JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security Attacks on Software Defined Networks

ROHINI SHARMA

Abstract

SDN (Software Defined Networking) is a network that allows sensor devices to communicate across the network. The sensor devices are responsible for sensing the conditions such as temperature, pressure etc. This network had decentralized in nature, thus, security becomes a main issue because of which network performance is affected. The security attacks are of two kinds: active and passive. The route misdirection is an active attack that facilitates malicious nodes to transmit data on the wrong directions. The preceding work suggested the method of threshold in order to detect the malicious nodes. This research work introduces a RSSI (Receive Signal Strength Indicator) method with trust based system to detect the malicious nodes in the network. It is expected that the introduced method will assist in boosting the network performance concerning certain metrics such as throughput, delay and packet loss.

Keywords: SDN, RSSI, API.

Introduction

1.1 Software Defined networking

SDN (Software Defined Networking) is a major concept which assists in overcoming the drawbacks of conventional computer networks architectures so that the requirements of complex networking can be fulfilled. Therefore, the simplified networks are managed. The concept of separation is established amid the network control logic and the underlying hardware for abstracting the lower-level functionality.

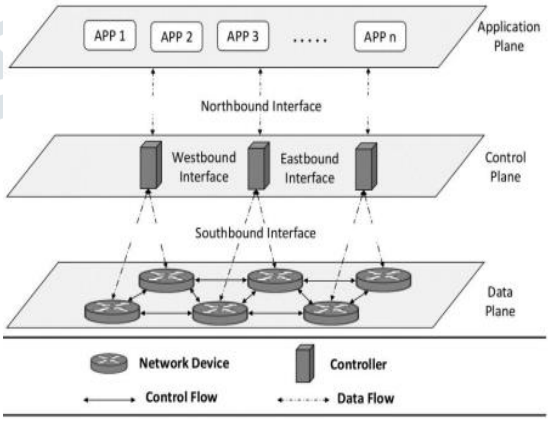

Figure 1: Software Defined Networking (SDN) General Architecture

Figure 1 represents that the SDN architecture is composed of data, control and application planes. Various forwarding devices namely switches, routers

and access points etc. are comprised in network devices of the underlying network architecture [1]. This leads to transmit the data among end-users available on the data plane. The control plane is utilized to manage and program this plane. The flow control is managed and the control logic is utilized in the control plane for making the decisions. This plane supports setting rules for the management of forwarding devices present within the data plane. This communication is established on the Southbound API (Application Programming Interface). In contrast, the communication of control plane is established with the application plane using the Northbound API. The controller is utilized for abstracting the complexity of architecture and enabling the simplified applications. The communication across these controllers is established over an east or west API, according to the direction, in case of deployment of multiple controllers in SDN architecture.

1.2 Scalability in SDN

The common denominator among SDN (software-defined networking) proposals is to shift the control function out of data plane elements. This decoupling assists both planes in evolving in a free manner and providing a number of benefits such as high flexibility, being vendor-agnostic, programmability and the possibility to understand a centralized network view. However, various issues, related to performance and scalability [2], are occurred with the commencement of this network. The control this network is centralized in nature due to which the concern regarding scalability and resiliency is occurred. In the end, despite of the controller capability, a central controller is incapable of scaling due to the development of the network and faces failure while handling all the incoming requests when the same service guarantees are offered. Furthermore, the initial benchmarks on NOX, which is the first controller of software-defined networking, indicate that it is able to handle only 30,000 flow initiations per second during the maintenance of a sub-10 ms flow install time. These benchmarks are applicable for tackling these kinds of concerns. Most of the preceding SDN approaches are based on flow, thus, additional flow initiation delay becomes another issue. Since, SDN scalability has not any inherent bottleneck. Thus, such issues are occurred from the implicit and extrinsic assumptions. To illustrate, the low flow setup throughput in NOX is represented as an implementation artefact. This allows to design a SDN control plane having scalability like any distributed system without considering these assumptions.

1.3. Problem Formulation

Software Defined Networking (SDN) is a technology that offers complete flexibility in the management of the various planes it operates. For this reason, big players such as Cisco, Juniper etc. in the networking domain are fully involved in this technology. Because of the openness function available in SDN, various kinds of attacks seem to be exposed to the SDN environment. The major objective for such attacks is the SDN controller that manages the whole system. Slowing down or closing down the whole network is the key purpose of such attacks. One such attack is a DoS (Denial of Service) attack in which an attacker aims to slow down the network by sending massive fake requests to the Controller. A type of DoS attack is DDoS (Distributed DoS) Where there are several compromised devices used to target

a Single system. Therefore, to achieve protection reducing such DDoS attacks is essential.

1.5. Objectives

The aims of the research are:

- To analyze various kinds of algorithms to detect and prevent the DDoS (Distributed Denial of Service) attack in SDN (software define network).
- To suggest a hybrid algorithm for detecting and alleviating the DDoS attack with the help of switch table statics to offer higher bandwidth, the impact of attack on packet rate and delays because of attack.
- To perform a comparison of the hybrid method with the existing method with regard to diverse performance parameters.

1.4. Research Methodology

This research work is conducted on the basis of detecting the malicious nodes which lead to launch several security attacks in the network. The location protection attack is an active attack that put impact on network performance. The method of node location and the trust based system are put forward to detect the malicious nodes. The initial technique includes a measurement known as RSSI (Receive Signal Strength Indicator) that is utilized to receive the condition of power in the anchor nodes. This measurement is employed through various extensive wireless communication standards. This factor is considered to define the size of electromagnetic wave energy in a media and computation of RSS (received signal strength). The changes in environment lay great impact on RSSI, a function of distance. The RSSI technique is deployed for forwarding the frames to the entire network and other sensors in the communication region. Moreover, the received RSSI values are considered to compute the distance. The unknown nodes send the RSSI to beacon nodes which further transmit it. The RSS without including the condition of signal gain's condition is calculated with the difference between the transmission of SS and signal propagation. The theoretical system of propagation path loss is applied to range the RSSI (Receive Signal Strength Indicator) with the purpose of computing the distance. In this method, the beacons are responsible for flooding the control messages within the network and nodes, to which the message is received, will reply with the route reply messages. The localized node is a beacon that received two replies from similar beacons. The exact location of sensor nodes can be obtained and the malicious nodes are detected after localizing the sensor nodes in the network. The second phase makes the implementation of trust based system in order to detect the malicious nodes. This system is useful for computing the energy level of every node. The sensor node which focuses on transmitting least number of packets and consuming more energy is considered as the malicious node. The malicious nodes are isolated from the network using multipath routing method. This method does not select the path at which malicious nodes are present. It is expected that the introduced method will lead to prolong the duration of the network as well as enhance the performance of network with regard to throughput and other metrics.

1.7Conclusion

This research work summarizes that the major concern of SDN (software define network) is security. The network performance is affected due to these security issues with regard to various metrics.

The existing research work implemented the threshold method with the purpose of detecting the malicious nodes. This method has yielded lower accuracy while detecting the malicious nodes. This research work establishes RSSI (Receive Signal Strength Indicator) technique for recognizing the position of malicious nodes as well as the nodes. This work also emphasizes on the trust based system for resisting against the malicious nodes. It is expected that the established method will offer superior performance regarding throughput, delay and packet loss.

References

[1] Roman Odarchenko, Oleh Tkalich, GeorgiyKonakhovych, AnastasiiaAbakumova, "Evaluation of SDN network scalability with different management level structure", 2016, Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)

[2] Alvaro Mauricio Diaz Tello, Mehran Abolhasan, "SDN Controllers Scalability and Performance Study", 2019, 13th International Conference on Signal Processing and Communication Systems (ICSPCS)

[3] Amin Yazdpour, Naser Movahedinia, "ConsciousCache: Improving SDN controller scalability using flows similarities", 2017, IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI)

[4] Saleh Asadollahi, Bhargavi Goswami, Ahmad SohaibRaoufy, Hedmilson Guimaraes Jose Domingos, "Scalability of software defined network on floodlight controller using OFNet", 2017, International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)

[5] Murat Karakus, Arjan Durresi, "A Scalability Metric for Control Planes in Software Defined Networks (SDNs)", 2016, IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)

[6] Mohamed A. Aglan, Mohamed A. Sobh, Ayman M. Bahaa-Eldin, "Reliability and Scalability in SDN Networks", 2018, 13th International Conference on Computer Engineering and Systems (ICCES).

[7] M. Z. Shaikh, Sachin H. Darekar, "Performance Analysis of Various Open Flow Controllers by Performing Scalability Experiment on Software Defined Networks", 2018, 3rd International Conference on Inventive Computation Technologies (ICICT)

[8]Renan C. A. Alves, Doriedson A. G. Oliveira, Gustavo A. Nunez Segura, Cintia B. Margi, "The Cost of Software-Defining Things: A Scalability Study of Software-Defined Sensor Networks", 2019, IEEE Access, Volume: 7

[9]Rafiza Ruslan, Nur'AqilaBalqis Othman, Mohd.FarisMohd. Fuzi, Norlizawati Ghazali, "Scalability Analysis in Mininet on Software Defined Network using ONOS", 2020, Emerging Technology in Computing, Communication and Electronics (ETCCE)

[10]Mohammed Amine Togou, Djabir Abdeld jalil Chek ired, Lyes Khoukhi, Gabriel-Miro Muntean, "A Hierarchical Distributed Control Plane for Path Computation Scalability in Large Scale Software-Defined Networks", 2019, IEEE Transactions on

Network and Service Management, Volume: 16, Issue: 3

[11]Hongli Xu, He Huang, Shigang Chen, Gongming Zhao, Liusheng Huang, "Achieving High Scalability Through Hybrid Switching in Software-Defined Networking", 2018, IEEE/ACM Transactions on Networking, Volume: 26, Issue: 1

[12]Ching-Chih Chuang, Ya-Ju Yu, Ai-Chun Pang, "Flow-Aware Routing and Forwarding for SDN Scalability in Wireless Data Centers", 2018, IEEE Transactions on Network and Service Management, Volume: 15, Issue: 4

[13]Doaa A. Hamdi, SamyGhoniemy, Yasser Dakroury, Mohammed A. Sobh, "A Scalable Software Defined Network Orchestrator for Photonic Network on Chips", 2021, IEEE Access, Volume: 9

[14]Wen-Kang Jia, Ruolan Ying, Xiaoning Shi, "Deploying a Fast Detection and Eviction Mechanism of Invalid Connection-Oriented Flow-Entries in SDNs: A Scalability Approach", 2020, IEEE Access, Volume: 8

[15]Abdijalil Abdullahi, Selvakumar Manickam, Shankar Karuppayah, "A Review of Scalability Issues in Software-Defined Exchange Point (SDX) Approaches: State-of-the-Art", 2021, IEEE Access, Volume: 9

[16]Hemanth Kumar Ravuri, Maria Torres Vega, Jeroen van der Hooft, Tim Wauters, Bin Da, Filip De Turck, "On Routing Scalability in Flat SDN Architectures", 2020, 11th International Conference on Network of the Future (NoF)

[17]Emad Alasadi, Hamed Al-Raweshidy, "OLC: Open-Level Control Plane Architecture for Providing Better Scalability in an SDN Network", 2018, IEEE Access, Volume: 6

[18]Shengru Li, Kai Han, Nirwan Ansari, Qinkun Bao, Daoyun Hu, Junjie Liu, Shui Yu, Zuqing Zhu, "Improving SDN Scalability with Protocol-Oblivious Source Routing: A System-Level Study", 2018, IEEE Transactions on Network and Service Management, Volume: 15, Issue: 1

[19]Lyndon Fawcett, Sandra Scott-Hayward, Matthew Broadbent, Andrew Wright, Nicholas Race, "Tennison: A Distributed SDN Framework for Scalable Network Security", 2018, IEEE Journal on Selected Areas in Communications, Volume: 36, Issue: 1