Enabling Disaster-Resilient SDN with Location Trustiness

Van-Quyet Nguyen, Sinh Ngoc Nguyen, Kyungbaek Kim
Dept. Electronics and Computer Engineering
Chonnam National University
Gwanjgu, South Korea
E-mail : quyetict@utehy.edu.vn, sinhngoc.nguyen@gmail.com, kyungbaekkim@jnu.ac.kr

***Abstract*— Software-Defined Networking (SDN) is promised as future of Internet which provides centralized network management. It provides detail information of underlay routers and makes a decision based on the global view of the current network. However, in the case of occurring unexpected natural disasters such as earthquakes or typhoons, the network infrastructure faces many challenges such as links and devices failures. Therefore, how to recover the network quickly under disaster situations is particularly essential for reliable SDN. In this paper, we propose a novel approach to enable disaster resilient SDN networks with location trustiness. We first present a method for calculating the trustiness of a location based on multimodal information including earthquake events and disaster sensor data. Then, we design a system to support disaster resilient SDN based on location-trustiness. To evaluate the feasibility of the proposed system, we simulate the responses to the network which affected by earthquake events. The results show that our approach reduces the recovering time significantly.**

Keywords*— *Trustiness of Location; Geographical Failure; Disaster Events; Multimodal Information; Fast Failover

I. INTRODUCTION

Recently, SDN has received much attention. The SDN controller provides detail information of underlay routers and makes a decision based on the global view of the current network via an open API, OpenFlow [1]. SDN enables to deal with some network problems such as links/devices failures or links congestion by providing flexible software network applications which reconfigure the network to restore or maintain network connectivity for all links/devices.

There were several studies on disaster resilient SDN networks [2][3][4]. To deal with link failures, there are two main approaches such as network restoration [2] and network protection [3][4]. For the network restoration approach, when a switch detects a link failure, it will send a packet-in message (OFP_PACKET_IN) to the controller for notifying the status of link failures. Once the controller received this packet-in message, it computes new routes based on the current status of the network, and writes an alternative flow entry into the related switches by sending packet-out messages (OFP_PACKET_OUT). This approach may take a long latency for recovering all the affected flows. For the network protection approach that relies 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 as 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 not be applicable when many switches are failed, in which the backup resources are also corrupted along with the primary ones. That is, it is essential to choose right backup resources for enabling reliable SDN.

In this paper, we focused on how to choose right backup resources by using location trustiness which is calculated from multimodal information such as disaster events and environmental sensor data. That is, our approach forecasts the trustiness of network links and devices based on previous and current multimodal data, and choose better backup resources which expedites network failover process.

Our work makes the following contributions:

- Firstly, we proposed a novel approach for calculating trustiness of location based on multimodal of disaster information including earthquake events and disaster sensor data.
- Secondly, we designed a system for supporting a disaster resilient SDN with location trustiness. In this system, a SDN controller application annotate the trustiness of links and nodes by using location trustiness.
- Finally, we deployed the proposed approach on OpenDayLight controller [6] and evaluated the performance via emulations on Mininet [7]. The results show that our approach reduce the time for recovering the network under disaster events.

The rest of this paper is organized as follows. Section II presents how to calculate location trustiness based on multimodal disaster information. In Section III, we describe our design of a system supporting disaster resilient SDN with location trustiness. Next, we evaluate our system in Section IV. Finally, Section V concludes the paper and discusses the future work.

II. LOCATION TRUSTINESS

In this section, we present an approach to calculate location trustiness by using multimodal of disaster information. First, we define a geo-mapping matrix (GMM), then calculate the impact of disaster event on each affected cell of GMM as the trustiness of the corresponding cell.

A GMM is defined by a matrix which covers a specific region with a set of locations $L = [L_{i,j}]_{nxm}$, where each location $L_{i,j}$ is a square with size equals *c* x *c,* and *c* can be a real number describing the length by kilometer. For each $L_{i,j}$, the corresponding location trustiness $T_{i,j}$ is assigned. The location trustiness is a real number in the range from 0.0 to 1.0 which indicates the likelihood that this area is stable under disaster events. That is, if location trustiness close to 1, the corresponding location is highly resilient to the disaster.

A. Location Trustiness from Disaster Event Information

Our approach for calculating location trustiness based on earthquake information is as follows: (1) find Possible Region Affected (cells) on the GMM where earthquake event e_i happened and (2) calculate location trustiness for those cells. Note that, the current location trustiness calculated based both of current disaster event and historical disaster events that affected to the same cell on the GMM.

To find Possible Region Affected (PRA), we used an equation in our previous work [5]. It shows the relationship between moment magnitude and surface rupture length of an earthquake event as follows:

$$L_R = 10^{0.862069*M - 4.37931} \qquad (1)$$

where M is the magnitude ($M \geq 5.7$) and L_R is the surface rupture length of the earthquake. Thus, the size of PRA is K×K, with K is the minimum number of odd integer satisfying $K \geq L_R/c$. In our approach, the impact of an earthquake is decreasing linearly with the distance from the epicenter to a location. We formulate the influence of an earthquake e at each cell in PRA as follows:

$$T_a = \begin{cases} 1 - \frac{M}{\rho} & if\ a = 1 \\ T_{a-1} + \frac{M}{\rho * R} & if\ a \geq 1 \end{cases} \qquad (2)$$

where a is an integers number that shows the distance by cells from epicenter cell (a=1) to R on the GMM, R is an integers number and $R = K/2 + 1$.

In practice, a location $L_{i,j}$ can be affected by a set of earthquake events **e** = {e$_1$, e$_2$, .., e$_n$}. Thus, before the current earthquake event e$_n$ happened, $L_{i,j}$ has a trust value $T_{i,j}^{e_{n-1}}$. To calculate $T_{i,j}^{e^n}$, our approach considers the previous trust value as follows :

$$T_{i,j}^{e_n} = \frac{n-1}{n} T_{i,j}^{e_{n-1}} + \frac{1}{n} t_{i,j}^{e_n} \qquad (3)$$

where $t_{i,j}^{e_n}$ is the trust value at the location $L_{i,j}$ caused by only the current earthquake event e$_n$.

B. Location Trustiness from Environmental Sensor Data

There are many kinds of sensors can be used to detect disaster events and they depend on certain characteristics of natural disasters. This section describes calculating trustiness of location using a sensor-based model, in which we combine the trust values of a location in GMM that are calculated based on sensor data.

In this model, we assume that several cells on the GMM are attached with some sensors such as temperature sensors shake sensors, and smoke sensors. Let $\boldsymbol{s} = \{s_1, s_2, .., s_n\}$ is a set kind of sensors that are used in the cells of GMM. Each kind of sensor is assigned with a weighted that indicates its degree of influence on location trustiness. We define $\boldsymbol{w} = \{w_1, w_2, .., w_n\}$ is a set of weighted corresponding to $\boldsymbol{s}$. For each s_i in a cell, we use m_i sensor(s). Let $s_{i,j}$ is the sensor jth in s_i, $x_{i,j}$ is location trustiness that is calculated from sensor $s_{i,j}$. For more details about calculating trustiness of location by each kind of sensor is presented in our previous work [5]. Thus, we can formulate for calculating location trustiness based on sensor data as follows:

$$f_{(x)} = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{m_i} \sum_{j=1}^{m_i} w_i x_{i,j} \qquad (4)$$

Equation 4 is used to calculate trust value for each cell on the GMM in which exists at least one sensor. In fact, many cells may not exist any sensor. Therefore, we define a factor for using trustiness of location with the sensor-based method in calculating final trustiness of location.

C. Combined Approach for Calculating Location Trustiness

This section shows an approach that combines location trustiness based on both earthquake information and sensor data. To do this, we define T_E is the location trustiness which is calculated based on earthquake events (see Equation 3), and T_S is the location trustiness using sensor-based (see Equation 4). Now, the final location trustiness T_L on each cell of GMM at a specific time is defined as follows:

$$T_L = w_E T_E + w_S T_S \qquad (5)$$

where ω_E is the weight for trustiness of location T_E, ω_S is the weight for T_S and $\omega_E + \omega_S = 1.0$. These weights indicate the degree impact of two kinds of trustiness of location in the same region (a single cell on the GMM).

III. Disaster Resilient SDN with Location Trustiness

A. System Design for Disaster Resilient SDN

The main goal of our system is to enable a disaster resilient SDN by choosing better backup paths based on location trustiness. With the proper backup paths, the network recovers from failures caused by a disaster event in short time.

To do this, we first design a Location Trustiness Framework which provides modules for collecting disaster related information and calculating location trustiness of links and switches. As shown in figure 1, This framework consists of five modules: (1) Disaster-Data Collector module (collecting earthquake information and data from disaster sensors); (2) Network Infrastructure module (maintaining actual topology of the network with the information of switches and links); (3) a Geo-Mapping Matrix module (defining the target region); (4) Location-Trustiness Calculator module (calculating location trustiness); and (5) Link/Switch-Trustiness Calculator module (mapping location trustiness to each link/switch).

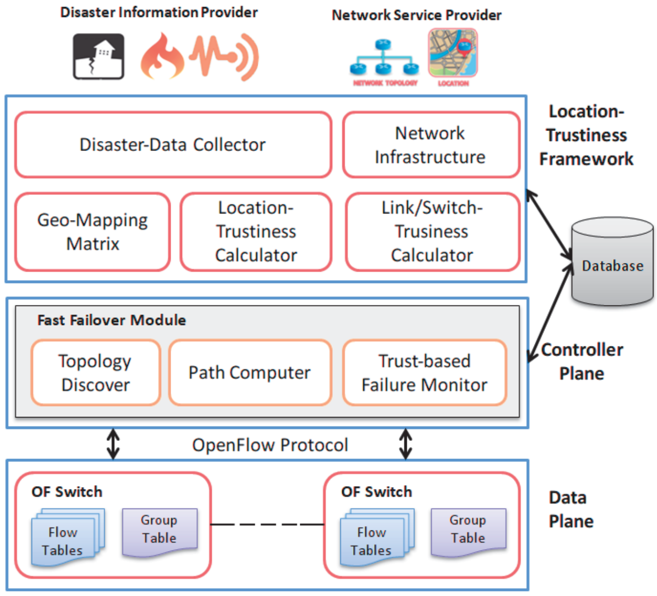


Figure 1. Overview of a System for Disaster Resilient SDN

After calculating location trustiness on the Location Trustiness Fromework, we can use it for setting up better backup paths for network failover against disasters. To do this, we design a SDN architecture with OpenFlow (OF) Switches and controller application, Fast Failover Module. The Fast Failover Module consists of three components : Trust-based Failure Monitor (monitoring changes of trustiness of links and switches from database or real-time event), Topology Discover (update the real-time trustiness of network topology), Path Computer (setting up backup paths for end-to-end flows based on location trustiness of network topology). The Fast Failover Module can be implemented as a SDN controller application. Whenever backup paths of a flow are calculated, the backup flows are installed on corresponding OF switches.

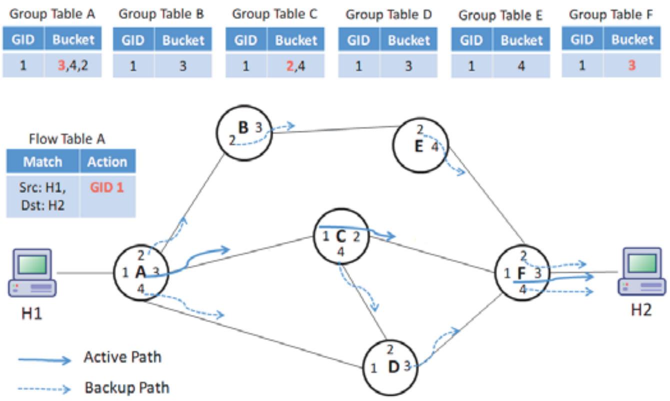
B. Backup Paths with Trustiness of switches and links

The trustiness of links and switches is defined as a real number in the range from 0.0 to 1.0 which indicates the likelihood that links/switches are reliable under a disaster.

We assume that a link L_i in the network topology can be represented by a polyline. We treat a polyline as a single object, including component segments. Each line segment is identified by two points: source location and destination location. So, we can make a line y between source location and destination location, and find all cells on the line y whose location trustiness is less than 1.0. Then, set the trustiness of the line y with the minimum location trustiness value.

After getting trustiness of network components such as links and switches, the network topology is annotated with the trustiness. With the trustiness annotated network topology, we can set up better backup paths which is more resilient against large scale disasters which may affect multiple network components at the same time.

In Figure 2, an ordinary backup path plan is shown. An end-to-end flow between H1 and H2 is tagged as GID 1, and each switch holds forwarding interfaces (primary and backups) in the bucket of a group table for the corresponding GID. When a packet related to this flow arrives a switch, the packet is forwarded to the primary interface. If forwarding the packet through the primary interface is failed, the packet is forwarded to the backup interfaces, and then so far. In figure 2, the primary path for the flow between H1 and H2 is H1-A-C-F-H2.



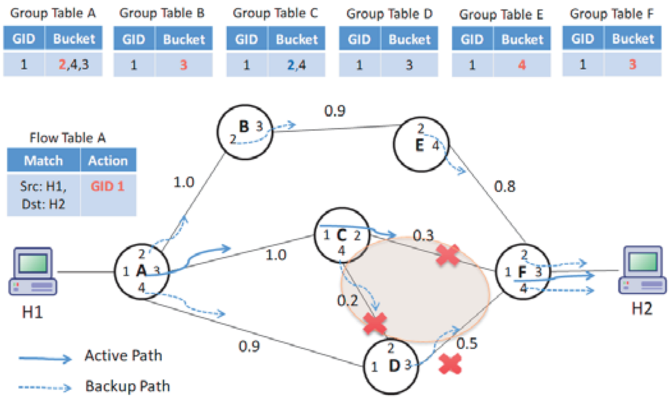
Group Table A		Group Table B		Group Table C		Group Table D		Group Table E		Group Table F	
GID	Bucket	GID	Bucket	GID	Bucket	GID	Bucket	GID	Bucket	GID	Bucket
1	3,4,2	1	3	1	2,4	1	3	1	4	1	3

Flow Table A

Match	Action
Src: H1, Dst: H2	GID 1

Figure 2. Ordinary setting of primary/backup paths of a flow

However, this ordinary setting may cause long recovery time under large scale network failures caused by a disaster. In figure 3, a scenario of large scale disaster is shown. This disaster event brings down three links (C-F, C-D, D-F) at the same time. So, the primary path of the ordinary plan is failed and one of backup path is also failed. That is, the recovery time for this flow becomes longer than expected.



Group Table A		Group Table B		Group Table C		Group Table D		Group Table E		Group Table F	
GID	Bucket	GID	Bucket	GID	Bucket	GID	Bucket	GID	Bucket	GID	Bucket
1	2,4,3	1	3	1	2,4	1	3	1	4	1	3

Flow Table A

Match	Action
Src: H1, Dst: H2	GID 1

Figure 3. Scenario of Large Scale Disaster

Otherwise, if we know the trustiness of network topology, we can set up primary and backup paths differently to the ordinary plan. In figure 3, the network topology is annotated by the trustiness of links which is calculated by disaster related information, and the paths for a flow are also annotated by the trustiness. For the trustiness of a path is set to the minimum trustiness among the trustiness of all segments in the path. For example, the flow between H1 and H2 has three paths A-C-F (trustiness 0.3), A-D-F (trustiness 0.5) and A-B-E-F (trustiness 0.8). Then, we can set A-B-E-F as primary path or the first backup path if we want most resilient network. Then, we can reduce the recovery time under large scale disasters.

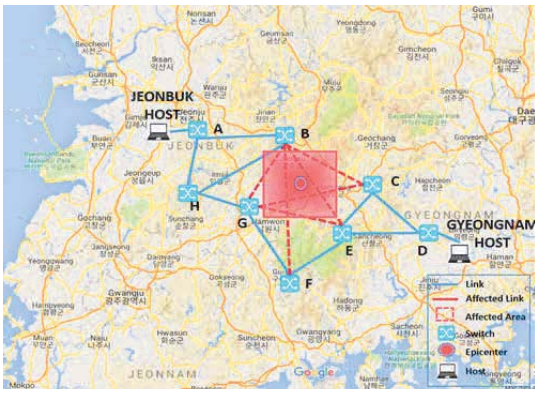


Figure 4. Emulation of a Large Scale Disaster

IV. Evaluation

In order to evaluate the proposed approach, we implement the proposed system with OpenDayLight and emulate the network operations under a large scale disaster with Mininet.

Assume that, we have a network topology to connect many cities together in Korea. We use Mininet [7] tool to emulate the network which is connected by 40 nodes and 70 links controlled by OpenDayLight. The controller will setup a new flow to switch when having the changing of network such as link down or failure of switch.

To show the effectiveness of our approach, we run Iperf between multiple machines on this network and measure the continuous throughput under a large scale disaster event. we install Iperf in two hosts, Jeonbuk host work as client and Gyeonnam host work as the server. Then, we measure the throughput on the network path between two above host in 60 seconds to evaluate the reliability of network when having disaster. We will measure the throughput and recovery time of network in two cases, first is one path between two hosts and the other case is multiple paths which connect to multiple hosts.

To issue a large scale disaster, we emulate a disaster event with 7 Richter magnitude, and the epicenter stays at Hamyang, Korea. Figure 4 shows affected topology, which is a part of the network from Jeonbuk to Gyeongnam. Although all of the links in an area are affected by disaster, not at all are go down. So, we select randomly a half of number affected link to set it to be down when having disaster event.

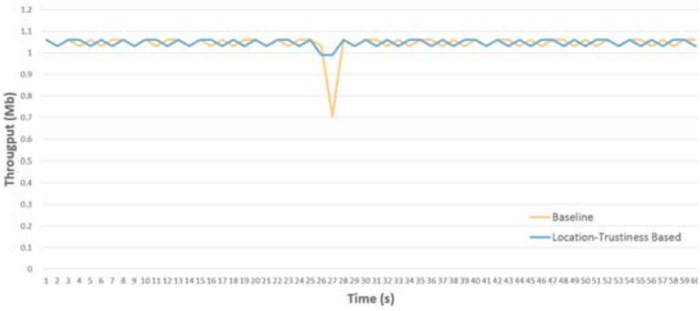


Figure 5. Throughput for a Single flow

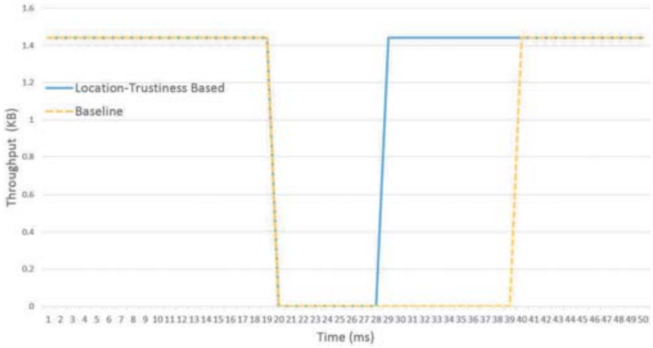


Figure 6. Throughput for Multiple flows

Figure 5 and Figure 6 show the throughput under a large scale disaster for a single Iperf flow and multiple Iperf flows, respectively. In these result, we obseved that our approach recover network much faster.

V. Conclusion

This paper proposed a novel approach for disaster resilient SDN by using location trustiness. In this approach, we setup more proper backup paths by using trustiness of links and switches derived by location trustiness. To evaluate the viability of the proposed approach, we implement the proposed system with OpenDaylight and show that the proposed approach reduce the recovery time under large scale disasters.

Acknowledgment

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). 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).

References

[1] McKeown, Nick, et al. "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review 38.2 (2008): 69-74.

[2] 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.

[3] Sharma, Sachin, et al. "OpenFlow: Meeting carrier-grade recovery requirements." Computer Communications 36.6 (2013): 656-665.

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

[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.

[6] Medved, Jan, et al. "Opendaylight: Towards a model-driven sdn controller architecture." Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. 2014.

[7] Team, Mininet. "Mininet Overview." URL: http://mininet.org/overview/ (visited on 2016/01/09).