Analyze Security Threats in Software Defined Network

Research question: Study the impact of topology-related attacks in Software Defined Network

TU Delft Delft University of Technology

Author: Darius Cristian Ivascu
Supervisor: Dr. Chhagan Lal
Responsible Professor: Mauro Conti

1. Background

- Software Defined Network (SDN) as can be seen in Fig. 1 is a new network paradigm
- It aims to solve the verticality problem of the existing network
- Proposes a separation between the programmable data plane and the control center
- Benefits: better scalability, improved network management, and cost saving

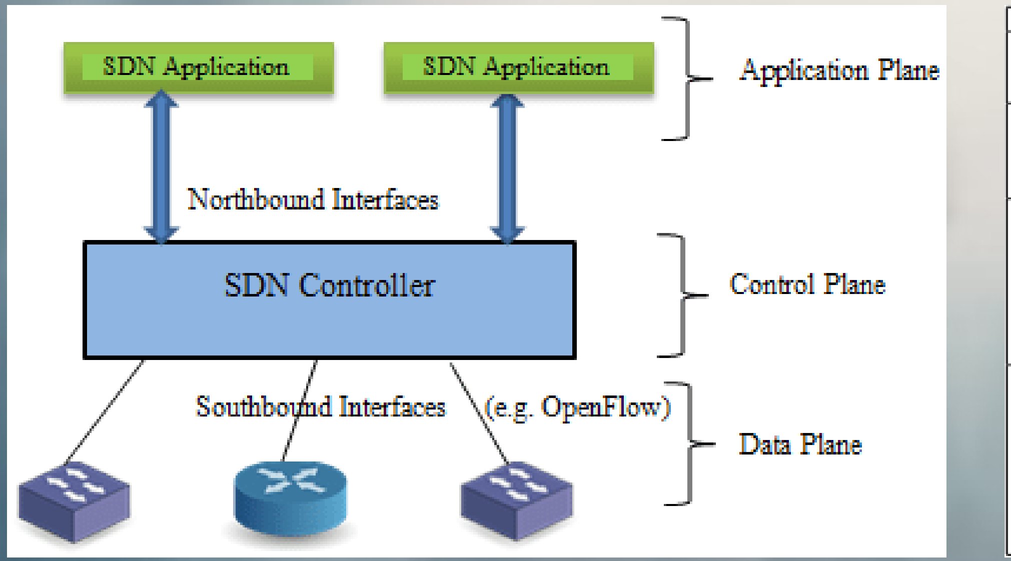
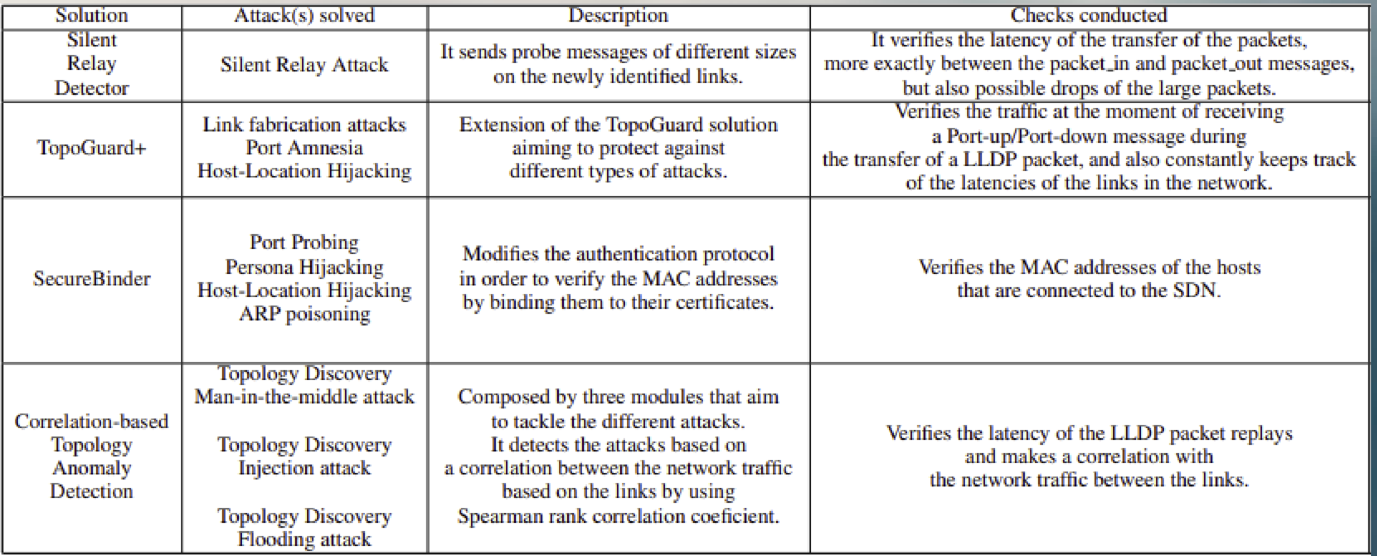


Fig. 1: Overview of the SDN architecture[1]



Solution	Attack(s) solved	Description	Checks conducted
Silent Relay Detector	Silent Relay Attack	It sends probe messages of different sizes on the newly identified links.	It verifies the latency of the transfer of the packets, more exactly between the packet_in and packet_out messages, but also possible drops of the large packets.
TopoGuard+	Link fabrication attacks Port Amnesia Host-Location Hijacking	Extension of the TopoGuard solution aiming to protect against different types of attacks.	Verifies the traffic at the moment of receiving a Port-up/Port-down message during the transfer of a LLDP packet, and also constantly keeps track of the latencies of the links in the network.
SecureBinder	Port Probing Persona Hijacking Host-Location Hijacking ARP poisoning	Modifies the authentication protocol in order to verify the MAC addresses by binding them to their certificates.	Verifies the MAC addresses of the hosts that are connected to the SDN.
Correlation-based Topology Anomaly Detection	Topology Discovery Man-in-the-middle attack Topology Discovery Injection attack Topology Discovery Flooding attack	Composed by three modules that aim to tackle the different attacks. It detects the attacks based on a correlation between the network traffic based on the links by using Spearman rank correlation coeficient.	Verifies the latency of the LLDP packet replays and makes a correlation with the network traffic between the links.

Table 1: Overview of the discussed solutions

2. Topology attacks

- There are multiple types of attacks that can be launched on an SDN to poison its topology
- Topology attacks (e.g. Fig. 2) are poisoning the controller with a fake overview of the structure of the network
- They can influence the reliability of the whole network by disturbing the topology discovery protocol by inserting fake links in the network

3. Method

- Identify and investigate the latest literature available on the subject
- Compare the different types of topology attacks and the proposed solutions
- Suggest the design of possible improvements

4. Discussion solutions

- The identified solutions in the state-of-the-art (Table 1) are proposing a response to the different types of attacks that are threatening the security of the SDN's topology
- Some of these solutions are not considered to be completely secure according to the latest research conducted
- Each solution aims to protect against the different types of topology attacks by conducting different checks on the network system

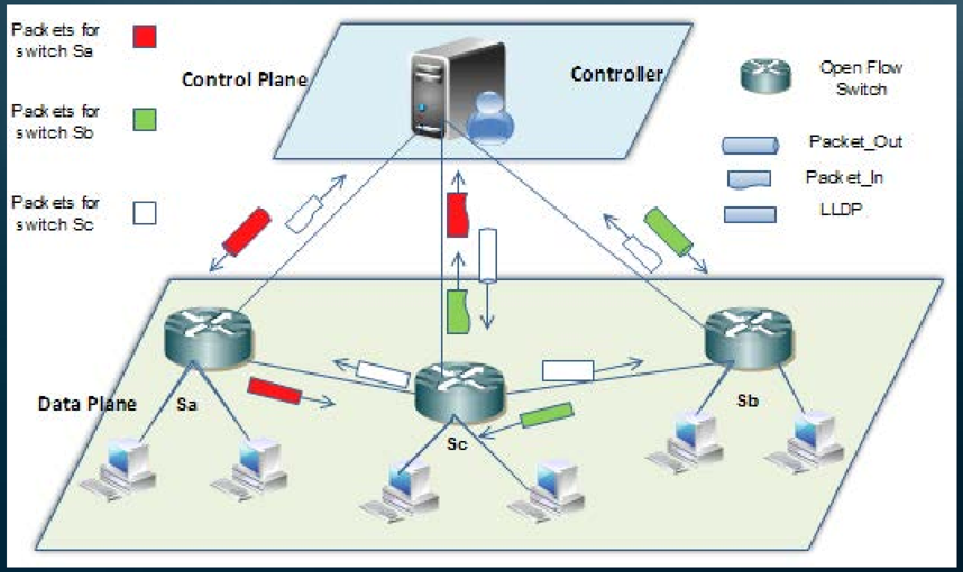


Fig. 2: Example of the impact of a topology attack on a SDN[2]

5. Future directions

- Further research on the impact of the Silent Relay Detector on the topology discovery process and possible improvements
- Verify the possibility to upgrade the switches' simple CPUs to overcome the processing limitations of the current ones used in the SDN
- Find a way to remove the old MAC tags used by TopoGuard+ in order to prevent the reusability of those tags
- Research the impact on the memory consumed by the network if the list of bindings used by SecureBinder is extended to contain the location of the connection of the host
- A partnership between the developers of TopoGuard+ and Securebinder to develop a more universal solution

References

[1] S. Mittal, Performance Evaluation of Openflow SDN Controllers, pp. 913–923. 03 2018.
[2] N. Kaur, A. K. Singh, N. Kumar, and S. Srivastava, "Performance impact of topology poisoning attack in sdn and its countermeasure," Proceedings of the 10th International Conference on Security of Information and Networks, 2017.

All the background information, attacks, and solutions presented in the poster are referenced in the paper.