future internet

MDPI

Article

SD-BROV: An Enhanced BGP Hijacking Protection with Route Validation in Software-Defined eXchange

Pang-Wei Tsai [1], Aris Cahyadi Risdianto [2], Meng Hui Choi [3], Satis Kumar Permal [3] and Teck Chaw Ling [3,*]

[1] Department of Information Management, School of Management, National Central University, Taoyuan 320317, Taiwan; pwtsai@ncu.edu.tw
[2] School of Computing, National University of Singapore, Singapore 117417, Singapore; dcsacr@nus.edu.sg
[3] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia; skywood0809@siswa.um.edu.my (M.H.C.); satiskumar0597@gmail.com (S.K.P.)
* Correspondence: tchaw@um.edu.my

Abstract: In global networks, Border Gateway Protocol (BGP) is widely used in exchanging routing information. While the original design of BGP did not focus on security protection against deliberate or accidental errors regarding to routing disruption, one of fundamental vulnerabilities in BGP is a lack of insurance in validating authority for announcing network layer reachability. Therefore, a distributed repository system known as Resource Public Key Infrastructure (RPKI) has been utilized to mitigate this issue. However, such a validation requires further deployment steps for Autonomous System (AS), and it might cause performance and compatibility problems in legacy network infrastructure. Nevertheless, with recent advancements in network innovation, some traditional networks are planning to be restructured with Software-Defined Networking (SDN) technology for gaining more benefits. By using SDN, Internet eXchange Point (IXP) is able to enhance its capability of management by applying softwarized control methods, acting as a Software-Defined eXchange (SDX) center to handle numerous advertisement adaptively. To use the SDN method to strengthen routing security of IXP, this paper proposed an alternative SDX development, SD-BROV, an SDX-based BGP Route Origin Validation mechanism that establishes a flexible route exchange scenario with RPKI validation. The validating application built in the SDN controller is capable of investigating received routing information. It aims to support hybrid SDN environments and help non-SDN BGP neighbors to get trusted routes and drop suspicious ones in transition. To verify proposed idea with emulated environment, the proof-of-concept development is deployed on an SDN testbed running over Research and Education Networks (RENs). During BGP hijacking experiment, the results show that developed SD-BROV is able to detect and stop legitimate traffic to be redirected by attacker, making approach to secure traffic forwarding on BGP routers.

Keywords: SDN; BGP; route validation

Citation: Tsai, P.-W.; Risdianto, A.C.; Choi, M.H.; Permal, S.K.; Ling, T.C. SD-BROV: An Enhanced BGP Hijacking Protection with Route Validation in Software-Defined eXchange. *Future Internet* **2021**, *13*, 171. https://doi.org/10.3390/fi13070171

Academic Editor: Izzat Alsmadi

Received: 4 June 2021
Accepted: 29 June 2021
Published: 30 June 2021

1. Introduction

One of the common vulnerabilities [1] in Border Gateway Protocol (BGP) is accidental announcement—the IP prefixes are misdirected to inaccurate Autonomous System (AS) due to misconfiguration or other intentional purposes. From the security point of view, this vulnerability may open up the door for breaches. For example, attackers might be able to interrupt routing updates by manipulating control messages to affect BGP advertisement, by sending repeated messages to the original source that force it to withdraw specific routes. For another, attacker can also extract messages from a BGP session, altering content as well as resending it to make inaccurate or collapsed route [2]. In addition, flooding of unnecessary routes may also cause routing tables to run out of space. Hence, there is a need to enhance routing security to prevent AS suffering from such attacks in the global network.

To mitigate the above issues, the Secure Inter-Domain Routing (SIDR) Working Group of IETF has proposed a distributed repository system known as the Resource Public Key Infrastructure (RPKI [3]), maintaining the allocation of IP address with AS Number (ASN) for improving BGP security [4]. The data in RPKI repository can be referenced by routers to draw conclusions about the validity of route advertisement, ensuring they only accept announcements of prefixes with authentic original ASes. Consequently, the decision made by BGP Routing Information Base (RIB) should be reflected at the Forwarding Information Base (FIB) as well for finding proper mitigation of abnormal situations. However, some mechanisms are already in use to provide BGP route validation, the advertisement verification is still not well described as to whether an AS is qualified to make an announcement for certain IP prefixes or not. If there is a way to engage route validation more easily, the route exchange progress among ASes could be more security and adaptation.

For enhancing the controllability of network, recently, there is a trend to restructure traditional network architecture to Software-Defined Networking (SDN [5]) one for gaining more benefits from flexibility in both data plane and control plane. SDN has several advantages [6], such as supporting self-assurance to minimize the complication of statical defined network, improving capability of hastening the delivery of new networking applications and services, simplifying the provisioning and management of network resources, and unlocking new potential in cross-domain traffic delivery. By applying SDN on WAN, network engineers are able to efficiently make use of bandwidth and ensure performance levels for critical applications without sacrificing security or data privacy. Furthermore, with the emergence of Software-Defined Wide-Area Network (SD-WAN [7]), when Internet Service Providers plan to deploy new services (such as cloud-based and on-demand applications) across the global network, it provides better adaptation and resilience that prevents inefficiency disruption on network communication.

Similar to SD-WAN, utilizing SDN-based solutions [8,9] at Internet eXchange Point (IXP) has become more and more popular. It allows multiple Internet Service Providers to peer and exchange their respective traffics with BGP protocol. Since ASes are interconnecting through IXP, some exchange operators are considering the use of SDN to develop a versatile control for manipulating traffic with precise manner [10], which eventually illustrates the concept of Software-Defined eXchange (SDX). By integrating RPKI with SDX, it is possible to enhance the security at the exchange point by installing forwarding entries with different policies [11]. Meanwhile, it also helps to mitigate the poisoning issue that some traditional networks may meet. Hence, the motivation of this research is to utilize softwarized-control advantages of SDN for enabling route validation in IXP, trying getting more security approaches in BGP route advertisement.

To mitigate route exchange vulnerabilities in BGP with SDN method, this paper proposes an alternative SDX development that aims to establish a flexible validation scenario with RPKI validation. In design, the validating application built in the SDN controller is capable of investigating routing information and controlling hybrid SDN environment to manage non-SDN BGP neighbors to get trusted routes and drop suspicious ones. By integrating ROV with RPKI, SDX is able to provide security protection that against deliberate or accidental routing events to its members. This implementation aims to reduce the time of stopping poisoned router spreading unauthorized routes and avoiding it hijacking the traffic from legitimate routers. It is expected to enhance the security of peering procedure in route exchange. The paper organization is as follows. Section 2 reviews the background information and related works of BGP hijacking. Section 3 explains how security breaches happened in BGP routing and what the strategy could be to mitigate such attack. Section 4 presents the proposed idea and its corresponding development, SD-BROV, an SDX-based BGP Route Origin Validation mechanism. It also shows the evaluation result of SD-BROV, which is experimented in an overlay network testbed based on Research and Education Networks (RENs). Finally, the conclusions are given in Section 5.

2. Background and Related Work

In global networks, AS is the fundamental element managed by the Internet Service Provider (ISP), and BGP is a widely used protocol to exchange routes among ASes. In the route exchange process (so-called peering), each AS has to use recognized ASN to announce its responsible IP prefixes. To advertise IP prefixes between two ASes, routers have to establish BGP session and send advertising messages first. On the next step, by collecting received advertisements, routers are able to calculate the route weight and update their forwarding tables. After the above steps, routers are capable of knowing where to forward the network traffic according to the destination IP address in the end.

Due to the complexity of global network architecture, it is common to find multiple AS paths to reach a specific destination IP prefix. However, because the advertised routing information is spreading among numbered peering routers, it is hard to guarantee whether the advertisement is reliable or not. For example, a misconfigured advertisement might simply cause the unreachable issue to affected BGP neighbors. Therefore, making sure received routes are coming from trusted sources is very important.

2.1. BGP Hijacking and Route Poisoning

In February 2008, there was a significant incident [12] of routing interference happening as a real-world case. Pakistan Telecom (AS17557) announced an unauthorized IP prefix 208.65.153.0/24 with an unknown reason in the beginning. After that, PCCW Global (AS3491) received such an advertisement and forwarded it to other peering neighbors. As a snowball gathers as it goes on, more and more BGP routers propagated such an incorrect IP prefix to the others in the global network. Before this happened, the IP prefix 208.65.153.0/24 was announced by YouTube (AS36561). As routers preferred to use the shortest path to forward traffic, this policy led routers to hand over the traffic to the poisoning AS path. As a result, it caused a BGP hijacking—traffic that initially went towards YouTube turned to Pakistan Telecom.

This situation quickly attracted the attention of network administrators. YouTube tried to use a routing mechanism to correct the misleading advertisement. It started to announce the two IP prefixes 208.65.153.128/25 and 208.65.153.0/25. According to the longest prefix match mechanism, in the lookup process, both 208.65.153.128/25 and 208.65.153.0/25 (leading to the correct path) were expected to be priority over 208.65.153.0/24 (leading to the poisoning path) in forwarding table. The mitigation successfully made affected routers change back to the original route again for reaching YouTube. Later, PCCW Global also blocked the misleading announcement made by Pakistan Telecom. The overall hijacking lasted about two hours, while it did make a massive impact on Internet users and content providers.

From this event, it can be briefly concluded that AS may suffer from few pain points. First, the current BGP advertisement is based on a default trust relationship. A router decides which neighbor can be trusted, while it is unable to determine whether the learned route from its neighbor is poisoned or not. Second, it is hard for a router to ensure that its advertisements are good without implementing a reliable validation mechanism. Once the BGP hijacking happened, the misleading claim may spread out and cause security incidents, finally leading to property loss. Hence, for security reason, it is necessary to strengthen route validation to prevent AS suffering from such circumstance today.

2.2. Route Validation with RPKI

Currently, RPKI is expected to be a way of protecting BGP routers against poisoning. By leveraging crypto signature method [4], IP prefix announcement will be binding with the advertised AS originally. This mechanism provides a route validation operation with reliable, trusted infrastructure [3] for routers connected to a global network.

Route Origin Authorization: Since the route exchange procedure is based on peering among ASes, it is a challenge to avoid routers suffering from learning poisoned advertisements from its neighbors. Therefore, the practice of RPKI is to add an out-of-band control

plane to help the router to determine which AS can announce which route. During the validation, RPKI provides the necessary information of IP and ASN pairs, which is called Route Origin Authorization (ROA [13]). It is a signed object that makes use of RFC3852 and RFC3779 with X.509 certification. A ROA record is shown in Figure 1. By comparing received advertisements with acquired ROA records, RPKI-enabled routers are able to filter the irrational routes to prevent BGP hijacking.

```
tein@quagga1:~$ whois -h whois.bgpmon.net " --roa 28001 200.7.86.0/24"
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN:       AS28001
Not valid Before: 2017-04-28 03:00:00
Not valid After:  2023-04-28 03:00:00  Expires in 2y296d4h41m38.2000000029802s
Trust Anchor:     repository.lacnic.net
Prefixes:         200.7.86.0/24 (max length /24)
                  2001:13c7:7002::/48 (max length /48)
                  200.3.12.0/22 (max length /24)
                  200.10.60.0/23 (max length /24)
                  2001:13c7:7012::/47 (max length /47)
                  2001:13c7:7010::/46 (max length /47)
```

Figure 1. An example of ROA record.

RPKI Certification: To establish RPKI, Internet Routing Registry (IRR) plays a vital role in its deployment and operation. The reason is that IRR has correct registration information for determining which AS is the real owner per IP prefix. In the RPKI certification scenario, IRR acts as the certificate authority, called Trust Anchors (TA). At present, the operational RPKI infrastructure in the world has five default TAs: AFRINIC, APNIC, ARIN, LACNIC, and RIPE NCC [14]. RPKI downstreams (i.e., BGP routers) have to keep in syncing validation information from repositories of TAs, making sure the ROA matches the latest allocation. The used protocol, RPKI to Router (RTR), carries the serial number, IP prefix (both IPv4 and IPv6), ASN, and max length parameter (optional) to help router make validation. The communication between router and RPKI validator is using TCP, and it is encouraged to enable TLS for strengthen transmission security. More detailed specification information can be found in [15].

Hosted and Delegated RPKI Services: By today, the default five IRRs have hosted RPKI service [16]. However, due to the scope of global network, it is not suitable to count on such a centralized service in supporting large-scale and distributed network architecture. In production operation, it is more graceful to interact with Regional Internet Registry (RIR), National Internet Registry (NIR), or Local Internet Registry (LIR) for processing RPKI validation. Furthermore, it is also available for a small-scale organization to set up delegated RPKI service in its domestic area. With authorization from parent TAs, a delegated RPKI server can be the child service of RIR/NIR/LIR, signing ROA for local end-customers.

2.3. Limitation and Motivation to Improve Current BGP Route Validation

Despite the importance of securing Internet and its extensive efforts by all the parties, RPKI deployment is still in a slow progress. To implement RPKI, AS has to issue ROAs covering their address blocks first. At the same time, AS should also configure BGP routers to do Route Origin Validation (ROV), discarding BGP advertisements with invalid ROAs. For enforcing such progress, every AS needs to enable ROV on its local routers. While some legacy routers may meet performance issues, and that is the reason that currently only a small part of ISPs with new equipment is able to enforce the ROV. On the other hand, this situation may cause compatible problem–the inconsistency of ROA makes non-registered IP prefixes to be marked as "invalid" and turns to be filtered.

As described above, to enable ROV for better security, it is important to simplify the validation process for speeding up the deployment. Hence, this research proposes an idea for improving ROV mechanism by leveraging SDN to IXP (i.e., SDX) to make further engagement. The used techniques and expected contributions are listed below:

- Implementing BGP ROV by validating each advertised route from participating routers in IXP through SDN controller in SDX.
- Deploying overlay SDX fabric that crosses multiple geographical locations to verify the proposed idea over large-scale and long-distance environment.
- Evaluating the development to make sure it is capable of detecting and preventing BGP hijacking event for peering members in the SDX.

3. SD-BROV: An SDX-Based BGP Route Origin Validation

3.1. Building Concepts

The responsibility of an IXP [17] is to operate and manage a physical infrastructure to support Internet interconnection among network service providers. It also makes a vibrant marketplace for network transmission, which is shown as Figure 2.

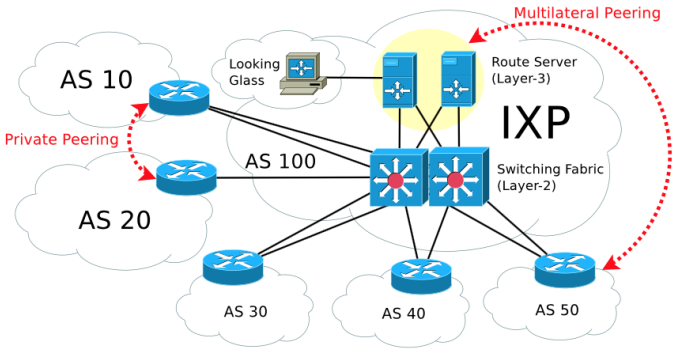

Figure 2. An example of IXP Architecture [17].

3.1.1. Layer 2 Versus Layer 3 IXP

Basically, AS with a public peering policy has to establish peering session with Router Server (RS) in IXP, enabling the exchange of IP traffic over this peering link across the IXP infrastructure. While members are also available to establish private sessions for exchanges, these private peers usually go with commercial agreement or service contract. In addition, Tier 1 ISP may also provide L3 IXP service with additional features of transit to the rest of Internet, which is primarily interested in selling global Internet transit/link to other regional ISPs within their region. The cost for such exchanges is cheaper than directly connecting to global party.

3.1.2. RPKI Cache/Validator

Since RPKI-based origin validation relies on the widespread facilities [3], the global RPKI is still in an early stage of deployment. Currently, there is no permanent, single root trust anchor. Several initial tests and deployments have been completed by the RIRs. To validate the origin ASes of BGP announcements, the validation mechanism should contain the following three basic elements:

- ROA information entries must come from RPKI database.
- Trusted route entries are determined by applied ROAs.
- RPKI cache server (RPKI Validator) has to stitch to RPKI database and router.

For supporting ROV, the cache server/validator has to query all of the distributed RPKI databases to collect all of the ROAs, trying to validate each entry's signature. To support validation, it replies to each router's request and forwards latest ROAs. In addition, routers do not have to worry about decrypting the certificates of RPKI signature because this part will be handled by cache server/validator initially.

3.1.3. RPKI-RTR Route Validation

To deduce the implementation difficulty, router requires to implement a simple and reliable mechanism to receive prefix data [18] from a trusted cache server/validator. The

design is intentionally constrained to be usable on much of the current generation of ISP router platforms. On the other hand, a border router is responsible for validating announcements that are originated by any network participating in Internet BGP routing, such as upper-level network service providers (e.g., stub or transit AS). Furthermore, the ROV implementation should be compatible with current routers with affordable hardware/software upgrades.

3.2. From IXP to SD-BROV

Since SDX is motivated to solve control capability with SDN Internet by focusing on how operators tackle these problems and show the easy-to-use applications [11], inbound traffic engineering, wide-area server load-balancing, application-specific peering, and specific traffic redirection through the middle box are the insight capabilities of SDX. For instance, AtlanticWave-SDX [19] is an SDX application that supports on-demand virtual circuit provisioning and bandwidth calendaring. For another, Google Espresso [20] is a centralized application-aware traffic engineering instance that enables host-based packet processing to offload Internet-scale routing to end-hosts with multiple strategies. To migrate legacy IXP to SD-BROV (i.e., SDX with BGP route origin validation capability), there are several issues should be considered:

SDN Switches/SDX Fabric: In recent times, Layer 2 based switching fabric [21] is evolving from simple LAN-based connection into WAN-based one. Meanwhile, it is common to utilize IP/MPLS [22] protocols over multiple sites, mapping to assigned optical fiber circuit as well. In contrast, for improving the performance of router with only Layer 3 connection, an alternative solution is to use Virtual Extensible Local Area Network (VXLAN [23]) to enable BGP tunnels. Since VXLAN tunnel is able to span across multiple sites over devices and connections, such an "SDX Fabric" can be easily utilized as a virtual network infrastructure. Based on the above points, deploying distributed IXP fabric over several routing facilities with SDN technologies (see Figure 3) is a good choice to gain more benefits from flexibility and resilience in the hybrid Layer 2 and Layer 3 architecture.

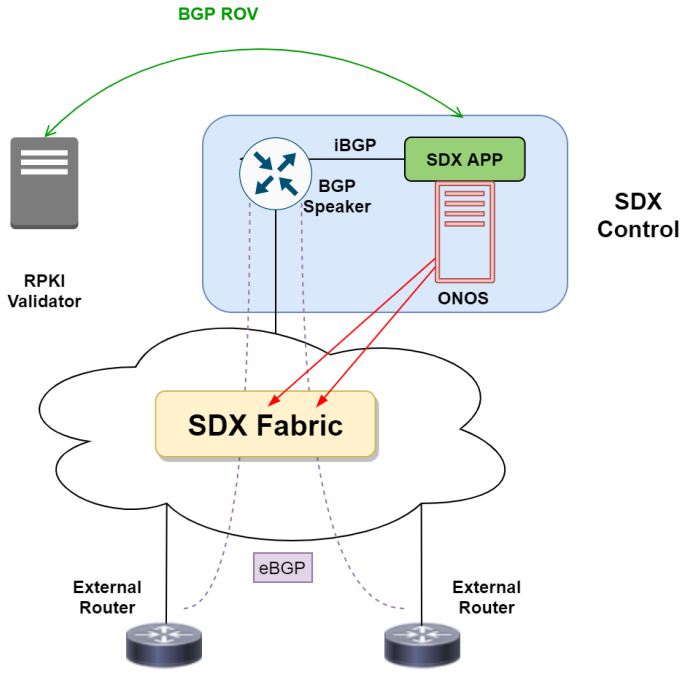

Figure 3. The operation scenario of SDX Virtual Fabric.

SDN Controller: In an exchange point that enables SDN [24], the SDN controller allows SDN switches to match on a variety of header fields (not just destination prefix), performing a range of actions (not just forwarding), and offers direct control over the data

plane in SDX. Controller applications should manage dataplane switches and integrate routing policies of multiple ASes to a coherent policy set in SDX. By doing this, SDX is able to perform better traffic forwarding by applying fabric-style management through the global view in the SDN controller. Furthermore, in order to apply policy based on global knowledge, SDX should collect and maintain BGP routes, and all SDX participants only need to interact with RS in SDX to receive trusted ones. Moreover, the SDN controller also collects the routes advertised by participating ASes, selecting the best route for each prefix, and re-advertises the best route to SDX participants.

Route Validation in SDX: For large-scale facility, filtering in IXP is a critical task [16]. There are basically three peering policies (i.e., open, selective, and restrictive) for IX members, and IX members use open policy in peering operation by default. Hence, peering sessions are usually overwhelming with multilateral interconnection, so an unconstrained routing leak at a route server could easily cause the problem, while with RPKI, prefix lists can be replaced with a single configuration statement pointing to a local RPKI validator—or more than one if multiple values are required for redundancy. Since SDX relies on the SDN controller to manage inter-domain routing, it means before applying BGP routes into the forwarding path, SDX would have a chance to make sure that specific AS owns their IP prefixes indeed. Nevertheless, to implement this process, gaining the controllability of high-level abstraction in datapath (e.g., flow and intent) is required.

3.3. Functionality of SDX-Based Route Validation

To make SDX capable of managing route validation adaptively, the design principles of proposed idea are listed below:

SDX-based Route Validation Application: In operation, the SDX controller application has to provide ROV service for SDX based on information from RPKI Validator. This application is responsible for checking each received route prefix from the BGP router of participating ASes with the latest ROA database. Meanwhile, in order to reduce verification time and increase the scalability, the application should not query to the RIR server directly for performance reasons. RPKI Validator is a local RPKI cache server (i.e., Routinator) that is used to offer such information. It will periodically synchronize with ROA database maintained by RIR, and the controller application counts on it to validate the originated route prefix and ASN.

Route-to-Intent/Flow Validation: To optimize ROV progress, SDX should be designed to translate route prefix into a high-level of rules to be forwarding rules (i.e., flow rule) for SDN components (such as SDN switch). However, flow-level abstraction may not be scaled with the massive number of route prefixes. Intent-level abstraction is the best mechanism for representing route prefix into "compiled" flow-level rules in the forwarding path.

Policies for Valid, Unknown, and Invalid Routes: To accommodate different route validation results from the RPKI validator, SDX application needs to define different actions for each prefix route. The mechanism logic of the application is shown in Figure 4. In development, intent with "forwarding" treatment is required to be applied as route entries. On the contrary, intent with "blocking" treatment is required to be setup an invalid prefix route. While for unknown prefix routes, depending on the SDX policy, different flow-based intent can be defined by the administrator. For example, if those need to be quarantined, the intent will be processed with "change-next-hop" treatment to a specific inspection device for investigation.

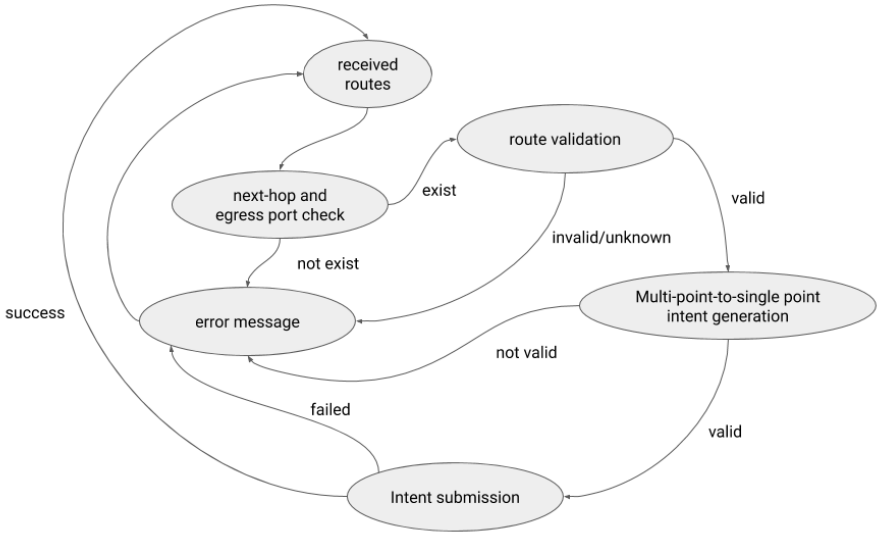

Figure 4. The designed logic of BGP route validation in SDX.

4. Implementation and Evaluation

4.1. Enabling SD-BROV over Multi-Site REN Testbed

At the very beginning for designing SDX application, preparing an affordable and experimental testing place is required. This research has collaborated with the National Research and Education Network (NREN) to acquire network testbed resources for supporting development and experiment facility. The testbed consists of two NREN sites, Malaysian Research & Education Network (MYREN [25]) and TaiWan Advanced Research & Education Network (TWAREN [26]), which are bridged by Trans-Eurasia Information Network (TEIN [27]) in behind. This testbed utilizes SDN and VXLAN to conduct multiple paths to emulate local links among BGP routers separately. Such an experiment network is shown as Figure 5. At MYREN site, the hardware components used during the experiment consist of Supermicro servers (with Intel Xeon D-1528 CPU, Micron DDR4 32 G RAM, Intel 545 s SSD 256 G, Intel I350 NIC) and Netgear M4300 switch, stitching to a Cisco router for Layer 3 forwarding. At TWAREN site, the hardware components used in the experiment include Cisco UCS C240 M3 server (with Intel E5520 CPU, Kingston DDR3 128 G RAM, 600 G SAS RAID 1 + 0 disk array, Intel I350 NIC) and Cisco C3K switch, stitching to Cisco ASR9K router for Layer 3 forwarding. Additionally, Table 1 lists used software components and related networking technologies in development.

Table 1. Software components and related technologies.

Software Component	Description
OpenvSwitch (OVS [28])	An open-source production quality, multilayer virtual switch that supports OpenFlow protocol, which is widely used as southbound protocol for allowing control communication between SDN controller and network components [5]). OVS provides support for tunnelling protocols, Virtual eXtensible Local Area Network (VXLAN), which is a stateless tunnelling framework that allows us to overlay Layer 2 networks on top of Layer 3 networks.
Open Networking Operating System (ONOS [29])	An open-source SDN controller maintained by Open Networking Foundation (ONF). It is designed by considering extensibility, modularity, and scalability to meet the needs of Internet Service Providers (ISPs). It provides a Java Application platform with an abstraction of the network and exposes services to the network functions.
Quagga [30]	A software suite provides BGP-4 routing protocol support. In implementation, Quagga daemon is running in LinuX Containers (LXCs) which acts as the BGP speaker and external BGP (eBGP) routers in developed SDX environment. It is responsible to handle route consolidation before it is sent to the SDN controller as well as manage routing information exchanges with external networks.
SDN-IP	It is an ONOS plug-in application that allows the SDN controller to connect with the external networks through Internet with BGP [31]. SDN-IP requires to co-work with one or more BGP speakers, forming internal BGP (iBGP) peers to receive and process the BGP routing information passively. When SDN-IP receives route information, it translates it into a multi-point to single-point (MP2SP) intent through ONOS intent service, which is eventually translated as OpenFlow rules for allowing connectivity between all eBGP peers in SDX.
Routinator	Routinator server is based on the RPKI validator developed by NLnetLabs (written in Rust language). It uses protocols such as RSYNC or RPKI Delta Protocol (RRDP) to download the certificates and Route Origin Authorization (ROA) from RIR's RPKI repositories and put them to a local cache for serving the route validation request. It also provides two ways to serve validation queries, either through RTR protocol or HTTP API.

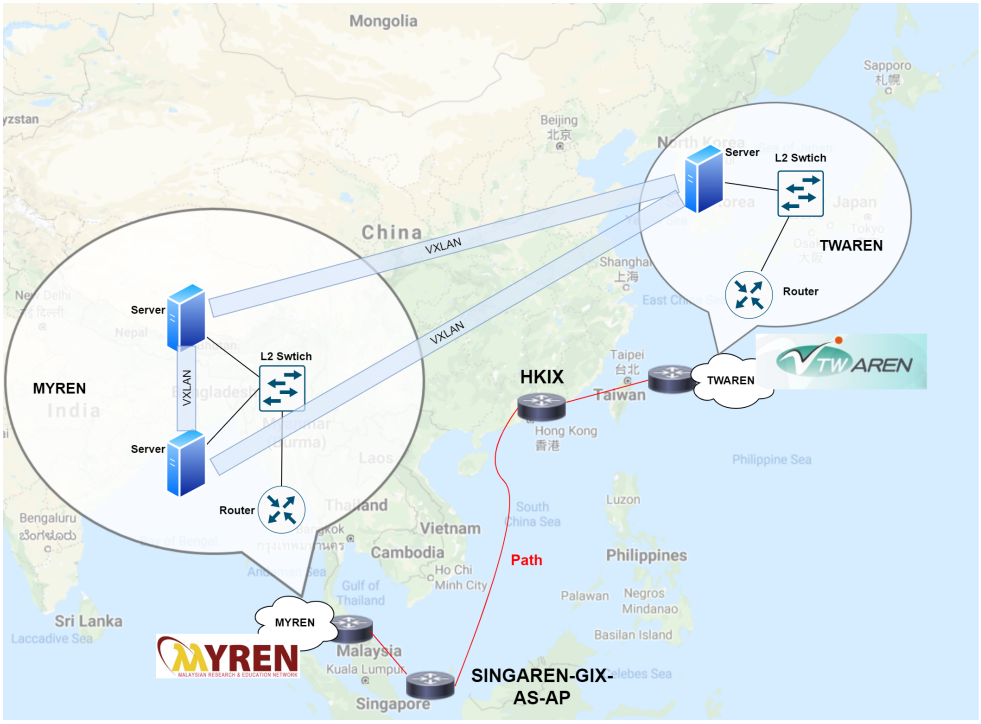

Figure 5. Physical network connection of the testbed.

In development, the overlay VXLAN fabric consists of three OVSes with full-mesh topology. One of OVS is hosted in TWAREN and the other two are hosted in MYREN. ONOS controller is the SDN controller for managing all connected OVSes. A modified SDN-IP controller application is used to communicate with RPKI validator server, which is responsible for validating all the BGP routes exchanged in the SDX. There is also another iBGP Router peering with the SDN-IP controller application to pass routing information to the ONOS for embedding flow rules in SDX data plane.

4.2. L3-SDX/Controller Application

In operation, the developed SDX controller application is co-operating with ONOS. After the peering session is activated, SDN-IP application then creates a Single-Point to Single-Point (SP2SP) intent between two eBGP routers and BGP speaker to establish the datapath communication. On the next step, when a new BGP route is identified, it creates Multi-Point to Single-Point (MP2SP) intent for all eBGP routers in the SDX and advises the best next-hop router towards the destination IP prefix. Finally, this process will establish a direct datapath for AS to carrying peering and transit traffic that traverses through the SDX.

According to design, Routinator is responsible for downloading certificates and ROA from RIR's RPKI repository and store the information at local cache. The local cache should be updated periodically, including checking the repositories serial numbers, and determining whether it is synced. During the operation, once a new BGP route update event is detected by the SDN-IP application, it conducts ROV against RPKI cache in the Routinator in order to determine the validity and integrity of prefix and associated ASN before installing it to associated intents. For SDX members, the validation information can be obtained by sending HTTP GET method requests to the Routinator HTTP Server. The server will return three types of validity status for specify that route (i.e., valid, invalid, and not-found) to help SDX members setup their filters if needed, which are listed below:

- If the route origin ASN and the route prefix are covered in validation data, in the meantime, there is an exact match ROA in RPKI database, then this route is considered as "valid".
- If a route prefix is covered by a ROA record but the route origin ASN or the prefix length does not match as stated in the ROA record, the route is identified as "invalid".
- If a route prefix is not covered by a ROA record, it will be judged as "unknown (not found)".

For instance, when there is an ROA record in the RPKI (182.176.19.0/24 belongs to AS17557). If AS17557 advertised a BGP route as stated in the ROA, the route will be valid. However, if it advertised a misconfigured route link 182.176.19.0/25, since this route is covered by an ROA record but with a different prefix length), the route is going to be recognized as invalid. Moreover, if AS17557 tried to advertise a route covered by other ROA record (for example, 115.186.169.0/24 that belongs to AS23674), this route is also going to be recognized as invalid. Nevertheless, if AS17557 attempted to advertise a route such as 192.168.200.0/24 that is not covered by any ROA records in the RPKI, this route should be classified as an unknown route. Figure 6 shows the logging information during the ROV progress. In the default policy of SDX application, only valid routes will trigger intent or datapath establishment. Note that MP2SP will only be created if the route is identified as valid. For other results, there will be neither intent created nor datapath established for such a route.

```
2020-07-05T12:09:31,358 | INFO  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=17557 ,prefix= 182.176.19.0/24, validity = valid
2020-07-05T12:09:31,359 | INFO  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Installing intent for 182.176.19.0/24
2020-07-05T12:09:36,361 | INFO  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=17557 ,prefix= 182.176.19.0/25, validity = invalid
2020-07-05T12:09:36,363 | WARN  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Invalid route : not installing intent for it!
2020-07-05T12:09:41,358 | INFO  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=17557 ,prefix= 115.186.169.0/24, validity = invalid
2020-07-05T12:09:41,359 | WARN  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Invalid route : not installing intent for it!
2020-07-05T12:09:46,360 | INFO  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=17557 ,prefix= 192.168.200.0/24, validity = Unknown
2020-07-05T12:09:46,361 | WARN  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Unknown route : not installing intent for it!
```

Figure 6. Example of BGP Route Origin Validation.

For further evaluation, Table 2 lists the results of experiment which was conducted for investigating the time cost of ROV process. According to the results, the number of routing entries is the reason for taking time. Nevertheless, the full table of IPv4 in global network includes more than 855,000 routing entries. The current prototyping system may take a long time to process RPKI validation when activating SD-BROV in SDX initially. The performance enhancement should be one of important topics in future work.

Table 2. Initial Performance Evaluation of ROV.

Valid Routes	Invalid Routes	Ratio	Required Time
10	1	10:1	0.178 s
100	10	10:1	1.574 s
1000	10	100:1	20.709 s
10,000	10	1000:1	682.085 s

4.3. BGP Hijacking Protection Evaluation

To verify the ROV protection capability in developed SDX, an experiment was conducted by intentionally triggering emulated incident to observe BGP hijacking in SDX. Without strict validation rules, there is a chance to advertise poisoning route and transit it to other IX members by innocent AS. The conducted experiment should be able to simulate such a breach in IX and verify whether developed SDX is able to mitigate it or not. Due to one of the most popular BGP prefix hijacking cases being the YouTube event in 2008, the experiment scenario was used to replay such an attack in a developed SDX environment,

which is shown as Figure 7. In the experiment, route prefix 208.65.152.0/22 is legitimated to AS36561(YouTube). The replayed hijacking scenario was starting when AS17557 (Pakistan Telecom) announced 208.65.153.0/24, and this prefix was propagated by its upstream provider AS3491(PCCW Global). Then, other affected BGP routers followed the rules and imported those routes into their routing tables, re-advertising such poisoned prefix to their respective neighbors.

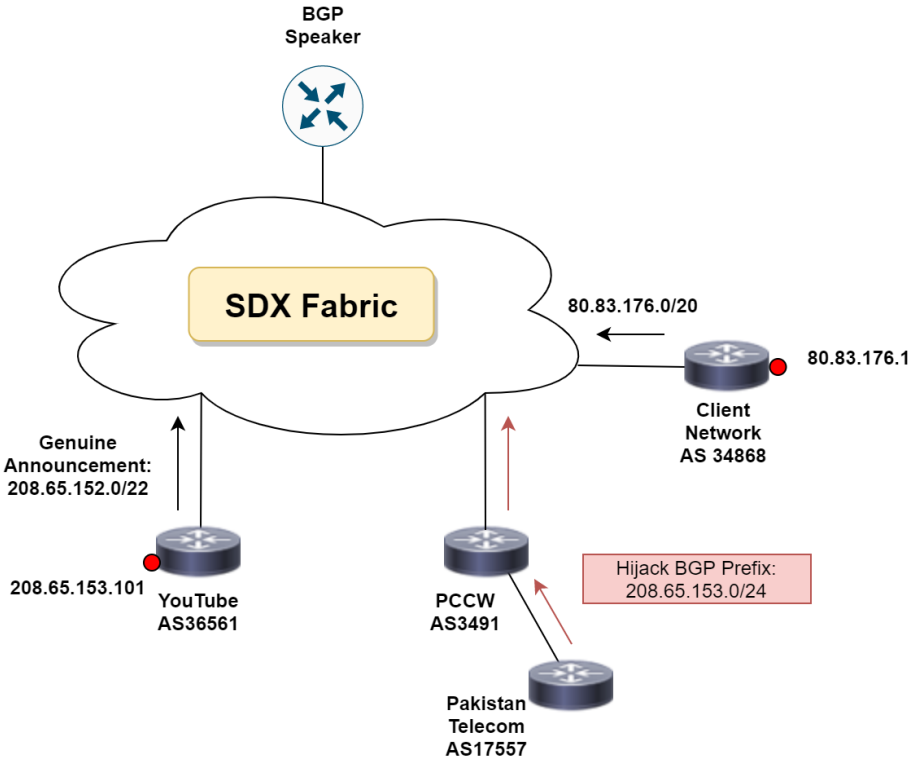

Figure 7. Hijacking in SDX with direct connection.

4.3.1. Peering Members in SDX

In traditional Internet exchange, when a hijacked prefix is advertised from an AS and successfully propagated out to Internet, the datapath for the traffic will be immediately established. In contrast, this situation should be avoided by an ROV mechanism of the SDX. The emulation scene is illustrated in Figure 7. In initial configuration, the RPKI validator for the YouTube (AS36561 and 208.65.152.0/22) was added, and YouTube, PCCW and Client Network (AS34868, for observation) was peering with the BGP speaker in the SDX.

4.3.2. Experiment: Direct Affection

At the beginning, when the legitimate AS first advertised their BGP routes in SDX, such routes had received by BGP speaker. BGP speaker then advertised the best routes to SDX application as well. After that, SDX application validated the routes received from the BGP speaker according to RPKI database before installing MP2SP intents. In Figures 8 and 9, the route 80.83.176.0/20 from AS 34868 and 208.65.152.0/22 from YouTube were valid. Therefore, SDX application installed corresponding intents and established the datapath. By completing these steps, end-hosts from these two networks will get reachability through the SDX.

```
2020-07-05T11:45:07,106 | INFO  | onos-route-listener-0 | SdnIpFib                      | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=34868 ,prefix= 80.83.176.0/20, validity = valid
2020-07-05T11:45:07,117 | INFO  | onos-route-listener-0 | SdnIpFib                      | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Installing intent for 80.83.176.0/20
2020-07-05T11:45:07,149 | INFO  | onos-route-listener-0 | SdnIpFib                      | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=36561 ,prefix= 208.65.152.0/22, validity = valid
2020-07-05T11:45:07,153 | INFO  | onos-route-listener-0 | SdnIpFib                      | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Installing intent for 208.65.152.0/22
```

Figure 8. Received routes for SDX application validating.

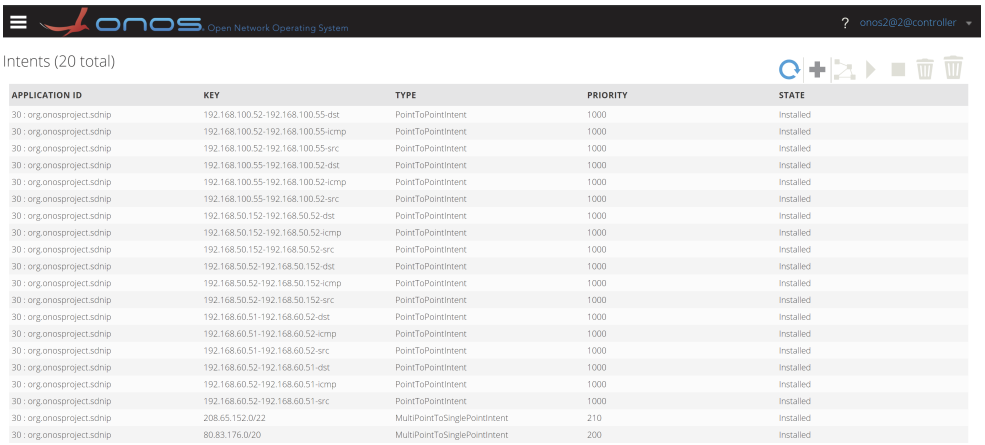

Figure 9. Created ONOS intents by SDX application.

In order to prove that the hijacking prefix will not affect the legit traffic exchange destined to a BGP peer network in the SDX, a route 208.65.153.0/24 from Pakistan Telecom AS 17557 intended to hijack the YouTube traffic, and SDX application received this route. However, the validation result showed an "invalid" status. As a result, there was no intent created for this hijacking prefix (see Figure 10).

```
2020-07-05T11:46:06,966 | INFO  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Found new route update ! ASN=17557 ,prefix= 208.65.153.0/24, validity = invalid
2020-07-05T11:46:06,967 | WARN  | onos-route-listener-0 | SdnIpFib                          | 215 - org.onosproject.onos-apps-s
dnip - 2.1.1.SNAPSHOT | Invalid route : not installing intent for it!
```

Figure 10. Detected invalid advertisement.

In this scene, invalid BGP route advertisement kept propagating to the eBGP peers in the SDX through the normal eBGP peering session. Figures 11 and 12 show the contents of the BGP routing table of BGP speaker and Client Network router. Even though the YouTube router received the invalid BGP route, traffic was still forwarded to the legitimate destination. As expected, traffic flow to YouTube 208.65.152.0/22 was not affected. The ping test result shows that even the BGP prefix of hijack targeting network, the constant reachability was still fine (see Figure 13).

```
BGPSpeaker# show ip bgp
BGP table version is 0, local router ID is 192.168.50.52
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 80.83.176.0/20   192.168.100.55           0             0 34868 i
*> 208.65.152.0/22  192.168.50.152           0             0 36561 i
*> 208.65.153.0     192.168.60.51                          0 3491 17557 i

Total number of prefixes 3
```

Figure 11. BGP routing table on BGP speaker.

```
clientrouter# show ip bgp
BGP table version is 0, local router ID is 192.168.100.55
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 80.83.176.0/20   0.0.0.0                  0         32768 i
*> 208.65.152.0/22  192.168.100.52                         0 65000 36561 i
*> 208.65.153.0     192.168.100.52                         0 65000 3491 17557 i

Total number of prefixes 3
```

Figure 12. BGP routing table on Client Network router.

```
root@clientrouter:~# ping -I 80.83.176.1 208.65.153.101 -c 5
PING 208.65.153.101 (208.65.153.101) from 80.83.176.1 : 56(84) bytes of data.
64 bytes from 208.65.153.101: icmp_seq=1 ttl=64 time=234 ms
64 bytes from 208.65.153.101: icmp_seq=2 ttl=64 time=234 ms
64 bytes from 208.65.153.101: icmp_seq=3 ttl=64 time=234 ms
64 bytes from 208.65.153.101: icmp_seq=4 ttl=64 time=234 ms
64 bytes from 208.65.153.101: icmp_seq=5 ttl=64 time=234 ms

--- 208.65.153.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 234.052/234.320/234.667/0.240 ms
```

Figure 13. Ping test result in first scene.

4.3.3. Experiment: Indirect Affection

For investigating what would have happened if the attack had been focused on downstreams of SDX members, an indirect connect scene (see Figure 14) was conducted for evaluation. In this scene, traffic destined for the hijacking route (prefix 208.65.153.0/24) in SDX was forwarding to Global Crossing AS3549 router. The reason is that traffic still matched the intent of the valid route from YouTube (prefix 208.65.152.0/22). The Global Crossing router received both routes, 208.65.152.0/22 from YouTube and 208.65.153.0/24 from the malicious AS Pakistan Telecom. Therefore, when traffic destined for YouTube (prefix 208.65.153.0/24) was sending to the Global Crossing Router, it tried to forward back the traffic to the Pakistan Telecom through SDX because of the longer prefix matches route. Figure 15 indicates the BGP routing table on Global Crossing Router. In this case, the traffic was dropped because there is no datapath in the SDX for such an invalid route in validation, while it also interrupted the ping test made by Client Network (see Figure 16). Hence, under these circumstances, the SDX is still available to stop half-way direction of the traffic affected by poisoning route. For further investigation and enhancement, To improve the protection scope of SDX in this situation, more developments are planned in future work.

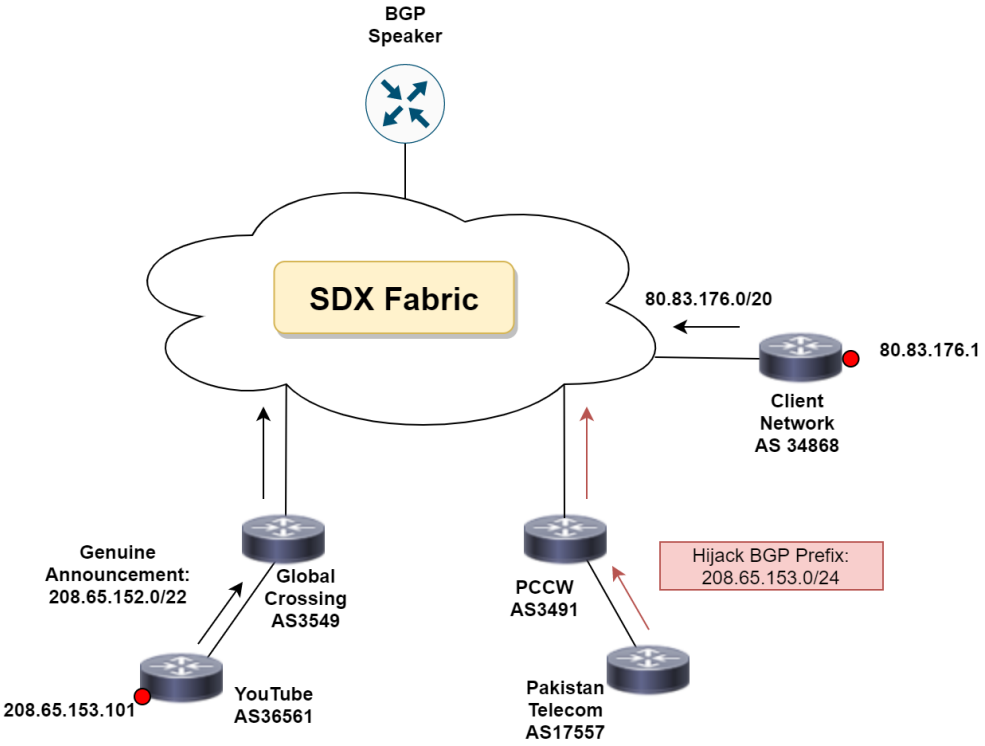

Figure 14. Hijacking in SDX with indirect connection.

```
GlobalCrossing# show ip bgp
BGP table version is 0, local router ID is 192.168.50.152
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 80.83.176.0/20   192.168.50.52                         0 65000 34868 i
*> 208.65.152.0/22  10.153.199.29            0            0 36561 i
*> 208.65.153.0     192.168.50.52                         0 65000 3491 17557 i

Total number of prefixes 3
```

Figure 15. BGP routing table on Global Crossing router.

```
root@clientrouter:~# ping -I 80.83.176.1 208.65.153.101 -c 5
PING 208.65.153.101 (208.65.153.101) from 80.83.176.1 : 56(84) bytes of data.

--- 208.65.153.101 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4080ms
```

Figure 16. Ping test resul in second scene.

5. Conclusions

To strengthen the security of BGP route exchange, this paper proposed SD-BROV—an idea that provides BGP route validation with flexibility and alternation in SDX. For enabling such functionality, an SDX application has built in ONOS controller to check received routes and investigate them with RPKI validation. By integrating ROV with RPKI, the implemented SDX is able to provide security protection against deliberate or accidental routing events to SDX members. The experiment results also show that the developed SDX is able to detect BGP hijacking incidents as well as prevent legitimate traffic to be redirected to the misleading routing path.

According to experiment result in the second scene, when the poisoned AS is not directly connected to the SDX, the SDX can only stop half-way in the direction of the traffic affected by the misleading route, and redirection is not going to happen because that there is no intent or datapath created. Nevertheless, there is a need to develop a monitoring mechanism in the SDX controller for preserving previous normal routes, triggering a fail-safe mitigation to keep traffic gracefully forwarding to original next-hop when detecting the attack. This improvement is planned in the future work of this research, and it is expected to provide better resilience in attack mitigation that against route poisoning in SDX. Furthermore, to investigate the issue in real-world deployment scenarios, using a large-scale environment to evaluate and improve developed systems [32] is important as well. Authors of this paper will try to find more practical ways and realistic scenarios in future evaluations.

Author Contributions: Conceptualization, P.-W.T. and A.C.R.; Data curation, M.H.C.; Formal analysis, M.H.C.; Investigation, P.-W.T., A.C.R., M.H.C. and S.K.P.; Supervision, T.C.L.; Validation, M.H.C. and S.K.P.; Writing—original draft, P.-W.T. and A.C.R.; Writing—review & editing, S.K.P. and T.C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Central University, Taiwan.

Data Availability Statement: Not Applicable, the study does not report any data.

Acknowledgments: Authors would like to thank the anonymous reviewers for their valuable comments and suggestions on this paper. This research was supported in part by the Ministry of Science and Technology of Taiwan, under Contracts MOST 109-2222-E-008-005-MY3. Authors are also grateful to TWAREN SDN research team members for their great help.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Murphy, S. RFC 4272: BGP Security Vulnerabilities Analysis. Available online: https://tools.ietf.org/rfc/rfc4272.txt (accessed on 10 May 2021).
2. Butler, K.; Farley, T.R.; McDaniel, P.; Rexford, J. A survey of BGP security issues and solutions. *Proc. IEEE* **2009**, *98*, 100–122. [CrossRef]
3. Huston, G.; Loomans, R.; Michaelson, G. RFC 6481: A Profile for Resource Certificate Pepository Structure. Available online: https://tools.ietf.org/rfc/rfc6481.txt (accessed on 10 May 2021).
4. Lepinski, M.; Kent, S. RFC 6480: An Infrastructure to Support Secure Internet Routing. Available online: https://tools.ietf.org/rfc/rfc6480.txt (accessed on 10 May 2021).
5. Kreutz, D.; Ramos, F.M.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-defined networking: A comprehensive survey. *Proc. IEEE* **2015**, *103*, 14–76. [CrossRef]
6. Nunes, B.A.A.; Mendonca, M.; Nguyen, X.-N.; Obraczka, K.; Turletti, T. A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1617–1634. [CrossRef]
7. Jain, S.; Kumar, A.; Mandal, S.; Ong, J.; Poutievski, L.; Singh, A.; Venkata, S.; Wanderer, J.; Zhou, J.; Zhu, M.; et al. B4: Experience with a globally-deployed software defined WAN. *ACM SIGCOMM Comput. Commun. Rev.* **2013**, *43*, 3–14. [CrossRef]
8. Michel, O.; Keller, E. SDN in wide-area networks: A survey. In Proceedings of the Fourth International Conference on Software Defined Systems, Valencia, Spain, 8–11 May 2017; pp. 37–42.
9. Cox, J.H.; Chung, J.; Donovan, S.; Ivey, J.; Clark, R.J.; Riley, G.; Owen, H.L. Advancing software-defined networks: A survey. *IEEE Access* **2017**, *5*, 25487–25526. [CrossRef]
10. Mambretti, J.; Chen, J.; Yeh, F. Software-Defined Network Exchanges (SDXs): Architecture, services, capabilities, and foundation technologies. In Proceeding of the 26th International Teletraffic Congress, Karlskrona, Sweden, 9–11 September 2014; pp. 1–6.
11. Gupta, A.; Vanbever, L.; Shahbaz, M.; Donovan, S.P.; Schlinker, B.; Feamster, N.; Rexford, J.; Shenker, S.; Clark, R.; Katz-Bassett, E. SDX: A software defined internet exchange. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 551–562. [CrossRef]
12. RIPE Network Coordination Centre. Youtube Hijacking: A RIPE NCC RIS Case Study. Available online: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study (accessed on 10 May 2021).
13. Lepinski, M.; Kent, S.; Kong, D. RFC 6482: A Profile for Route Origin Authorizations (ROAs). Available online: https://tools.ietf.org/rfc/rfc6482.txt (accessed on 10 May 2021).
14. Chung, T.; Aben, E.; Bruijnzeels, T.; Chandrasekaran, B. RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins. In Proceedings of the Internet Measurement Conference, Amsterdam, The Netherlands, 21 October–23 October 2019; pp. 406–419.
15. Bush, R.; Austein, R. RFC 6810: The Resource Public Key Infrastructure (RPKI) to Router Protocol. Available online: https://tools.ietf.org/rfc/rfc6810.txt (accessed on 10 May 2021).
16. Hilliard, N. IXP Manager Adds RPKI Support in New Release. Available online: https://blog.apnic.net/2019/06/19/ixp-manager-adds-rpki-support-in-new-release/ (accessed on 29 June 2021).
17. Brito, S.H.B.; Santos, M.A.S.; Fontes, R.D.R.; Perez, D.A.L.; da Silva, H.D.L.; Rothenberg, A.C.R.E. An Analysis of the Largest National Ecosystem of Public Internet eXchange Points: The Case of Brazil. *J. Commun. Inf. Syst.* **2016**, *31*, 256–271. [CrossRef]
18. Bush, R.; Austein, R. RFC 8210: The Resource Public Key Infrastructure (RPKI) to Router Protocol. Available online: https://tools.ietf.org/rfc/rfc8210.txt (accessed on 10 May 2021).
19. Chung, J.; Cox, J.; Ibarra, J.; Bezerra, J.; Morgan, H.; Clark, R.; Owen, H. RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins. In Proceedings of the Software Defined Networking for Scientific Networking Workshop, Amsterdam, The Netherlands, 21 October–23 October 2015; pp. 1–7.
20. Yap, K.-K.; Motiwala, M.; Rahe, J.; Padgett, S.; Holliman, M.; Baldus, G.; Hines, M.; Kim, T.; Narayanan, A.; Jain, A.; et al. Taking the edge off with espresso: Scale, reliability and programmability for global internet peering. In Proceedings of the Conference of the ACM Special Interest Group on Data Communication, Los Angeles, CA, USA, 21 August–25 August 2017; pp. 432–445.
21. Hou, W.; Shi, L.; Wang, Y.; Wang, F.; Lyu, H.; St-Hilaire, M. An improved SDN-based fabric for flexible data center networks. In Proceedings of the International Conference on Computing, Networking and Communications, Silicon Valley, CA, USA, 26–29 January 2017; pp. 432–436.
22. Xiao, X.; Hannan, A.; Bailey, B.; Ni, L.M. Traffic Engineering with MPLS in the Internet. *IEEE Netw.* **2017**, *14.2*, 28–33.
23. Mahalingam, M.; Dutt, D.; Duda, K.; Agarwal, P.; Kreeger, L.; Sridhar, T.; Bursell, M.; Wright, A.C. RFC 7348: Virtual Extensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. Available online: https://tools.ietf.org/rfc/rfc7348.txt (accessed on 10 May 2021).
24. Martins, L.F.C.; Cunha, I.; Guedes, D. An SDN-based Framework for Managing Internet Exchange Points. In Proceeding of IEEE Symposium on Computers and Communications, Natal, Brazil, 25–28 June 2018; pp. 996–1001.
25. Malaysian Research & Education Network (MYREN). Available online: https://myren.net.my/ (accessed on 10 May 2021).
26. TaiWan Advanced Research & Education Network (TWAREN). Available online: http://www.twaren.net/english/ (accessed on 10 May 2021).
27. Trans-Eurasia Information Network (TEIN). Available online: https://www.tein.asia/ (accessed on 10 May 2021).

28. Pfa, B.; Pettit, J.; Koponen, T.; Jackson, E.; Zhou, A.; Rajahalme, J.; Gross, J.; Wang, A.; Stringer, J.; Shelar, P.; et al. The design and implementation of open vswitch. In Proceeding of Symposium on Networked Systems Design and Implementation, Oakland, CA, USA, 4–6 May 2015; pp. 117–130.
29. Berde, P.; Gerola, M.; Hart, J.; Higuchi, Y.; Kobayashi, M.; Koide, T.; Lantz, B.; O'Connor, B.; Radoslavov, P.; Snow, W.; et al. ONOS: towards an open, distributed SDN OS. In Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, Chicago, IL, USA, 22 August 2014; pp. 1–6.
30. Jakma, P.; Lamparter, D. Introduction to the quagga routing suite. *IEEE Netw.* **2014**, *28.2*, 42–48. [CrossRef]
31. Lin, P.; Hart, J.; Krishnaswamy, U.; Murakami, T.; Kobayashi, M.; Al-Shabibi, A.; Wang, K.-C.; Bi, J. Introduction to the quagga routing suite. In Proceedings of the ACM SIGCOMM Conference, Hong Kong, China, 12–16 August 2013; pp. 475–476.
32. Mostafaei, H.; Kumar, D.; Lospoto, G.; Chiesa, M.; Battista, G.D. DeSI: A Decentralized Software-Defined Network Architecture for Internet eXchange Points. *IEEE Trans. Netw. Sci. Eng.* **2021**. [CrossRef]