TOPOLOGICAL SECURE ROUTING PATHS IN SOFTWARE SWITCHED NETWORKS

G. SURESH
Assistant Professor, CSE Dept., KMIT,
Narayanaguda, Telangana

Abstract— *Software-Switched Networks (SSN) decouples the control plane and the data plane in network switches and routers, which enables the rapid innovation and optimization of routing and switching configurations. However, traditional routing mechanisms in SSN, based on the Dijkstra shortest path, do not take the capacity of nodes into account, which may lead to network congestion. Moreover, security resource utilization in SSN is inefficient and is not addressed by existing routing algorithms. Here proposed a Topological Routing, a reliable security- oriented SSN routing mechanism, which considers the capabilities of SSN switch nodes combined with a Network Security Virtualization framework.*

This scheme employs the distributed network security devices effectively to ensure analysis of abnormal traffic and malicious node isolation. Furthermore, Topological Routing supports dynamic routing reconfiguration according to the latest network status. Here prototyped Topological Routing and conducted theoretical analysis and performance evaluation.

Keywords— Software-Switched Networks (SSN), Topological Routing, Dijkstra shortest path routing.

1. INTRODUCTION

Software-Switched Networks (SSN) is a typical centralized network architecture for managing and operating networks. It facilitates network management and eases the burden of solving networking problems via the logically centralized control offered by a controller [1]. SSN decouples the control layer from the data layer and provides new ways for the dynamic control and management of packet forwarding and processing in switches.

In SSN, a centralized controller defines network behaviors and configures network devices via a set of policies, which control where network traffic flows, e.g., whether or when network traffic should go through a particular security device. Therefore, the network intelligence in SSN is logically centralized in the controllers, while the devices in the infrastructure layer are simple packet-forwarding devices.

Many security modules, devices, and middle- boxes are employed to improve the security of SSN networks. Although these security resources can provide many security benefits to SSN networks, they may not be deployed in the physical locations that can best meet the diverse and increasing security demands of different users. SSN offers the opportunity to use security resources in a network flexibly. For example, a new concept of Network Security Virtualization (NSV) is presented which uses SSN technology to virtualize security functions and resources to network administrators/users and thus improve the utilization of existing security devices [2].

However, NSV does not consider network capacity when virtualizing security resources in the network, which introduces unexpected network loads. If the load exceeds the network capacity near a security device, this results in congestion and denial of service.

Proposed Topological Routing, a reliable security-oriented routing mechanism, which enables the SSN controller to make full use of security resources and ensures the reliability of established routing paths. Topological Routing provides a weighted shortest- path routing algorithm, in which the weighting is derived from the network nodes' capabilities, including the network and security capabilities.

Topological Routing supports adaptive routing path reconfiguration when the controller perceives practical congestion caused by attack events or other network accidents in the established paths [3].

Here prototyped an approach and deployed Topological Routing on a POX controller. Extended an existing Application Layer and POX controller with Topological Routing modules. Evaluated the effectiveness and performance of Topological Routing and demonstrated its effectiveness [4].

In summary the following are contributions in this paper, proposed a reliable security-oriented SSN routing mechanism, Topological Routing, according to the capabilities of SSN switch nodes combined with an NSV framework. This scheme effectively employed the distributed network security devices to ensure analysis of abnormal traffic and malicious node isolation. Furthermore, Topological Routing supports dynamic routing reconfiguration according to the latest network status.

Ddeveloped a reliable security-oriented routing algorithm. The proposed algorithm takes the network and security capabilities of network switches as inputs, and makes use of the k-shortest path algorithm to ensure minimum cost to the network when establishing a routing path. This algorithm offers a good balance of efficiency, availability, reliability, and security [5].

Finally, implemented a prototype of Topological Routing, and evaluate its performance. The results demonstrate that the approach can optimally use the existing security devices and mechanisms in SSN, and effectively ensure the abnormal flow isolation with dynamic routing path reconfiguration. proposed reliable security-oriented routing scheme.

2. RELIABLE SECURITY-ORIENTED ROUTING

In this section, presented the reliable security-oriented routing scheme.

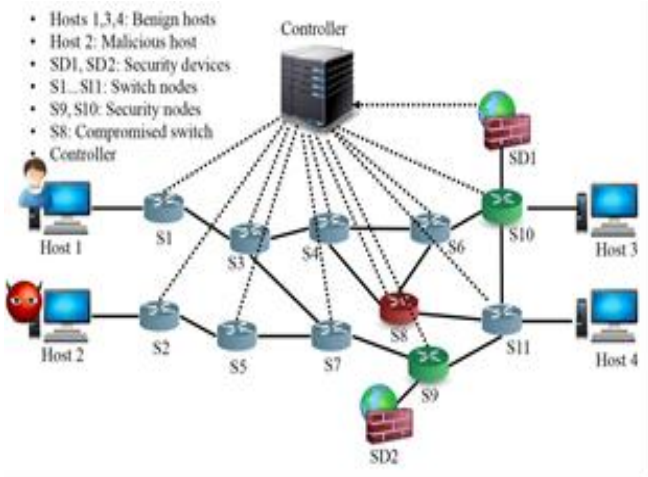

Figure.1: Overall topology

The SSN network topology is shown in Figure. 2 and consists of three types of entities: Controller, Hosts, and Switches. Hosts 1, 3, and 4 are benign hosts and Host 2 is a malicious client. The nodes S1→ S11 are switch nodes. Switch nodes equipped with security resources (e.g., firewall or IDS) are called security nodes, e.g., S9 and S10 in Figure.1, which are equipped with security devices SD1 and SD2, respectively [6].

2.1 Network capability

Presents a novel model for constructing secure routing paths through security entities and nodes with high capabilities in SSN. This will improve the security of data delivery in SSN and prevent adversaries from launching attacks through malicious or non-trusted node selection.

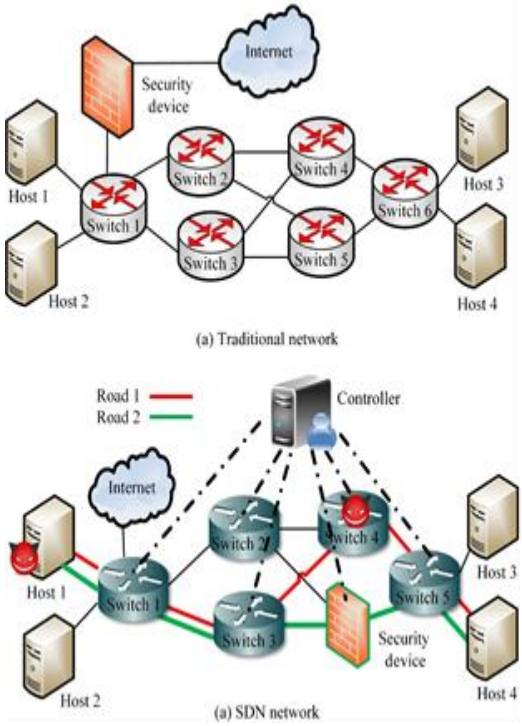

Figure. 2: Routing path construction in SSN and traditional networks.

The method of constructing secure routing paths is significantly different in SSN compared with traditional networks. As illustrated in Figure. 2a, the security policies in traditional networks are enforced by physically forcing traffic to flow through a certain device (e.g., an intrusion detection system, or a firewall). However, SSN topology is virtual. As illustrated in Figure. 2b, the logically centralized controller in SSN provides a high- level view of the whole network to control programs. This means that the controller has a strong ability to control network flow and can deploy security policies generated by corresponding applications to switches [7].

Therefore, the architecture of SSN makes it more flexible to control if and when the network traffic goes through a security device.

For example, in an SSN network, as illustrated in Figure. 2b, if Host 1, which is controlled by an attacker, wants to visit Host 4 for a malicious service, Host 1 should first send its request to the nearest switch. As switch 1 is unable to find a flow rule/policy to respond to the request that requires rerouting, it reports this request to the SSN controller as a Packet-In message. With centralized control of the SSN controller, the routing application that communicates with it can build a global view of the topology of all the switches connected to the controller [8].

Then, the controller runs a routing algorithm, based on the current topology information, to compute a new route from the source to the destination, and pushes a route update to the involved switches for future communication between Hosts 1 and 4.

Then, if the green road (Road 2) in Figure. 2b is pushed to these involved switches, once the compromised Host 1 is detected by the security device deployed in this road, Host 1 is immediately isolated. However, if the red road (Road 1) in Figure. 2b is pushed, as there is no filtering or security protection in this road, Host 4 would be attacked.

Routing rules/policies in SSN, which are assigned by the controller to switches, control where and when traffic flow goes through a certain device. If the controller does not consider the network and security capabilities of the nodes in the SSN

network, it cannot find the optimal routing paths that match the reliability and security requirements of the users.

With increasing security demands, more and more nodes need to be deployed in the already complicated SSN networks. Thus, the centralized controller is required to push more security polices when constructing routing paths, which makes constructing secure routing paths in SSN more and more error-prone and challenging.

3. TOPOLOGICAL ROUTING

In this section, presented the system design of the security-oriented routing path mechanism, Topological Routing, which resides in the SSN controller. In this system, Topological Routing timely monitors the status of network resources in the SSN, thereby perceiving the network and security capabilities of the network nodes. Topological Routing calculates the security-oriented routing paths based on the transmission and security requirements specified by users and the network nodes' capabilities.

Benefiting from the network resource virtualization infrastructure, Topological Routing ensures that the established routing path satisfies the network security and reliability requirements effectively. If there is any abnormal traffic detected by the network security resources deployed in the selected routing path, Topological Routing will react in a timely manner according to the security policies and dynamically reconfigure the routing paths [9].

3.1 Overall architecture

As shown in Figure. 3, Topological Routing extends regular controllers with four additional modules [10]:

(1) Policy Parser

(2) Resource Status Monitor

(3) Routing Rule Generator

(4) Incident Reactor.

Policy Parser: This module is an interface that mediates a set of high-level security requirements into the corresponding security policies. For example, if the security requirement of a user in SSN specifies that all network packets from Host 1 to port 80 of Host 2 should be blocked, then the Policy Parser module translates this security requirement into a corresponding security policy that the Routing Rule Generator module can accept when constructing routing paths.

As illustrated in Figure. 3, if SD2 (security device) just has a rule to block network packets from Host 1 to port 80 of Host 2, then SD2 would be selected as the necessary passing security device when the Routing Rule Generator constructs the secure routing paths from Host 1 to Host 2.

Resource Status Monitor: As the status of nodes and the bandwidth in SSN is dynamic and time-sensitive, the Resource Status Monitor module periodically collects the status of switch nodes, bandwidth, and security devices in the network, and stores this information in the Capability Value database. The information collected by this module is critical metrics/input data for the Routing Rule Generator module to construct an optimal routing path that meets the security requirements of a user.

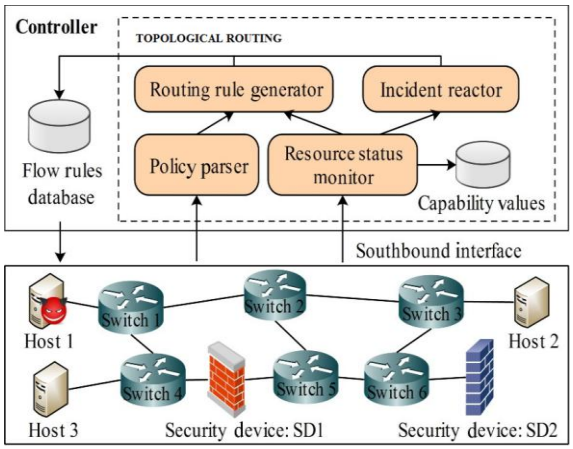

Figure. 3: Conceptual architecture of Topological Routing

Routing Rule Generator: The Network Capability based Routing Algorithm and the Security-oriented Routing and Dynamic Reconfiguration Algorithm run in this module. This module constructs routing paths based on the latest status of the nodes and the various security needs of users in SSN. Specifically, based on the realtime security requirements of a user in SSN, this module outputs the max-capacity path from the source node to the destination node satisfying the security requirements.

Incident Reactor: This module creates response strategies corresponding to the security policies, e.g., isolating the malicious node/host that creates abnormal traffic, dropping the malicious packets, etc. Meanwhile, the Resource Status Monitor module updates the capability status of the network resource and the SSN controller reconfigures the routing paths according to the outputs of the Routing Rule Generator module.

3.2 Typical operations of Topological Routing

In this subsection, used Figure. 4 to illustrate typical operations of Topological Routing.

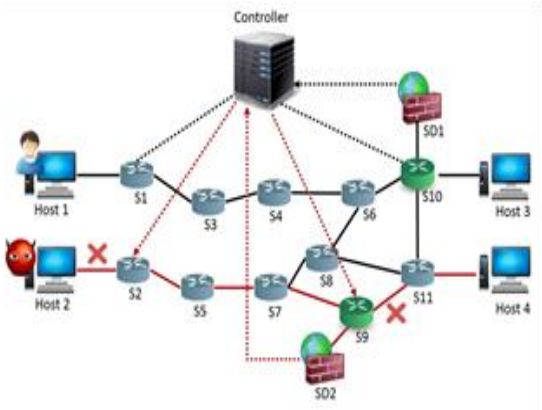

Figure. 4: Secure routing path establishment and security response.

Security-oriented routing path construction. When a user applies for a secure routing path from its host node Host 1 to a destination node Host 3, Host 1 should first send its request to the nearest switch S1. Then, S1 sends a routing establishment request to the controller. The Policy Parser module creates the corresponding reliability and security policies according to the capability and security requirements included in the routing request sent by Host1. The Resource Status Monitor module timely collects the capability status of the network resources. The Routing Rule Generator module calculates and outputs routing/flow rules according to the polices and capability status of the network resources using the Security-oriented Routing and Dynamic Reconfiguration Algorithm. The controller assigns the secure routing flow rules to the switch nodes included in the routing path, and establishes the required route ensuring the security and reliability requirements simultaneously.

Security Response and Reconfiguration. Once there is malicious traffic (such as the red-line shown in Figure. 4) inspected by a security node (e.g., S9), the security node will inform the controller. The Incident Reactor module

creates the response strategies corresponding to the security policies, e.g., isolating the malicious node/host (e.g., Host 2) that creates the abnormal traffic, dropping the malicious packets, etc. Meanwhile, the Resource Status Monitor module updates the capability status of the network resources and the controller reconfigures the routing paths according to the output of the Routing Rule Generator module.

4. CONCLUSION

Here proposed a Topological Routing Network, a new mechanism based on NSV, which dynamically establishes reliable secure-oriented routing paths in SSN, and aggregates switch node capabilities. Topological Routing takes the nodes network and security capabilities as critical metrics, thus ensuring the establishment of a reliable routing path and enforcing malicious traffic detection, isolation, and dynamic routing reconfiguration. Prototyped the approach and the experiment results demonstrate that Topological Routing supports robust secure routing path establishment and effectively utilizes the existing security devices distributed in SSN. Performance of Topological Routing can be improved in the future work, and aim to deploy it to distributed controllers to improve control plane scalability.

REFERENCES

[1] *N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks", SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008.*

[2] *M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh, N. McKeown, and S. Shenker, "SANE: A protection architecture for enterprise networks", in 15th USENIX Security Symposium, USENIX Association, 2006, pp. 1– 15.*

[3] *D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky and S. Uhlig, "Software defined networking: A comprehensive survey", Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015.*

[4] *B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka and T. Turletti, "A survey of software-defined networking: Past, present and future of programmable networks", IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617–1634, 2014.*

[5] *X. Li, H. Wu, D. Gruenbacher, C. Scoglio, and T. Anjali, "Efficient routing for middle box policy enforcement in software defined networking", Computer Networks, vol. 110, pp. 243–252, 2016.*

[6] *S. Shin, L. Xu and S. Hong, "Enhancing network security through Software Defined Networking (SDN)", in Proceedings of 25th International Conference on Computer Communication and Networks (ICCCN'16), Waikoloa, HI, USA, 2016.*

[7] *S. Shin, V. Yegneswaran, P. Porras and G. Gu, "Avant- guard: Scalable and vigilant switch flow management in software-defined networks", in 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS13, Berlin, Germany, 2013, pp. 413–424.*

[8] *P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran, "Securing the software-defined network control layer", in Proceedings of 2015 Annual Network and Distributed System Security Symposium, NDSS15, San Diego, CA, USA, 2015, pp. 1–15.*

[9] *P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for openflow networks", in Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN12, Helsinki, Finland, 2012, pp. 121–126.*

[10] *S. Hong, L. Xu, H. Wang and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures", in Proceedings of 2015 Annual Network and Distributed System Security Symposium, NDSS15, San Diego, CA, USA, 2015.*