PROCEEDINGS OF SCIENCE

Research on Security Threat Monitoring and Testing Framework in Software - Defined Network Based on Depth Learning

Shumian Yang[1a]**; Lianhai Wang**[2b]

Shandong Computer Science Center (National Supercomputer Center in Jinan);
Shandong Provincial Key Laboratory of Computer Networks
Qilu University of Technology (Shandong Academy of Sciences)
Jinan, 250014, China
E-mail:[a]`yangshm@sdas.org;` [b]`wanglh@sdas.org`

Dawei Zhao[c]**; Xiaohui Han**[d]**; Shuhui Zhang**[e]

Shandong Computer Science Center (National Supercomputer Center in Jinan)
Shandong Provincial Key Laboratory of Computer Networks
Qilu University of Technology (Shandong Academy of Sciences)
Jinan, 250014, China
E-mail:[c]`zhaodw@sdas.org;` [d]`hanxh@sdas.org;` [e]`zhangshh@sdas.org`

Software definition networking is a revolutionary network architecture, which realizes the separation of the control plane and data plane of a network. While providing the centralized controllability and the software programmability, the network itself is encountering many security problems. In order to solve the problem of security threats in SDN networks, there are different layers of unique security challenges and the relevant research on SDN security problems. This paper introduces the depth learning technology into the field of security threat detection in SDN, and propose a security threat detection framework based on depth learning. The framework is based on the research on model establishment, abnormal behavior recognition and decision algorithm design. The software system based on physical memory analysis is under development in SDN. The system verifies the feasibility of this framework ,and to finally generate the work plan on SDN infrastructure.

ISCC2017
16-17 December 2017
Guangzhou, China

[1]Speaker

[2]This work is supported by the National Natural Science Foundation of China (Grant Nos. 61572297, 61702309, and 61602281), Shandong Provincial Natural Science Foundation of China (Grant Nos.ZR2016YL014, ZR2016YL011, ZR2014FM003, and ZY2015YL018), Shandong Provincial Outstanding Research Award Fund for Young Scientists of China (Grant Nos. BS2015DX006, andBS2014DX007), and Shandong Academy of Sciences Youth Fund Project, China (Grant Nos. 2015QN003).

1. Introduction

With the development of new technologies such as large data and cloud computing, traditional networks confronts with bottlenecks in terms of security, flexibility and scalability. All countries over the world are actively investing on the development of next-generation of internet architecture. The software definition network [1-3] is one of the important directions. In spite of the benefits brought by SDN's technical features in management focus, programmability, and openness, there are also new and unique challenges in terms of security. in terms of security, they also brought new and unique challenges.

1.1 Control-level challenges

Management centralization enables network configuration, and network service access control and network security services are concentrated on SDN controllers. Once the attacker achieves the control on SDN controller, a large amount of network services will be paralyzed, affecting the entire range of the controller. Due to the programmability of SDN network, the importance of SDN controller security is much greater than that of traditional network management system. So the attack and defence around the controller is the most critical node in SDN's own system security.

1.2 Application-level challenges

The controller provides a large number of programmable interfaces to the application layer, which may carry a lot of security threats. For instance, the operation of the application layer which was installed with worms Trojan programs can cause network information stealing,the network configuration change, and network resources being occupied, to name a few. Thus, they affect the reliability and availability of the network, and these interfaces can be utilized to prevent service attacks or network eavesdropping.

1.3 Security risks brought by openness for SDN

Application plug-ins of security and network are entiltled with privileges forrule writing. With the adoption of the complex, multiple applications, there will appear conflicts between the security rules, which will result in network confusion on management, neglecting of security rules, service interruption and so on. Third-party applications or plug-ins may have malicious features, unprotected features, security vulnerabilities and other risks.

A series of corresponding protection strategies are proposed for security risks which may exist in SDN. Security threat detection is the prerequisite and key link of all the strategies. By monitoring the network system and the network running state, the intrusion intention is taken and the corresponding security response is made to improve the security performance of the whole network system. Due to the fact that SDN is still a new technology, its new features such as centralized control and openness make it difficult to adopt the traditional security threat detection technology, and the current research on SDN security threat detection is still insufficient. Therefore, it is urgent to carry out more and deeper research on the SDN security threat detection technology.

2. Related Research

In view of the various security problems existing in SDN, there have been domestic and foreign scholars studied and analyzed the vulnerability of the controller [4-5], the legitimacy and consistency of the flow rules [6-7], the vulnerability of the south interface OpenFlow protocol [8 -9]. In the ITU standard conference, SDN security standards are divided into two categories including security SDN and SDN itself, the relevant researches are as follows:

(1) Texas University and SRI research team conducted a study on the safety of SDN, and proposed a variety of security solutions in 2012. Among these proposals, CloudWatcher [10] is a cloud environment based on SDN control platform to implement security monitoring method. At the same time, FRESCO works as a new development framework for SDN security [11], which quickly implements and deploys multiple common network security features in SDN networks.

(2) In April 2013, Radware Corporation developed a set of software Defense FlowTM [12], which can prevent service attacks, on the basis of SDN technology. It can help network operators to provide automatic DoS and DDoS in the form of pure network services through network programming. This technology makes full use of the data collection function for the controller to detect the traffic distribution, so as to realize the discovery of the attack.

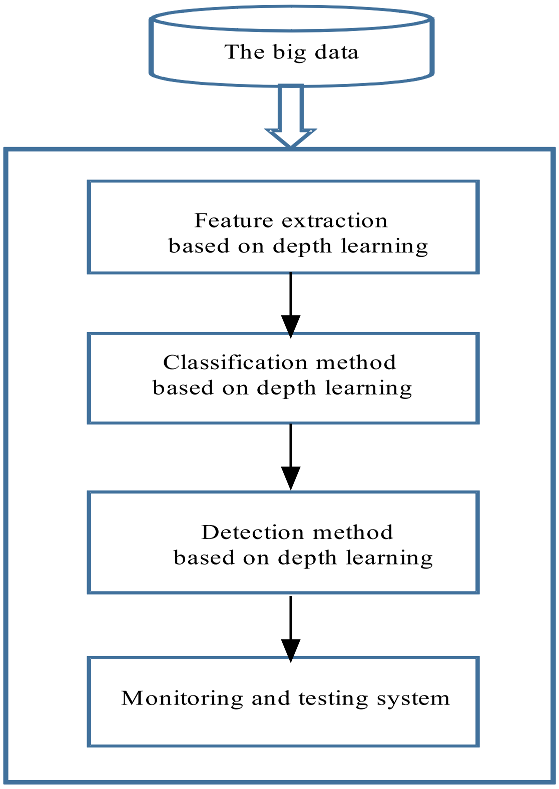
(3) In June 2013, Microsoft announced that its self-developed network streaming aggregation platform (known as distributed Ethernet monitoring, DEMON) based on OpenFlow , which can be used to handle large-scale traffic in Microsoft's cloud network. By using flexible programmable switches and other network devices for the purpose of serving as packet blocking and redirecting platforms, the security team can detect and defend against current common attacks.

(4) In 2013, Kloti et al. [13] designed a threat detection model that could effectively analyse OpenFlow security in conjunction with the STRIDE threat detection model and the attack tree technology solving security threats such as DoS/DDoS attacks in SDN .The [14] describes DoS attack method by OpenFlow detection. [15] proposed a system that achieves network mobility target defence through OpenFlow, which systematically changes the IP address of the internal host to increase the difficulty of external network detection and attack. Up to now, there have been several theoretical research results with respect to the threats and challenges of SDN network security, as well as the application of SDN thinking and architecture in network security [16-19] , with a specific SDN security as the foundation.

There several findings based on domestic and foreign research es: (1) SDN Security threat detection is still in the preliminary research phase, while the effective application of the audit model is missing, which make dynamic detection of security threats more effort consuming. (2) The current SDN network in many third-party developments of commercial applications is not usually open source, which makes the traditional application detection no longer applicable.

3. Security Threat Monitoring Detection Framework for SDN

The framework mainly studies the set-up of security threat identification model, feature extraction and determination detection method, as well as abnormal behaviour recognition model as shown in Figure 1. The specific explanation is as follows:


The big data
Feature extraction based on depth learning
Classification method based on depth learning
Detection method based on depth learning
Monitoring and testing system

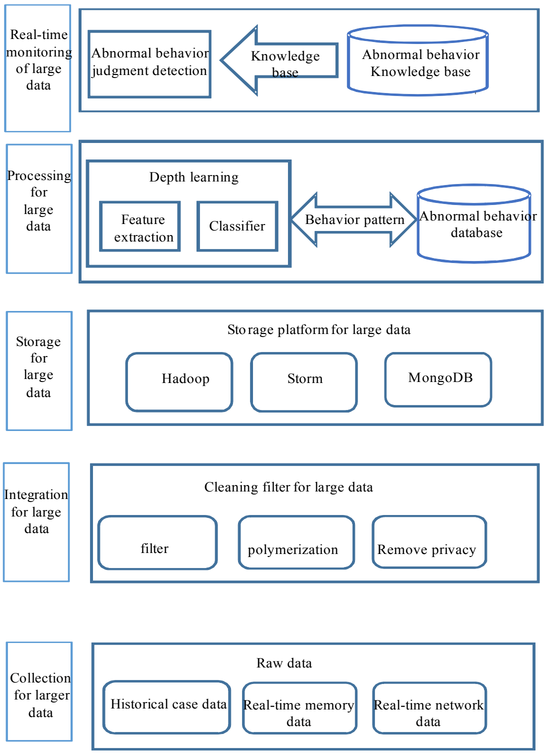

Real-time monitoring of large data
Abnormal behavior judgment detection
Knowledge base
Abnormal behavior Knowledge base
Processing for large data
Depth learning
Feature extraction
Classifier
Behavior pattern
Abnormal behavior database
Storage for large data
Storage platform for large data
Hadoop
Storm
MongoDB
Integration for large data
Cleaning filter for large data
filter
polymerization
Remove privacy
Collection for larger data
Raw data
Historical case data
Real-time memory data
Real-time network data

Figure 1：Technical Route Frame Diagram **Figure 2**：Security Threat Detection Framework

3.1 Security Threat Identification Model for SDN Based on Security Threats Intrusion, Latency and Operational Mechanism

Taking APT as the research object, the module is designed by simulating the user environment, executing the APT code segment, capturing and recording all the behaviours of the APT attack. In the way of auditing the bandwidth occupancy of the application in the network, the APT attack source is found. The model in the SDN network environment is built to guide each aspect of the security threat decision, including feature extraction, classification, judgment, real-time detection of security threats in the system.

3.2 Security Threats Abnormal Behaviour Extraction based on the Depth Learning

The basic idea is: each layer of the network adopts unsupervised methods to learn the characteristics. Based on the last training, the unsupervised learning methods will be applied for training each layer, and the training results are as the input for the next layer. Finally, the module fine-tunes the entire network by the supervision learning methods , to make the model input and output as similar as possible. The main routes are as follows:

3.2.1 Feature Extraction of the Exception Behaviour

The abnormal behavioural characteristics is obtained through a multi-layer neural network in a depth learning architecture. Feature extraction expresses unusual behaviour through some common features, which are derived from large-scale electronic data using deep learning. In particular, the collected electronic data is processed in an unsupervised manner by a deep neural network which is consisted of a layer of noise reduction automatic decoders. As a result, there will be the generation of a stable structure and a regular pattern that together constitute an abnormal behaviour feature. By reducing the amount of noise data, the late abnormal behaviour recognition performance can be more stable. By feature extraction and selection, detection of security threats will be armed with a higher accuracy rate.

3.2.2 Building Signature Library of Abnormal Behaviour with Security Threats

The characteristics of the knowledge base is created by physical memory analysis and unsupervised depth learning. On one hand, the detection system categorizes the abnormal behaviour into the knowledge base in real-time. On the other hand, the knowledge base is incooperated to ensure the accuracy of the detection test.

3.3 Detection Method Based on Depth Learning and Identification Model of Abnormal Behaviour

On the basis of the previous theoretical research, the security threat detection framework which is designed based on the depth learning for SDN is complete. The route is as follows: the data input set is selected from physical memory data, network data, case history data of the server and the host in real-time, then a library of abnormal behaviour features is generated. Through further classification, the normal and abnormal characteristics are determined, finally the detection is completed as shown in Figure 2.

This problem is based on the unsupervised depth learning method, the sample consisting of the real-time data flow from SDN network, the server, the host and its log, and the abnormal behaviour is trained. Different types of data are obtained from distinct layers. From the application plane, runtime log information is received. From the control plane, memory and runtime log information are gained. From the data plane, memory, network packet and runtime log information are generated. Runtime logs and memory and disk information are obtained from the hosts. In this paper, the set of sample sets P = {P1, P2, ..., Pn} is given for $P_i \in P$, the set of behaviour features Fi = {fi1, fi2, ..., fik} is established by the specific feature selection method. A reasonable model M is created: M can determine whether the Pi belongs to the category C ($C \in \{malicious, normal\}$) based on the feature set Fi and minimizes the predicted error rate. The difficulty lies in how to select the feature set Fi which is trained from the SDN sample after deep learning, as well as how to reduce the false positive rate and improve the detection rate by stepwise reasoning. After the first two stages of data processing and optimization, there is low redundancy and the characteristic weight. And then, this part of the data is used as the input for deep learning, and ultimately to identify the categories of security threats by classification.

3.4 Realization of the Prototype System

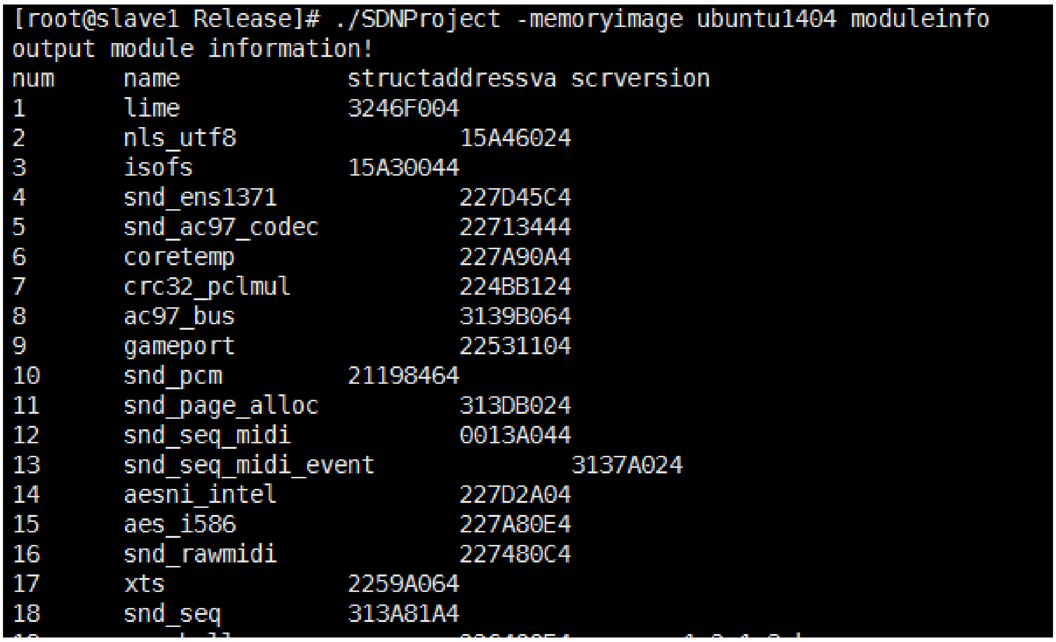
The real-time monitoring system for security threat detection is developed based on depth learning and physical memory analysis. The development of software in this section is divided into two parts:

3.4.1 Depth Learning Model

The big data from SDN is trained by depth learning. The system can dynamically detect real-time security threats without affecting the operation of SDN, which solves the difficulty in security threat identification.

3.4.2 Development of A Security Threat Detection System Based on Physical Memory Analysis

The malicious process, the network information, the hidden dynamic link library, and the injection of dynamic link library are dynamically detected by the physical memory analysis. ApiHook is studied for the purpose of creating the knowledge base for security threats, which is used to determine the abnormal behaviour of SDN. The driver module information is acquired from the physical memory of a server, as shown in Figure 3:



```
[root@slave1 Release]# ./SDNProject -memoryimage ubuntu1404 moduleinfo
output module information!
num     name            structaddressva scrversion
1       lime            3246F004
2       nls_utf8                15A46024
3       isofs           15A30044
4       snd_ens1371             227D45C4
5       snd_ac97_codec          22713444
6       coretemp                227A90A4
7       crc32_pclmul            224BB124
8       ac97_bus                3139B064
9       gameport                22531104
10      snd_pcm         21198464
11      snd_page_alloc          313DB024
12      snd_seq_midi            0013A044
13      snd_seq_midi_event              3137A024
14      aesni_intel             227D2A04
15      aes_i586                227A80E4
16      snd_rawmidi             227480C4
17      xts             2259A064
18      snd_seq         313A81A4
```

Figure 3：A Part of the Module Information by Analysing the Physical Memory of A Server

4. Conclusions and Future Work

This paper mainly discusses the security problems in the software definition network and the current relevant research, in order to introduce a specific framework of SDN security threat detection and the related approaches for monitoring and detection. The next step is to apply the depth learning into the evaluation method and the acquisition of anomaly problem in SDN. Software development of a monitoring system is underway. Meanwhile, the research on data extraction and the depth learning is in progress. Security is an inevitable and essential impact on the development of SDN. Therefore, based on the above research results, the safety of SDN can be strengthened with the theory and technology of monitoring and detection on security threat. It is believed that the research of this topic will inspire more insightful theories and technologies.

References

[1]Open Networking Foundation. *Software-defined Networking:The New Norm for Networks*[S],2012.

[2]Stanford University. *Clean slate program*. 2006. http://cleanslate.stanford.edu/.

[3]McKeown N. *Software-Defined networking. In: Proc. of the INFOCOM Key Note*. 2009. http://infocom2009.ieee-infocom.org/ technicalProgram.htm.

[4]Porras P, Cheung S, Fong M, Skinner K, Yegneswaran V. *Securing the software-defined network control layer*. In:Proc. of the 2015 Annual Network and Distributed System Security Symp. (NDSS 2015). San Diego: Internet Society, 2015. 1-15.

[5]Wang H, Xu L, Gu G. *FloodGuard: A DoS attack prevention extension in software-defined networks*. In: Proc. of the 45th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN 2015). Rio de Janeiro, 2015.

[6]Dai B, Wang HY, Xu G, Yang J. *Opportunities and threats coexist in SDN security*. Application Research of Computers,2014,(8):2254-2262(in Chinese with English abstract).

[7]Lara A, Kolasani A, Ramamurthy B. *Network innovation using OpenFlow: A survey. IEEE Communications Surveys & Tutorials*,2014,16(1):493-512.

[8]Dai B, Wang HY, Xu G, Yang J. *Opportunities and threats coexist in SDN security*. Application Research of Computers, 2014,(8):2254-2262 (in Chinese with English abstract).

[9]Lara A, Kolasani A, Ramamurthy B. *Network innovation using OpenFlow: A survey. IEEE Communications Surveys & Tutorials*,2014,16(1):493-512. [doi: 10.1109/SURV.2013.081313.00105]

[10]SHIN S,GU G. Cloud Watcher:*Network Security Monitoring Using OpenFlowi n Dynamic Cloud Networks* (or:How to Provide Security Monitoring as a Service in Clouds?).[C]//USA:Proc. of the 20th IEEE International Conference on Network Protocols(INCP),2012:1-6.

[11]SHIN S, PORRAS P,YEGNESWARAN V,et al. FRESCO: *Modular Composable Security Sevices for Software-defined Networks*[C] //USA:Proc. of NDSS2012:1-5.

[12]http://safe.it168.com/a2013/0722/1510/000001510885.shtml.

[13]Kloti R, Kotronis V, Smith P. *OpenFlow: A security analysis*. In: Proc. of the 21st IEEE Int'l Conf. on Network Protocols (ICNP). Goettingen, 2013. 1-6. [doi: 10.1109/ICNP.2013.6733671].

[14]BRAGA R,MOTA M,PASSITO P.*Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow*[C] //USA:Proc. of IEEE LCN,2010:408-415.

[15]JAFARIAN J H,AL-SHAER E. DUAN Q. *Open Flow Random Host Mutation: Transparent Moving Target Defence Using Software Defined Networking* [C] // Finland Proc. of HostSDN'12,2012:127-132.

[16] En He, Dezhi Zhang, Ping Hao. *Software definition of network security research* [J]. Communication Technology, 2014 (1): 86-90.

[17]Shuling Wang , Jihan Li, Yunyong Zhang, etc. *SDN architecture and security research* [J]. Telecommunications Science, 2013 (3): 117-122.

[18]Chunmei Guo, Ruhui Zhang, Xueyao Bi. *SDN network technology and its security research* [J]. Information Network Security, 2012 (8): 112-114.

[19]Xinchang Zhang, Yinglong Wang, Jianwei Zhang, Lu Wang,Yanling Zhao, *two-way link loss measurement approach for software-defined networks*, In Proc. IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), pp. 1-10, 2017.