Demo: The Design and Implementation of Intelligent Software Defined Security Framework

Shasha Zhang, Shuyu Song, Fan Yang
Rongpeng Li, Zhifeng Zhao, Honggang Zhang
{21760225,sysong,21760226,lirongpeng,zhaozf,honggangzhang}@zju.edu.cn

ABSTRACT

Software-defined security (SDS) overcomes the limitations of traditional security mechanisms, which brings significant merits for design, deployment and management. However, existing researches are usually limited to some independent algorithms, while not able to apply multiple algorithms to accommodate various types of attack in actual deployment. In this paper, we propose and implement a novel SDS framework, which aims to flexibly deploy a variety of security functions and artificial intelligence (AI) algorithms to automatically learn ongoing threats and proactively protect the network from attacks.

CCS CONCEPTS

• **Networks** → **Network architectures**; *Network security*; Network experimentation.

KEYWORDS

Software Defined Security, Intelligence, Defense, Autodetection

ACM Reference Format:
Shasha Zhang, Shuyu Song, Fan Yang and Rongpeng Li, Zhifeng Zhao, Honggang Zhang. 2019. Demo: The Design and Implementation of Intelligent Software Defined Security Framework. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19), October 21–25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3300061.3343365

1 INTRODUCTION

Software-Defined Networking (SDN) enabled networks have already proven to be successful in various deployment scenarios (Google's backbone network [1], etc.). SDS [2] is a novel network security architecture inspired by SDN. Given the centralized management and global network visibility in SDS, the cooperation between security functions becomes much more flexible and efficient [3].

The implementation of SDS architectures [2][4] generally does not apply AI algorithms to realize automatic security mechanisms but requires manual updating for security policies. Consequently, it is impracticable and cumbersom to defend anonymous attack timely. As one of the most widely used security mechanism, Intrusion Detection Syetem (IDS) has high-grade performance in detecting malicious traffic. However, recent researches [5][6] are limited to some independent AI algorithms, thus being incapable to accommodate various types of attack even in simple deployment scenarios. Moreover, existing network security solutions are dedicated to either wired or wireless networks rather than a heterogeneous case.

To overcome the above shortcomings, we propose the IntelligentSDS, an intelligent and collective software-defined security framework. It integrates a variety of virtual security functions on a cloud computing platform which makes it possible to apply AI algorithms. Taking advantages of AI algorithms, complicated attacks can be detected intelligently in multi-scenarios and corresponding security strategies can be generated automatically. Further, new security policies will be timely delivered to appropriate devices contributing to the software-defined firewall (SDF) built in SDN controller which manages the entire protected network. Last but not least, the access point (AP) is extended to monitor the WLAN as the security agent and accesses the SDN network to achieve protection across the wireless network.

2 DESIGN AND IMPLEMENTATION

2.1 AI-based autodetection and defense system

The framework of IntelligentSDS is divided into three layers, namely the data & intelligence layer, the management & control layer and the security agent layer. Figure 1 depicts the corresponding framework of IntelligentSDS. Based on the proposed framework, we implement an autodetection and defense system which includes an IntelligentSDS cloud, an SDN controller and security agents.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
MobiCom '19, October 21–25, 2019, Los Cabos, Mexico
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6169-9/19/10.
https://doi.org/10.1145/3300061.3343365

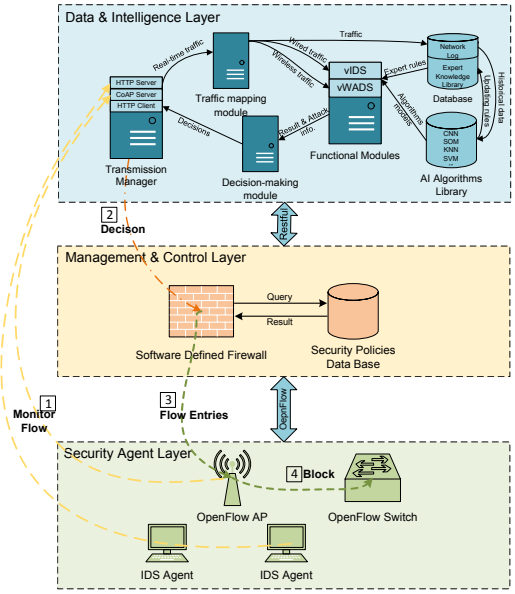

Figure 1: The IntelligentSDS Framework Overview

IntelligentSDS cloud. The IntelligentSDS cloud includes the transmission manager, the traffic mapping module, the decision-making module, the functional module, AI algorithms library, and databases.

- The transmission manager mainly receives network data from agents and transmits data in the form of JSON to the SDN controller through HTTP protocol.
- The traffic mapping module dispatches network data to appropriate security functions in functional module and back up data into the network log database.
- The functional module including virtual intrusion detection system (vIDS) and virtual wireless attack detection (vWADS), respectively analyze wired and wireless data intelligently.
- The decision-making module analyzes the detection result and makes defense decisions which are delivered to SDN controller by transmission manager.
- The database contains the network log database and the expert knowledge library which stores expert rules for detecting anomaly traffic.
- The AI algorithms library stores pre-trained models such as CNN, SVM, SOM, K-means, KNN which are trained by KDD-99 dataset and AWID [7] dataset.

SDN controller. In order to issue decisions generated by the IntelligentSDS cloud efficiently, an SDF application is integrated into the SDN controller which parses decisions to the form of flow entry and issues security policy to OpenFlow (OF) switches and APs.

Security agents. IDS agents and OF APs continuously collect the real-time traffic and report to the IntelligentSDS

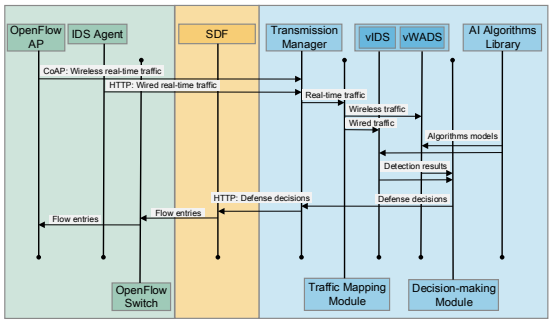

Figure 2: The Sequence Diagram of Autodetection and Defense Procedure

cloud. The IDS agent is composed of a packet sniffing module for capturing network packets and a transmission module for uploading the network traffic through HTTP protocol. Similarly, on the AP, we extend a sniffer to capture wireless environment data, a CoAP client to upload data through CoAP protocol considering the constraint of hardware resources and an Open vSwitch to adapt to OpenFlow protocol.

2.2 Autodetection and Defense Procedure

A typical autodetection and defense procedure includes following steps and releated the sequence diagram is shown in Figure 2:

(1) OF APs and IDS agents upload network traffic to the IntelligentSDS cloud in real time. (2) After receiving data from the security agents, the IntelligentSDS cloud immediately dispatches different virtual security functions to analyze data. When abnormal traffic is detected, the intelligentSDS cloud would forward decisions to the SDN controller immediately. (3) Based on the decision, the SDN controller issues flow entries to underlying related devices. (4) Finally, network devices execute actions to protect from attacks.

3 DEMONSTRATOR

In this section, we provide an evaluation of our IntelligentSDS considering its system performance. Our Demonstrator implementation is shown in Figure 3. We briefly introduce involved experimental devices, setup requirements, and testing process as follows.

3.1 Devices and Setup

The setup includes an SDN Controller, an Intelligence Cloud, an OF Switch, an OF AP, an IDS agent, two hosts playing roles of attacker and victim.

- An OpenStack [8] based intelligence cloud and an OpenDaylight [9] based SDN controller, whose software version is Libery and Boron repectively, are deployed on local lab servers with CPU processor of Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz.

- The CENTEC's Whitebox switch is chosen as the OF switch.
- The OF AP (TP-Link WR842N) is embedded with OpenWrt operating system for futher developing.
- The IDS agent is installed on the victim host.

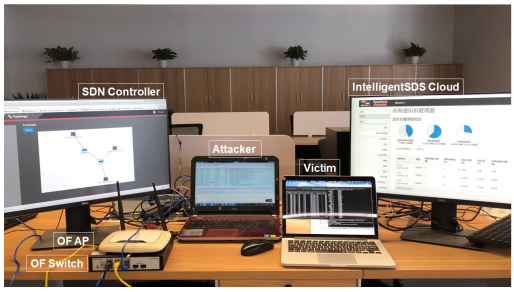

Figure 3: Demonstrator setup consisting of an SDN Controller, an IntelligentSDS Cloud, an OF Switch, an OF AP, a Victim and an attacker

3.2 Experimental Procedure

We simulate attacks and monitor traffic on the protected network.

- **Attack flow simulating:** the attacker launches 3 kinds of DoS flooding attacks (TCP SYN flooding, UDP flooding, and ICMP Ping flooding) to the victim. Among the 3 attack scenarios, the source IP, source port and destination port is randomly generated while the destination IP is fixed.
- **Network monitoring:** the IDS agent captures per 100 network packets to generate one PCAP file and uploads.
- **Local traffic monitoring:** we utilize Wireshark on both attacker host and victim host to monitor the traffic and testify the system effectiveness.

Figure 4 shows the defense latency and effect in terms of confronting real network enviroment attacks. The result illustrates the delay of UDP flood attack is 8s while the delay of TCP flood attack and ICMP flood attack is 20s and 19s respectively. It is obvious that all the attack packets are dropped, which verifies the availibility of our system for network protection.

4 CONCLUSION

In this paper, we present the IntelligentSDS framework leveraging AI algorithms based on traditional SDS framework. By deploying and collaborating AI-based virtual security functions in the IntelligentSDS cloud, our framework efficiently detects novel attacks and continuously updates the expert knowledge library to achieve self-evolution. With centralized control and policy delivery, SDN controller accurately

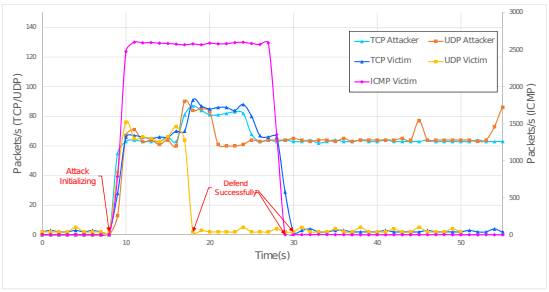

Figure 4: Latency Test of Autodetection and defense

schedules network devices to defend attacks. Overall, the framework accomplishes the procedure from detection to defense automatically and intelligently.

ACKNOWLEDGEMENTS

This work was supported in part by National Key R&D Program of China (No. 2018YFB0803702), National Natural Science Foundation of China (No. 61701439, 61731002), Zhejiang Key Research and Development Plan (No. 2019C01002), the Fundamental Research Funds for the Central Universities. The corresponding authors are Rongpeng Li and Zhifeng Zhao.The authors are with Zhejiang University, Hangzhou, China. Z. Zhao is also with Zhejiang Lab.

REFERENCES

[1] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, et al. B4: Experience with a globally-deployed software defined wan. In *ACM SIGCOMM Computer Communication Review*, volume 43, pages 3–14. ACM, 2013.

[2] Mahmoud Al-Ayyoub, Yaser Jararweh, Elhadj Benkhelifa, Mladen Vouk, Andy Rindos, et al. Sdsecurity: A software defined security experimental framework. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 1871–1876. IEEE, 2015.

[3] Jiaqi Li, Zhifeng Zhao, Rongpeng Li, Honggang Zhang, and Tianhao Zhang. Ai-based two-stage intrusion detection for software defined iot networks. *IEEE Internet of Things Journal*, 2018.

[4] Seung Won Shin, Phillip Porras, Vinod Yegneswara, Martin Fong, Guofei Gu, and Mabry Tyson. Fresco: Modular composable security services for software-defined networks. In *20th Annual Network & Distributed System Security Symposium*. NDSS, 2013.

[5] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. Survey on sdn based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, 12(2):493–501, 2019.

[6] Mohammed A Ambusaidi, Xiangjian He, Priyadarsi Nanda, and Zhiyuan Tan. Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE transactions on computers*, 65(10):2986–2998, 2016.

[7] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Stefanos Gritzalis. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials*, 18(1):184–208, 2016.

[8] OpenStack. Build the future of open infrastructure., 2018.

[9] OpenDaylight. Home - opendaylight, 2018.