SDN-Based Intrusion Detection System

Literature review

Juma Ibrahim
Computer science and informatics
School of Electrical Engineering
Belgrade, Serbia
jumaibrahim04@yahoo.com

Slavko Gajin
Computer science and informatics
School of Electrical Engineering
Belgrade, Serbia
slavko.gajin@rcub.bg.ac.rs

Abstract—**The word of the network has been changed from a small group of interconnected devices to billions of devices - servers, hosts, printers, Smartphone etc. This phenomena increase the requirements in term of network security.**
Decoupling the data and control planes Software Define Network (SDN) transforms traditional network architecture to reliable centralized manageable structure with programming ability. However, computer and network security is still the main concern for network and system administrator. Different types of software and hardware solutions are used to eliminate the dangers of attackers, but new type of attacks appear on daily bases. Intrusion Detection System (IDS) has the availability to locate and identify malicious activity in the network by examining network traffic in real time. It gives administrators visibility and reliability to monitor and control their systems. This paper present a survey of various research efforts towards the development of intrusion detection system based on software define network.

Keywords-SDN; IDS; OpenFlow

I. INTRODUCTION

A successful attack will allow intruders to get authorized access to the system resources, but we have to prevent attacks. It is important to build security features and techniques to prevent attacks and protect the infrastructure, such as access control, permissions, firewalls, and other secure software and hardware. However, in complex system it is very hard to achieve full protection, as well as manage and maintain such environments. Therefore it is a cheaper to prevent some attacks and detect the rest and this is the idea of Intrusion Detection System (IDS). They have the availability to locate and identify malicious activity in the network by examining network traffic in real time.
The function of IDS is to monitor and analyze events within a computers and network. When attacks happen we should know about them, and can take technical measures to stop the threat and protect our system.
SDN is an emerging architecture that allows network administrators to manage network devices through a separation of data and control functions. It provides centralized control and view of the network, with the ability to program the network through external applications.
A lot of papers and research proposal have been published regarding intrusion detection system in classical IP-based networks, but few of them introduce the concept of intrusion detection system based on software define network technology.
This paper present a survey of various research efforts towards the development of intrusion detection system based on software define network. Section I providesa brief introduction, while Section II gives an overview of the SDN technology. In section III the different types of IDS and its detection techniques is introduced. The concept of SDN-based IDS and a comparison of different approaches are discussed in Section IV. Finally, we draw conclusions and future work in Section V.

II. SOFTWARE DEFINE NETWORK (SDN)

The existing network devices such as routers and switches have their own operating systems which have a limited set configuration options. If network administrators or security engineers what to make significant changes deploying new protocols or technologies which is not currently supported, they must change the whole device must be changed which is costly and unacceptable approach.
The concept of Software Define Network (SDN) involves managing network services through abstraction of lower level functionality. In other words, separation of data and control planes with well-defined Application Programmable Interface (API) is the main characteristic of SDN.
Data plane functionalities cover all activities related to data packets transmitting, such as forwarding, fragmentation, reassembly, replicating for multicasting etc.
The Control plane defines functional logic for network communication equipment (routers or switches) that determines how one device communicates with other devices in the network. All the routing protocols in routers or other protocols with switches are control plane protocols. It includes all activities that are necessary to operate data plane, but do not involve end-user data packets (making routing tables, setting packet handling policies, base station beacons announcing availability of services). Figure 1 depicts a logical view of the SDN architecture. Network intelligence is (logically) centralized in software-based SDN controllers, which maintain a global view of the network [1].

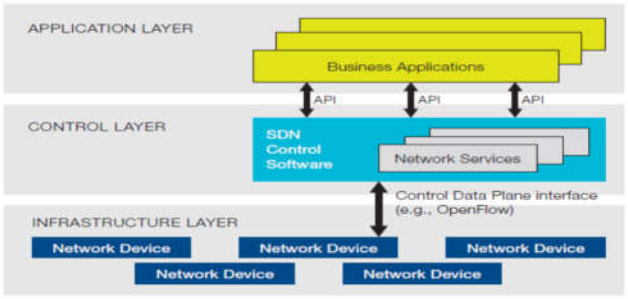

Figure 1. Software-Defined Network Architecture [1]

Open Flow Protocol (OPF) is a programmable network protocol which is designed to manage the traffic in SDN network [2]. OpenFlow Protocol is the first standard communications interface defined between the controllers and forwarding layers of SDN architecture. It is a programmable open protocol designed to direct and manage communication between network devices and central network controller.

III. INTRUSION DETECTION SYSTEM (IDS)

The Intrusion Detection System (IDS) is a software or hardware that used by system administrators and security engineers to monitor the characteristic of a single host or monitoring and analyses the whole network traffic in order to distinguish between legitimate and attacks traffic. It case of attacks it generates alarms keep tracks about malicious activities.

A. Types of attackers

The following types of attackers are recognized and classified in the literature.

- Masquerader
  An individual who is not authorized to use the computer and who penetrates system access control to exploit a legitimate user accounts. It's likely to be outsider.
- Misfeasor
  There are two subtypes of attackers: one is a legitimate user with no permission to access an application, while the other is a legitimate user but misuses the privileges. Both of them are likely to be insiders.
- Clandestine user
  An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. It could be either insider or outsider.

B. Types of Intrusion Detection System

Intrusion Detection Systems can be categorized based on what they target into the following:

- *Host-based Intrusion Detection System* (HIDS)
  It is a special software on a computer that monitors what happen in that computer, with the aim of detecting is there someone intruding or not.
- *Distributed host-based Intrusion Detection system* (DHIDS)
  Intrusion detection software is distributed in many computers or special devices, monitoring for malicious activities. They often report back to some other central computer to improve the chance of detecting the intrusions.
- *Network-based Intrusion Detection system* (NIDS)
  Inspects network traffic to identify suspicious activity by monitoring network traffic behaviour at different points across the network and correlating this information they can recognize anomaly in traffic patterns. The analysis may be done in the sensors or may be sent information back to the management server that does the analysis for all of them.
- *Wireless Intrusion Detection system* (WIDS)
  It uses to monitor the wireless LAN using sensors distributed in a wide physical network detection placement within a range of existing wireless signals.

C. Common components

The main components that are used in almost every intrusion detection system are:

- Sensors: collect data, e.g. packets using tcp-dump or wireshark, log files (with respect to applications), system call traces (with respect to the operating system).
- Analyzer: received collected data, analyze it and determine if intrusion.
- User interface: allow security experts, system administrators, and other users to view the output and control behaviour of IDS.

D. Intrusion Detection Methods

The source of data that is analysed by the IDS is either whole packet data, which is the transitional IDS used to inspect the whole payload or flow-based IDS which only takes basic accounting information of the communication in the network (header of the packet, number of bytes and packets in both directions). Therefore, flow-based IDS reduces the amount of data to be analysed, what makes them specially interest in SDN-based system.

IDS use a variety of detection and analyses methods in order to evaluate the traffic crossing the network, and can be categorized based on how they identify intrusion into the following:

- Signature-based detection (Packet-based)

  Known as knowledge-based or misuse-detection it defines the behaviour or attacks by set of rules or patterns; compare observed behaviour against these rules/patterns

Usually, techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. This method is widely used because many attacks have clear and distinct signature [3].

- Rule-based anomaly detection: define rules based on past observed normal behaviour. It also involves an attempt to define a set of rules or attacks patterns that can be used to decide that a given behaviour is that of an intruder.
- Rule-based penetration identification: define rules based on attacks. Typically, the rules used in these systems are specific to the machine and operating system, the most fruitful approach to developing such rules is to analyse attack tools and scripts collected on the internet. These rules can be supplement with rules generated by knowledgeable security personal.

It is used for the expert intelligent system that tries to analyse the user packets and from that analysis the classification between legitimate and illegal users is made.

The problem with this approach is that new attack cannot be detected either because the database is out of date or signature not available yet. Another weakness is the time taken since it supposes to compare all the signatures. However, it achieve high accuracy with low number of false alarms [4]

- Anomaly-based Detection (Flow-based)

Known as statistical anomaly-based, behaviour-based, or baselining, it involves the collection of data relating to the behaviour of legitimate users over a period of time. Statistical tests are applied to observed behaviour to determine whether it is legitimate user or not. There are two types:

- Threshold detection: threshold based on frequency of occurrence of events, independent of user. It involves counting the number of occurrences of a specific event type over an interval of time. If the count surpasses what is considered a reasonable number that one might expect to occur, then intrusion is assumed. By itself is a crude and ineffective detector of even moderately sophisticated attacks.
- Profile-based: A profiles of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.

The advantages of this technique are the abilities to detect new types of attacks. It has the disadvantages which require more overhead, processing capacity and produces a false alarm.

IV. SDN-BASED IDS

The SDN as a new promising technology for network architecture with a lot of advantages as follows.

- Effective traffic monitoring: because SDN controller have direct or indirect control over entire network traffic so it can potentially detect any abnormal traffic
- Vulnerability discovered shortly: the operators can deal with any attacks as soon as it is discovered immediately by programming the control logic to stop this type of attacks, without waiting for software updates whether it is operating system or application.

At the same time it has a lot of disadvantages as well:

- Controller is a single point of failure: if the controller is seized by an attacker then, the network is compromised and this is high possibly happened due to the SDN support for cloud computing platforms
- Open programming interface: SDN is more vulnerability for security threats because the software is fully exposed to attackers due to open nature of this technology, another point is a numerous number of programming interface for application layer
- Many points for attacks: as SDN has three layers (application, control, and data) and the interface between these layers is point of attack to the network as described in Figure 2.

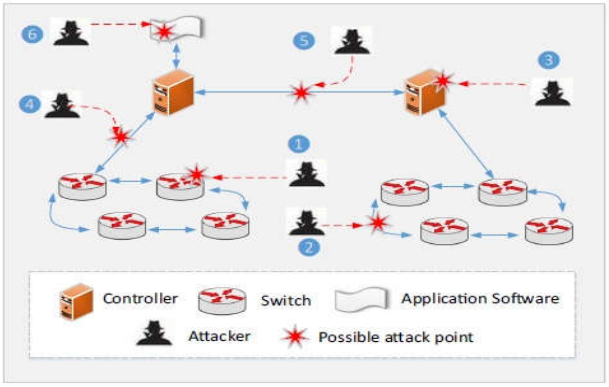

Figure 2. Possible attack points [10]

In [2], the authors propose the concept of new Open Flow switch that contains IDS in it which makes Open Flow protocol more secure. In [5], the authors propose a system with the advantages of programmability offered by SDN to provide the architecture for IDS which will detect suspicious packets. In [6], the authors present the conception classifies unauthorized activities performed in SDN environment. In [7], the authors propose a concept of using SDN technology and machine learning algorithms for monitoring and detecting of malicious activities in the SDN data plane. They improve the efficiency of detecting U2R attacks, and achieve

higher TPR values for DOS, Probe, U2R, classes compared to other methods. In [8], the authors propose flow-based anomaly detection system based on SDN using deep learning. They conclude that the basic information about the network traffic can be extracted easily by the controller and evaluated by the deep learning IDS module. Table 1 shows the accuracy comparison of different algorithms. In [11], authors proposed a new framework (FRESCO) for creating security applications with SDN. In [12], anomaly-based detection algorithm is defined for NOX controller which inspects only the first packet which is makes it very effective for port scanning attack. In [13], also anomaly-based detection is used by gathering flow information using sFlow tools and communicates with an anomaly detector in order to exclude any potential threats. In [14], a botnet DDOS detection proposal is presented by the authors in OpenFlow networks. This design overloads the network card when the process of attack started. In [15], XenFlow propose a scheme to prevent DoS attacks from a malicious tenant of the virtual network, which depends on the isolation of traffic and resources, but it cannot prevent flooding DoS attacks in the virtual network. In [16], the authors propose a SnortFlow IDS/IPS signature-based detection based on Snort rules.

TABLE 1. ACCURACY COMPARISON OF DIFFERENT ALGORITHM [8]

Algorithm	Accuracy (%)
J48	**81.05**
Naïve Bayes (NB)	**76.56**
NB-Tree	**82.02**
Random Forest	**80.67**
Random Tree	**81.59**
Multi-layer Perceptron	**77.41**
Support Vector Machine (SVM)	**69.52**
Authors algorithm	**75.75**

V. CONCLUSION

With the nature of SDN technology as open interface and the controller as the core of this new technology made the security risk as the main concern.

With SDN technology we can achieve the flexibility, programmability, dynamicity, manageability and intelligence to current network architecture by using single viewpoint, planning and saving cost. Many features that may contain valuable information could be extracted or it can be a focus on one specific type of attack. Collection and analysis of network flow information are more efficient compared to deep packet inspection (DPI) and protects the privacy of users.

Recent research has shown that SDN technology with machine learning approaches gives better results in attack detection.

VI. REFERENCES

[1] Software-Defined Networking: The New Norm for Networking. White paper. s.l. : Open Network Foundation, April 2012.

[2] Open Flow Switch With Intrusion Detection System. Sures Kumar, Tarun Kumar, Ganesh Singh, Maninder Singh Nehra. 7, s.l. : International Journal Of Scientific Research & Technology (IJSRET), October 2012, Vol. 1. ISSN 2278 - 0882.

[3] Michael E. Whitman, Herbert J. Mattord. Principles Of Information Security. Boston, USA: Cengage Learning Customer & Sales Support, 2011. 978-111-13821-9.

[4] Hashem Alaidaros, Massudi Mahmuddin, Ali Almazari. An Overview of Flow-Based And Packet-Based Intrusion Detection Performance in High-Speed Networks.

[5] Software Defined Networking with Intrusion Detection System. Yogita Hande, Aishwarya Jadhav, Achaleshwari Patil, Rutuja Zagade. 10, s.l. : International Journal Of Engineering And Technical Research (IJETR), 2014, Vol. 2. 2321-0869.

[6] Damian Jankowski, Marek Amanowicz. Intrusion Detection in Software Defined Networks with Self-Organized Maps. s.l. : Journal of Telecommunication and Information Technology, 2015.

[7] On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks. Damian Jankowski, Marek Amanowicz. 3, s.l. : International Journal of Electronic and Telecommunications, 2016, Vol. 62. 247-252.

[8] Tuan A Tang, Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, Mounir Ghogho. Deep Learning Approach for Network Intrusion Detection in Software Defined Networking. Leeds: White Rose, 2016.

[9] A Survey of Network Flow Applications. Bingdong Li, jeff springer, George Bebis, Mehmet Hadi Gunes. s.l. : Journal of Network and Computer Applications, 2013, Vol. 36. 567-581.

[10] Security in Software-Defined Networking: Threats and Countermeasures. Jim fun Wan. Di Li, Athanasios Vasilakos. s.l. : ResearchGate, 2016.

[11] FRESCO: Modular Composable Security Services for Software-Defined Networks. Seung Shin, Phil Porras, Vinod Yegneswaran, Martin Fong, Guofei Gu, Mabry. s.l. : In Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS' 13), February 2013.

[12] Revisiting traffic anomaly detection using software defined network. S. A. Mehdi, J. Khalid, and S. A. Khayam. s.l. : Springer, Sep. 2011.

[13] Combining OpenFlowand sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environment. K. Giotis, C.Agyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris. s.l. : Computer Networks, Apr. 2014, Vol. 62.

[14] An SDN-oriented DDoS blocking scheme for botnet-based attacks. S. Lim, J. Ha, H. Kim, Y.Kim, and S.Yang. s.l. : 16th International Conference on Ubiquitous and Future Networks, Jul. 2014.

[15] XenFlow: Seamless migration primitive and Quality of Services for Virtual Networks. D. M. F. Mattos, and O.C. M. Duarte. s.l. : IEEE Global Communications Conference - GLOBECOM, Dec. 2014.

[16] SnortFlow: An OpenFlow-Based intrusion prevention system in the cloud environment. T. Xing, D. Huang, L. Xu, C.-j. Chung, and P.Khatkar. s.l. : 2nd GENI Research and Educational Experiment Workshop, Oct. 2013.