT services and blocks utmost all the path of the IoT network. DDoS occurrences cut down the IoT network performance and drop the throughput of the devices. The IoT network used firewalls, intrusion prevention system and intrusion detection systems for DoS attack prevention and detection. DDoS attacks are basically from more than one IoT network attack systems. DDoS attacks are originated from multiple IoT systems and therefore difficult to detect. DDoS attacks can deafening the IoT services or flooding the IoT network services. The flood DDoS attacks are SYN flood, buffer overflow and ICMP flood.

B. ICMP DDoS Flood

It influences the misconfigured IoT network components by pointing faked packets that ping every single IoT devices on the under attack IoT network, in its place of impartial one definite IoT device. ICMP DDoS flood attack is also identified as the smurf or ping of death attack.

C. DDoS Buffer Overflow Attacks

It is the most common type DDoS attack in IoT network. The concept behind attack is to send added traffic to an IoT network devices.

D. SYN DDoS Flood

It sends an ultimatum to link to an IoT server, but never finalizes the handshake signal. Residues up while waiting for all exposed ports are inundated with demands and none are attainable for trustworthy users to connect to.

III. LITERATURE SURVEY

In order to defend against the new-flow attack with the consideration of low cost monitoring and dynamic access control at the attackers' access switch paper propose a smart security mechanism (SSM)[10]. The SSM uses the standard southbound and northbound interfaces of SDN, and it includes a low-cost method that monitors the new-flow attack by reusing the asynchronous messages on the control link. The monitor method can differentiate the new-flow attack from the normal flow burst by checking the hit rate of the flow entries. Based on the monitoring result, the SSM uses a dynamic access control method to mitigate the new-flow attack by perceiving the behavior of the security middleware in the IoT. The dynamic access control method can intercept the attack flows at their access switch. Two specific traffic features are designed to monitor the new-flow attack. According to the monitoring results, SSM first redirects suspicious flows to the security middleware in the IoT, then it perceives the filtering results of the security middleware. Based on that, SSM assigns the access control rules to intercept the attack flows at their access switch in SDN-based IoT. The author developed SSM as an application and test SSM in testbed, the experiment results prove that SSM is a practical solution to defend against the new-flow attack.

A DoS attack is type of an attack with the perseverance of avoiding genuine users from using an identified IoT network resource [11]. The novel DoS attacks intention to dissipate the IoT network devices of the control

plane and the data plane in the SDN architecture. This type of assaults threats the operational basis of the SDN architecture. For that reason, numerous studies attempt to defend and discuss contrary to the novel DoS assaults in SDN.

St-Hilaire and Mousavi[12] represents how the DoS attack dissipates controller IoT resources and recommend a solution to discover such an attack. The author observe the entropy features of requests acknowledged by the controller. The authors assume that, as soon as the DoS attack flows use spoofed target addresses, the entropy features and the arbitrariness of flows decrease obviously. The suggested method aims to identify the attack contained by the first five hundred data packets of the attack traffic flow.

Antikainen and Kandoi [13] suggested the DoS attack to switch's flow table and the control link bandwidth. The authors prove that the control pane bandwidth and the timeout data of flow entries, influence the performance of this type of attack. If not constituted properly, SDN can be inactivated by this type of attack. The authors also propose some probable mitigation approaches based on their implementations.

Yi and Yu[14] suggested a collaborative methodology of security associated to occasional shrew DDoS attacks in the small frequency domain. The proposed methodology recognized shrew DDoS attacks with the assistance of frequency-domain features from the auto-correlation prearrangement of IoT network data traffic.

Lee and Wu[15] and suggested a DDoS attack recognition method by using the procedure of one step guess Kalman filtering. The proposed scheme discovered the characteristics of system traffic observed at the target end as soon as the attack initiated. The error amongst one step estimate and the optimum estimation is applied as the beginning for detection.

Recommendation Based Trust Model[16] by means of an Effective Defense System for MANETs make available reference created trust prototypical with a safety structure, which make use of grouping procedure to enthusiastically filter out occurrences related to dishonest recommendations applying guaranteed time constructed on amount of interactions, compatibility of information and closeness between the nodes. It simply detect bad mounting cyber-attack. The scheme does not make available detection and prevention from DDoS type attacks.

Kwak and Choi[17] suggests a safe SDN-based IoT structure. The framework provides the SDN control plane which is reconstructed to make available safety services such as IDS/IPS, authentication/access control, and lightweight encryption. Based on that, the author explained the working procedures of these safety services and appraise authors proposal underneath an SYN flooding attack.

FlowRanger [18] attempts to expand the controller performance as soon as the controller is under DoS attack. Once the controller is busy handling the requests of the data plane, the FlowRanger provides precedence to the request. The request as of the user which has look as if numerous times for the duration of the normal condition i.e. no sign of DoS attacks has a greater priority. The request as of the user which look as if during the attack has a lesser priority. In this method, it increases the serving speed of the average users' requests.

Bull *et al.* [19] summarizes the safety issues of together the IoT network and the IoT device. They recommend a technique to mitigate and detect inconsistent behavior at the SDN-based IoT gateway. By means of presetting flow records in the SDN-based IoT gateway, the method collect source and destination data of flows and categorize the network condition. In addition, three probable mintage movements are arranged to deal with the identified inconsistent behavior.

Dong *et al.* [20] suggests a recognition technique for the DoS based attack to the controller by observing the low-traffic flows. In low-traffic flows smaller amount of packets flows than the normal flows. It can lead to noteworthy resources ingestion in the control plane. The author detected such DoS attack by applying Sequential Probability Ration Test (SPRT) method to control the false positive and false negative error rates. On the other hand, the observing mitigation strategy and cost are not duly considered. The integration of IoT and SDN unquestionably brings remarkable advantage in network management simplification and network resources visualization. As an outcome, plenty of research try to make safe the IoT with the SDN architecture.

Yu *et al.* [21] suggests the DoS based attack to the OpenFlow-enabled switch. The author suggest a QoS-aware peer provides approach that assimilates idle flow table IoT resources to alleviate the flow table congestion attack. The author attempt to make SDN additional resistant to such type of DoS attack and evade severe indemnities at the beginning the attack.

Chakrabarty *et al.* [22] express anxiety about the safety methods provided by the prevailing IoT protocols. The author recommend Black SDN, which provides an SDN-based architecture for safe IoT communication. The author propose a method in which both the payload and packet header are encrypted. To forward the scrambled packets proficiently, the method used the SDN controller as reliable third party. The technique try to alleviate the passive attacks, like inference attack and traffic analysis.

Flauzac *et al.* [23] give emphasis to that the customary Ad-Hoc network is nonexistence of access control and traffic monitoring, because of the nonexistence of the network infrastructure. The author propose an SDN-based IoT architecture for traffic monitoring. In authors suggested architecture, for each node in the Ad-Hoc network is observed as an amalgamation of legacy host and SDN-enable switch. Then author used safety controllers to observe traffic and accomplish security rules in the Ad-Hoc network.

Sandor *et al.* [24] attempt to expand the resilience of IoT communication by means of SDN's flexible data routing feature. The author assume there are many redundant routers aimed at the communication in IoT networks. As soon as the original communication link is inactivated by cyber-attacks, they apply the SDN controller to get a novel link for the data communication.

IV. CONCLUSION

The Internet of Things (IoT) is considered as one future networking paradigm because of its promise that people and things can be connected at anytime and anyplace. Recently,

software-defined networking (SDN) provides a new way to achieve the idea of IoT. The combination of IoT and SDN definitely brings tremendous advantage in network resources visualization and network management simplification. A distributed denial-of-service attack is an event that take place when an attacker takings action that avoids appropriate users from retrieving under attack IoT network resources, and devices. DDoS attack prevents users from accessing the IoT services. In DDoS attack node sends excessive messages to block the IOT network, devices and services. In order to defend against the DDoS attack and new-flow attack with the consideration of low cost monitoring and dynamic access control at the attackers' access switch the novel method is required. This paper provides the survey of different techniques to handle DDoS attacks in SDN network of IoT services. This paper also provides prevention and detection methods of DDoS attacks in IoT.

REFERENCES

[1] CHANGSHENG YU, LI YU1, YUAN WU, YANFEI HE, AND QUN LU, Uplink Scheduling and Link Adaptation for Narrowband Internet of Things Systems, Vol-5, IEEE 2017, pp. 1724-1735
[2] IEEE Standard for Local and Metropolitan Area Networks_Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer, IEEE Standard 802.15.4e-2012 (Amendment to IEEE Standard 802.15.4-2011), 2012, pp. 1_225.
[3] K. Sood, S. Yu, and Y. Xiang, ``Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review," IEEE Internet Things J., vol. 3, no. 4, pp. 453_463, Aug. 2016.
[4] Y. Xu and Y. Liu, ``DDoS attack detection under SDN context," in Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), San Francisco, CA, USA, Apr. 2016, pp. 1_9.
[5] R. Klöti, V. Kotronis, and P. Smith, ``OpenFlow: A security analysis," in Proc. 21st IEEE Int. Conf. Netw. Protocols (ICNP), Göttingen, Germany, Oct. 2013, pp. 1_6.
[6] Q.Yan and F.Yu, ``Distributed denial of service attacks in software-defined networking with cloud computing," IEEE Commun. Mag., vol. 53, no. 4, pp. 52_59, Apr. 2015.
[7] Y. Jararweh, M. Al-ayyoub, Ala, ``Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, ``SDIoT: A software defined based Internet of Things framework," J. Ambient Intell. Humanized Comput., vol. 6, no. 4, pp. 453_461, Aug. 2015.
[8] J. Granjal, E. Monteiro, and J. S. Silva, ``Security for the Internet of Things: A survey of existing protocols and open research issues," IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294_1312, 3rd Quart., 2015.
[9] L. Richardson and S. Ruby, RESTful Web Services. Sebastopol, CA, USA: OReilly Media, 2008.
[10] TONG XU, DEYUN GAO, PING DONG, HONGKE ZHANG, CHUAN HENG FOH, AND HAN-CHIEH CHAO, "Defending Against New-Flow Attack in SDN-Based Internet of Things", IEEE 2017, pp. 3431-3444
[11] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39_53, Apr. 2004.
[12] S. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Venice, Italy, Feb. 2015, pp. 77_81.
[13] R. Kandoi and M. Antikainen, "Denial-of-service attacks in OpenFlow SDN networks," in Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM), Ottawa, ON, Canada, May 2015, pp. 1322_1326.
[14] Zhijun Wu, Liyuan Zhang, and Meng Yue , Low-Rate DoS Attacks Detection Based on Network Multifractal, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 5, SEPTEMBER/OCTOBER 2016, pp-559-567
[15] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, " On a mathematical model for low-rate shrew DDoS," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.
[16] Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2114
[17] S. Choi and J. Kwak, "Enhanced SDIoT security framework models," Int. J. Distrib. Sensor Netw., vol. 2016, pp. 1_12, May 2016.
[18] L. Wei and C. Fung, "FlowRanger: A request prioritizing algorithm for controller DoS attacks in software de_ned networks," in Proc. IEEE Int. Conf. Commun. (ICC), London, U.K., Jun. 2015, pp. 5254_5259.
[19] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, Flow based security for IoT devices using an SDN gateway," in Proc. IEEE 4th Int.Conf. Future Internet Things Cloud (FiCloud), Vienna, Austria, Aug. 2016, pp. 157_163.
[20] P. Dong, X. Du, H. Zhang, and T. Xu, "A detection method for a novel DDoS attack against SDN controllers by vast new low-traf_c _ows," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, May 2016, pp. 1_6.
[21] B. Yuan, D. Zou, S. Yu, H. Jin,W. Qiang, and J. Shen, "Defending against flow table overloading attack in software-defined networks," IEEE Trans. Serv. Comput., to be published.
[22] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in Proc. IEEE 12th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS), Dallas, TX, USA, Oct. 2015, pp. 190_198.
[23] O. Flauzac, C. González, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," in Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), Gwangiu, South Korea, Mar. 2015, pp. 688_693.
[24] H. Sándor, B. Genge, G. Sebestyén-Pál, "Resilience in the Internet of Things: The software defined networking approach," in Proc. IEEE Int. Conf. Intell. Comput. Commun. Process. (ICCP), Cluj-Napoca, Romania, Sep. 2015, pp. 545_552.

