

A Secure control plane with Dynamic Multi-NOS for SDN

Zhenping Lu, Fucai Chen, Jiangxing Wu, Guozhen Cheng

Background

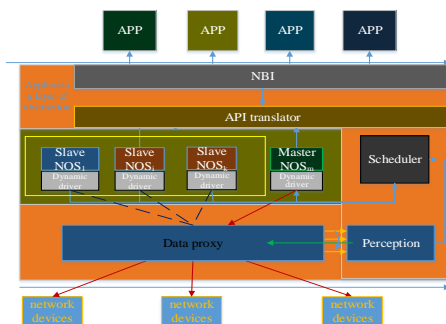
- As critical components in SDN, security of NOS is of importance to network operation and service guarantee.
- Backdoors can be preset when devising NOSs.
- Bugs are bound to exist no matter how perfectly a NOS is designed.



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 abnormality.

- ① If detection results exceed the pre-defined threshold. the perception will consider the network running unhealthy.
- ② Subsequently, an alert message will be sent to the scheduler.

Data proxy

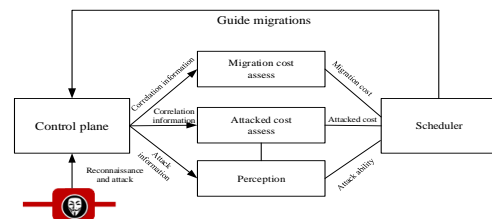
- Gathering network information.
 - Transmit collected information to all controllers.
- Some NOSs merely update corresponding data while Master is required to generate instructions.

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