2016 Joint International Conference on Economics and Management Engineering (ICEME 2016) and
International Conference on Economics and Business Management (EBM 2016)
ISBN: 978-1-60595-365-6

Implementation of an SDN-based Security Defense Mechanism Against DDoS Attacks

Hsiao-Chung LIN[1,a], Ping WANG[1,b,*]

[1]No.195, Kunda Rd., YongKang Dist., Tainan City 710-03, Taiwan

[a]fordlin@mail.ksu.edu.tw, [b]pingwang@mail.ksu.edu.tw

*Corresponding author

Keywords: Software-defined Networking, DDoS attack, NIDS, OpenFlow.

Abstract. Although mobile devices and IoT devices with an SDN (Software Defined Networking) architecture for cloud appliances have improved the convenience of our daily lives, they also pose a threat to network attacks, including DDoS (distributed denial-of-service) attacks. Consequently, these attacks make their service unavailable to its intended users and cause the improper disclosure or sharing of information. Accordingly, this paper implements an SDN-based information security defense mechanism (ISDM) incorporating three OpenFlow management tools with sFlow standard for network intrusion detection system (NIDS), to perform anomaly detection, mitigation and reduce the loss caused by the DDoS attack. The experimental results proved that the SDN controller enables a defender to response to discover the security threats and develop mitigation strategies for DDoS attacks by using behavioural analysis with logs collecting from Openflow switches.

Introduction

To enhance network security management, Sun Microsystems proposed Software Defined Networking (SDN) concept associated with its architecture in 1995. SDN architectures decouple network control and data forwarding functions, enabling network control to be directly programmable and the underlying infrastructure to be abstracted from applications with an OpenFlow protocol. SDN is a dynamic, manageable, cost-effective, and adaptable architecture suitable for the high-bandwidth, dynamic nature of today's applications. [1]

In smart living appliances, Internet of Things (IoT) devices are connected through a home network to enable control by using a centralised network controller associated with remote network devices from the Internet. When integrated by wireless sensing and information communication technologies for IoT devices, home systems and appliances are advantageous because they can communicate in a collective manner that provides living convenience, health promotion, and safety benefits. In practice, networking manufacturers generally collect personal information and private habits without warning. Because personal information in smart living services cannot be disclosed without legal permission, using private information, including personal IDs, locations, biometrics, and secret data, requires ensuring its security.

In practice, devices in smart homes provide network-layer security and privacy control mechanisms to ensure the privacy and information security of family members by monitoring network activity and detecting suspicious network behaviour. Recently, researchers focus on using SDN as a network-wide control mechanism for resolving high-risk security concerns, including distributed denial of service (DDoS) detection and mitigation [2-3], worm propagation [4], and botnet protection [5].

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Compared to DoS attack, DDoS attack is the most serious attack where the attack source is more than one, often thousands of, unique IP addresses. In the DDoS attack, attackers first select the vulnerable services which will be used to perform the attack target. Generally, attackers exploit the vulnerabilities of the services and insert the hidden code such that the malicious code can be protected from detection. After the attackers have compromised adequate hosts, they use the encrypted communication channels to attack the victims. [6] Most existing approaches for solving the DDoS problem focus on the specific security mechanisms, for example, network intrusion detection system (NIDS) detection, firewall configuration, rather than on the packet routing approaches to defend DDoS threats by new flow management techniques. Accordingly, this paper implements an SDN-based information security defense mechanism (ISDM) incorporating three OpenFlow protocol management tools, Open vSwitch, Ryu SDN Framework, and sFlow-RT toolset to perform traffic management for anomaly detection, react to new types of DDoS attacks in SDN architectures.

DDoS Attack Detection and Migration of Threat Analysis Process

Assume that partial system vulnerabilities of a cloud service are known and a set of behavioural profiles associated with each threat source has been identified. The following adaptive DDoS detection scheme includes a new resolution process of dynamic traffic analysis to track the attack sources of DDoS according to the behavioural profiles of an AS, thereby developing a resolution process of DDoS attacks by using NIDS snort for network defender, in which decision rule is supported by the analysis results from sFlow toolset, as shown in Fig.1. Fig. 1 shows that the penetration testing associated with malware behavioural analysis incorporated in the framework is suitable for DDoS attack detection and migration analysis by using sFlow agent and sFlow-RT to identify the ASs of the DDoS.

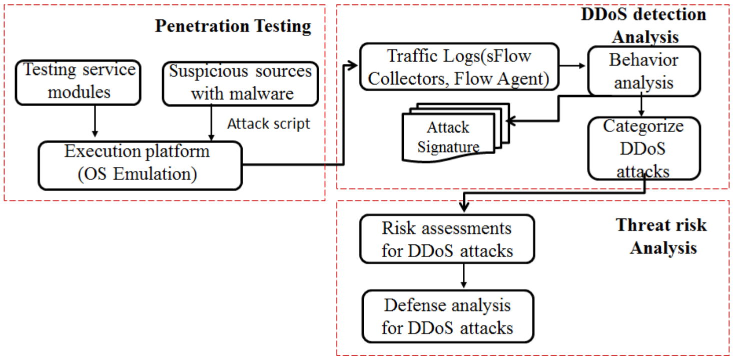

Penetration Testing
Testing service modules
Suspicious sources with malware
Attack script
Execution platform (OS Emulation)
DDoS detection Analysis
Traffic Logs(sFlow Collectors, Flow Agent)
Behavior analysis
Attack Signature
Categorize DDoS attacks
Risk assessments for DDoS attacks
Threat risk Analysis
Defense analysis for DDoS attacks

Figure 1. The resolution process of DDoS detection and migration.

Four subprocesses for detection and migration of a DDoS attacks were shown as follows.

Step 1: Construct an SDN-based Information Security Defense Mechanism

In the proposed SDN system, OpenFlow protocol and switch enables the remote administration of a layer 3 switch's packet forwarding tables by adding, modifying, and removing packet matching rules and actions with two basic components: (1) controller: for determining the network packet flow, and (2) Flow Table: use the OpenFlow routing table to select the network packet transmission path. In further, security managers use OpenFlow enabled switch to collect and analyze traffic information from SDN controller incorporating the sFlow-RT toolset, i.e., sFlow Agent and sFlow Collector.

Step 2: Acquiring Traffic Information

Fig. 2 illustrates, two management tools for OpenFlow are incorporated into the ISDM to form flow statistics for detecting the suspicious behaviour: (1) sFlow Collector, which is used to collect traffic information from Openflow switches for further network traffic analysis; and (2) sFlow Agent, uses as a monitoring tool to manage the SDN control layer for traffic security monitoring by capturing datagrams of the traffic passing through its monitored ports, and sends these samples to the sFlow collector.

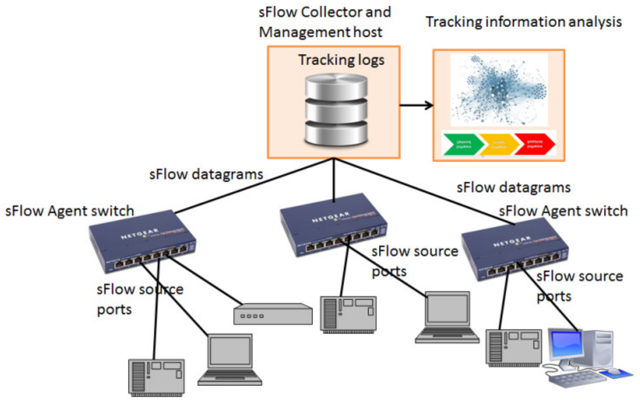


Figure 2. SFlow network analysis for SDN-based appliances.

Step 3: DDoS Attack Detection

As shown in Fig. 3, the execution sequence of exploits represents the signature of a threat source *i* (*i* = 1,...,*m*) and comprises a set of methods used in evaluating the attack signature. When deciding the execution sequence of malicious code, determining the exact pattern of the attack actions is difficult. On the basis of the concept of an intrusion detection system, the occurrence of DDoS attack is solved using frequent episode rules [8] by accumulating and associating the security logs as follows. Generally, episodes are partially ordered sets of events. The frequent episode rule is used to determine the specific event sequences for appropriately determining the malicious instruction sets of a threat source, as shown in Fig. 4.

Given an event sequence $s = (s; T_s; T_e)$ and a window width *win*, let the time window of an episode be given by $w = (w; T_s; T_e)$. The support degree of an episode is defined as the fraction of windows where the episode occurs. Theoretically, given *s* and *win*, the support degree of an episode (α) (i.e., MISs) for a single taint path *j* in *s* is

$$\sup(\alpha) = \frac{|\{\alpha \text{ occurs in } \omega\}|}{|\{W(s,win)\}|}. \tag{1}$$

Once sup(α) is obtained, it can be used to predict the probability of an attack occurrence p_{ij} from a threat source for an information flow *j* from threat source *i*. In other words, sup(α) reveals the connections between attack events in the given security event sequence.

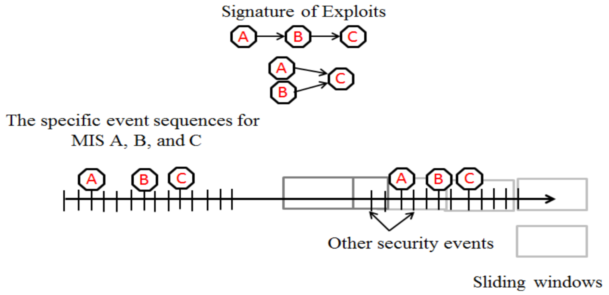


Figure 3. Determine the exact pattern of the threat using sliding windows.

Step 4: Migration of DDoS Attacks

Because of rate-limiting available, traffic filtering is the basis for most defensive approaches. The defense mechanism in our study addresses the resolution of the problem by limiting the amount of traffic sent to target. Providing the characteristics of the traffic are correctly identified, loss of attack can be low. Notably, there is no guarantee that enough packets have been dropped in mostly approaches. In practice, rate-limiting drops packets depending on basis of the exact amount of traffic. On the other hand, filtering technique is done in the IP-layer which does assure that target is not overcome, but part of the legitimate traffic might also be dropped.

Implementation of ISDM on SDN Environments

In the experiment the network intrusion detection for smart home system is constructed using the following four-step procedure as follows.

Step 1: Construct an SDN-based Information Security Defense Mechanism

As Fig. 4 and Table 1 illustrate, Open vSwitch tool assists OpenFlow switches in communicating with each other by using the OpenFlow protocol via a secure channel to connect the SDN controller. In the proposed SDN project, the SDN controller uses a Ryu SDN framework in an Ubuntu operation system to decide the configuration and network packet flow of network devices, such as access control and security monitoring devices.

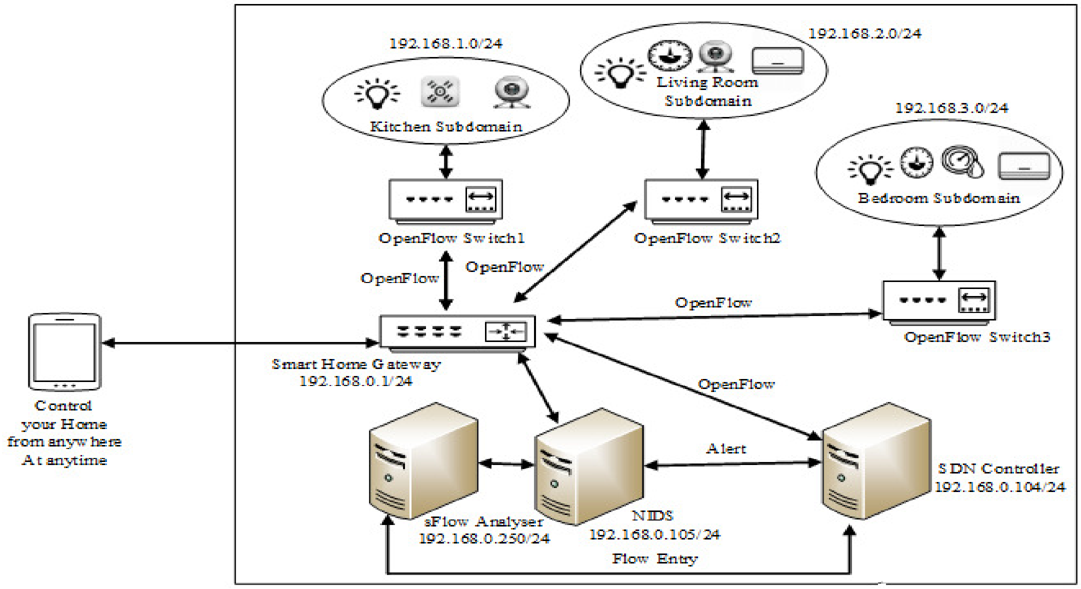
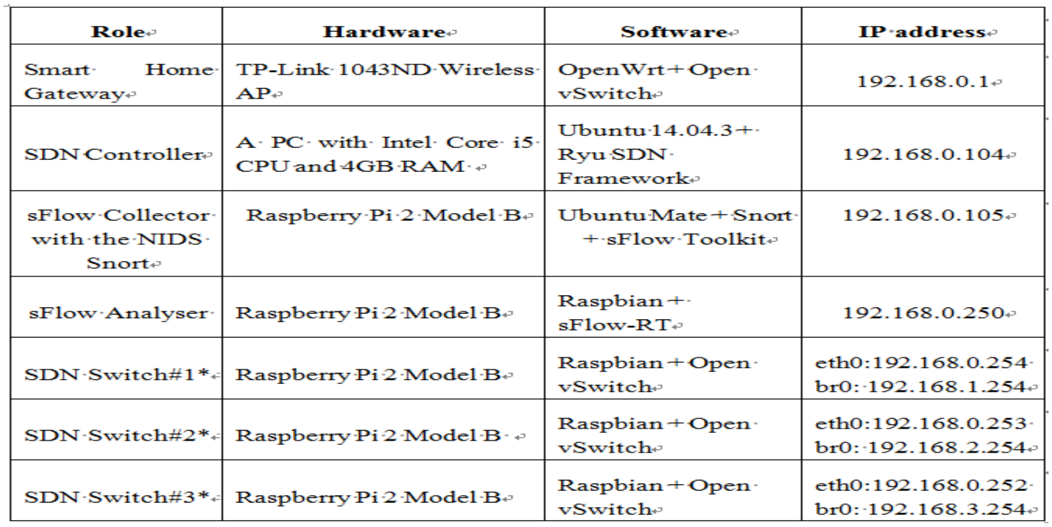


Figure 4. SDN-based smart home security management.

Table 1. Experiment environment.



Role	Hardware	Software	IP address
Smart Home Gateway	TP-Link 1043ND Wireless AP	OpenWrt + Open vSwitch	192.168.0.1
SDN Controller	A PC with Intel Core i5 CPU and 4GB RAM	Ubuntu 14.04.3 + Ryu SDN Framework	192.168.0.104
sFlow Collector with the NIDS Snort	Raspberry Pi 2 Model B	Ubuntu Mate + Snort + sFlow Toolkit	192.168.0.105
sFlow Analyser	Raspberry Pi 2 Model B	Raspbian + sFlow-RT	192.168.0.250
SDN Switch#1*	Raspberry Pi 2 Model B	Raspbian + Open vSwitch	eth0:192.168.0.254 br0: 192.168.1.254
SDN Switch#2*	Raspberry Pi 2 Model B	Raspbian + Open vSwitch	eth0:192.168.0.253 br0: 192.168.2.254
SDN Switch#3*	Raspberry Pi 2 Model B	Raspbian + Open vSwitch	eth0:192.168.0.252 br0: 192.168.3.254

Step 2: Acquiring traffic Information

The experiment uses the Snort to cooperate with a remote sFlow Collector to gather the datagram sent from switches using the following instruction. Deploying the Snort can ensure the rapid identification and resolution of any threat to the network. As the sFlow Collector receives packets, it updates the counters inside the monitoring module on a basis of sliding time-window mechanism. Consequently, this approach may reduce the complexity of the flow collection algorithm, thus requiring less CPU resources.

```
$ sudo snort -T -i eth0 -c /etc/snort/snort.conf
```

Then, both the sFlow datagrams and the Snort alerts were aggregated to be transmitted to the Snort and Ryu SDN Controller for identifying traffic anomaly using the command of sFlow Toolkit.

```
$ sflowtool -t | sudo snort -A unsock -q -r - -c /etc/snort/snort.conf
```

Step 3: DDoS Attack Detection

Step 3.1: Deploy the sFlow Data Collector

sFlow Analyser with sFlow-RT provides visualization and identification of network-wide surveillance of complex multilayer switched and routed environments. sFlow-RT toolkit can assist manager to send information collected to the sFlow-RT using the following instruction:

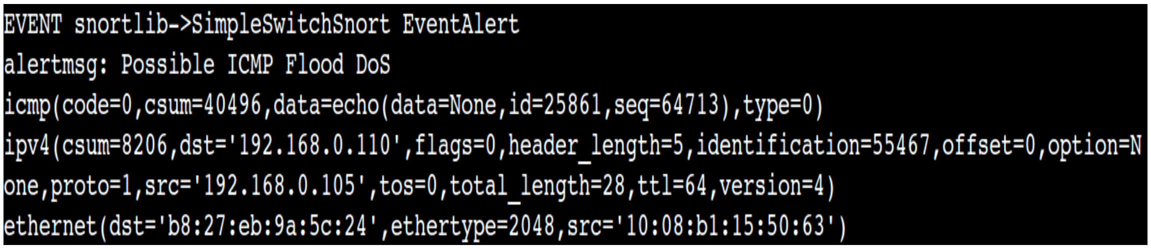
```
$ sudo tcpdump -p -s 0 -w - udp port 6343 | sflowtool -r - -f 192.168.0.250/6343
```

Step 3.2: Detect the DDoS Attack on SDN Environments

Ryu SDN Framework provides the capability of integration with the Snort to communicate with each other. The SDN controller and Snort were installed in distinct hosts the Snort is mostly served as the client, SDN controller as the server. The Snort transmits the security alerts to the SDN controller for further analysis by running pigrelay.py which can download at https://github.com/John-Lin/ pigrelay.

```
$ sudo python pigrelay.py
```

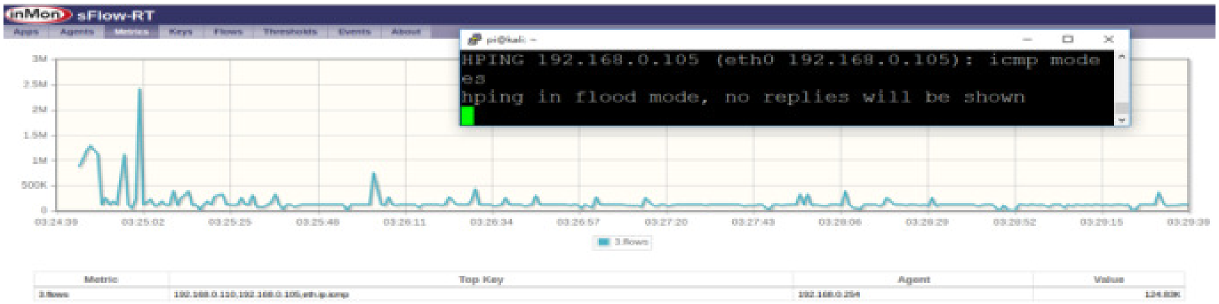
Collect information collection of SFlow and alerts of Snort for ICMP Flood attack and then sent to the SDN controller, as shown in Fig. 5



```
EVENT snortlib->SimpleSwitchSnort EventAlert
alertmsg: Possible ICMP Flood DoS
icmp(code=0,csum=40496,data=echo(data=None,id=25861,seq=64713),type=0)
ipv4(csum=8206,dst='192.168.0.110',flags=0,header_length=5,identification=55467,offset=0,option=N
one,proto=1,src='192.168.0.105',tos=0,total_length=28,ttl=64,version=4)
ethernet(dst='b8:27:eb:9a:5c:24',ethertype=2048,src='10:08:b1:15:50:63')
```

Figure 5. Alert messages of Snort for ICMP Flood attack.

Use visualization function of sFlow-RT to examine traffic information during ICMP Flood attack, as shown in Fig. 6.



```
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode
es
hping in flood mode, no replies will be shown
```

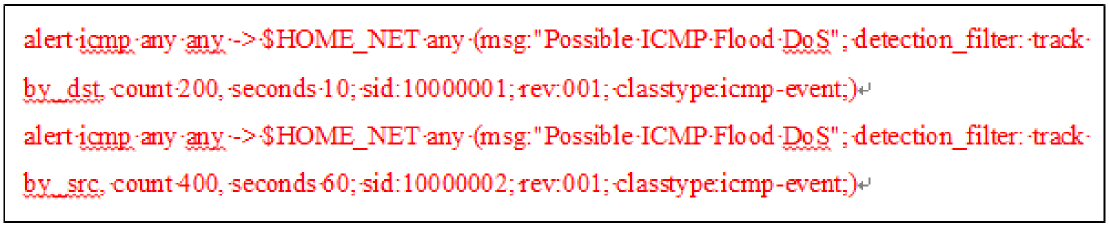
Metric	Top Key	Agent	Value
3.flows	192.168.0.110,192.168.0.105,eth.ip.icmp	192.168.0.254	124.83K

Figure 6. Traffic information of ICMP Flood attack.

Step 4: Migration of DDoS Attacks

An example for DDoS attack detection and mitigation by using ICMP Flood is discussed. To identify ICMP Flood attack, manager sets up the detection rules in Snort as shown in Fig.7:

```
$ sudo nano /etc/snort/rules/local.rules
```



```
alert icmp any any -> $HOME_NET any (msg:"Possible ICMP Flood DoS"; detection_filter: track
by_dst, count 200, seconds 10; sid:10000001; rev:001; classtype:icmp-event;)
alert icmp any any -> $HOME_NET any (msg:"Possible ICMP Flood DoS"; detection_filter: track
by_src, count 400, seconds 60; sid:10000002; rev:001; classtype:icmp-event;)
```

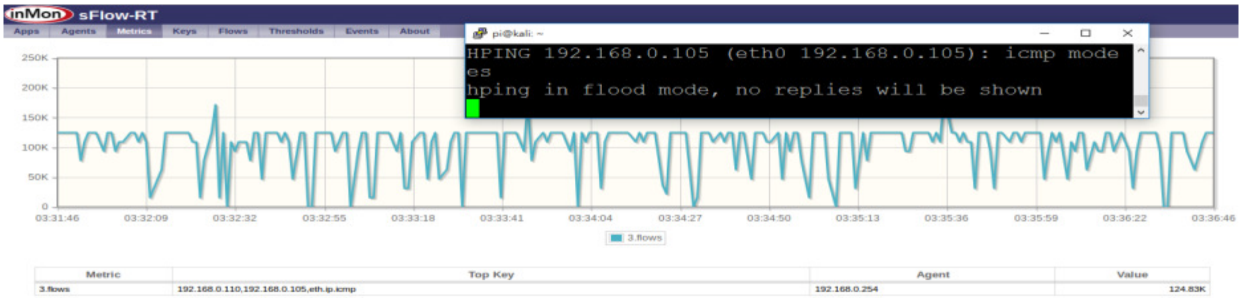
Figure 7. Set up two detection rules in Snort.

Use Hping3 to simulate ICMP Flood attack in the offense host for verifying the effectiveness of the information gathering of the sFlow and alert sending of the Snort.

```
$ hping3 --icmp --flood 192.168.0.105
```

To against ICMP Flood attack, the SDN controller sends the following commands to OpenFlow switch for dropping datagrams, when the flow information entering. It shows that the flood traffic has reduced after a period of time, as shown in Fig. 8.

```
$ curl -X POST -d '{"dpid":"963371335886", "priority":"32765",
"actions":[{"type":"DROP"}],"match":{"eth_type":0x0800,"ip_proto":"1", "ipv4_src": "0.0.0.0/0",
"ipv4_dst":"192.168.0.0/24"}}' http://192.168.0.104:8080/stats/flowentry/add
```



```
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode
es
hping in flood mode, no replies will be shown
```

Metric	Top Key	Agent	Value
3.flows	192.168.0.110,192.168.0.105,eth.ip.icmp	192.168.0.254	124.83K

Figure 8. Migration of ICMP Flood attack.

Conclusion

The experiment results show that SDN controller can screen out suspicious IP addresses associated with domain names by creating a blacklist suggested by analysis outcomes from ISDM. In further, the real-time update of detection rules determined by attack signatures in our model can be used as an effective intrusion detection mechanism to discover suspicious network connections based on anomaly behavior analysis in the Snort.

Acknowledgement

This work was supported jointly by the Ministry of Science and Technology of Taiwan under Grant Nos. MOST 104-2627- E-168-001 and MOST 104-2410-H-168-001.

References

[1] Open Networking Foundation, Software-defined networking: The new norm for networks, ONF White Paper, April 13, 2012.

[2] R. Braga, E. Mota and A. Passito. Lightweight DDoS flooding attack detection using NOX/OpenFlow. IEEE 35th Conf. on Local Computer Networks, 2010 pp.408–415.

[3] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras and V. Maglaris, Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments, Computer Networks 62 (2014) 122–136.

[4] R. Jin and B. Wang, Malware detection for mobile devices using software-defined networking. Research and Educational Experiment Workshop, 81-88, 2013.

[5] N. Feamster, Outsourcing home network security. In Proceedings of the 2010 ACM SIGCOMM workshop on Home networks, 2010, pp.37–42.

[6] S. Lin, T. C. Chiueh, A Survey on solutions to distributed denial of service attacks, Technical report, Department of Computer Science, Stony Brook University (2013).

[7] H. Mannila, H. Toivonen, and I.A. Verkamo, Discovery of frequent episodes in event sequences, Data Mining and Knowledge Discovery 1(3) (1997) 259-289.