위치 신뢰도를 이용한 복원력 강한 네트워크 제공 방안

뉘엔반퀴엣, 뉘엔신응억, 김경백
전남대학교 전자컴퓨터공학부
quyetict@utehy.edu.vn, sinhngoc.nguyen@gmail.com, kyungbaekkim@jnu.ac.kr

Enabling Resilient Network Provisioning by using Location-Trustiness

Van-Quyet Nguyen, Sinh-Ngoc Nguyen, Kyungbaek Kim
Dept. Electronics and Computer Engineering, Chonnam National University

요 약

Software-Defined Networking (SDN) is promised to be the future of Internet, which not only provides detail information of underlay routers, but also makes a decision for controlling the network based on its current global view. However, in the case of unexpected nature disasters; such as earthquakes or typhoons; happen, the network would face many challenges like links and devices failures. Therefore, how to provide a resilient network in disaster situations is particularly evident for network provisioning. In this paper, we propose a novel approach, location-trustiness based reliable SDN, to enable resilient network provisioning. The trustiness of location could be estimated based on disaster information. We then apply location-trustiness to calculate the trust value of the network elements (e.g., links, switches). Finally, these trust values; instead of the hop count; are used as the metrics in network routing, which the path with higher trust value would be chosen. To evaluate the feasibility of location-trustiness based approach, we simulate the responses to the network which is affected by a disaster event. The results prove that our approach reduces significantly the time of recovering the network compare to the baseline method.

I. Introduction

In recent years, network services' trend of service-oriented demands call for more flexible and resilient network provisioning. Resilience is the ability of a network to provide and maintain an acceptable level of service in the face of various challenges to normal operations such as link or switch failures. There are several researchers have been studied on disaster resilient networks [1][2]. To deal with link failures, there are two main approaches proposed including network restoration [1] and network protection [2]. For the network restoration approach, when a switch detects a link failure, it will send a packet-in messages to the controller to notify about the status of failed link. Once the controller receives that packet, it would compute new routes based on the actual status of the network and write an alternative flow entry into the related switches by sending packet-out messages. This approach may take a long latency for recovering all the affected flows. For the network protection approach relying on the backup resources, the controller computes multiple paths for each flow and pre-installs the flow entries into the related switches. Whenever a link is detected in failure status, the switch will forward directly the affected flows to an alternative path without waiting for the packet-out from the controller. However, this approach may fail to deal with many broken switches whose backup resources also are corrupted.

Recently, SDN has received much attention, because it provides centralized network management which not only focuses on data plane functions but also control plane functionality. The controller introduced in SDN provides detail information of underlay routers and makes a decision based on the global view of the current network. Hence, SDN is enabled to deal with some network problems such as links/devices failures or links congestion by reconfiguring the network to restore or maintain network connectivity for all links/devices.

The resiliency of the SDN network can be improved by pre-configuring backup links in the switches [3]. The authors proposed algorithms to improve this resiliency by maximizing the possibility of fast failover which we achieve through resilience-aware controller placement and control-traffic routing in the network. In [4], the authors proposed a SDN based architecture to enhance the reliability of network against disaster failures. To do this, they designed algorithms for geographic-based backup topologies generation and splicing. But, in the case of the network affected by disaster events, this work could not evaluate the impact of events to affected region. In this paper, we propose a novel approach, location-trustiness based reliable SDN, to enable resilient network provisioning.

II. Methodology

In this section, we present our method of enabling resilient network provisioning by using location-trustiness. Before we take into account the idea, there are some terms we need to consider. First, the term a *location-trustiness* is used to indicate the impact of disaster events on a location, which is a real number in the range [0.0,1.0]. Thus, if the location-trustiness equals 0, it means this location may be seriously affected by disaster (no trust); meanwhile, if the location-trustiness equals 1, so this location may be not affected (full trust). The location-trustiness could be obtained by estimating based on multimodal information as presented in our previous work [5]. Similarly, the trustiness of link/switch is a real number in the range [0.0,1.0] which indicates the likelihood of link/switch failure (down).

The basic idea of our approach is to calculate trust value of links in the network by using location-trustiness. We then propose an algorithm to find out top k paths between every end-to-end pair in order by trust value. Here, a path contains at least one link, and its trust value is determined by the minimum trust value from a set of links belong to that path. Finally, we use SDN controller to set the selected paths to the SDN switches in SDN data plane.

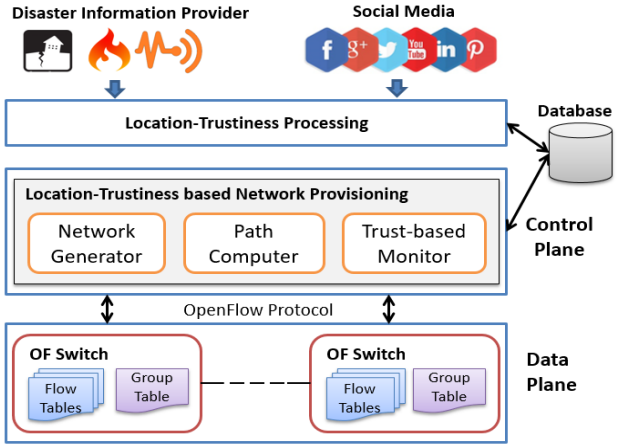

Fig. 1. Overview of system design

For network provisioning, our design is based on SDN architecture which typically composes of *Control Panel* and *Data Panel* including OpenFlow (OF) Switches as shown in Fig.1. We build a *Location-Trustiness based Network Provisioning* module which consists of three components: *Trust-based Monitor*, *Topology Discover*, and *Path Computer*. First, *Trust-based Monitor* component periodically read the trust value of links from the database. Whenever these values changed, they would be noticed to *Path Computer* module to compute multiple paths for each end-to-end pair. Once paths computing is finished, a new network topology could be created, and its information will be used by the *Network Generator* module to establish flow entries and group entries, then be sent to related OF switches via OpenFlow protocol. As a result, a new resilient network could be made, which could maintain an acceptable level of service in the challenges of normal operations such as link or switch failure.

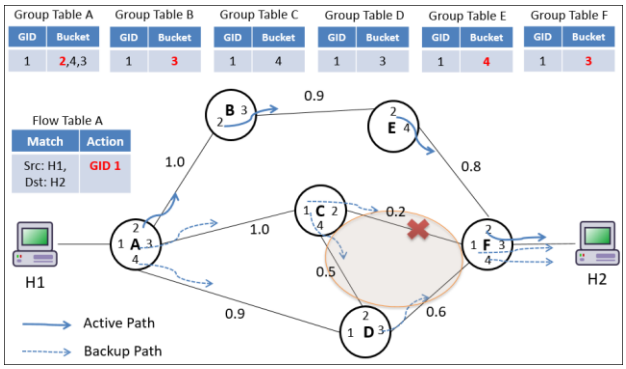

Fig. 2. Example of Location-Trustiness based Network Recovery

Fig. 2 illustrates an example of using location-trustiness for the fast failover as a case study of resilient network provisioning. Here, we assume that there is a mesh network topology, whose switch having a few ports. We consider the flows from host H1 to host H2. Without considering about trust value of the links, it is not difficult to find that <ACF> could be an active path since it has the lowest number of hops from H1 to H2. We assume that a disaster happened, and it made link <CF> down, and the links <CD> and <DF> are in the affected region. Typically, the link <ADF> could be chosen as an alternation path. However, our method use location-trustiness, in which each link is assigned a trust value. In the case of disaster happened, the affected links <CF>, <CD>, and <DF> are calculated and assigned with low trust value 0.2, 0.5, and 0.6, respectively. In this case, the path <ABEF> is set to be an active path, and two backup paths in order of priority are <ADF> and <ACDF>.

III. Evaluation

We used Mininet tool to simulate a network with 40 nodes and 128 links. We installed OpenDayLight as the controller. In additional, we set up randomly the delay value of each link between two nodes from 1 to 20 milliseconds to make a different throughput for each path. We used Iperf to measure the throughput and recovery time of the network when disasters occur. We simulated baseline method, which supports fast failover mechanism using network parameters and our method in the case study of location-trustiness based network recovery.

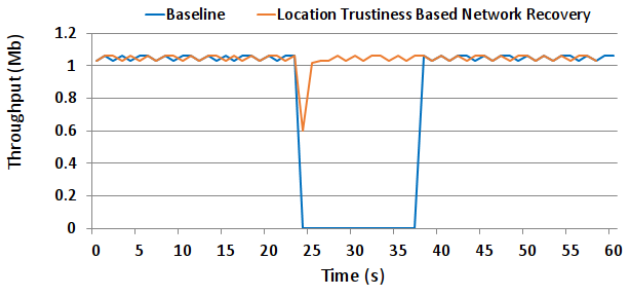

Fig. 2. Efficient of location-trustiness based network recovery

As the result illustrated in Fig. 2, the baseline draws the throughput lower than our method. Also, it saves time to recover the network connectivity when disasters happen. It could be seen that our method recover the connectivity of network at second 23 instead of second 37 in the baseline method.

IV. Conclusion

In this paper, we proposed a novel approach, location-trustiness based reliable SDN, to enable resilient network provisioning. We apply location-trustiness to calculate the trust value of the network elements. Then, these trust values, instead of using number of hop, are used as the metrics in network routing, which a path with higher trust value would be chosen. The experimental results showed that our approach outperforms baseline method.

Acknowledgment

This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2016-0-00314) supervised by the IITP(Institute for Information & communications Technology Promotion). This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2017R1A2B4012559)

References

[1] Sharma, Sachin, et al. "Enabling fast failure recovery in OpenFlow networks." Design of Reliable Communication Networks (DRCN), 2011 8th International Workshop on the. IEEE, 2011.

[2] Sgambelluri, Andrea, et al. "OpenFlow-based segment protection in Ethernet networks." Journal of Optical Communications and Networking 5.9 (2013): 1066-1075.

[3] Beheshti, Neda, and Ying Zhang. "Fast failover for control traffic in software-defined networks." Global Communications Conference (GLOBECOM), 2012 IEEE. IEEE, 2012.

[4] Xie, An, et al. "Designing a disaster-resilient network with software defined networking." Quality of Service (IWQoS), 2014 IEEE 22nd International Symposium of. IEEE, 2014.

[5] Nguyen-Van, Quyet, and Kyungbaek Kim. "Study on Location Trustiness based on Multimodal Information.". In Proceedings of the 4th International Conference on Smart Media and Applications (SMA), January 11-12, 2016, Danang, Vietnam.