Poster: A Secure control plane with Dynamic Multi-NOS for SDN

Zhenping Lu, Fucai Chen, Jiangxing Wu, Guozhen Cheng
National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, China
Email: 13203728376@163.com

***Abstract*—Vulnerabilities and backdoors in NOS (Network operating system) allow malicious actors to disrupt network or hijack NOS. The current work proposes a NOS architecture called secure control plane (SCP) that enhances security through a rotation of hetergeneous and multiple NOSs.Theory analysis proves validity and availability of the SCP and its more effective security performance over traditional architectures.**

I. INTRODUCTION

Software defined network (SDN) introduce separation of data and control planes to achieve highly programmable switch infrastructures [1]. This new concept indicates the application of network operating system (NOS) (i.e.control plane) that determines the actions of all forwarding components in the network. NOS is responsible for processing and distributing data flows between application and data plane. As critical components in SDN, they also interact with switches within their network domain or slice. Therefore, security of NOS is of importance to network operation and service guarantee.

In current architectures of control plane, the mapping of NOSs to data plane is stable, which enables attackers to probe without time limits under such circumstance. Clearly, adopting multiple controllers is an effective method to alleviate this issue. Recently. ONOS [2] employ master and backup controllers to operate network. Wang et al. [3] attempt to deal with load imbalance among controllers via dynamic controller assignment, which achieves satisying performance. In [4], Eldefrawy propose a prototype SDN controller to tolerate Byzantine faults in both the control and data planes. This design can handle single point of compromise and failure to construct resilient programmable networks. However, backdoors can be preset when devising NOSs and bugs are bound to exist no matter how perfectly a NOS is designed. Hence, it is certain that NOSs will be exploited eventually as long as sufficient time is owned by attackers. Due to the critical function of NOS, the influence is significant once they are hijacked.

In this paper, we propose a SCP which associates with various and hetergeneous NOSs to address hijacking NOS in figure.1. SCP is a novel NOS architecture migrating multiple NOSs, while ensuring that the system is available for legitimate users. Here, the surface of attack opportunities decreases and the cost of an attack increases. Further, even if an attacker succeeds in finding a vulnerability at one point, it may not be effective at other times because of the dynamic-scheduling mechanism, thus making control plane more secure. That is to say, vulnerabilities of NOS can be mitigated effectively under this architecture.

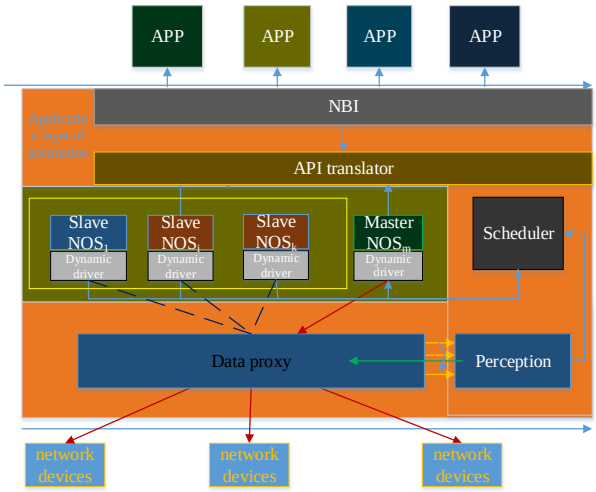


Fig 1. The overview of SCP

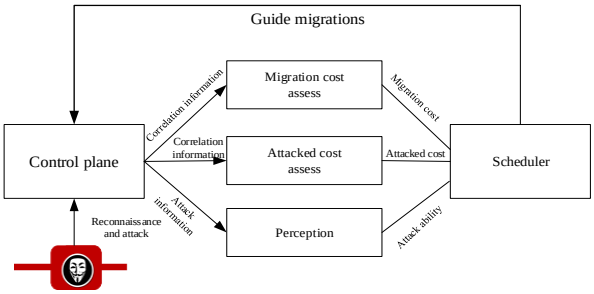


Fig 2. WorkFlow of the SCP framework

II. DESIGN

A.Architecture

We extend the control layer of SDN to assist the deployment of virtual functions in SCP, The constitution and functions of each plane are described below:

Data Plane and Application Plane: They are identical to that in existing SDNs.

Control Plane: Instead of deploying one NOS, it consists a set of hetergeneous NOS which can be “moved around” by scheduler. Master manages the whole network, while others are alternative set. Futhermore, to enhance the level of security, controllers are deployed on diverse hosts with different operation systems (Ubuntu, CentOS, etc.) through docker.

And it consists of three virtual function modules: Data proxy, Perception, and Scheduler whose functions are depicted as follows.

- **Scheduler**：Its chief duty is selecting NOSs for the network. In general, it picks randomly one (called Master) from N NOSs and manages the data plane as described in Fig.1. And there are two mechanisms under which the scheduler may switch Master NOS. One is timer mechanism indicating that the scheduler will re-select a new Master NOS at fixed intervals. The other is that only when an alert or a notification message arrives at the scheduler does it execute the formal actions. Lastly, the scheduler will notify the control plane to make adaptations.

- **Perception**： The main goal of perception is monitoring network state and detecting abnormity. For example, it will analyze the link data to inspect whether the link has suddenly become congested compared to historical records. Also, it perceives the changes of service latency and throughput of the network and determines whether network performance declines abruptly. If detection results exceed the pre-defined threshold, the perception will consider the network running unhealthily. Subsequently, an alert message will be sent to the scheduler.

- **Data proxy**: Its primary purpose is to gather network information including state, port information of switches, etc. Then collected information will be transmitted to all NOSs. On receiving messages, some NOSs merely update corresponding data while Master is required to generate instructions（eg.packet out） relying on the messages. And the role assigned to each NOS is guided by the scheduler.

B.Workflow

First, the data proxy collects the information of data plane and delivers them to control plane. The perception claps eyes on anomaly detection at the same time. The scheduler selects Master NOS which sends the valid instructions to network devices. Then, once any mechanism of the scheduler is activated, new Master will be elected. And if perception tells anomaly to scheduler, the scheduler will shut down the corresponding Master and pick the new Master from executive resource next time. Otherwise, there is no extra adjustment needed to be done. Finally, above actions will repeat to keep the control plane in a secure, robust and resilient state.

III. EVALUATION

Now, a dynamic-scheduling method based on BSG (Bayesian Stackelberg Games) is put forward to maxize security reward of NOS during each migration.We present the experimental results related to generation of optimal strategies of the defender, the performance of the DOBSS based MIQP method, and the gain in the reward values for the defender compared to the case where a random strategy and pure strategy are adopted.

Table 1: Results of strategy

Migration patterns	**Reward**
BSG	-0.62
Random strategy	-1.45
Pure strategy	-5.15

First, we show the results obtained when a working example as input. The optimal mixed strategy obtained is:0.3,0.16,0.27,0.27 respectively for the four NOSs available for the control plane and the corresponding optimal reward value is -0.62 whereas the reward value when using a uniform mixed strategy (0.25 for each NOS) is −1.45,pure strategy is -5.15. Since we considered negative reward values for losing positions and positive for winning positions, clearly using BSGs leads to winning strategies for the control plane whereas a uniform mixed strategy and a pure strategy could be losing ones.

IV. CONCLUSIONS

Security of NOS is a crucial issue for ensuring effective SDN management. Focusing on the hijacking NOS attack, we propose SCP which develops a dynamic heterogeneous redundant architecture to prevent that threat proactively. And theory analysis proves validity of this method. Furthermore, the defending concept that combines heterogeneity, dynamism and redundancy of existing means and elements can be applied in sundry occasions.

REFERENCES

[1] Ahmad I, Namal S, and Ylianttila M, et al. Security in Software Defined Networks: A Survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4):1-1.

[2] Pankaj, N., Matteo, G., Jonathan, H., et al.: ‘ONOS: towards an open, distributed SDN OS’. HotSDN, 2014, pp. 1–6.

[3] Wang, T., Liu, F., Guo, J., et al.: ‘Dynamic SDN controller assignment in data center networks: stable matching with transfers’. Proc. of INFOCOM, 2016

[4] Eldefrawy, K., and Kaczmarek, T.: ‘Byzantine fault tolerant software defined network (SDN) controllers’. IEEE Computer Society Int. Conf. on Computers, Software and Applications, 2016.

[5] Kreutz D,Ramos F M V,and Verissimo P. Towards secure and dependable software-defined networks[C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined NETWORKING. 2013:55-60..

A Secure control plane with Dynamic Multi-NOS for SDN

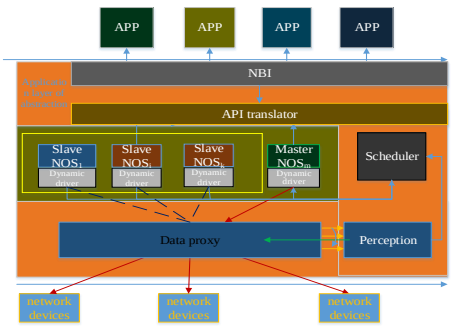
Zhenping Lu, Fucai Chen, Jiangxing Wu, Guozhen Cheng

Background

- As critical components in SDN, security of NOS is of importance to network operation and service guarantee.
- Backdoors can be preset when devising NOSs.
- Bugs are bound to exist no matter how perfectly a NOS is designed.

How to defense?

SCP Architecture



- **SCP** is a novel NOS architecture migrating multiple NOSs, while ensuring the system is available for legitimate users.
- **Data Plane and Application Plane** are identical to that in existing SDNs.
- Three virtual function modules: **Data proxy, Perception, and Scheduler**.

Perception

Monitoring network state and detecting abnormity.

① If detection results exceed the pre-defined threshold. the perception will consider the network running unhealthily.

② Subsequently, an alert message will be sent to the scheduler.

Data proxy

- Gathering network information.
- Transmit collected information to all controllers.

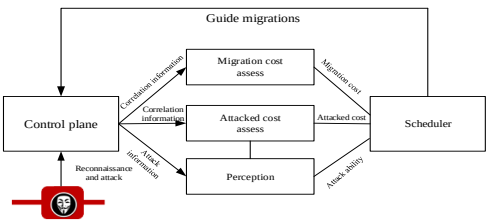
➢ Some NOSs merely update corresponding data while Master is required to generate instructions.

Scheduler

Two mechanisms:

- One is timer mechanism indicating the scheduler will re-select a new Master at fixed intervals.
- The other is that only when an alert or a notification message arrives at the scheduler does it execute the formal actions.

Workflow



1. Data proxy collects the information of data plane and delivers them to controllers.
2. Perception claps eyes on anomaly detection at the same time. Scheduler selects Master NOS which sends the valid instructions to switches.
3. If perception reports anomaly to scheduler, the scheduler will shut down the corresponding Master and pick the new Master from executive resource next time.

Evaluation

Migration patterns	Reward
BSG	-0.62
random strategy	-1.45
pure strategy	-5.15

➢ First, we show the results obtained when a working example as input. Since we considered negative reward values for losing positions and positive for winning positions, clearly using BSGs leads to winning strategies for the control plane whereas a uniform mixed strategy and a pure strategy could be losing ones.

Summary

- **SCP** develops a dynamic heterogeneous redundant architecture to prevent that threat proactively. And theory analysis proves validity of this method. Furthermore, the defending concept that combines heterogeneity, dynamism and redundancy of existing means and elements can be applied in sundry occasions.

For more information, please contact 2011301200300@whu.edu.cn