Received 25 November 2022; revised 20 December 2022; accepted 29 December 2022. Date of publication 6 January 2023; date of current version 3 February 2023.

Digital Object Identifier 10.1109/OJCOMS.2022.3233833

The Juice Is Worth the Squeeze: Analysis of Autonomous System Provider Authorization in Partial Deployment

NAOKI UMEDA [1], TAIJI KIMURA [2,3], AND NAOTO YANAI [1] (Member, IEEE)

[1]Graduate School of Information Science and Technology, Osaka University, Suita 565-0871, Japan

[2]Graduate School of Media and Governance, Keio University, Tokyo 108-8345, Japan

[3]Engineering Department, Japan Network Information Center, Tokyo 101-0047, Japan

CORRESPONDING AUTHOR: N. YANAI (e-mail: yanai@osaka-u.ac.jp)

This work was supported in part by the Ministry of Internal Affairs and Communications, Japan, through "Research and Development on New Generation Cryptography for Secure Wireless Communication Services" among "Research and Development for Expansion of Radio Wave Resources" under Grant JPJ000254, and in part by JSPS KAKENHI under Grant 22H03591.

ABSTRACT BGP, the de-facto standard protocol for exchanging routes on a network-wide basis called AS employs invalid routes. Recently, a data object called Autonomous System Provider Authorization (ASPA) was proposed as a new specification for verifying PATH information in BGP security. In this paper, we shed light on the effectiveness of ASPAs in a *partial deployment* alongside the conventional BGP through experiments based on a real AS topology. To this end, we also present a novel simulation tool, LOTUS, for BGP route exchange, including ASPAs. We then evaluate deployments of ASPAs and their verification with LOTUS for two cases on network topology in Japan: the case in deployment from ASes whose number of connections with other ASes is large, i.e., deployment from top ASes, and the case in deployment from ASes at the end of the network topology, i.e., deployment from leaf-node ASes. As a result, we confirm that the number of victim ASes decreases in the former case, while ASPAs provide no advantage in the latter case. Notably, the number of victim ASes decreases by about 96% on average by deploying the verification with ASPAs in the top-eight ASes. Based on these results, we further conduct extensive experiments in the deployment from the top ASes, whereby ASes outside the network topology advertise malicious routes to the victim ASes. We also discuss a case whereby an adversary tries to leverage ASPAs. Our promising results show that the adversary will no longer obtain an advantage even by leveraging ASPAs.

INDEX TERMS ASPA, BGP security, partial deployment, PATH information, AS topology.

I. INTRODUCTION

A. BACKGROUND

THE INTERNET consists of a connection of large networks called Autonomous Systems (ASes) [20], managed by organizations such as Internet Service Providers (ISPs) and universities. Border Gateway Protocol (BGP) [45] is used as the de-facto standard protocol for exchanging routing information between ASes. Although there are various protocols for exchanging routing information, BGP has been used as the only inter-AS protocol which supports composing the worldwide Internet.

Despite such an important role, BGP has been reported to have various security issues [39]. Specifically, even if an AS advertises a malicious route, other ASes can receive the route. By exploiting the issue mentioned above, a malicious AS can change the routing information of a broad group of ASes into malicious information [4]. Despite such an important role, BGP has been reported to have various security issues [39]. Specifically, even if an AS advertises a malicious route, other ASes can receive the route. By exploiting the issue mentioned above, a malicious AS can change the routing information of a broad group of ASes into malicious information [4].

Although various countermeasures against the above issues have been proposed [25], [27], [32], [33], [60], [69], [71] so far, few are deployed into ASes in the real world. It is because overheads significantly affect their operation [60] due to the deployment of these countermeasures, and their effectiveness itself depends on their penetration rate on the Internet.

Based on the above background, Autonomous System Provider Authorization (ASPA) has been proposed for standardization as a countermeasure against the malicious advertisement of routing information [7]. To describe roughly, ASPA indicates authorization for a specified AS called provider, such as an upstream AS, to advertise the routing information to AS called customer. ASPAs verify the correctness of the information by digital signatures with route advertisements by pre-approved service providers. Accordingly, ASPAs achieve both security and connectivity of the Internet infrastructure.

However, to the best of the author's knowledge, it has yet to evaluate the effectiveness of ASPA so far, and it is uncertain whether the partial deployment of ASPA improves BGP security. The evaluation mentioned above is essential to encourage the deployment of ASPAs. Indeed, in the case of BGPsec [33] which is a standardized BGP security technology, its partial deployment does not improve the security despite the high cost of deployment [34], [38]. Consequently, BGPsec is supposed to be deployed fewer in future [6]. As mentioned above, it is crucial to clarify whether the partial deployment of ASPA improves the BGP security to promote its deployment.

B. SECURITY WITH PARTIALLY-DEPLOYED ASPA

Towards social deployment of ASPAs, it is considered that the deployment status of ASPAs is different for each AS in general. Indeed, the deployment of ROAs [31], an existing BGP security tool, differs in each AS [12]. Similarly, for ASPAs, there will be a mishmash of ASes that have implemented ASPAs.

In this paper, we investigate the effectiveness of ASPAs in a situation where ASPA has been partially deployed. Specifically, the research question of this paper is as follows: *what are the effects of the partial deployment of ASPAs?*

The above question aims to show when each AS should deploy ASPAs by unveiling the effective deployment case of ASPAs and their verification process (referred to as ASPV for the sake of convenience). Our primary motivations are described below.

First, routes advertised in BGP are verified with ASPV for ASPAs, then the propagation of malicious routes should be prevented. However, an AS network consists of propagating routing information. That is, the routing information received in each AS often depends on each other; hence, preventing a malicious route by some AS will also affect the routing information for other ASes. In other words, depending on how partial deployment is conducted, an AS deploying ASPV may be unable to prevent the propagation of malicious routes. As mentioned above, some past BGP security mechanisms have been shown to no longer work in partial deployments [34], [38]. Second, it is also essential to consider the most effective deployment case. For instance, it is often difficult to estimate how many malicious routes can be prevented for an AS network in advance. Since route advertisements are often biased depending on the relationships among ASes [44], it is desirable to identify how the effectiveness of ASPAs and their correspondence ASPV is affected when they are deployed in each AS, respectively.

We note that our research question is non-trivial. As described above, the effects of ASPAs and ASPV may differ depending on how partial deployment is conducted. It is not easy to appropriately guess how they work through partial deployment since there are various network topologies. Although there are existing works [34], [38] to discuss the BGP security in partial deployment, these works discussed only the conventional mechanisms, i.e., BGPsec [33], S-BGP [27], and RPKI [31]. The conventional mechanisms described above do not contain the authorization to a specified AS, such as upstream AS, which is essential for ASPAs. Thus, the answer to our research question would no longer be implied from the results of the existing works.

C. CONTRIBUTIONS

In this paper, we evaluate the effectiveness of ASPAs and ASPV by conducting simulation experiments to confirm whether the propagation of malicious routes is prevented when they are partially deployed in an AS network. To make the evaluation more realistic, we utilize an actual AS topology on the Internet. In this paper, we make three technical contributions as described below.

First, to conduct the experimental evaluation of ASPA, we develop a novel simulation tool named lightweight routing simulation with ASPA (LOTUS).[1] The exchange of routing information in BGP is executed independently based on the rules (called policies) for each AS. Consequently, the expressiveness assuming a simple graph structure is incapable of accurate simulation. To evaluate the effectiveness of ASPAs in partial deployment, we need to flexibly represent the deployment of ASPAs and ASPV. LOTUS enables ASes to advertise malicious route advertisements upon setting policies for each AS, the connection relationship between ASes, route advertisements, issues of ASPAs, and their ASPV. LOTUS can thus simulate the evaluation of ASPA/ASPV in an AS network accurately.

Second, assuming a partial deployment of ASPA, we identify the deployment case of ASPA/ASPV that effectively prevents the propagation of malicious routes. We evaluate two cases with malicious route advertisements: the deployment of ASPV in ASes with many connections with other ASes, i.e., top ASes, and the deployment of ASPV in ASes near the end of the experimental network. As a result, we demonstrate that the deployment of ASPV in top ASes

1. https://github.com/han9umeda/LOTUS

prevents the propagation of malicious routes in a quantitative fashion as the effectiveness of ASPA/ASPV. In contrast, the deployment of ASPV in ASes near the end of the experimental network has no advantage. Specifically, the former is able to reduce the average number of victim ASes for the malicious route advertisements by as much as 96%, while the latter reduces the average number of damaged ASes by only 8.8% at most. We also identify that, in the latter case, the ASes with ASPV may also become victims due to the malicious route advertisements.

Finally, we evaluate a novel attack, called an ASPA-aware attack, in the networks with ASPAs and ASPV. Since the contents of issued ASPAs are publicly available, an adversary can use the information for his/her attacks. Through the evaluation of the ASPA-aware attacks, we also confirm that the average number of victim ASes rarely increases even when an adversary uses ASPAs. Therefore, we believe that ASPAs and ASPV are effective as long as they are appropriately deployed, as demonstrated in this paper.

II. PRELIMINARIES

In this section, we describe the background of BGP, its vulnerabilities and those related works.

A. BORDER GATEWAY PROTOCOL (BGP)

1) PROTOCOL SPECIFICATION

BGP which is an inter-AS routing protocol to exchange network reachability information includes the list of ASes that reachability information traverses [45]. The list of AS called `AS_PATH` attribute. We call the attribute as `AS_PATH` simply.

BGP routers then decide the best routes to each IP prefix in accordance with the received route information and the static policy defined locally by the operators if there are multiple routes for the IP prefix. In doing so, the ASes append their own AS numbers to `AS_PATH` and advertise the IP prefix and the `AS_PATH` to the AS adjacencies as the best route. As a result, chains of `AS_PATH` to reach each IP prefix are configured.

BGP requires operators to prepare various configuration files, e.g., information on the AS adjacencies, policies in transmission, and reception of route information between ASes. Such a complicated setting may lead even experts to mis-configure BGP settings.

Meanwhile, operators of each AS just prepare for its configuration file, and thus BGP has no function to manage the whole Internet from a higher perspective. BGP cannot guarantee the validity of the route information nor detect invalid route advertisement, i.e., mis-configuration or route hijacking.

Incorrect routing information can be either just misconfigurations or malicious configurations to lead incorrect `AS_PATH` propagation to other ASes.

Hereafter, we use the word "path" to describe the AS number sequence in `AS_PATH` represents the path which IP packets is delivered through. The word "routes" for more general description.

There are two types of connection relationships between ASes: peer and customer-provider. A peer relationship is a connection between ASes in an equivalent relationship. Conversely, a customer-provider relationship is a connection in which one AS is upstream, and the other is downstream. In a customer-provider relationship, it is common that the provider benefits from the customer based on the amount of data exchanged in the connection.

2) VULNERABILITIES ON BGP ROUTING

We describe a routing vulnerability that is a problem of BGP. First, in general, the specifications of BGP assume that when a connection is established directly between ASes, the intended AS is verified by using a password. In other words, it is assumed that a connection is established only with the intended AS. Nonetheless, the routing information advertised by neighbor ASes cannot be verified. For instance, consider a situation in which the origin AS or an AS in `AS_PATH` attributes advertises malicious routing information. In doing so, ASes that receive the routing information may adopt it even though it is malicious.

Indeed, on average, there are 4.8 incidents per day of propagation of malicious route advertisements on the Internet [68]. These are two types: malicious route advertisements [11] by adversary ASes, and route leaks due to misconfiguration in some AS [59].

Malicious route advertisements are an attack in which an adversary targets an AS and advertises malicious routes through its own AS to impede the reachability of the network. Such an attack is performed by modifying the origin information and rearranging the `AS_PATH` information. When malicious routes are advertised, the targeted AS may lose its connectivity to the Internet. It is because the adversary ASes, which have no connection to the target AS, propagate routes that disguise the fact that they are reachable to the target AS. As an actual incident, the reachability to the AS for Facebook's DNS servers was lost in 2021 [4].

On the other hand, a route leak is an event that incorrectly advertises a particular route due to misconfiguration. The route leaks to peers and providers are defined in [59], respectively. As an actual incident, the route leak by Google occurred in 2017 [1].

Hereafter, we simply say both types of malicious route advertisements for the sake of convenience.

3) ROUTING MODEL

We follow the arguments by Lychev et al. [35]. AS-level topology is represented by an undirected graph $G = (V, E)$ where V is a set of vertices representing ASes and E is a set of edges representing direct BGP links neighboring ASes.

Each edge in E is annotated with a business relationship, i.e., customer-to-provider where the customer purchases connectivity from its provider, or peer-to-peer where two Ases transit each other's customer traffic for free.

ASes with BGP computes routes to each destination AS $d \in V$ independently. For any destination $d \in V$, each source AS $s \in V \backslash d$ repeatedly uses its local BGP decision process to select a single best route to d from routes it learns from neighboring ASes. Then, the source AS s announces this route to a subset of its neighbors according to its local export policy. An AS s learns a route or has an available route R if R was announced to s by one of its neighbors. The source AS s has or uses R if it selects R from its set of available routes. The source AS s also has a route to a customer if its neighbor on that route is the customer.

B. EXISTING COUNTERMEASURES

Several tools have been developed as countermeasures against the vulnerabilities described in the previous subsection. We describe RPKI [31], ROA [32]/ROV [25], and BGPsec [33] below as their typical approaches.

1) RESOURCE PUBLIC KEY INFRASTRUCTURE (RPKI)

The Resource Public Key Infrastructure (RPKI) is an infrastructure that guarantees the validity of resources such as network addresses and AS numbers in inter-AS routing information exchanges using public key cryptography [31]. The data structure is a tree structure with a specific Certificate Authority (CA) as a trust anchor, similar to the conventional PKI. It differs from conventional PKI in two points: the trust anchor is the Regional Internet Registries (RIRs), of which there are only five worldwide, and the reliable information is the network addresses and AS numbers. Deployment of RPKI is successfully underway [12]. ASPA, our main subject, ROA/ROV, and BGPsec described below are assumed to utilize RPKI.

2) ROUTE ORIGIN AUTHORIZATION/VERIFICATION (ROA/ROV)

Route Origin Authorization (ROA) is a data object of publishing legitimate information about the origin of routing information [32]. The holders of IP address and AS number that are certified in RPKI, publishes ROA having the origin of routing information with a signature using his/her key. This enables the creation of a data set of the origin of routing information that can be verified by digital signatures.

Route Origin Verification (ROV) can verify whether a route is valid by comparing the origin information of the received routing information with the published ROA [25]. If ROA published in RPKI is correct and a route different from ROA is advertised, the route is regarded as invalid.

In ROVs, the concept of "different from ROA" is defined in precisely three senses [25]: `Valid` meaning that the ROA was verified correctly by ROV, `Invalid` meaning that the ROA was not verified, or `Unknown` meaning that the ROA was not issued, or prefix length is too long.

Currently, ROA is deployed in about 30% of network addresses, and many routes are evaluated as `Unknown`. Consequently, routes evaluated as `Invalid` are often dismissed, and `Valid` and `Unknown` are treated equivalently [3].

3) BGPSEC

BGPsec is a protocol that verifies the validity of `AS_PATH` attributes by requiring the advertising AS to sign the `AS_PATH` attributes. RPKI provides public keys used for signature verification. BGPsec also introduces a function to verify the order of AS numbers in the `AS_PATH` attributes. The above function is vital because the origin of `AS_PATH` and the distance to a specific AS can be falsified by changing the order of the AS numbers. Specifically, all the information, including the signatures that have been given in the previous route exchanges, are signed. Thereby, it is difficult for an adversary to generate signatures corresponding to routes, including different AS numbers.

BGPsec has not been widely deployed. There are two main problems. First, BGPsec involves a significant overhead for handling routing information. In BGPsec, after routing information is advertised, signatures on the received routing information are verified, and then a new signature is added to the routing information. This process is computationally expensive compared to ROV, where signatures can be verified in advance. Moreover, since digital signatures are sent together with routing information, the cost of memory storage to store this information also increases.

Second, when an adversary advertises routes in the conventional BGP, they are processed by the conventional BGP process. In order to maintain compatibility with the conventional BGP, BGPsec uses BGP's extended region to add digital signatures. Therefore, an AS interpreting BGPsec can receive route advertisements of the conventional BGP. As a result, if an adversary advertises malicious routes with the conventional BGP, even if the route information is malicious, other ASes may receive without the signature verification [34]. That is, BGP security can only be improved if BGPsec is deployed fully [38], [40].

C. RELATED WORKS

1) BGP SECURITY

The closest works are research on the partial deployment of the BGP security [35], [38], [74]. Lychev et al. [35] proved that the partial deployment of S-BGP and its extensions cannot improve the BGP security, and then Miller and Pelsser [38] showed similar results for BGPsec and RPKI. We are motivated by these works. In recent years, Yang et al. [74] theoretically proved the stability of the BGP security in partial deployment. Their work focus on a general scenario including not only ASPA but also other path verification mechanisms, while we discuss the partial deployment of ASPA through extensive experiments.

While various studies have been published on BGP routing in the Internet [17], [28], [37], [48], [56], [57], [72], [75], S-BGP [27] was proposed as a secure protocol to guarantee the BGP security even against a malicious adversary. The secure origin BGP (soBGP) [71], which is a distributed version of S-BGP, was then proposed. Afterward, the pretty secure BGP (psBGP) [69] was also proposed, considering

the trade-off between the security and computational overheads of S-BGP and soBGP. However, it was pointed out that the interaction with the conventional BGP causes new vulnerabilities and degrades security [26]. Consequently, these protocols were never developed although RPKI and ROA have been deployed until now [12], [48], [53], [61].

Through research developments in the past years, there are many protocols with advanced cryptography [47], [52], [60], [73]. Several extensions [21], [24], [40], [65] of the BGP security have also been developed. These works' motivations differ from our paper because we focus on analyzing an existing protocol that may be standardized.

In the current AS network operations, the most widely deployed method is filtering [18], [36], [50], [51], limiting the routing information received based on policy. It has been shown to prevent the propagation of malicious routes with a high probability without signature verification [36], [50]. However, it only checks whether a route follows a particular policy, and the filtering is overridden if an adversary advertises a route that circumvents the policy.

2) EMPIRICAL ANALYSIS OF INVALID ROUTES

In recent years, attacks on BGP have been investigated [9], [10], [19], [22], [23], [38], [67]. In addition to attacks by malicious ASes, route leaks caused by mis-configuration of an AS administrator have also been analyzed [59]. Examples of attacks include a malicious route advertisement attack [4] that targets ASs with Facebook DNS servers and a Google case [1] as an example of a route leak. While the scale of damage caused by BGP is significant, as shown in these cases, an average of 4.8 malicious route advertisement events occur per day [68]. In recent years, DNS is also important in providing BGP security [22], [23].

Since the advertisement of fraudulent routes can pull in traffic, an attack [5], [13], [64], which steals cryptocurrency by pulling in blockchain transactions, has been observed. By contrast, to mitigate cyber attacks such as DoS attacks, a blackhole service has been proposed to intentionally update routing information and block traffic to the targeted AS [16], [30], [42], [58].

3) DEVELOPMENT OF NETWORK SIMULATION TOOLS

There are various tools for network experiments. The tools are classified into two categories: tools provided as a service and tools provided as stand-alone applications.

Tools provided as services correspond to CloudLab [46], XSEDE [63], and Emulab [70], which provide hardware available as computing resources. Notably, Emulab provides simulations that take network delays into account, and many tools based on Emulab have been proposed as extensions [54], [55]. In addition, PlanetLab [43] and the WIDE project [14] provide an experimental environment where participants bring their computing resources to configure a network. To utilize the above tools, participants need to meet several conditions, such as providing two Linux machines with global IP addresses or permission from a responsible project leader.

For BGP research, there are cases where experiments should be conducted by referring to information on the actual Internet. PEERING [49] is a tool designed for such research on BGP. PEERING can conduct experiments using data available in AS on the Internet.

Tools provided as stand-alone applications are DOCKEMU [62] and SQUAB [66]. These tools are based on virtual containers with software routers. LOTUS is more advanced than these tools because it can evaluate the conventional BGP extensions and ASPA.

III. AUTONOMOUS SYSTEM PROVIDER AUTHORIZATION (ASPA)

This section begins with an explanation of the design and the specifications of ASPA, followed by a discussions of our focusing on ASPA's effectiveness in the Internet.

A. THREAT MODEL

We recall insecure and secure routing policies in [35]. We say the policy of an AS is insecure if routes to a destination $d \in V$ are selected in the following order: (1) The AS prefers customer routes over peer routes and/or prefers peer routes over provider routes; (2) The AS prefers shorter routes over longer routes; (3) The AS use intradomain criteria to break ties among remaining routes; and, (4) in the event that the route is via a customer, the route is exported to all neighbors, otherwise, the route is exported to customers only.

We say policy of an AS is secure if routes to a destination $d \in V$ is selected in the following order: the AS prefers a secure route over an insecure route.

There are three models for incorporating the secure policy [35], i.e., security first model, security second model, and security third model. The security first model is that a secure route is placed before the first step of the insecure policy. The security second model is that a secure route is placed between the first and second steps of the insecure policy. Finally, the security third model is that a secure route is placed between the second step and the third step of the insecure policy.

In the model mentioned above, we define a routing attack. In particular, we focus on the scenario where a single adversary AS *adv* attacks a single destination AS d. Here, we assume that all ASes except *adv* use the policies described above. The *adv*'s objective is to maximize the number of source ASes that send traffic to *adv* rather than d. This objective function is commonly used [9], and reflects *adv*'s incentive to attract traffic from as many source ASes as possible [35].

As the main strategy, *adv* wants to convince ASes to route to *adv*, instead of the legitimate destination AS d that is authorized to originate the prefix under attack. It is executed by sending bogus AS-path information using legacy BGP. To this end, we focus on the arguably simplest attack [9]: the goal of *adv*, which is not a neighbour of d, is to pretend to

be connected to d. Since the models described above do not include IP prefixes explicitly, it translates to adv announcing the bogus AS-level path (adv, d) using legacy BGP to all its neighbor ASes. The received ASes will not validate it and thus will not determine that it is bogus because the path is announced via legacy BGP.

We also assume RPKI [31] and ROA [32] are deployed. Namely, if ROA is not deployed, it will be insecure due to prefix hijack, regardless of how much ASPA and ASPV are deployed. For this reason, we assume that ROA is deployed fully. We hence disregard attacks that can be prevented by ROA. Instead, we focus on attacks that are effective even in the presence of ROA.

In this paper, we assume a leaf-node AS and an outside AS as an adversary. In other words, we do not consider a case where a provide AS is an adversary. We describe the reason below.

First, we describe the reasons why a provider AS with customers is rarely an adversary inside an AS network. The reason is that if some routing error occurs, the provider AS needs to take action to provide services to the customers under their contracts. As described above, the goal of an adversary, which is not a neighbor of a destination, is to pretend to be connected there. In doing so, if an adversary who is a provider AS maliciously advertises routing information that differs from the original connection relationships, the adversary must take action by itself in accordance with the customers' requests. Consequently, it is unrealistic to assume that a provider AS is an adversary. We, therefore, consider that an adversary is limited to a leaf-node AS in the target AS network.

Next, for an outside AS, as opposed to a provider AS, there may be various motivations, such as a criminal act for fun or a political intention. Hence, we suggest that malicious routes are propagated from the outside AS to ASes in the network.

In the setting described above, an adversary executes the normal attack utilizing ROAs and the ASPA-aware attack utilizing ASPAs. We also assume that an adversary does not execute attacks that can be prevented by ROAs, e.g., forged-origin hijack [15], because we assume that ROA is fully deployed.

B. DESIGN OF ASPA

For the BGP security vulnerabilities as noted in RFC4272 [41], besides issues related to TCP used for BGP, there are vulnerabilities related to BGP messages origination and AS path modification in a BGP update message. In addition to BGPsec described in Section II-B3), ASPA is proposed in the Internet-Draft [8]. ASPA adopts the concepts of the provider and the customer to express AS adjacency. The provider means an AS providing BGP routes including the customer's AS number in the `AS_PATH`. In practical BGP operation, the provider is called upstream and the customer is called downstream, respectively. ASPA objects expressing AS adjacency in each are used for detecting whether `AS_PATH` is correct or not.

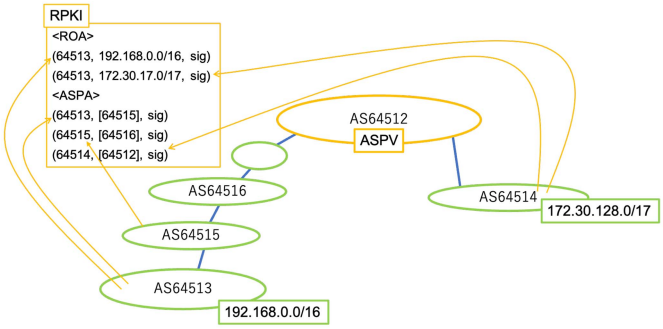


FIGURE 1. Description of the publication phase: The figure shows the publication phase for ASPV. ASPAs in the left yellow box have been published together with ROAs in RPKI. Each ASPA contains an AS number specified and a digital signature shown as "sig" by each AS.

An ASPA object indicates authorization to compose the `AS_PATH` representing the existence of an authorizing AS to a specified AS, i.e., the upstream AS for the authorizing AS generally.

The ASPA data format called "profile" is defined in [8]. The data fields of an ASPA data object to be used for `AS_PATH` verification are `AS_number`, `[Set of Provider ASes (SPAS)]` and `Address Family Identifier (AFI)`. The `AS_number` field has the number of AS which issues the ASPA object. The `[SPAS]` field has authorized AS number as the provider AS. The `AFI` field has "IPv4" or "IPv6" which applies for the ASPA objects.

For ASes which has no providers such as Global Tier-1 or Internet eXchange (IX), the `[SPAS]` field has `[0]`. The value `[0]` is a reserved AS number to express that no applicable AS exists. ASPA objects are issued to be referred globally as same as ROA. An ASPA object has a digital signature by the issuing AS then the object can be verified by using resource certificates of RPKI. The provider AS number in `[SPAS]` is adequate to verify `AS_PATH` [7].

ASPAs have been published via RPKI. The publication phase is shown in Figure 1. The corresponding AS publishes each ASPA. Since an ASPA is with a digital signature that can be verified by a public key associated with RPKI, it is possible to verify the validity of ASPA even if various ASes issue ASPAs on the Internet.

C. `AS_PATH` VERIFICATION WITH ASPA

The `AS_PATH` verification process by using ASPA has two phases. One is the preparation phase to collect issued RPKI objects includes ASPA into a cache server. The other is the verification phase to evaluate whether the received BGP route has correct `AS_PATH` information.

1) PREPARATION PHASE

The preparation phase is the phase to download ASPAs, as shown in Figure 2. ASes executed ASPV downloads ASPA

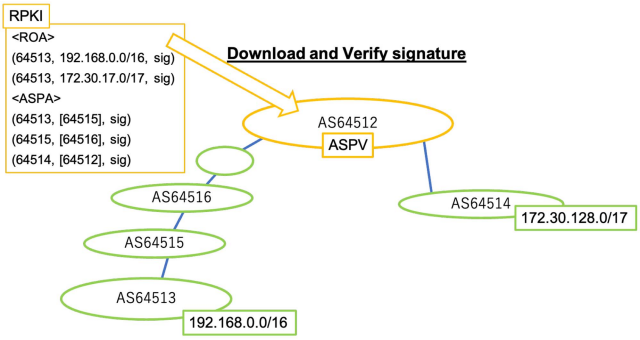


FIGURE 2. Description of the preparation phase: The figure shows the ASPV preparation phase. Whole ROAs and ASPAs in RPKI, shown in the left yellow box, will be downloaded and verified for their signatures. The downloads and the verification are executed before checking the routing information.

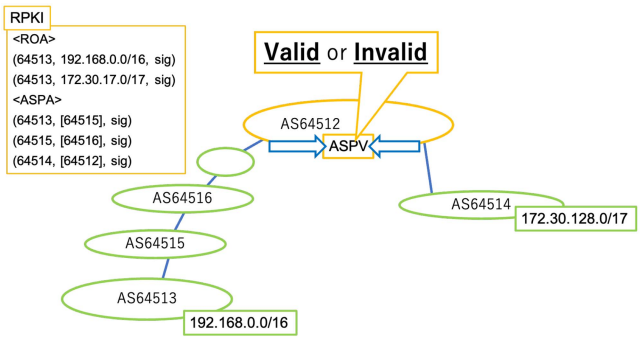


FIGURE 3. Description of the verification phase: The figure shows the ASPV verification phase. The BGP update messages, called routing information generally, are checked using data contained in ROAs and ASPAs. The ASPV is done in AS64512, for example. The routing information via AS64514 and the information via blank AS can be flagged as Valid or Invalid.

published in RPKI via their cache servers in advance. The ASes then verify digital signatures for all the ASPAs.

The cache server verifies digital signature on downloaded ASPA, is basically prepared separately with BGP router. The digital signature verification process is able to be done before verifying AS_PATH information. At the end of the preparation phase, contents of ASPA stored in the cache server are assumed to be correct.

2) VERIFICATION PHASE

The verification phase is the phase to verify AS adjacency in BGP routes using collected ASPA contents in the preparation phase, as shown in Figure 3.

The target to be verified using ASPA is AS_PATH attribute in BGP routes. AS_PATH indicates AS number sequence that the BGP routes propagated through. The AS's adjacencies are also indicated in the attribute value. Because intermediate routers can modify the value on the AS_PATH, malicious routes may have a modified value that is different from the original.

In the verification process using ASPA, the result will be Invalid when there is invalid adjacency at least one in the sequence, Unknown when Unknown adjacency in any position in the sequence, Valid when all adjacency is Valid except the "boundary" described in the next paragraph.

The verification process is outlined below. The details are described in an Internet-draft [7].

1) From the beginning of the AS_PATH attribute, that is, from the origin side of the BGP route, toward the AS being verified, one by one, it is checked whether the adjacent AS is as specified in the ASPA. The observing ASPA is different when the focused AS is in the upstream or downstream. For the ASes in the upstream, ASPAs issued by an AS on the origin side are used. For the ASes in downstream, ASPAs issued by an AS on the verifying AS side are used. In BGP routes

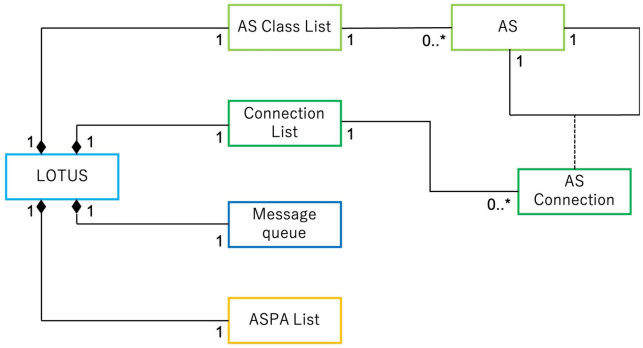


FIGURE 4. The class diagram of LOTUS: The LOTUS class is used as the core module, and several other classes share the data with the LOTUS class. The LOTUS class then performs operations for the shared data.

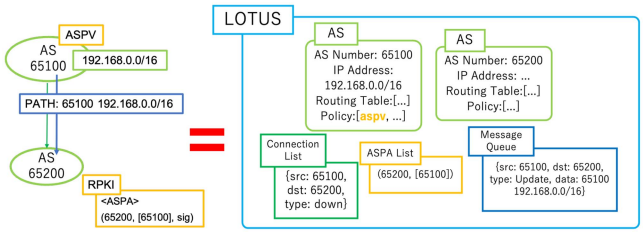


FIGURE 5. An example of an experimental network to be simulated by LOTUS. The left-side is the original network to be simulated. The network is configured over LOTUS as shown on the right side.

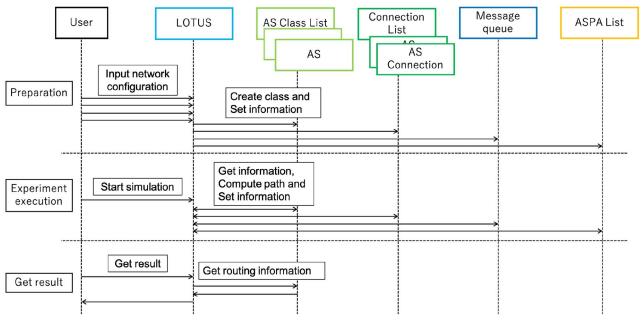


FIGURE 6. The sequence diagram to show the entire process of LOTUS for experiments: There are three phases in LOTUS. The preparation phase, the experiment execution phase, and the resulting phase. The first phase is for network configuration to be simulated. In the second phase, experiments are executed. The last phase takes results into the user. The separation of phases enables changing conditions that denote ASPV deployment rates.

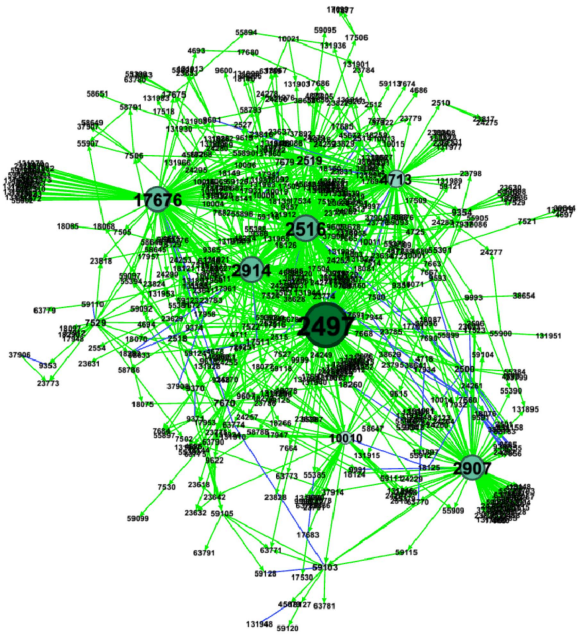


FIGURE 7. An AS networks consisting of ASes with AS numbers assigned from JPNIC and a global Tier-1 AS: The network is utilized for the experiments. In this figure, each node represents an AS and each edge represents a connection relation. A node in the figure is drawn so that its size increases in proportion to the number of connections with other ASes. The green edges are direction edges, where the destination indicates the provider from the customer's perspective, and the blue edges indicate that the ASes are peers.

propagated from the provider to the AS for verification, it is assumed that the upstream and downstream boundary exists in the `AS_PATH`. In the BGP routes propagated from its peer or customer, no boundary is assumed to be existing in the sequence.

2) If AS_SET instead of AS_SEQUENCE at least one in `AS_PATH`, the result is `Unverifiable`.
3) If the observing AS has issued no ASPA, adjacency AS as its provider is resulted as unknown.
4) If the observing AS has issued an ASPA and `[SPAS]` in the ASPA has adjacency AS as provider, the result is valid.
5) If the observing AS has issued an ASPA and `[SPAS]` in the ASPA do not have adjacency AS as its provider, the result is invalid.
6) If an AS is evaluated as invalid and the route is received from its peer or customer, the entire path is `Invalid`.
7) The boundary between upstream and downstream is assumed when an AS is evaluated as invalid and the route is received from its provider and the evaluation (as invalid) is the first. If the evaluation as invalid is the second, the entire path is `Invalid`.
8) If the tailing AS in the `AS_PATH` is different from the adjacency AS for the verifying AS, the result is `Invalid`.
9) If the route is received from its peer or customer and all ASes in the `AS_PATH` are evaluated as valid, the entire path is `Valid`. Alternatively, if the route is received from a provider and up to one AS in the `AS_PATH` is invalid and the other ASes are valid, the result is `Valid`.
10) If none of the above apply, the result will be `Unknown`.

For the AS sequence having a boundary between upstream and downstream, AS adjacency relationships in the `AS_PATH` are assumed to be changed between "customer" and "provider" at the boundary. For the AS before the boundary, the nearer AS for the verifying AS is assumed as "provider". For the AS after the boundary, the nearer AS for the verifying AS is assumed as "customer". The adjacency AS flagged as `Invalid` is used to detect the boundary. The result is because no adjacency AS is shown in `[Set of Provider ASes]` in the ASPA issued by the AS.

3) PARTIAL DEPLOYMENT

We define the setting of partial deployment of ASPA and ASPV below. As described in Section II-A3), the routing model is represented by an undirected graph $G = (V, E)$. Here, let $V' \subseteq V$ be a set of ASes with ASPV. Then, the partial deployment is defined as $V \backslash V' \neq \varnothing$, where $\backslash$ is an operation for the set partition, and $\varnothing$ is an empty set. In other words, at least one AS exists in V. We specify ASes in V' with ASPV in Section V.

D. RESEARCH QUESTION AND SUBJECTS OF THIS STUDY

In this paper, we focus on the security first model. As described in Section I, our work is the first step to shed light on the advantages of ASPAs and their verification. We leave it as an open problem to discuss them in more complicated models, i.e., the security second and third models. Specifically, we focus on revealing the effects on propagated malicious BGP messages which has different `AS_PATH` value from intended by ASes in the AS path, when ASPV has been deployed partially.

As we mentioned above, ASPV is able to be used to avoid propagating malicious BGP messages in which the AS networks have deployed ASPV. Also, as we mentioned in Section I, ASPV is expected to be deployed partially in the Internet. In this commonly happened situation, validation effects using ASPV may not be appeared as expected, shown in [34], [38].

Therefore, the key question will be how ASPV can be deployed to be effective. Purposing to minimize the effects of malicious BGP messages, we examine to see if the effects can be limited to the whole Internet. To this end, we define metrics to evaluate the effectiveness of ASPA and ASPV quantitatively. (See Section V-B for detail.)

Note that our focus is not simply on increasing the covered AS which has been effected by deploying ASPV. However, more ASPA objects should be issued to cover more AS paths, which is a prerequisite for ASPV. When ASPA coverage to AS paths is sufficient, the SUBJECT in this study is at which ASes should adopt ASPV. The goal is to determine

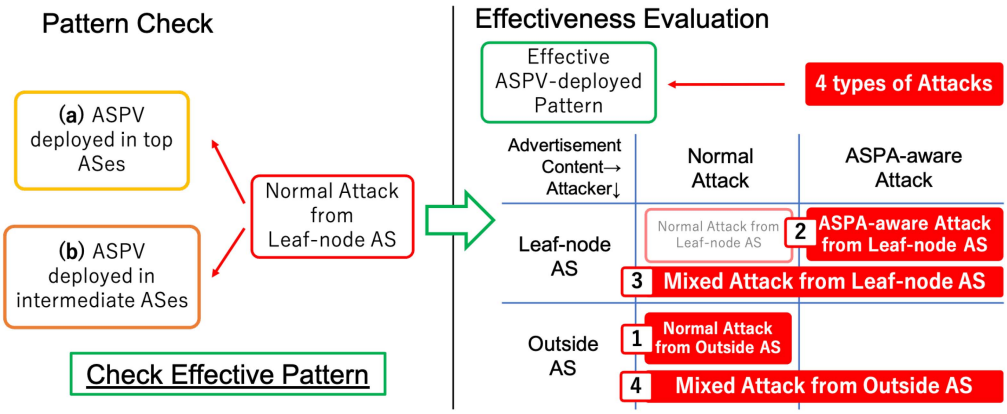


FIGURE 8. Overview of malicious route advertisements: experiments in this paper are divided into two phases. The left side shows the first phase, and effective deployment for ASPV is selected by utilizing the normal attack described below against (a) deployment in top ASes and (b) that in intermediate ASes. We also assume that ASPAs are issued only by a target AS designated in the experiments. The right side shows the second phase, and various malicious route advertisements are executed on the effective deployment, which was selected in the first phase. There are four kinds of malicious route advertisements, i.e., 1. normal attack from outside ASes, 2. ASPA-aware attack from leaf-node ASes, 3. normal attack from outside ASes, and 4. mixed attack from outside ASes. Each setting is described later.

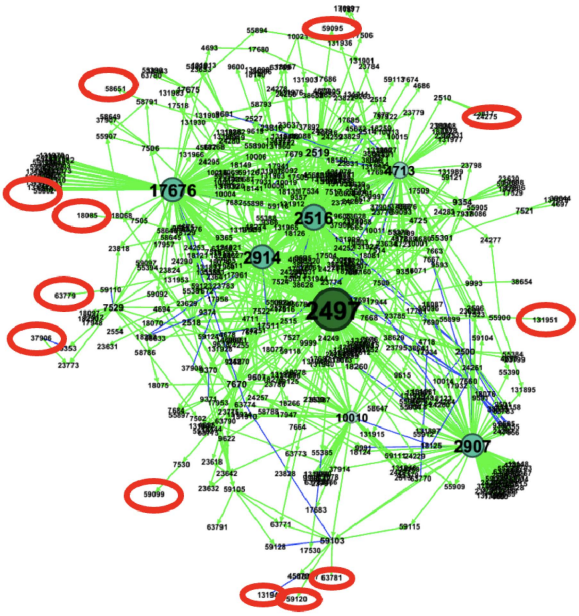


FIGURE 9. The twelve chosen leaf-node ASes: these ASes are utilized as ASes controlled by an adversary.

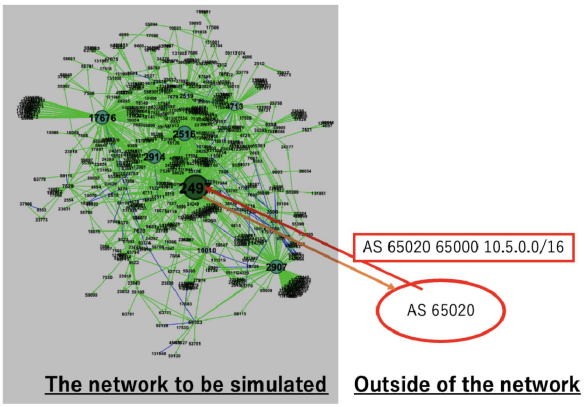


FIGURE 10. An example of the normal attack from an outside AS: The figure shows an example of the normal attack by the outside AS, AS65020, shown in the red right circle. The malicious route advertisement having AS65020 and AS65000 is from a customer of AS2497 in the center of the simulated network.

how many ASes are protected by the deployment rate in each case. In addition, with ASPV partially deployed, a new type of attack can occur that considers the presence of ASPA. This study will also consider that attack.

IV. DESIGN OF LOTUS

In this section, we develop a novel simulator named LOTUS to evaluate ASes with ASPA/ASPV. We describe requirements and its architecture below.

A. REQUIREMENTS

For evaluation of ASes with ASPA/ASPV, we need to collect routing information for each AS in an AS network topology in the following three cases: a propagation of malicious routes does not occur; it occurs in a network without ASPA/ASPV; and it occurs in a network with ASPA/ASPV. LOTUS is then required to describe network states and the propagation of malicious routes in the above cases.

In particular, the following functions are required for LOTUS.

1) Network configuration: A network consisting of defined ASes and their connection relationships can be represented.
2) Path computation: Routing information based on policies for each AS can be computed.
3) Reference to routing tables: Information in routing tables for each AS can be referenced.
4) Propagation of malicious routes: By specifying an adversary AS, malicious routes can be advertised.
5) ASPA function: The issue states that ASPA can be expressed.

6) ASPV function: ASes with ASPV can be defined, and the ASes can execute APSV.

We note that LOTUS does not provide a simulation for all the behaviors of BGP. For instance, LOTUS does not cover prefix/path filters and other routing information priorities, such as local preferences.

B. IMPLEMENTATION

To achieve the requirements, we design LOTUS. The architecture of LOTUS is shown in Figure 4 with a class diagram. We describe each class below. The LOTUS class defines interfaces with a user, generates other classes, and sets their values. It also performs path computation based on information from those other classes. The AS class represents an AS on an experimental network and provides information for the AS, i.e., AS numbers, network addresses, routing tables, and routing policies. All the AS classes on the experimental network are stored in the AS class list. Likewise, the AS connection class represents a connection relationship between two ASes in the experimental network by their AS numbers and connection types. All the AS connection classes on the experimental network are stored in the connection list. The message queue stores the routing information advertised on the experimental network. In the experimental network, we used a queue data structure to process messages in time-sequence order. The ASPA list stores ASPAs published in the experimental network. Figure 5 is an example that represents an experimental network to be simulated by LOTUS. The figure shows that LOTUS can represent the experimental network through the above data.

Next, we describe the process of LOTUS for an experiment. The entire process is shown in Figure 6 with a sequence diagram. A user first inputs information of an experimental network to be simulated in LOTUS at the beginning step of the experiment. Given the input by the user, the LOTUS class generates other classes and sets their values. The user then starts the experiment with the experiment execution command. The LOTUS class reads/writes data and computes paths to the other classes. LOTUS will stop and wait for the user's command when the experiment is completed. The user can then obtain an experimental result from LOTUS. The network configuration as the requirements is thus achieved.

For the path computation, we introduce an array to store policies of an AS in the AS class object and then implement a function to select routes based on the array. The result is stored in a routing table in the AS class object. The above implementation enables each AS to operate routing information based on its policies.

For the reference to routing tables, we implement a function to display routing tables in the AS class object. In our experiments, it is necessary to compare routing tables between ASes in each case. Each routing information is displayed in a single row to realize a comparison between routing tables. The implementation described above enables us to identify the differences in the routing information.

For the propagation of malicious routes, we implement a function to store route advertisements performed on the AS network in a queue. Routing information to arbitrary destination ASes is stored for any source AS in the queue. The above implementation can provide even propagation of malicious routes that are different from the connection relationships of the target AS network.

For the ASPA function, a list to store arbitrary ASPAs is implemented. Likewise, for the ASPV function, the ASPV deployment is represented by a policy in the AS class object, and the verification is executed when the received route information is operated.

We implemented LOTUS in Python 3.9.12 on macOS 12.3. In addition to the standard library, we use the pyyaml library. We have released the source code of LOTUS via our GitHub repository (https://github.com/han9umeda/LOTUS).

V. EXPERIMENTS

In this section, we evaluate the effectiveness of ASPA for preventing the propagation of malicious routes. In our experiments, we evaluate various cases where ASPV is partially deployed in order to identify a case for effectively preventing the propagation of malicious routes. Hereafter, we describe an experimental setting based on an actual AS network. Then, we show experimental results.

A. PURPOSE

The experimental purpose is to show the effectiveness of ASPA in preventing the propagation of malicious routes in partial deployments, as described above. We then focus on a leaf-node AS and an outside AS as an adversary because they may advertise malicious routes in the real world as described in Section III-A. We also focus on ASes with AS numbers assigned from JPNIC as the authors' most relevant environment to evaluate the effectiveness under an AS network topology in the real world. As evaluation metrics of the effectiveness, we measure the number of victim ASes by malicious route advertisements and their reduction rate. We identify whether ASPA and ASPV can prevent the propagation of malicious route advertisements through the metrics described above.

B. SETTING

1) AS NETWORK TO BE SIMULATED

An AS network in the experiments consists of 549 ASes, i.e., ASes with AS numbers assigned from JPNIC and a global Tier-1 AS. A list of ASes with AS numbers assigned from JPNIC has been published [2], and we gathered their connection relationships by BGPview.[2] Figure 7 shows the network. The reason for using this network is to evaluate ASPA/ASPV in an environment whereby the authors can gather information of the Internet in the real world. An AS network consisting of only ASes with AS numbers assigned from JPNIC is an approximate representation of the Internet

2. https://bgpview.io/

locally, and adding a global Tier-1 AS to the AS network described above is considered a more appropriate representation of the Internet in the real world. We simply refer to this AS network as the experimental network for convenience.

2) ROUTE ADVERTISEMENTS

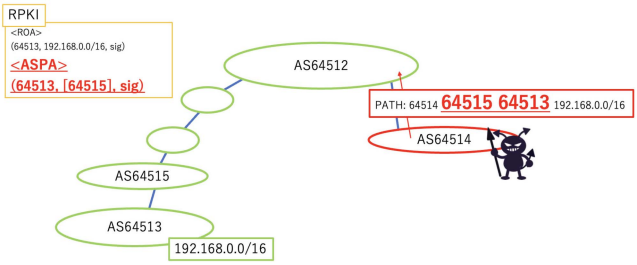
We measure the impact of malicious route advertisements on the experimental network described in Section V-B1) in the six cases described in this section. An overview of malicious route advertisements is shown in Figure 8.

We first define several notions for route advertisements in the experiments and then define malicious route advertisements.

1) Notions in the Experimental Networks: We describe several notions for the experiments. First, we define the notions for ASes. Let a target AS be an AS whose routes become invalid due to malicious route advertisements in the experimental networks. Let a top AS be an AS with the largest connections to other ASes. Similarly, let top-x AS be an AS whose number of connections to other ASes is the x-th largest for any integer x. Then, let intermediate AS be an AS with three hops as the distance from AS2497, the center of the experimental network, and leaf-node AS be an AS located at the end of the experimental network. Also, let chosen leaf-node ASes be leaf-node ASes randomly chosen for experiments as shown in Figure 9. Let outside AS be an AS which exists outside the experimental network on the real Internet, although it is not included in the experiments. Because the experimental network consists of ASes whose AS numbers are assigned from JPNIC and a global Tier-1 AS, ASes neighboring them on the real Internet correspond to the outside ASes. In the experiment, outside ASes are represented as ASes connected to the outside of the experimental network, as shown in Figure 10. Here, the number of ASes connecting to the outside ASes in the experimental network is 33.

Next, we define the notions for attacks. There are three kinds of attacks, i.e., normal attack, ASPA-aware attack, and mixed attack. The normal attack is an attack whereby an adversary advertises its own AS number in addition to the origin information of the target AS as malicious routes. The ASPA-aware attack is, as shown in Figure a, an attack whereby an adversary advertises its own AS number considering ASPAs in addition to the origin information of the target AS as malicious routes. In other words, the adversary tries to avoid `AS_PATH` that is evaluated as `Invalid` by ASPV for considering connection relations specified in ASPAs. The mixed attack is an attack whereby an adversary executes the ASPA-aware attack and then the normal attack. Meanwhile, we do not consider prefix hijack [18] and sub-prefix hijack [40] because they can be prevented by the deployment of ROA and its extensions [40].

2) Malicious Route Advertisements: We describe malicious route advertisements in the experiments below. The malicious route advertisements are executed in two phases: the selection of effective deployment for ASPA and ASPV, and their detailed evaluation for preventing the propagation of malicious routes.



First, to select an effective deployment approach for preventing the propagation of malicious routes by ASPA and ASPV, we evaluate the impact of malicious route advertisements by varying deployment cases of ASPV in the experimental network. In doing so, we suggest two cases for the deployment of ASPV, i.e., (a) deployment from the top AS and (b) deployment from the intermediate ASes. We also assume that only the target AS issues ASPAs. Although the above two cases can coexist in deployment in the real world, they are evaluated independently to identify which case is more effective in deploying ASPA/ASPV for ASes. In both cases, we assume that the adversary ASes are among chosen-leaf-node ASes, and a target AS is one of chosen leaf-node ASes different from the adversary ASes. We also assume that the adversary executes only the normal attack in this experiment.

Second, we evaluate ASPA and ASPV in more detail by executing malicious route advertisements in the experimental network with the case of ASPV, which was effective in the experiment for the selection of effective deployment for ASPA and ASPV. The adversary utilizes the normal attack and the ASPA-aware attack as malicious route advertisements with the chosen leaf-node ASes and outside ASes. Specifically, the adversary executes the attack 1 to attack 3 in Figure 8, i.e., the normal attack with the outside ASes to the ASPA-aware attack with the leaf-node ASes. As described above, the target AS in both attacks is among chosen leaf-node ASes, and the target AS issues ASPAs.

As the aim of the experiments described above, we explain that the target AS is among chosen leaf-node ASes. Since leaf-node ASes are often located at the end of the Internet, routes whose destination is a leaf-node AS may be a long `AS_PATH` length. Namely, these routes may be vulnerable to malicious route advertisements from the viewpoint of the `AS_PATH` length. If the propagation of malicious route advertisements for such long `AS_PATH` lengths can be prevented, ASPA and ASPV are considered effective even in situations where the adversary has an advantage. Likewise, we explain that the adversary utilizes the outside ASes. In this case, unlike leaf-node ASes, an adversary can advertise malicious routes even to ASes with many connections with other ASes. By evaluating such attacks, we can evaluate the impact of ASPA/ASPV on malicious route advertisements

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	141	NoN	36	106	4	13	50	34	31	1	2
3	59095	3	69	2	NoN	64	4	10	4	4	22	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	267	76	177	129	NoN	86	143	61	38	1	2
3	63779	4	111	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	166	48	96	111	6	13	53	NoN	31	1	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	1	2
NoN	131948	544	544	544	544	544	544	544	544	544	544	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	543	1	NoN

FIGURE 11. Impact of the normal attack by chosen leaf-node ASes on the experimental networks, where ASPA/ASPV is not deployed: each row represents a target AS and its distance from AS2497 and each column is an adversary AS and its distance from AS2497, respectively. Here, each AS is listed in descending order of distance from the top AS from the table's upper left.. For the same distance, each AS is listed from the left of the table in descending order of the impact of malicious route advertisements. Each cell represents the number of ASes that select malicious routes due to advertisements from the adversary AS.

in the real world from viewpoints different from those of chosen leaf-node ASes.

3) EVALUATION METRICS

We confirm the effectiveness of the deployment of ASPA and ASPV in preventing the propagation of malicious routes, both with and without ASPA and ASPV. First, for each AS, we measure the number of ASes whose the best `AS_PATH` is changed due to malicious route advertisements. We call such an AS *victim ASes*. It indicates the impact of malicious route advertisements in the experimental network. If the number of ASes that select malicious routes are decreased, we can confirm the effectiveness of ASPA and ASPV.

We define the metrics of the effectiveness below. For the experimental network $G = (V, E)$, we denote a subset of ASes in the experimental network by $N \subset V$. For any AS $as \in N$, as deploys ASPV. In other words, an AS $as \notin N$ does not deploy ASPV. In the above setting, when some attack A occurs, we measure the total number d of routes for all victim ASes $as \in V$ as follows:

$$d(N, G, A).$$

If the above d decreases, the propagation of malicious routes advertisements is prevented.

Likewise, we also define the reduction rate R to represent how many the number of routes are protected from A with respect to N as follows:

$$R(N, G, A) = \frac{d(\varnothing, G, A) - d(N, G, A)}{d(\varnothing, G, A)},$$

where $\varnothing$ means an empty set, i.e., without ASPV for any $as \in V$. If the above R increases, the propagation of malicious routes advertisements is prevented.

C. RESULTS ON SELECTION OF EFFECTIVE DEPLOYMENT

We show results on the selection of effective deployment for ASPA and ASPV through the setting described in the previous subsection.

1) DEPLOYMENT IN TOP ASES

To select an effective deployment, we first compare the deployment of ASPV in the top ASes with the deployment of ASPV in the intermediate ASes.

The result on the experimental network without ASPA and ASPV is shown in Figure 11. The figure shows that even in networks without ASPA/ASPV, the number of victim ASes is quite different for each target AS. For instance, when the adversary uses AS131951 or AS59099, the victim ASes tend to decrease. In contrast, when AS59120 is the target, the victim AS tends to increase regardless of ASes used by the adversary.

Next, we describe the results on the deployment of ASPAs and ASPV from the top AS. For the deployment in the top ASes, the results are shown in Figure 22 to Figure 29 in Appendix A. A visualization of the average number of victim ASes in these results is shown in Figure 12. According to Figure 12, when ASPV is deployed up to the top-7 and top-8 ASes, the number of victimized ASes is smaller than 10%. Namely, according to the evaluation metrics, the reduction rates were $R(N = (top - 7ASes), G, A) = 93.6\%$ and $R(N = top - 8ASes, G, A) = 95.8\%$, respectively. Intuitively, the impact is minor for the entire experimental network, and it is considered that the propagation of malicious routes could be prevented in most of the ASes.

2) DEPLOYMENT IN INTERMEDIATE ASES

Next, we describe the results on the deployment of ASPAs and ASPV from intermediate ASes. In these experiments, there may be different results depending on the chosen

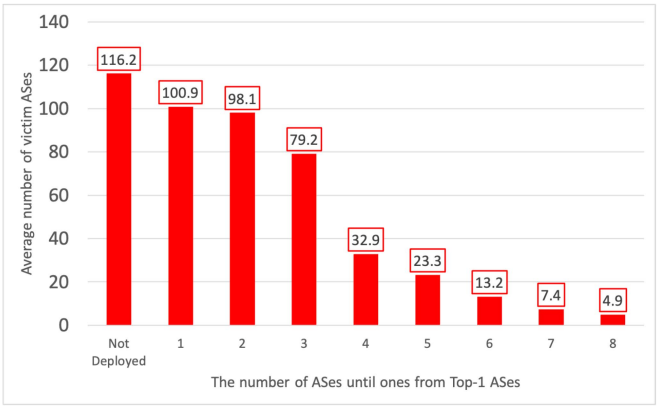


FIGURE 12. The transition of the average number of victim ASes of the normal attack by the chosen leaf-node ASes, where ASPV is deployed from the top ASes to intermediate ASes. The Horizontal axis represents the number of ASes until ones from top-1 ASes. Not Deployed represents the case where ASPV is no longer deployed.

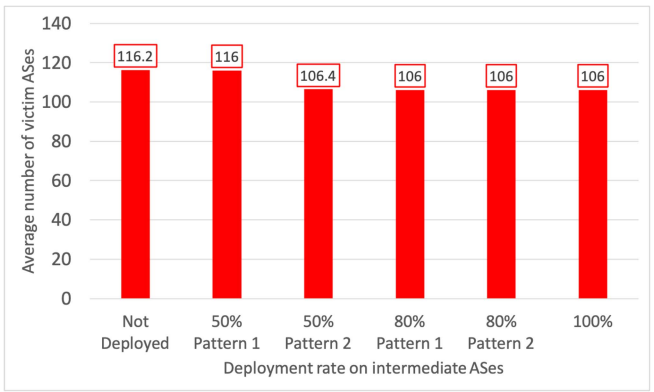


FIGURE 13. The transition of the average number of victim ASes of the normal attack by the chosen leaf-node ASes, where ASPV is deployed in the intermediate ASes. Other setting is common with Figure 11.

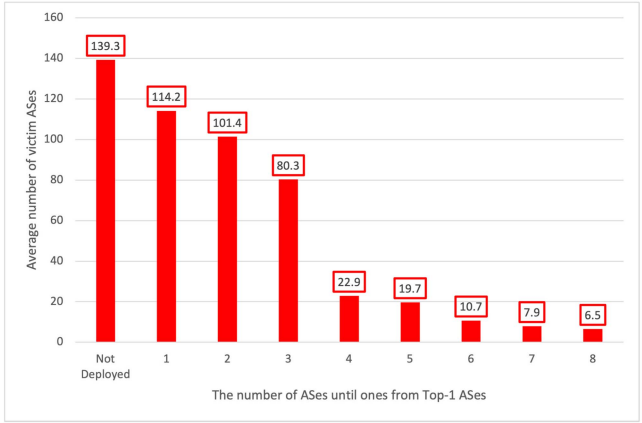


FIGURE 14. The transition of the average number of victim ASes of the normal attack by the outside ASes, where ASPV is deployed in the top ASes.

intermediate ASes to deploy ASPV. Accordingly, for the deployment rates of ASPV of 50% to 80%, we conducted the experiments by randomly choosing two patterns, referred to as Pattern 1 and Pattern 2, respectively. Details of the ASes in each pattern are omitted from this paper due to the large

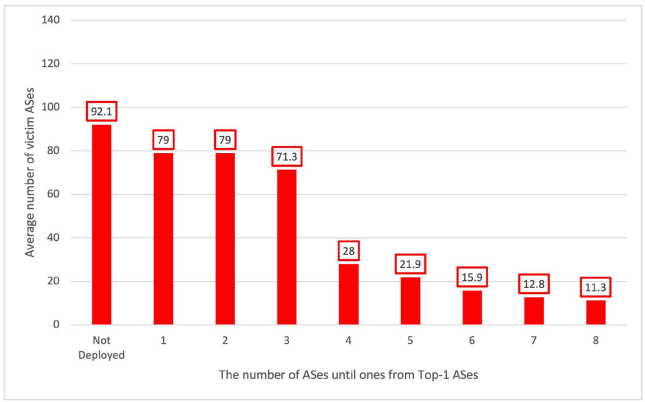


FIGURE 15. The transition of the average number of victim ASes of the ASPA-aware attack by the chosen leaf-node ASes, where ASPV is deployed in the top ASes.

number of ASes, and the code to reproduce them is available in the GitHub repository.[3] For the deployment from the leaf-node ASes to the intermediate ASes, the results are shown in Figure 30 to Figure 34 in Appendix B. A visualization of the average number of victim ASes in these results is shown in Figure 13.

According to Figure 13, even as the deployment rate increases, there is no decrease in the number of victim ASes across the experimental network. For instance, the average number of victim ASes varies only 0.2 between the rows of Not Deployed and 50% Pattern 1. In the row of 50% Pattern 2, the number of victim ASes decreased by about 10 ASes, but it is considered to be largely due to the chosen intermediate ASes rather than the deployment rate. Indeed, the number of victim ASes remains stable when Pattern 2 changes from 80% to 100%. The result of increasing the number of victim ASes from 50% to 80% in Pattern 1 is also similar. According to the evaluation metrics, the reduction rate was $R(N = \{(100\% \text{ intermediate ASes})\}, G, A) = 8.78\%$. It is considered that the effectiveness of ASPA is significantly limited. To summarize, despite the increase in the number of ASes with ASPV, no decrease in the number of victim ASes can be expected when ASPV is deployed in intermediate ASes.

From the results described above and the results of the previous section, we confirmed that, for the deployment of ASPV, the propagation of malicious routes could be prevented by deploying ASPV in top ASes.

D. RESULTS ON DETAILED EVALUATION FOR PREVENTING PROPAGATION OF MALICIOUS ROUTES

In this section, we evaluate the propagation of various malicious routes in the deployment of ASPV from the top ASes. Through the following evaluation, we confirm that, for the deployment of ASPV, the propagation of malicious routes can be prevented by deploying ASPV from top ASes.

3. https://github.com/han9umeda/LOTUS/tree/master/experiment

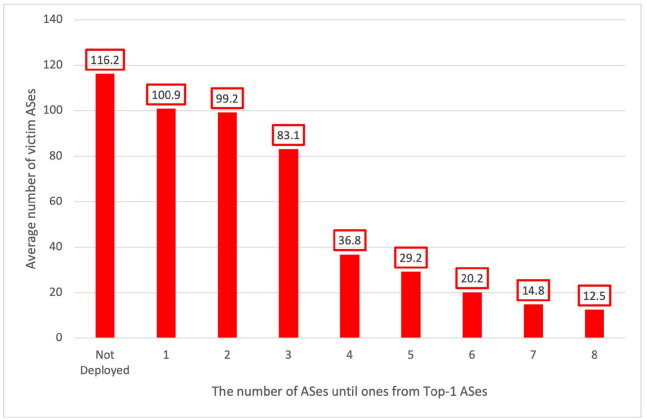


FIGURE 16. The transition of the average number of victim ASes of the mixed attack by the chosen leaf-node ASes, where ASPV is deployed in the top ASes.

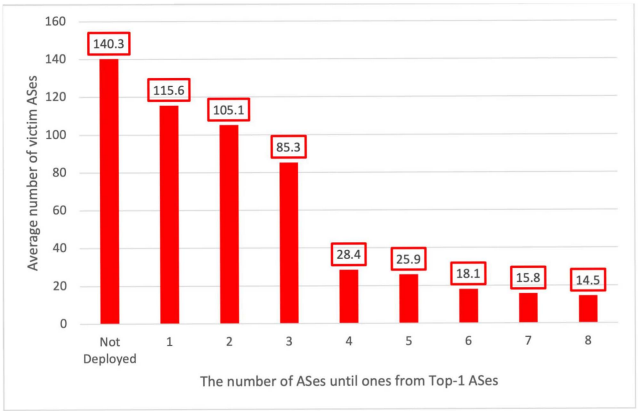


FIGURE 17. The transition of the average number of victim ASes of the mixed attack by the outside ASes, where ASPV is deployed in the top ASes.

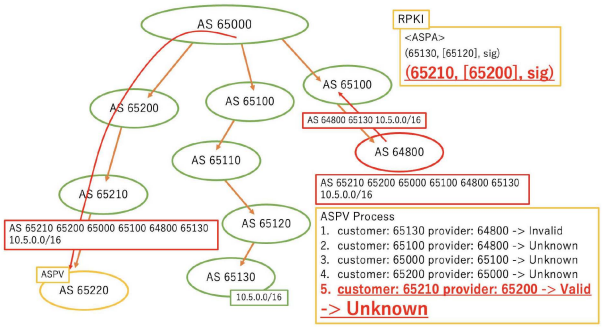


FIGURE 18. A phenomenon contrary to the ASPA's intuition: The result of ASPV on overall `AS_PATH` will be `Unknown` as shown in the right-bottom box. Even when ASes in the path towards its downstream issue ASPA as shown in the up-right box and the adjacency for the ASPA is Valid.

1) NORMAL ATTACK FROM OUTSIDE ASES

We first evaluate the normal attacks from the outside ASes. We measure the normal attacks on the experimental network without ASPAs and ASPV, and then the results are shown in Figure 35 in Appendix C. Likewise, we measure them on the experimental networks with ASPAs, where ASPV is deployed from the top AS to top-8 ASes. Their results

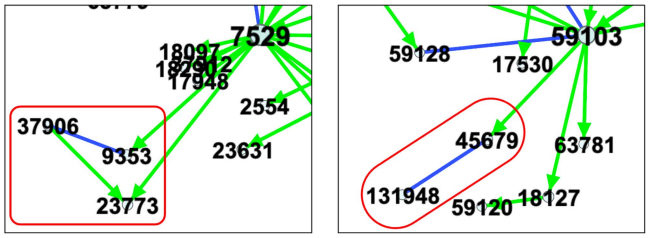


FIGURE 19. The difference between AS topologies around AS37906 and AS131948: The figure shows the topology difference near AS37906 in the left box and AS131948 in the right box.

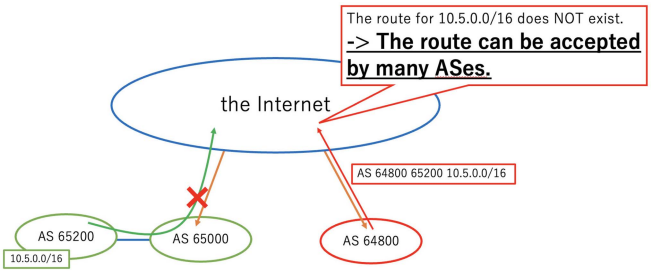


FIGURE 20. The worst case of the propagation of malicious routes: The figure shows the case when victim AS's routing information has not been propagated widely on the Internet. The malicious route from AS64800 in the red circle will be highly affected because the route for 10.5.0.0/16 does not exist on the Internet, as shown in the right-top box.

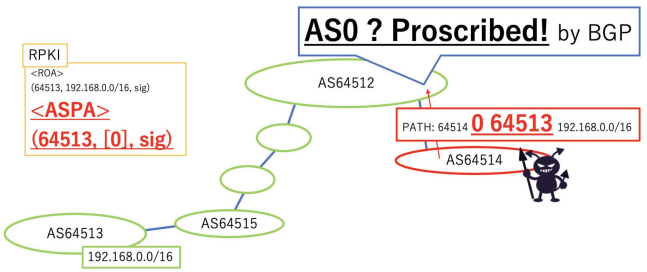


FIGURE 21. A negative example of the ASPA-aware attack: The figure shows a malicious route includes AS number 0. An ASPA specifying AS0 exists shown in the left yellow box. For conducting ASPA-aware attack, an adversary on the right advertise the route include AS0 and AS64513 shown in the right red box. But the malicious route will not success because AS0 is not allowed in BGP.

are shown in Figure 36 to Figure 43 in Appendix C. A visualization of the average number of victim ASes in these results is shown in Figure 14.

According to Figure 43 in Appendix C, although the average number of victim ASes is more than 40 for AS59105 and more than 90 for AS7500, most of the propagation of malicious routes is prevented. According to the evaluation metrics, the reduction rate was $R(N = \{(\text{top-8 ASes})\}, G, A) = 95.3\%$. Compared to the experimental network without ASPAs and ASPV, the average number of victim ASes could be reduced by 96% in the experimental network where ASPV was installed in the top-8 ASes. Therefore, when ASPV is deployed from the top AS, the propagation of malicious routes against the normal attacks from the outside ASes in the network can be prevented.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	141	NoN	36	106	4	13	50	34	31	1	2
3	59095	3	69	2	NoN	64	4	10	4	4	22	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	267	76	177	129	NoN	86	143	61	38	1	2
3	63779	4	111	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	166	48	96	111	6	13	53	NoN	31	1	2
4	59120	4	234	106	254	0	10	132	222	75	NoN	1	2
NoN	131948	4	505	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	504	504	518	504	504	504	504	518	504	1	NoN

FIGURE 22. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-1 AS. Other setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	96	11	16	35	2	4	6	9	28	1	2
2	55902	3	NoN	9	9	30	2	2	1	4	23	1	2
3	24275	3	141	NoN	30	101	4	13	50	28	26	1	2
3	59095	3	69	2	NoN	64	4	10	4	4	22	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	233	75	116	124	NoN	86	142	54	33	1	2
3	63779	4	110	9	23	47	5	NoN	4	14	29	1	2
3	18085	4	0	9	20	30	4	2	NoN	14	26	1	2
3	58651	4	166	48	55	111	6	13	53	NoN	31	1	2
4	59120	4	234	106	161	0	10	132	222	75	NoN	1	2
NoN	131948	4	505	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	504	504	518	504	504	504	504	518	504	1	NoN

FIGURE 23. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-2 AS from the top-1 AS. Other setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	0	11	13	33	2	4	3	9	26	1	2
2	55902	3	NoN	9	9	30	2	2	1	4	23	1	2
3	24275	3	0	NoN	27	99	4	13	1	28	24	1	2
3	59095	3	0	2	NoN	64	4	10	1	4	22	1	2
3	63781	3	0	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	0	72	113	122	NoN	86	73	51	31	1	2
3	63779	4	0	9	20	45	5	NoN	1	14	27	1	2
3	18085	4	0	9	20	30	4	2	NoN	14	26	1	2
3	58651	4	0	48	52	109	6	13	1	NoN	29	1	2
4	59120	4	0	106	161	0	10	132	129	75	NoN	1	2
NoN	131948	4	0	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	0	504	518	504	504	504	504	518	504	1	NoN

FIGURE 24. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-3 AS from the top-1 AS. Other setting is common with Figure 11.

2) ASPA-AWARE ATTACK FROM LEAF-NODE ASES

Next, we evaluate the ASPA-aware attacks as malicious route advertisements from leaf-node ASes. The results are shown in Figure 44 to Figure 52 in Appendix D. A visualization of the average number of victim ASes in these results is shown in Figure 15.

distance	↓ Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	0	9	11	31	2	2	1	7	26	1	2
2	55902	3	NoN	9	9	30	2	2	1	4	23	1	2
3	24275	3	0	NoN	27	99	4	13	1	28	24	1	2
3	59095	3	0	2	NoN	64	4	10	1	4	22	1	2
3	63781	3	0	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	0	72	113	122	NoN	18	1	51	31	1	2
3	63779	4	0	9	20	45	5	NoN	1	14	27	1	2
3	18085	4	0	9	20	30	4	2	NoN	14	26	1	2
3	58651	4	0	48	52	109	6	13	1	NoN	29	1	2
4	59120	4	0	106	161	0	10	16	1	75	NoN	1	2
NoN	131948	4	0	222	287	260	19	23	1	132	260	NoN	2
NoN	37906	4	0	223	288	261	19	21	1	132	261	1	NoN

FIGURE 25. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-4 AS from the top-1 AS. Other setting is common with Figure 11.

distance	↓ Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	0	9	11	13	2	2	1	7	8	1	2
2	55902	3	NoN	9	9	12	2	2	1	4	5	1	2
3	24275	3	0	NoN	27	38	4	13	1	28	13	1	2
3	59095	3	0	2	NoN	13	4	10	1	4	11	1	2
3	63781	3	0	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	0	72	113	46	NoN	18	1	51	13	1	2
3	63779	4	0	9	20	27	5	NoN	1	14	9	1	2
3	18085	4	0	9	20	12	4	2	NoN	14	8	1	2
3	58651	4	0	48	52	40	6	13	1	NoN	11	1	2
4	59120	4	0	106	161	0	10	16	1	75	NoN	1	2
NoN	131948	4	0	222	287	59	19	23	1	132	59	NoN	2
NoN	37906	4	0	223	288	60	19	21	1	132	60	1	NoN

FIGURE 26. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-5 AS from the top-1 AS. Other setting is common with Figure 11.

distance	↓ Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	0	2	4	13	2	2	1	7	8	1	2
2	55902	3	NoN	2	2	12	2	2	1	4	5	1	2
3	24275	3	0	NoN	27	38	4	13	1	28	13	1	2
3	59095	3	0	2	NoN	13	4	10	1	4	11	1	2
3	63781	3	0	2	22	NoN	5	12	1	23	1	1	2
3	59099	4	0	2	50	46	NoN	18	1	51	13	1	2
3	63779	4	0	2	13	27	5	NoN	1	14	9	1	2
3	18085	4	0	2	13	12	4	2	NoN	14	8	1	2
3	58651	4	0	2	3	40	6	13	1	NoN	11	1	2
4	59120	4	0	2	73	0	10	16	1	75	NoN	1	2
NoN	131948	4	0	2	109	59	19	23	1	132	59	NoN	2
NoN	37906	4	0	2	109	60	19	21	1	132	60	1	NoN

FIGURE 27. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-6 AS from the top-1 AS. Other setting is common with Figure 11.

Since the ASPA-aware attack is an attack whereby an adversary avoids `AS_PATH` that is evaluated as `Invalid` by ASPV, it seems that the propagation of malicious routes cannot be prevented even if the number of ASes with ASPV is increased. Nevertheless, the propagation of malicious routes to specific ASes, such

distance	↓ Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	0	2	3	13	2	2	1	6	8	1	2
2	55902	3	NoN	2	1	12	2	2	1	3	5	1	2
3	24275	3	0	NoN	3	38	4	13	1	6	13	1	2
3	59095	3	0	2	NoN	13	4	10	1	4	11	1	2
3	63781	3	0	2	3	NoN	5	12	1	6	1	1	2
3	59099	4	0	2	3	46	NoN	18	1	6	13	1	2
3	63779	4	0	2	3	27	5	NoN	1	4	9	1	2
3	18085	4	0	2	3	12	4	2	NoN	4	8	1	2
3	58651	4	0	2	3	40	6	13	1	NoN	11	1	2
4	59120	4	0	2	3	0	10	16	1	7	NoN	1	2
NoN	131948	4	0	2	3	59	19	23	1	32	59	NoN	2
NoN	37906	4	0	2	3	60	19	21	1	32	60	1	NoN

FIGURE 28. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-7 AS from the top-1 AS. Other setting is common with Figure 11.

distance	↓ Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	0	2	3	11	2	2	1	6	6	1	2
2	55902	3	NoN	2	1	10	2	2	1	3	3	1	2
3	24275	3	0	NoN	3	11	4	13	1	6	11	1	2
3	59095	3	0	2	NoN	11	4	10	1	4	9	1	2
3	63781	3	0	2	3	NoN	5	12	1	6	1	1	2
3	59099	4	0	2	3	11	NoN	18	1	6	11	1	2
3	63779	4	0	2	3	11	5	NoN	1	4	7	1	2
3	18085	4	0	2	3	10	4	2	NoN	4	6	1	2
3	58651	4	0	2	3	11	6	13	1	NoN	9	1	2
4	59120	4	0	2	3	0	10	16	1	7	NoN	1	2
NoN	131948	4	0	2	3	10	19	23	1	32	10	NoN	2
NoN	37906	4	0	2	3	11	19	21	1	32	11	1	NoN

FIGURE 29. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-8 AS from the top-1 AS. Other setting is common with Figure 11.

distance	↓ Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→		131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	32	0	2
2	55902	3	NoN	9	15	35	2	2	1	11	27	0	2
3	24275	3	141	NoN	36	106	4	13	50	34	31	0	2
3	59095	3	69	2	NoN	64	4	10	4	4	21	0	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	0	2
3	59099	4	267	76	177	129	NoN	86	143	61	38	0	2
3	63779	4	111	10	29	52	5	NoN	5	21	33	0	2
3	18085	4	0	9	26	35	4	2	NoN	21	30	0	2
3	58651	4	166	48	96	111	6	13	53	NoN	30	0	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	0	2
NoN	131948	544	544	544	544	544	544	544	544	544	544	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	543	0	NoN

FIGURE 30. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to 50% of the intermediate ASes with Pattern 1. Other setting is common with Figure 11.

as AS131948 and AS37905, has been prevented. It means that ASPAs and ASPV are effective against the ASPA-aware attacks in certain situations. We discuss the reason in Section V-C. According to the evaluation metrics, the reduction rate was $R(N = \{(\text{top-8 ASes})\}, G, A) = 87.7\%$.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→		131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	0	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	0	1	2
3	24275	3	141	NoN	36	106	4	13	50	34	0	1	2
3	59095	3	69	2	NoN	64	4	10	4	53	0	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	0	1	2
3	59099	4	267	76	177	129	NoN	86	143	61	0	1	2
3	63779	4	111	10	29	52	5	NoN	5	21	0	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	0	1	2
3	58651	4	166	48	96	111	6	13	53	NoN	0	1	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	1	2
NoN	131948	544	544	544	544	544	544	544	544	544	0	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	0	1	NoN

FIGURE 31. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to 50% of the intermediate ASes with Pattern 2. Other setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→		131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	0	0	2
2	55902	3	NoN	9	15	35	2	2	1	11	0	0	2
3	24275	3	141	NoN	36	106	4	13	50	34	0	0	2
3	59095	3	69	2	NoN	64	4	10	4	4	0	0	2
3	63781	3	128	30	50	NoN	5	12	1	23	0	0	2
3	59099	4	267	76	177	129	NoN	86	143	61	0	0	2
3	63779	4	111	10	29	52	5	NoN	5	21	0	0	2
3	18085	4	0	9	26	35	4	2	NoN	21	0	0	2
3	58651	4	166	48	96	111	6	13	53	NoN	0	0	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	0	2
NoN	131948	544	544	544	544	544	544	544	544	544	0	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	0	0	NoN

FIGURE 32. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to 80% of the intermediate ASes with Pattern 1. Other setting is common with Figure 11.

3) MIXED ATTACK FROM LEAF-NODE ASES

Next, we evaluate the mixed attacks as malicious route advertisements from leaf-node ASes. The results are shown in Figure 53 to Figure 61 in Appendix E. A visualization of the average number of victim ASes in these results is shown in Figure 16.

Consistent with the results shown in the previous experiments, as the number of ASes with ASPVs increases, the average number of victim ASes in the top-8 is suppressed to 12.5 against the mixed attacks. According to the evaluation metrics, the reduction rate was $R(N = \{(\text{top-8 ASes})\}, G, A) = 89.2\%$.

4) MIXED ATTACK FROM OUTSIDE ASES

Finally, we evaluate the mixed attacks as malicious route advertisements from leaf-node ASes. The results are shown in Figure 62 to Figure 70 in Appendix F. A visualization of the average number of victim ASes in these results is shown in Figure 17.

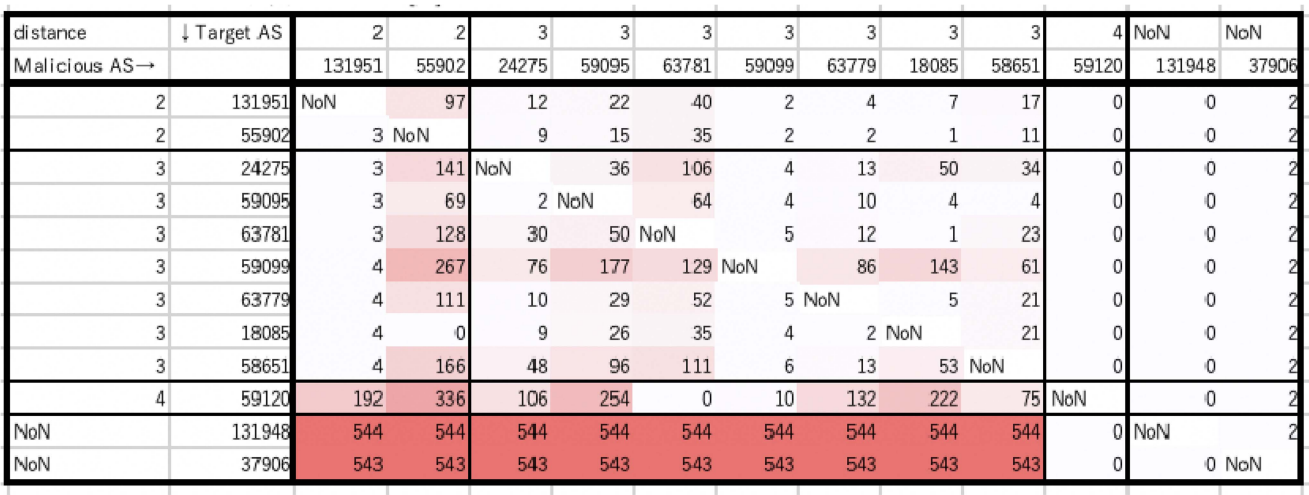
Consistent with the previous results, as the number of ASes with ASPVs increases, the propagation of malicious routes could be prevented. According to the evaluation metrics, the reduction rate was $R(N = \{(\text{top-8 ASes})\}, G, A) = 90.0\%$. Thus, it is considered that the deployment of ASPAs and ASPV from top ASes are significantly effective for preventing the propagation of malicious routes.

VI. DISCUSSION

In this section, we provide four considerations of our results in the experiments.

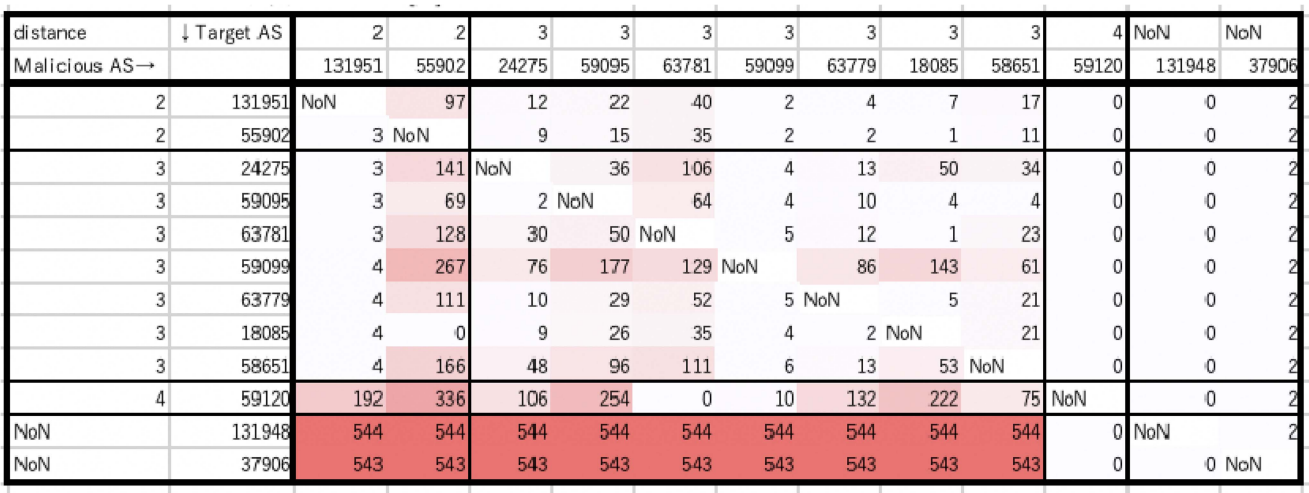
A. CASES OF PARTIAL DEPLOYMENT

Our primary goal is to show an effective case of partial deployment and how the case is expressed. In general,



distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→		131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	0	0	2
2	55902	3	NoN	9	15	35	2	2	1	11	0	0	2
3	24275	3	141	NoN	36	106	4	13	50	34	0	0	2
3	59095	3	69	2	NoN	64	4	10	4	4	0	0	2
3	63781	3	128	30	50	NoN	5	12	1	23	0	0	2
3	59099	4	267	76	177	129	NoN	86	143	61	0	0	2
3	63779	4	111	10	29	52	5	NoN	5	21	0	0	2
3	18085	4	0	9	26	35	4	2	NoN	21	0	0	2
3	58651	4	166	48	96	111	6	13	53	NoN	0	0	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	0	2
NoN	131948	544	544	544	544	544	544	544	544	544	0	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	0	0	NoN

FIGURE 33. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to 80% of the intermediate ASes with Pattern 2. Other setting is common with Figure 11.



distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→		131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	0	0	2
2	55902	3	NoN	9	15	35	2	2	1	11	0	0	2
3	24275	3	141	NoN	36	106	4	13	50	34	0	0	2
3	59095	3	69	2	NoN	64	4	10	4	4	0	0	2
3	63781	3	128	30	50	NoN	5	12	1	23	0	0	2
3	59099	4	267	76	177	129	NoN	86	143	61	0	0	2
3	63779	4	111	10	29	52	5	NoN	5	21	0	0	2
3	18085	4	0	9	26	35	4	2	NoN	21	0	0	2
3	58651	4	166	48	96	111	6	13	53	NoN	0	0	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	0	2
NoN	131948	544	544	544	544	544	544	544	544	544	0	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	0	0	NoN

FIGURE 34. Impact of the normal attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to 100% of the intermediate ASes. Other setting is common with Figure 11.

it is necessary to consider a practical scenario of partial deployment in the real world [34].

As the results of our experiments in the previous section, the deployment for ASPV from the top AS was effective. It is obvious by comparing Figure 12 with Figure 13. In the former case, the number of victim ASes decreases if the number of ASes with ASPV increases. In contrast, in the latter case, the number of victim ASes hardly decreases.

1) DEPLOYMENT OF ASPV IN TOP ASES

Compared to the case without ASPV, i.e., Figure 11 with the case where ASPV is deployed to the top AS, i.e., Figure 22, the deployment in the top AS cannot prevent malicious route advertisements properly. It means that, even when an AS with the most peers deploys ASPV, the routing information is propagated through other ASes.

Next, according to Figure 12, when ASPV is deployed until the top-4 ASes, the number of victim ASes decreases largely. It indicates that these ASes can cover many routes in the experimental network. We believe a similar result would be obtained for a network equivalent to the experimental network.

Furthermore, when ASPV is deployed in the top-8 ASes, the number of victim ASes against the mixed attack inside the network is decreased by 96% compared with the network without ASPV. In the experiments on other attacks, the deployment of ASPV decreased the average number of victim ASes by about 89% against the mixed attacks from inside the network, according to Figure 16. Likewise, the number of victim ASes against the mixed attack outside the network is decreased by 90% according to Figure 17. From the above results, it is found that deploying ASPV from the top ASes is effective for various types of attacks.

2) DEPLOYMENT OF ASPV IN INTERMEDIATE ASES

When ASPV is deployed in the intermediate ASes, the number of victim ASes is no longer decreased despite that the number of ASes with ASPV increases. For instance, it is shown by comparing Figure 11 and Figure 34. The number of victim ASes is expected to decrease for each case because 42 intermediate ASes, identical to all the ASes, deploy ASPV. Nevertheless, the results differ and are instead increasing.

The results described above are caused by the process of ASPV described in Section III-C. The overall `AS_PATH` attributes in the route advertisements from customers and peers are evaluated as `Invalid` when they contain even one invalid in the attributes. By contrast, in the route advertisements from providers, the overall `AS_PATH` attributes are evaluated as `Invalid` only when they contain more than one invalid. The reason is that the first invalid is assumed to be the switching point from upstream and downstream for the `AS_PATH` attributes. The number of invalids will be up to one since only the target AS issues ASPAs in our experiments. If a provider advertises malicious routes, ASPV cannot reject these routes.

To reject malicious route advertisements by the provider, it is required that the target AS issues ASPAs and any of ASes in the upstream of the routes issue ASPA, as well as deployment of ASPV in the received ASes. Under the conditions above, two invalids will appear on the malicious routes. The overall `AS_PATH` attributes will be evaluated as `Invalid`. In contrast, the reason not resulting in `Invalid` even when ASes on the downstream issue ASPAs is that the range of the downstream in the malicious routes is evaluated as `Valid` as shown in Figure 18.

B. ASES EXTREMELY AFFECTED BY MALICIOUS ROUTE ADVERTISEMENT

According to Figure 11, when AS131948 or AS37906 is designated as a target AS, 544 or 543 AS becomes the victim ASes, respectively. These values are extremely significant: in particular, the whole number of ASes is 547 except for the target AS and an adversary AS, and routing information for most of them is affected.

Such a situation is caused when the routes into the target AS are not advertised before the malicious route advertisement. The extremely affected ASes are an AS having only adjacency with peers and the AS having adjacency with peers and customers as shown in Figure 19. In this case, adjacent ASes that receive routing information do not advertise this information to the entire network, and thus most ASes in the network no longer have routing information for the target AS.

In the experiment network where most ASes do not have routes to a target AS, malicious routes tend to be selected according to Figure 20. For these ASes, the malicious routes for the target AS are accepted. In this situation, BGP routes for any new destination will be accepted unless any of

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500
2	131951	0	95	75	98	79	22	21	22	55	30	11
2	55902	0	7	0	0	32	14	14	9	22	12	8
3	24275	282	171	207	142	0	59	59	64	70	35	7
3	59095	141	0	96	70	0	7	7	10	0	22	1
3	63781	192	156	130	129	107	35	35	8	74	24	2
3	59099	516	353	380	268	224	209	209	202	104	165	150
3	63779	157	129	0	112	95	19	19	19	60	27	9
3	18085	113	81	0	0	67	16	16	16	45	19	9
3	58651	268	206	195	167	100	134	134	132	0	77	60
4	59120	261	343	282	337	321	384	384	349	232	330	324
NoN	131948	545	545	545	545	545	545	545	545	545	545	545
NoN	37906	544	544	544	544	544	544	544	544	544	544	544

Distance from 2497	↓ Target AS	1	1	1	1	1	1	1	1	1	1	1
Outside AS with→	NoN	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999
2	131951	18	11	21	4	4	7	11	3	2	0	2
2	55902	14	8	12	4	1	5	5	1	2	4	1
3	24275	14	7	18	27	6	5	11	1	6	4	2
3	59095	7	1	15	3	5	5	10	1	6	4	1
3	63781	9	1	17	20	7	5	11	1	7	4	2
3	59099	100	143	92	58	77	79	0	75	1	5	2
3	63779	15	8	1	13	7	5	10	1	7	5	2
3	18085	16	8	14	13	6	5	10	1	6	5	2
3	58651	62	54	22	3	8	5	17	1	8	5	2
4	59120	280	323	265	221	264	262	196	262	194	193	193
NoN	131948	545	545	545	545	545	545	545	545	545	545	545
NoN	37906	544	544	544	544	544	544	544	544	544	544	544

Distance from 2497	↓ Target AS	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	41	18	14	14	42	20	9	17	13	7	5
2	55902	36	8	8	8	33	1	1	12	10	5	3
3	24275	107	61	57	57	45	57	52	50	12	5	5
3	59095	65	9	5	4	28	10	6	5	3	5	4
3	63781	0	6	2	2	7	14	2	4	6	5	6
3	59099	130	196	196	196	61	108	145	68	19	5	6
3	63779	53	16	12	12	40	17	7	29	16	5	6
3	18085	36	13	9	9	37	12	3	12	10	5	5
3	58651	112	105	101	100	39	66	55	39	12	5	6
4	59120	0	303	303	303	31	137	224	26	8	5	6
NoN	131948	545	545	545	545	545	545	545	545	545	545	6
NoN	37906	544	544	544	544	544	544	544	544	544	544	6

FIGURE 35. **Impact of the normal attack by the outside ASes on the experimental networks, where ASPA is not deployed. The measurement setting is common with Figure 11.**

Distance from 2497	↓Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	95	75	98	79	22	21	22	55	30	11	18	11	21	4	4	7	11	3	2	0	2	41	18	14	14	42	20	9	17	13	7	5
2	55902	0	7	0	0	32	14	14	9	22	12	8	14	8	12	4	1	5	5	1	2	4	1	36	8	8	8	33	1	1	12	10	5	3
3	24275	0	171	207	142	0	59	59	64	70	35	7	14	7	18	27	6	5	11	1	6	4	2	107	61	57	57	45	57	52	50	12	5	5
3	59095	0	0	96	70	0	7	7	10	0	22	1	7	1	15	3	5	5	10	1	6	4	1	65	9	5	4	28	10	6	5	3	5	4
3	63781	0	156	130	129	107	35	35	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	353	380	268	224	209	209	202	104	165	150	100	143	92	58	77	79	0	75	1	5	2	130	196	196	196	61	108	145	68	19	5	6
3	63779	0	129	0	112	95	19	19	19	60	27	9	15	8	1	13	7	5	10	1	7	5	2	53	16	12	12	40	17	7	29	16	5	6
3	18085	0	81	0	0	67	16	16	16	45	19	9	16	8	14	13	6	5	10	1	6	5	2	36	13	9	9	37	12	3	12	10	5	5
3	58651	0	206	195	167	100	134	134	132	0	77	60	62	54	22	3	8	5	17	1	8	5	2	112	105	101	100	39	66	55	39	12	5	6
4	59120	0	269	165	235	229	298	299	246	93	249	236	165	235	134	76	141	130	13	130	11	5	2	0	303	303	303	31	137	224	26	8	5	6
NoN	131948	0	506	506	506	506	506	506	506	520	506	506	506	506	506	520	506	506	506	506	506	5	2	506	506	506	506	506	506	506	506	506	506	6
NoN	37906	0	505	505	505	505	505	505	505	519	505	505	505	505	505	519	505	505	505	505	505	5	2	505	505	505	505	505	505	505	505	505	505	6

FIGURE 36. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	75	97	78	16	15	16	54	22	4	9	3	21	4	4	7	11	3	2	0	2	36	11	7	7	37	19	8	10	7	7	5
2	55902	0	0	0	0	32	8	8	3	22	5	2	7	1	12	4	1	5	5	1	2	4	1	31	1	1	1	28	1	1	5	4	5	3
3	24275	0	0	207	142	0	53	53	58	70	29	2	8	1	18	27	6	5	11	1	6	4	2	102	55	51	51	40	57	52	44	6	5	5
3	59095	0	0	96	70	0	7	7	10	0	22	1	7	1	15	3	5	5	10	1	6	4	1	65	9	5	4	28	10	6	5	3	5	4
3	63781	0	0	130	129	107	35	35	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	380	234	182	162	162	157	103	98	83	10	75	92	57	77	79	0	75	1	5	2	125	143	143	144	56	107	144	61	13	5	6
3	63779	0	0	0	111	94	13	13	13	59	20	3	8	1	1	13	7	5	10	1	7	5	2	48	9	5	5	35	16	6	22	10	5	6
3	18085	0	0	0	0	67	10	10	10	45	12	3	9	1	14	13	6	5	10	1	6	5	2	31	6	2	2	32	12	3	5	4	5	5
3	58651	0	0	195	167	100	99	99	98	0	24	8	9	1	22	3	8	5	17	1	8	5	2	112	58	54	54	39	66	55	39	12	5	6
4	59120	0	0	165	235	229	213	214	135	93	146	132	10	130	134	76	141	130	13	130	11	5	2	0	223	223	224	31	137	224	26	8	5	6
NoN	131948	0	0	506	506	506	506	506	506	520	506	506	506	506	506	520	506	506	506	506	506	5	2	506	506	506	506	506	506	506	506	506	506	6
NoN	37906	0	0	505	505	505	505	505	505	519	505	505	505	505	505	519	505	505	505	505	505	5	2	505	505	505	505	505	505	505	505	505	505	6

FIGURE 37. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-2 AS from the top-1 AS. The measurement setting is common with Figure 11.

IEEE ComSoc
IEEE Open Journal of the Communications Society

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	75	0	75	13	12	11	51	22	4	9	3	21	4	4	7	11	3	2	0	2	34	8	4	4	35	14	5	7	4	7	5
2	55902	0	0	0	0	32	8	8	3	22	5	2	7	1	12	4	1	5	5	1	2	4	1	31	1	1	1	28	1	1	5	4	5	3
3	24275	0	0	207	0	0	4	4	9	70	29	2	8	1	18	27	6	5	11	1	6	4	2	100	6	2	2	38	12	3	41	3	5	5
3	59095	0	0	96	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	65	6	2	1	28	7	3	5	3	5	4
3	63781	0	0	130	0	107	35	35	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	379	0	179	77	77	72	100	98	83	10	75	92	54	77	79	0	75	1	5	2	123	74	74	75	54	18	75	58	10	5	6
3	63779	0	0	0	0	91	10	10	10	56	20	3	8	1	1	13	7	5	10	1	7	5	2	46	6	2	2	33	13	3	19	7	5	6
3	18085	0	0	0	0	67	10	10	10	45	12	3	9	1	14	13	6	5	10	1	6	5	2	31	6	2	2	32	12	3	5	4	5	5
3	58651	0	0	195	0	100	53	53	52	0	24	8	9	1	22	3	8	5	17	1	8	5	2	110	6	2	2	37	18	3	36	9	5	6
4	59120	0	0	165	0	229	108	109	9	93	146	132	10	130	134	76	141	130	13	130	11	5	2	0	130	130	131	31	16	131	26	8	5	6
NoN	131948	0	0	506	0	506	506	506	215	110	506	506	506	506	506	110	506	506	506	506	506	5	2	506	506	506	506	506	18	506	506	215	506	6
NoN	37906	0	0	505	0	505	505	505	216	110	505	505	505	505	505	110	505	505	505	505	505	5	2	505	505	505	505	505	18	505	505	216	505	6

FIGURE 38. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-3 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	0	0	73	11	10	11	51	20	2	9	1	19	4	2	5	9	1	2	0	2	32	6	2	2	33	14	3	5	4	5	5
2	55902	0	0	0	0	32	8	8	3	22	5	2	7	1	12	4	1	5	5	1	2	4	1	31	1	1	1	28	1	1	5	4	5	3
3	24275	0	0	0	0	0	4	4	9	70	29	2	8	1	18	27	6	5	11	1	6	4	2	100	6	2	2	38	12	3	41	3	5	5
3	59095	0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	65	6	2	1	28	7	3	5	3	5	4
3	63781	0	0	0	0	107	35	35	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	0	0	126	77	77	72	100	32	9	10	1	24	54	3	5	0	1	1	5	2	123	6	2	2	54	18	3	58	10	5	6
3	63779	0	0	0	0	91	10	10	10	56	20	3	8	1	1	13	7	5	10	1	7	5	2	46	6	2	2	33	13	3	19	7	5	6
3	18085	0	0	0	0	67	10	10	10	45	12	3	9	1	14	13	6	5	10	1	6	5	2	31	6	2	2	32	12	3	5	4	5	5
3	58651	0	0	0	0	100	53	53	52	0	24	8	9	1	22	3	8	5	17	1	8	5	2	110	6	2	2	37	18	3	36	9	5	6
4	59120	0	0	0	0	121	108	109	9	93	29	2	10	1	18	76	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
NoN	131948	0	0	0	0	223	223	223	215	110	33	97	10	1	24	110	20	5	20	1	20	5	2	261	6	2	2	287	18	3	85	215	5	6
NoN	37906	0	0	0	0	224	224	224	216	110	33	98	10	1	22	110	20	5	20	1	20	5	2	262	6	2	2	288	18	3	86	216	5	6

FIGURE 39. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-4 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	0	0	73	11	10	11	51	20	2	9	1	19	4	2	5	9	1	2	0	2	14	6	2	2	15	14	3	5	4	5	5
2	55902	0	0	0	0	32	8	8	3	22	5	2	7	1	12	4	1	5	5	1	2	4	1	13	1	1	1	10	1	1	5	4	5	3
3	24275	0	0	0	0	0	4	4	9	70	29	2	8	1	18	27	6	5	11	1	6	4	2	39	6	2	2	27	12	3	41	3	5	5
3	59095	0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	14	6	2	1	17	7	3	5	3	5	4
3	63781	0	0	0	0	107	35	35	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	0	0	126	77	77	72	100	32	9	10	1	24	54	3	5	0	1	1	5	2	47	6	2	2	36	18	3	58	10	5	6
3	63779	0	0	0	0	91	10	10	10	56	20	3	8	1	1	13	7	5	10	1	7	5	2	28	6	2	2	15	13	3	19	7	5	6
3	18085	0	0	0	0	67	10	10	10	45	12	3	9	1	14	13	6	5	10	1	6	5	2	13	6	2	2	14	12	3	5	4	5	5
3	58651	0	0	0	0	100	53	53	52	0	24	8	9	1	22	3	8	5	17	1	8	5	2	41	6	2	2	19	18	3	36	9	5	6
4	59120	0	0	0	0	121	108	109	9	93	29	2	10	1	18	76	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
NoN	131948	0	0	0	0	223	223	223	215	110	33	97	10	1	24	110	20	5	20	1	20	5	2	60	6	2	2	90	18	3	85	215	5	6
NoN	37906	0	0	0	0	224	224	224	216	110	33	98	10	1	22	110	20	5	20	1	20	5	2	61	6	2	2	91	18	3	86	216	5	6

FIGURE 40. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-5 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	0	0	0	4	3	10	51	20	2	9	1	19	4	2	5	9	1	2	0	2	14	6	2	2	15	14	3	5	3	5	5
2	55902	0	0	0	0	0	1	1	2	22	5	2	7	1	12	4	1	5	5	1	2	4	1	13	1	1	1	10	1	1	5	3	5	3
3	24275	0	0	0	0	0	4	4	9	70	29	2	8	1	18	27	6	5	11	1	6	4	2	39	6	2	2	27	12	3	41	3	5	5
3	59095	0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	14	6	2	1	17	7	3	5	3	5	4
3	63781	0	0	0	0	0	4	4	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	0	0	0	4	4	9	100	32	9	10	1	24	54	3	5	0	1	1	5	2	47	6	2	2	36	18	3	58	9	5	6
3	63779	0	0	0	0	0	3	3	9	56	20	3	8	1	1	13	7	5	10	1	7	5	2	28	6	2	2	15	13	3	19	6	5	6
3	18085	0	0	0	0	0	3	3	9	45	12	3	9	1	14	13	6	5	10	1	6	5	2	13	6	2	2	14	12	3	5	3	5	5
3	58651	0	0	0	0	0	4	4	9	0	24	8	9	1	22	3	8	5	17	1	8	5	2	41	6	2	2	19	18	3	36	8	5	6
4	59120	0	0	0	0	0	4	4	9	93	29	2	10	1	18	76	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
NoN	131948	0	0	0	0	0	4	4	10	110	33	97	10	1	24	110	20	5	20	1	20	5	2	60	6	2	2	90	18	3	85	10	5	6
NoN	37906	0	0	0	0	0	4	4	10	110	33	98	10	1	22	110	20	5	20	1	20	5	2	61	6	2	2	91	18	3	86	10	5	6

FIGURE 41. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-6 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	0	0	0	4	3	10	0	20	2	9	1	19	3	2	5	9	1	2	0	2	14	6	2	2	15	14	3	5	3	5	5
2	55902	0	0	0	0	0	1	1	2	0	5	2	7	1	12	3	1	5	5	1	2	4	1	13	1	1	1	10	1	1	5	3	5	3
3	24275	0	0	0	0	0	4	4	9	0	29	2	8	1	18	3	6	5	11	1	6	4	2	39	6	2	2	27	12	3	41	3	5	5
3	59095	0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	14	6	2	1	17	7	3	5	3	5	4
3	63781	0	0	0	0	0	4	4	8	0	24	2	9	1	17	1	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	0	0	0	4	4	9	0	32	9	10	1	24	3	3	5	0	1	1	5	2	47	6	2	2	36	18	3	58	9	5	6
3	63779	0	0	0	0	0	3	3	9	0	20	3	8	1	1	3	7	5	10	1	7	5	2	28	6	2	2	15	13	3	19	6	5	6
3	18085	0	0	0	0	0	3	3	9	0	12	3	9	1	14	3	6	5	10	1	6	5	2	13	6	2	2	14	12	3	5	3	5	5
3	58651	0	0	0	0	0	4	4	9	0	24	8	9	1	22	3	8	5	17	1	8	5	2	41	6	2	2	19	18	3	36	8	5	6
4	59120	0	0	0	0	0	4	4	9	0	29	2	10	1	18	3	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
NoN	131948	0	0	0	0	0	4	4	10	0	33	97	10	1	24	3	20	5	20	1	20	5	2	60	6	2	2	90	18	3	85	10	5	6
NoN	37906	0	0	0	0	0	4	4	10	0	33	98	10	1	22	3	20	5	20	1	20	5	2	61	6	2	2	91	18	3	86	10	5	6

FIGURE 42. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-7 AS from the top-1 AS.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	0	0	0	0	0	4	3	10	0	20	2	9	1	19	3	2	5	9	1	2	0	2	12	6	2	2	13	14	3	3	3	5	5
2	55902	0	0	0	0	0	1	1	2	0	5	2	7	1	12	3	1	5	5	1	2	4	1	11	1	1	1	8	1	1	3	3	5	3
3	24275	0	0	0	0	0	4	4	9	0	29	2	8	1	18	3	6	5	11	1	6	4	2	12	6	2	2	25	12	3	12	3	5	5
3	59095	0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	12	6	2	1	15	7	3	3	3	5	4
3	63781	0	0	0	0	0	4	4	8	0	24	2	9	1	17	1	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3	59099	0	0	0	0	0	4	4	9	0	32	9	10	1	24	3	3	5	0	1	1	5	2	12	6	2	2	34	18	3	21	9	5	6
3	63779	0	0	0	0	0	3	3	9	0	20	3	8	1	1	3	7	5	10	1	7	5	2	12	6	2	2	13	13	3	3	6	5	6
3	18085	0	0	0	0	0	3	3	9	0	12	3	9	1	14	3	6	5	10	1	6	5	2	11	6	2	2	12	12	3	3	3	5	5
3	58651	0	0	0	0	0	4	4	9	0	24	8	9	1	22	3	8	5	17	1	8	5	2	12	6	2	2	17	18	3	2	8	5	6
4	59120	0	0	0	0	0	4	4	9	0	29	2	10	1	18	3	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
NoN	131948	0	0	0	0	0	4	4	10	0	33	97	10	1	24	3	20	5	20	1	20	5	2	11	6	2	2	45	18	3	34	10	5	6
NoN	37906	0	0	0	0	0	4	4	10	0	33	98	10	1	22	3	20	5	20	1	20	5	2	12	6	2	2	46	18	3	34	10	5	6

FIGURE 43. Impact of the normal attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-8 AS from the top-1 AS. The measurement setting is common with Figure 11.

AS_PATH validation. Therefore, most of the ASes were affected by malicious routes.

In terms of deploying ASPA or ASPV, by facilitating ASPV deployment appropriately, ASPV will be effective to prevent the propagation of malicious routes as shown in Section V-D. According to Figure 22 to Figure 29, the number of victims AS becomes less in proportion to the deployment of ASPV.

These data are the results of ASes whose routing information is never advertised on the Internet, e.g., non-operated AS numbers or privately operated AS on the Internet. In this case, an adversary tries to use such AS numbers illegally. Our results demonstrate that such an adversary's malicious activity can be prevented by adequately deploying ASPA and ASPV.

C. ASPA-AWARE ATTACK

We found a potential threat named the ASPA-aware attack that utilized existing ASPAs and discussed the effect of the attack. According to the experimental results in Section V-D, we identify that no additional effects will be caused for a victim AS. The above results indicate that appropriately deploying ASPA and ASPV is also effective in preventing malicious route advertisements in a sophisticated fashion. We discuss such an insight in detail below.

1) IMPACT ON AS_PATH LENGTH

Leveraging ASPAs to advertise malicious routes for an ASPA-aware attack brings an advantage and a disadvantage to an adversary. The advantage is that the adversary can let ASes deploying ASPV accept malicious routes even when an ASPA exists already. On the other hand, the disadvantage for the adversary is that the AS_PATH length of malicious routes needs to be longer to include adjacency in the ASPAs. We discuss how ASPAs affect the security of BGP from the viewpoint of the ASPA-aware attack.

We then confirm that the ASPA-aware attack is no longer apparent to be a new threat. When we compare the average number of victim ASes in the experimental network where ASPV is deployed until the top-8 ASes, we found 4.9 ASes for the normal attack, 11.3 ASes for the ASPA-aware attack, and 12.5 ASes for the mixed attack in Figure 29, Figure 12, Figure 61 and Figure 16, respectively. Although the average number of victim ASes has slightly increased, it is considered to be a minimal impact taking into account that the total number of ASes is 549.

In our experiments, we assumed that only a target AS issues ASPAs. The effectiveness of the ASPA-aware attack will be further impeded if a provider AS issues ASPAs as well as the target AS. As described above, the AS_PATH length in malicious routes becomes longer by composing the AS_PATH as including the AS_PATH in ASPAs. If ASPAs are issued continuously, the effect of the attack is weakened because the enumeration of matching ASes is longer. The above observation indicates that the security of BGP improves in proportion to the deployment of ASPA and ASPV. We must have a situation of partial deployment in the real Internet, and thus ASPA and ASPV are superior to existing technologies [27], [33] that cannot guarantee security unless full deployment [34], [38].

2) IMPACT ON AS TOPOLOGY

The ASPA-aware attack is a potential approach to circumvent the detection of malicious routes by ASPV, and hence one might think that the number of victim ASes is not decreased even if ASPA and ASPV are deployed primarily. Notably, Figure 15 shows the number of victim ASes decreases in proportion to the deployment of ASPV. We shed light on the reasons for the results in detail.

When we deeply analyze the number of victim ASes from Figure 44 to Figure 52, decreasing the victim ASes has happened only when the target AS is AS131948 or AS37906. These ASes have a special AS topology around them as shown in Fig. 19. From the viewpoint of ASPAs, since these ASes do not have a provider, if an ASPA is issued, AS0 should be set in [SPAS] of the ASPAs.

When such ASPAs have been issued, an adversary cannot bypass ASPV even using the ASPA-aware attack as shown in Figure 21: because the malicious routes composed in the manner of the ASPA-aware attack have AS0 in AS_PATH, but it is not allowed in the BGP protocol specification [29].

In summary, the decrease in the victim ASes against the ASPA-aware attacks in proportion to the deployment of ASPV was caused by the fact that the ASPA-aware attack itself became disallowed by the issued ASPAs. We believe that the above fact is strong evidence for an advantage of ASPV and ASPV.

In practical operations, ASPAs can be used for protecting AS numbers themselves besides issuing ASPAs having AS0 as [SPAS] by ASes do not have its provider AS. Indeed, ROA described in RFC6483 [25] is used to prevent unauthorized use of IP address resources by issuing a ROA with AS0 as the origin AS for IP address resources assigned but not advertised as BGP route. Similarly, to prevent unauthorized use of AS numbers, it can be a method issuing ASPAs with AS0 as [SPAS] for ASes that have been assigned but not announced BGP routes on the Internet at that point.

D. THREATS TO VALIDITY

1) SPECIFICITY OF EXPERIMENTAL NETWORK

Our experimental network is with AS numbers assigned from JPNIC, a national level of an Internet registry. For similar topologies such that routes are concentrated to a small number of ASes, similar results will be obtained. Meanwhile, we know that there are biases between routes observed at different points. Our evaluation method, including LOTUS, can be applied in other regions or countries using BGP data observed at each point. However, their results may be different in these points from this paper. Namely, the number of victim ASes may increase for regions with well-distributed connections. Further evaluation should be undertaken for other/broader results in the future.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	544	544	544	544	544	544	544	544	544	544	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	543	1	NoN

FIGURE 44. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPA is not deployed. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	505	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	504	504	518	504	504	504	504	518	504	1	NoN

FIGURE 45. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	505	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	504	504	518	504	504	504	504	518	504	1	NoN

FIGURE 46. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-2 AS from the top-1 AS. The measurement setting is common with Figure 11.

2) AS POLICIES

In the real-world operation on Internet, each AS has an individual routing policy for BGP. However, such a routing policy in each AS was not considered in our evaluation. The AS's routing policies may not be implemented as same as publicly available ones (i.e., from IRR). For example, there are ASes that take their specific routes other than the shortest path in practical. For those ASes, the results in this

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	0	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	0	504	518	504	504	504	504	518	504	1	NoN

FIGURE 47. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-3 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	0	222	287	260	19	23	1	132	260	NoN	2
NoN	37906	4	0	223	288	261	19	21	1	132	261	1	NoN

FIGURE 48. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-4 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	0	222	287	59	19	23	1	132	59	NoN	2
NoN	37906	4	0	223	288	60	19	21	1	132	60	1	NoN

FIGURE 49. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-5 AS from the top-1 AS. The measurement setting is common with Figure 11.

manuscript may be different from the actual results involving AS's policies. Actual evaluation on the real Internet will be needed to evaluate ASPA and ASPV with AS policies.

3) ASSUMPTION OF ROA DEPLOYMENT

We also put an assumption that ROAs are fully deployed. Without the deployment of ROAs, vulnerabilities will remain through prefix hijacking [18] even if ASPAs exist. In

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	0	2	109	59	19	23	1	132	59	NoN	2
NoN	37906	4	0	2	109	60	19	21	1	132	60	1	NoN

FIGURE 50. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-6 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	0	2	3	59	19	23	1	32	59	NoN	2
NoN	37906	4	0	2	3	60	19	21	1	32	60	1	NoN

FIGURE 51. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-7 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	33	2	4	7	13	31	1	2
2	55902	1	NoN	9	15	27	2	2	1	11	28	1	2
3	24275	2	48	NoN	8	31	2	2	4	11	24	1	2
3	59095	2	3	1	NoN	22	2	2	1	3	16	1	2
3	63781	2	0	2	4	NoN	2	2	1	5	1	1	2
3	59099	3	94	10	20	38	NoN	2	5	15	33	1	2
3	63779	1	4	10	20	34	2	NoN	5	11	31	1	1
3	18085	1	0	9	15	31	2	2	NoN	11	28	1	2
3	58651	3	51	9	8	31	2	2	4	NoN	26	1	2
4	59120	3	128	30	50	0	5	12	1	23	NoN	1	2
NoN	131948	4	0	2	3	10	19	23	1	32	10	NoN	2
NoN	37906	4	0	2	3	11	19	21	1	32	11	1	NoN

FIGURE 52. Impact of the ASPA-aware attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-8 AS from the top-1 AS. The measurement setting is common with Figure 11.

other words, the deployment of ROAs is dominant for the effectiveness of ASPV. The deployment rate of ROAs should be considered for further appropriate evaluation of ASPAs.

VII. CONCLUSION

In this paper, we discussed the effectiveness of ASPAs which provide the path validation on BGP in a partial deployment. To this end, we developed a novel simulation tool, LOTUS,

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	141	NoN	36	106	4	13	50	34	31	1	2
3	59095	3	69	2	NoN	64	4	10	4	4	22	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	267	76	177	129	NoN	86	143	61	38	1	2
3	63779	4	111	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	166	48	96	111	6	13	53	NoN	31	1	2
4	59120	192	336	106	254	0	10	132	222	75	NoN	1	2
NoN	131948	544	544	544	544	544	544	544	544	544	544	NoN	2
NoN	37906	543	543	543	543	543	543	543	543	543	543	1	NoN

FIGURE 53. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPA is not deployed. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	141	NoN	36	106	4	13	50	34	31	1	2
3	59095	3	69	2	NoN	64	4	10	4	4	22	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	267	76	177	129	NoN	86	143	61	38	1	2
3	63779	4	111	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	166	48	96	111	6	13	53	NoN	31	1	2
4	59120	4	234	106	254	0	10	132	222	75	NoN	1	2
NoN	131948	4	505	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	504	504	518	504	504	504	504	518	504	1	NoN

FIGURE 54. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	97	12	22	40	2	4	7	17	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	141	NoN	36	106	4	13	50	34	31	1	2
3	59095	3	69	2	NoN	64	4	10	4	4	22	1	2
3	63781	3	128	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	234	76	122	129	NoN	86	143	61	38	1	2
3	63779	4	111	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	166	48	55	111	6	13	53	NoN	31	1	2
4	59120	4	234	106	161	0	10	132	222	75	NoN	1	2
NoN	131948	4	505	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	504	504	518	504	504	504	504	518	504	1	NoN

FIGURE 55. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-2 AS from the top-1 AS. The measurement setting is common with Figure 11.

for the exchange of routing information between ASes in an AS network. LOTUS can simulate any AS network by varying the deployment of ASPAs and ASPV. The simulation results by LOTUS showed that the most effective deployment for preventing the propagation of malicious routes is the case where ASPVs are deployed from top ASes. Remarkably, by introducing ASPV to the top-eight ASes, the number of the victim ASes by the normal attack could be decreased by 96% on average. In contrast, the deployment of ASPV to intermediate ASes has no advantage for

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	12	22	40	2	4	7	17	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	48	NoN	33	106	4	13	4	34	29	1	2
3	59095	3	3	2	NoN	64	4	10	1	4	22	1	2
3	63781	3	0	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	94	73	122	129	NoN	86	77	59	38	1	2
3	63779	4	4	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	51	48	52	111	6	13	4	NoN	29	1	2
4	59120	4	128	106	161	0	10	132	129	75	NoN	1	2
NoN	131948	4	0	505	519	505	505	505	505	519	505	NoN	2
NoN	37906	4	0	504	518	504	504	504	504	518	504	1	NoN

FIGURE 56. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-3 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	38	2	4	7	15	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	48	NoN	33	106	4	13	4	34	29	1	2
3	59095	3	3	2	NoN	64	4	10	1	4	22	1	2
3	63781	3	0	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	94	73	122	129	NoN	18	5	59	38	1	2
3	63779	4	4	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	51	48	52	111	6	13	4	NoN	29	1	2
4	59120	4	128	106	161	0	10	16	1	75	NoN	1	2
NoN	131948	4	0	222	287	260	19	23	1	132	260	NoN	2
NoN	37906	4	0	223	288	261	19	21	1	132	261	1	NoN

FIGURE 57. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-4 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	38	2	4	7	15	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	48	NoN	33	56	4	13	4	34	29	1	2
3	59095	3	3	2	NoN	24	4	10	1	4	22	1	2
3	63781	3	0	30	50	NoN	5	12	1	23	1	1	2
3	59099	4	94	73	122	71	NoN	18	5	59	38	1	2
3	63779	4	4	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	51	48	52	60	6	13	4	NoN	29	1	2
4	59120	4	128	106	161	0	10	16	1	75	NoN	1	2
NoN	131948	4	0	222	287	59	19	23	1	132	59	NoN	2
NoN	37906	4	0	223	288	60	19	21	1	132	60	1	NoN

FIGURE 58. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-5 AS from the top-1 AS. The measurement setting is common with Figure 11.

preventing the propagation of malicious routes because the ASes with ASPV receive malicious route advertisements. Furthermore, we also evaluated the impact of the ASPA-aware attacks, whereby an adversary leverages the issued ASPAs. As a result of the experiment, we confirmed that the number of victim ASes by malicious route advertisements did not increase significantly and that ASPA and ASPV no longer provide an advantage to an adversary.

Although we conducted the experiments with the AS network consisting of ASes with AS numbers assigned

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	38	2	4	7	15	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	48	NoN	33	56	4	13	4	34	29	1	2
3	59095	3	3	2	NoN	24	4	10	1	4	22	1	2
3	63781	3	0	2	22	NoN	5	12	1	23	1	1	2
3	59099	4	94	10	64	71	NoN	18	5	59	38	1	2
3	63779	4	4	10	29	52	5	NoN	5	21	34	1	2
3	18085	4	0	9	26	35	4	2	NoN	21	31	1	2
3	58651	4	51	9	10	60	6	13	4	NoN	29	1	2
4	59120	4	128	30	100	0	10	16	1	75	NoN	1	2
NoN	131948	4	0	2	109	59	19	23	1	132	59	NoN	2
NoN	37906	4	0	2	109	60	19	21	1	132	60	1	NoN

FIGURE 59. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-6 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	38	2	4	7	15	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	48	NoN	10	56	4	13	4	13	29	1	2
3	59095	3	3	2	NoN	24	4	10	1	4	22	1	2
3	63781	3	0	2	4	NoN	5	12	1	7	1	1	2
3	59099	4	94	10	20	71	NoN	18	5	15	38	1	2
3	63779	4	4	10	20	52	5	NoN	5	12	34	1	2
3	18085	4	0	9	17	35	4	2	NoN	12	31	1	2
3	58651	4	51	9	10	60	6	13	4	NoN	29	1	2
4	59120	4	128	30	50	0	10	16	1	24	NoN	1	2
NoN	131948	4	0	2	3	59	19	23	1	32	59	NoN	2
NoN	37906	4	0	2	3	60	19	21	1	32	60	1	NoN

FIGURE 60. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-7 AS from the top-1 AS. The measurement setting is common with Figure 11.

distance	↓Target AS	2	2	3	3	3	3	3	3	3	4	NoN	NoN
Malicious AS→	NoN	131951	55902	24275	59095	63781	59099	63779	18085	58651	59120	131948	37906
2	131951	NoN	6	10	20	38	2	4	7	15	33	1	2
2	55902	3	NoN	9	15	35	2	2	1	11	28	1	2
3	24275	3	48	NoN	10	31	4	13	4	13	29	1	2
3	59095	3	3	2	NoN	24	4	10	1	4	22	1	2
3	63781	3	0	2	4	NoN	5	12	1	7	1	1	2
3	59099	4	94	10	20	38	NoN	18	5	15	38	1	2
3	63779	4	4	10	20	38	5	NoN	5	12	34	1	2
3	18085	4	0	9	17	35	4	2	NoN	12	31	1	2
3	58651	4	51	9	10	33	6	13	4	NoN	29	1	2
4	59120	4	128	30	50	0	10	16	1	24	NoN	1	2
NoN	131948	4	0	2	3	10	19	23	1	32	10	NoN	2
NoN	37906	4	0	2	3	11	19	21	1	32	11	1	NoN

FIGURE 61. Impact of the mixed attack by the chosen leaf-node ASes on the experimental networks, where ASPV is deployed to the top-8 AS from the top-1 AS. The measurement setting is common with Figure 11.

from JPNIC, it is also considered that the effectiveness of ASPAs and ASPV is different on network topologies in each region. Further studies, which take the difference in each region into account, will need to be undertaken. Moreover, we are in the process of investigating experiments on the actual Internet because each AS operates an individual policy to select routing information in the real world.

CODE AVAILABILITY

We have released the source code of LOTUS via our GitHub repository (https://github.com/han9umeda/LOTUS).

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	96	76	99	80	23	22	23	56	31	12	19	12	22	5	5	8	12	4	3	1	3	42	19	15	15	43	21	10	18	14	8	6
2	55902	1	8	1	1	33	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	283	172	208	143	1	60	60	65	71	36	8	15	8	19	28	7	6	12	2	7	5	3	108	62	58	58	46	58	53	51	13	6	6
3	59095	142	1	97	71	1	8	8	11	1	23	2	8	2	16	4	6	6	11	2	7	5	2	66	10	6	5	29	11	7	6	4	6	5
3	63781	193	157	131	130	108	36	36	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	517	354	381	269	225	210	210	203	105	166	151	101	144	93	59	78	80	1	76	2	6	3	131	197	197	197	62	109	146	69	20	6	7
3	63779	158	130	1	113	96	20	20	20	61	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	114	82	1	1	68	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	269	207	196	168	101	135	135	133	1	78	61	63	55	23	4	9	6	18	2	9	6	3	113	106	102	101	40	67	56	40	13	6	7
4	59120	262	344	283	338	322	385	385	350	233	331	325	281	324	266	222	265	263	197	263	195	194	194	1	304	304	304	32	138	225	27	9	6	7
NoN	131948	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	546	7
NoN	37906	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	7

FIGURE 62. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPA is not deployed. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	96	76	99	80	23	22	23	56	31	12	19	12	22	5	5	8	12	4	3	1	3	42	19	15	15	43	21	10	18	14	8	6
2	55902	1	8	1	1	33	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	172	208	143	1	60	60	65	71	36	8	15	8	19	28	7	6	12	2	7	5	3	108	62	58	58	46	58	53	51	13	6	6
3	59095	1	1	97	71	1	8	8	11	1	23	2	8	2	16	4	6	6	11	2	7	5	2	66	10	6	5	29	11	7	6	4	6	5
3	63781	1	157	131	130	108	36	36	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	316	381	269	225	210	210	203	105	166	151	101	144	93	59	78	80	1	76	2	6	3	131	197	197	197	62	109	146	69	20	6	7
3	63779	1	130	1	113	96	20	20	20	61	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	82	1	1	68	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	207	196	168	101	135	135	133	1	78	61	63	55	23	4	9	6	18	2	9	6	3	113	106	102	101	40	67	56	40	13	6	7
4	59120	193	270	166	236	230	299	300	247	94	250	237	166	236	135	77	142	131	14	131	12	6	3	1	304	304	304	32	138	225	27	9	6	7
NoN	131948	1	507	507	507	507	507	507	507	521	507	507	507	507	507	521	507	507	507	507	507	6	3	507	507	507	507	507	507	507	507	507	507	7
NoN	37906	1	506	506	506	506	506	506	506	520	506	506	506	506	506	520	506	506	506	506	506	6	3	506	506	506	506	506	506	506	506	506	506	7

FIGURE 63. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	11	76	99	80	23	22	23	55	31	12	18	12	22	5	5	8	12	4	3	1	3	42	19	15	15	43	21	10	18	14	8	6
2	55902	1	8	1	1	33	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	208	143	1	60	60	65	71	36	8	15	8	19	28	7	6	12	2	7	5	3	108	62	58	58	46	58	53	51	13	6	6
3	59095	1	1	97	71	1	8	8	11	1	23	2	8	2	16	4	6	6	11	2	7	5	2	66	10	6	5	29	11	7	6	4	6	5
3	63781	1	1	131	130	108	36	36	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	381	236	184	169	169	164	105	107	91	19	84	93	58	78	80	1	76	2	6	3	131	151	151	152	62	109	146	69	20	6	7
3	63779	1	8	1	113	96	20	20	20	60	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	8	1	1	68	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	196	168	101	100	100	99	1	25	9	10	2	23	4	9	6	18	2	9	6	3	113	59	55	55	40	67	56	40	13	6	7
4	59120	193	157	166	236	230	214	215	136	94	147	133	11	131	135	77	142	131	14	131	12	6	3	1	224	224	225	32	138	225	27	9	6	7
NoN	131948	1	1	507	507	507	507	507	507	521	507	507	507	507	507	521	507	507	507	507	507	6	3	507	507	507	507	507	507	507	507	507	507	7
NoN	37906	1	1	506	506	506	506	506	506	520	506	506	506	506	506	520	506	506	506	506	506	6	3	506	506	506	506	506	506	506	506	506	506	7

FIGURE 64. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-2 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	11	76	7	77	23	22	21	52	31	12	18	12	22	5	5	8	12	4	3	1	3	42	19	15	15	43	19	10	18	14	8	6
2	55902	1	8	1	1	33	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	208	50	1	14	14	19	71	36	8	15	8	19	28	7	6	12	2	7	5	3	108	16	12	12	44	16	7	51	13	6	6
3	59095	1	1	97	4	1	5	5	8	1	23	2	8	2	16	4	6	6	11	2	7	5	2	66	7	3	2	29	8	4	6	4	6	5
3	63781	1	1	131	1	108	36	36	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	380	96	184	87	87	82	105	107	91	19	84	93	55	78	80	1	76	2	6	3	131	85	85	86	62	23	80	69	20	6	7
3	63779	1	8	1	5	93	20	20	20	57	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	8	1	1	68	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	196	53	101	57	57	56	1	25	9	10	2	23	4	9	6	18	2	9	6	3	113	10	6	6	38	22	7	40	13	6	7
4	59120	193	157	166	130	230	109	110	10	94	147	133	11	131	135	77	142	131	14	131	12	6	3	1	131	131	132	32	17	132	27	9	6	7
NoN	131948	1	1	507	1	507	507	507	216	111	507	507	507	507	507	111	507	507	507	507	507	6	3	507	507	507	507	507	19	507	507	216	507	7
NoN	37906	1	1	506	1	506	506	506	217	111	506	506	506	506	506	111	506	506	506	506	506	6	3	506	506	506	506	506	19	506	506	217	506	7

FIGURE 65. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-3 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	11	3	7	77	21	20	21	52	31	12	18	12	22	5	5	8	10	4	3	1	3	40	19	15	15	41	19	10	16	14	6	6
2	55902	1	8	1	1	33	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	1	50	1	14	14	19	71	36	8	15	8	19	28	7	6	12	2	7	5	3	108	16	12	12	44	16	7	51	13	6	6
3	59095	1	1	1	4	1	5	5	8	1	23	2	8	2	16	4	6	6	11	2	7	5	2	66	7	3	2	29	8	4	6	4	6	5
3	63781	1	1	1	1	108	36	36	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	75	96	131	87	87	82	105	41	17	19	10	25	55	4	6	1	2	2	6	3	131	17	13	13	62	23	8	69	20	6	7
3	63779	1	8	1	5	93	20	20	20	57	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	8	1	1	68	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	1	53	101	57	57	56	1	25	9	10	2	23	4	9	6	18	2	9	6	3	113	10	6	6	38	22	7	40	13	6	7
4	59120	193	157	131	130	122	109	110	10	94	30	3	11	2	19	77	14	6	14	2	12	6	3	1	7	3	3	32	17	4	27	9	6	7
NoN	131948	1	1	1	1	224	224	224	216	111	34	98	11	2	25	111	21	6	21	2	21	6	3	262	7	3	3	288	19	4	86	216	6	7
NoN	37906	1	1	1	1	225	225	225	217	111	34	99	11	2	23	111	21	6	21	2	21	6	3	263	7	3	3	289	19	4	87	217	6	7

FIGURE 66. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-4 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	11	3	7	77	21	20	21	52	31	12	18	12	22	5	5	8	10	4	3	1	3	40	19	15	15	41	19	10	16	14	6	6
2	55902	1	8	1	1	33	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	1	50	1	14	14	19	71	36	8	15	8	19	28	7	6	12	2	7	5	3	58	16	12	12	44	16	7	51	13	6	6
3	59095	1	1	1	4	1	5	5	8	1	23	2	8	2	16	4	6	6	11	2	7	5	2	26	7	3	2	29	8	4	6	4	6	5
3	63781	1	1	1	1	108	36	36	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	75	96	131	87	87	82	105	41	17	19	10	25	55	4	6	1	2	2	6	3	73	17	13	13	62	23	8	69	20	6	7
3	63779	1	8	1	5	93	20	20	20	57	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	8	1	1	68	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	1	53	101	57	57	56	1	25	9	10	2	23	4	9	6	18	2	9	6	3	62	10	6	6	38	22	7	40	13	6	7
4	59120	193	157	131	130	122	109	110	10	94	30	3	11	2	19	77	14	6	14	2	12	6	3	1	7	3	3	32	17	4	27	9	6	7
NoN	131948	1	1	1	1	224	224	224	216	111	34	98	11	2	25	111	21	6	21	2	21	6	3	61	7	3	3	91	19	4	86	216	6	7
NoN	37906	1	1	1	1	225	225	225	217	111	34	99	11	2	23	111	21	6	21	2	21	6	3	62	7	3	3	92	19	4	87	217	6	7

FIGURE 67. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-5 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	11	3	7	11	21	20	21	52	31	12	18	12	22	5	5	8	10	4	3	1	3	40	19	15	15	41	19	10	16	14	6	6
2	55902	1	8	1	1	8	15	15	10	23	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	1	50	1	14	14	19	71	36	8	15	8	19	28	7	6	12	2	7	5	3	58	16	12	12	44	16	7	51	13	6	6
3	59095	1	1	1	4	1	5	5	8	1	23	2	8	2	16	4	6	6	11	2	7	5	2	26	7	3	2	29	8	4	6	4	6	5
3	63781	1	1	1	1	32	5	5	9	75	25	3	10	2	18	21	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	75	96	78	21	21	20	105	41	17	19	10	25	55	4	6	1	2	2	6	3	73	17	13	13	62	23	8	69	20	6	7
3	63779	1	8	1	5	9	20	20	20	57	28	10	16	9	2	14	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	8	1	1	8	17	17	17	46	20	10	17	9	15	14	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	1	53	50	15	15	14	1	25	9	10	2	23	4	9	6	18	2	9	6	3	62	10	6	6	38	22	7	40	12	6	7
4	59120	193	157	131	130	108	36	36	10	94	30	3	11	2	19	77	14	6	14	2	12	6	3	1	7	3	3	32	17	4	27	9	6	7
NoN	131948	1	1	1	1	1	5	5	11	111	34	98	11	2	25	111	21	6	21	2	21	6	3	61	7	3	3	91	19	4	86	11	6	7
NoN	37906	1	1	1	1	1	5	5	11	111	34	99	11	2	23	111	21	6	21	2	21	6	3	62	7	3	3	92	19	4	87	11	6	7

FIGURE 68. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-6 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	131951	1	11	3	7	11	21	20	21	2	31	12	18	12	22	5	5	8	10	4	3	1	3	40	19	15	15	41	19	10	16	14	6	6
2	55902	1	8	1	1	8	15	15	10	2	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	1	50	1	14	14	19	25	36	8	15	8	19	5	7	6	12	2	7	5	3	58	16	12	12	44	16	7	51	13	6	6
3	59095	1	1	1	4	1	5	5	8	1	23	2	8	2	16	4	6	6	11	2	7	5	2	26	7	3	2	29	8	4	6	4	6	5
3	63781	1	1	1	1	32	5	5	9	20	25	3	10	2	18	3	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	75	96	78	21	21	20	56	41	17	19	10	25	5	4	6	1	2	2	6	3	73	17	13	13	62	23	8	69	20	6	7
3	63779	1	8	1	5	9	20	20	20	11	28	10	16	9	2	5	8	6	11	2	8	6	3	54	17	13	13	41	18	8	30	17	6	7
3	18085	1	8	1	1	8	17	17	17	11	20	10	17	9	15	5	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	1	53	50	15	15	14	1	25	9	10	2	23	4	9	6	18	2	9	6	3	62	10	6	6	38	22	7	40	12	6	7
4	59120	193	157	131	130	108	36	36	10	75	30	3	11	2	19	23	14	6	14	2	12	6	3	1	7	3	3	32	17	4	27	9	6	7
NoN	131948	1	1	1	1	1	5	5	11	1	34	98	11	2	25	4	21	6	21	2	21	6	3	61	7	3	3	91	19	4	86	11	6	7
NoN	37906	1	1	1	1	1	5	5	11	1	34	99	11	2	23	4	21	6	21	2	21	6	3	62	7	3	3	92	19	4	87	11	6	7

FIGURE 69. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-7 AS from the top-1 AS. The measurement setting is common with Figure 11.

Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	NoN
Outside AS with →	NoN	2497	2516	2914	17676	4713	23637	17941	7679	2519	2518	7500	17511	17661	7529	7690	7671	55391	9607	55392	131896	55900	9999	59103	17675	24295	7682	59105	4725	4694	24257	131976	7521	10021
2	13195	1	11	3	7	11	21	20	21	2	31	12	18	12	22	5	5	8	10	4	3	1	3	40	19	15	15	41	19	10	16	14	6	6
2	55902	1	8	1	1	8	15	15	10	2	13	9	15	9	13	5	2	6	6	2	3	5	2	37	9	9	9	34	2	2	13	11	6	4
3	24275	1	7	1	50	1	14	14	19	25	36	8	15	8	19	5	7	6	12	2	7	5	3	33	16	12	12	44	16	7	24	13	6	6
3	59095	1	1	1	4	1	5	5	8	1	23	2	8	2	16	4	6	6	11	2	7	5	2	26	7	3	2	29	8	4	6	4	6	5
3	63781	1	1	1	1	32	5	5	9	20	25	3	10	2	18	3	8	6	12	2	8	5	3	1	7	3	3	8	15	3	5	7	6	7
3	59099	1	92	75	96	78	21	21	20	56	41	17	19	10	25	5	4	6	1	2	2	6	3	40	17	13	13	62	23	8	34	20	6	7
3	63779	1	8	1	5	9	20	20	20	11	28	10	16	9	2	5	8	6	11	2	8	6	3	40	17	13	13	41	18	8	16	17	6	7
3	18085	1	8	1	1	8	17	17	17	11	20	10	17	9	15	5	7	6	11	2	7	6	3	37	14	10	10	38	13	4	13	11	6	6
3	58651	1	54	1	53	50	15	15	14	1	25	9	10	2	23	4	9	6	18	2	9	6	3	35	10	6	6	38	22	7	8	12	6	7
4	59120	193	157	131	130	108	36	36	10	75	30	3	11	2	19	23	14	6	14	2	12	6	3	1	7	3	3	32	17	4	27	9	6	7
NoN	131948	1	1	1	1	1	5	5	11	1	34	98	11	2	25	4	21	6	21	2	21	6	3	12	7	3	3	46	19	4	35	11	6	7
NoN	37906	1	1	1	1	1	5	5	11	1	34	99	11	2	23	4	21	6	21	2	21	6	3	13	7	3	3	47	19	4	35	11	6	7

FIGURE 70. Impact of the mixed attack by the outside ASes on the experimental networks, where ASPV is deployed to the top-8 AS from the top-1 AS. The measurement setting is common with Figure 11.

APPENDIX

We show raw data on experimental results in Section V below.

A. RESULTS ON TOP ASES WITH ASPV AGAINST NORMAL ATTACK FROM LEAF-NODE AS

We show results on the normal attack from a leaf-node AS where ASPV is deployed to top ASes.

B. RESULTS ON INTERMEDIATE ASES WITH ASPV AGAINST NORMAL ATTACK FROM LEAF-NODE AS

We show results on the normal attack from a leaf-node AS where ASPV is deployed to intermediate ASes.

C. RESULTS ON TOP ASES WITH ASPV AGAINST NORMAL ATTACK FROM OUTSIDE AS

We show results on the normal attack from an outside AS, where ASPV is deployed to top ASes. We also show results without ASPV for comparison.

D. RESULTS ON TOP ASES WITH ASPV AGAINST ASPA-AWARE ATTACK FROM LEAF-NODE AS

We show results on the ASPA-aware attack from a leaf-node AS, where ASPV is deployed to top ASes. We also show results without ASPV for comparison.

E. RESULTS ON TOP ASES WITH ASPV AGAINST MIXED ATTACK FROM LEAF-NODE AS

We show results on the mixed attack from a leaf-node AS, where ASPV is deployed to top ASes. We also show results without ASPV for comparison.

F. RESULTS ON TOP ASES WITH ASPV AGAINST MIXED ATTACK FROM OUTSIDE AS

We show results on the mixed attack from an outside AS, where ASPV is deployed to top ASes. We also show results without ASPV for comparison.

ACKNOWLEDGMENT

The authors would like to appreciate the reviewers for their valuable comments.

REFERENCES

[1] "BGP leak causing Internet outages in Japan and beyond. — BGPmon." 2017. [Online]. Available: https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

[2] "List of as number—JPNIC." [Online]. Available: https://www.nic.ad.jp/ja/ip/as-numbers.txt

[3] "RPKI route server deployment at JPNAP." 2021. [Online]. Available: https://apix.asia/23/jpnap-rpki-deployment.pdf

[4] "Understanding how Facebook disappeared from the Internet." 2021. [Online]. Available: https://blog.cloudflare.com/october-2021-facebook-outage/

[5] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE SP*, 2017, pp. 375–392.

[6] A. Azimov. "BGP route security cycling to the future!" [Online]. Available: https://pc.nanog.org/static/published/meetings/NANOG76/1978/20190611_Azimov_Bgp_Route_Security_v1.pdf

[7] A. Azimov, E. Bogomazov, R. Bush, K. Patel, and J. Snijders, "Verification of AS_PATH using the resource certificate public key infrastructure and autonomous system provider authorization," Internet-Draft draft-ietf-sidrops-aspa-verification-08, Internet Eng. Task Force, Aug. 2021.

[8] A. Azimov, E. Uskov, R. Bush, K. Patel, J. Snijders, and R. Housley, "A profile for autonomous system provider authorization," Internet-Draft draft-ietf-sidrops-aspa-profile-07, Internet Eng. Task Force, Jan. 2022.

[9] H. Ballani, P. Francis, and X. Zhang, "A study of prefix hijacking and interception in the Internet," in *Proc. SIGCOMM*, 2007, pp. 265–276.

[10] H. Birge-Lee, L. Wang, J. Rexford, and P. Mittal, "SICO: Surgical interception attacks by manipulating BGP communities," in *Proc. CCS*, 2019, pp. 431–448.

[11] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, "BGP hijacking classification," in *Proc. TMA*, 2019, pp. 25–32.

[12] T. Chung et al., "RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins," in *Proc. IMC*, 2019, pp. 406–419.

[13] P. Ekparinya, V. Gramoli, and G. Jourjon, "The attack of the clones against proof-of-authority," in *Proc. NDSS*, 2020, pp. 1–14.

[14] H. Esaki, A. Kato, and J. Murai, "R&D activities and testbed operation in WIDE project," in *Proc. SAINTW*, 2003, pp. 172–177.

[15] Y. Gilad, S. Goldberg, K. Sriram, J. Snijders, and B. Maddison, "The use of maxLength in the resource public key infrastructure (RPKI)," IETF, RFC 9319, Oct. 2022.

[16] V. Giotsas, G. Smaragdakis, C. Dietzel, P. Richter, A. Feldmann, and A. Berger, "Inferring BGP blackholing activity in the Internet," in *Proc. IMC*, 2017, pp. 1–14.

[17] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, "Pathlet routing," in *Proc. SIGCOMM*, 2009, pp. 111–122.

[18] S. Goldberg, "Why is it taking so long to secure Internet routing?" *Commun. ACM*, vol. 57, no. 10, pp. 56–63, 2014.

[19] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, "How secure are secure interdomain routing protocols," in *Proc. SIGCOMM*, 2010, pp. 87–98.

[20] J. A. Hawkinson and T. J. Bates, "Guidelines for creation, selection, and registration of an autonomous system (AS)," IETF, RFC 1930, Mar. 1996.

[21] T. Hlavacek et al., "DISCO: Sidestepping RPKI's deployment barriers," in *Proc. NDSS*, 2020, pp. 1–17.

[22] T. Hlavacek, P. Jeitner, D. Mirdita, H. Shulman, and M. Waidner, "Behind the scenes of RPKI," in *Proc. CCS*, 2022, pp. 1413–1426.

[23] T. Hlavacek, P. Jeitner, D. Mirdita, H. Shulman, and M. Waidner, "Stalloris: RPKI downgrade attack," in *Proc. USENIX Security*, 2022, pp. 4455–4471.

[24] T. Hlavacek, H. Shulman, and M. Waidner, "Smart RPKI validation: Avoiding errors and preventing hijacks," in *Proc. ESORICS*, 2022, pp. 509–530.

[25] G. Huston and G. G. Michaelson, "Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs)," IETF, RFC 6483, Feb. 2012.

[26] G. Huston, M. Rossi, and G. Armitage, "Securing BGP—A literature survey," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 199–222, 2nd Quart., 2011.

[27] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 4, pp. 582–592, Apr. 2000.

[28] B. Kumar, "Integration of security in network routing protocols," *ACM SIGSAC Rev.*, vol. 11, no. 2, pp. 18–25, Apr. 1993.

[29] W. A. Kumari, R. Bush, H. Schiller, and K. Patel, "Codification of as 0 processing," IETF, RFC 7607, Aug. 2015.

[30] W. A. Kumari and D. R. McPherson, "Remote triggered black hole filtering with unicast reverse path forwarding (uRPF)," IETF, RFC 5635, Aug. 2009.

[31] M. Lepinski and S. Kent, "An infrastructure to support secure Internet routing," IETF, RFC 6480, Feb. 2012.

[32] M. Lepinski, D. Kong, and S. Kent, "A profile for route origin authorizations (ROAs)," IETF, RFC 6482, Feb. 2012.

[33] M. Lepinski and K. Sriram, "BGPsec protocol specification," IETF, RFC 8205, Sep. 2017.

[34] R. Lychev, S. Goldberg, and M. Schapira, "BGP security in partial deployment: Is the juice worth the squeeze?" in *Proc. SIGCOMM*, 2013, pp. 171–182.

[35] R. Lychev, S. Goldberg, and M. Schapira, "BGP security in partial deployment: Is the juice worth the squeeze?" *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 171–182, 2013.

[36] R. Lychev, M. Schapira, and S. Goldberg, "Rethinking security for Internet routing," *Commun. ACM*, vol. 59, no. 10, pp. 48–57, 2016.

[37] R. Mahajan and D. Wetherall, "Mutually controlled routing with independent ISPs," in *Proc. NSDI*, 2007, p. 26.

[38] L. Miller and C. Pelsser, "A taxonomy of attacks using BGP blackholing," in *Proc. ESORICS*, 2019, pp. 107–127.

[39] A. Mitseva, A. Panchenko, and T. Engel, "The state of affairs in BGP security: A survey of attacks and defenses," *Comput. Commun.*, vol. 124, pp. 45–60, Jun. 2018.

[40] R. Morillo, J. Furuness, A. Herzberg, C. Morris, B. Wang, and J. Breslin, "ROV++: Improved deployable defense against BGP hijacking," in *Proc. NDSS*, 2021, pp. 1–18.

[41] S. L. Murphy, "BGP security vulnerabilities analysis," IETF, RFC 4272, Jan. 2006.

[42] M. Nawrocki, J. Blendin, C. Dietzel, T. C. Schmidt, and M. Wählisch, "Down the black hole: Dismantling operational practices of BGP blackholing at IXPs," in *Proc. IMC*, 2019, pp. 435–448.

[43] L. Peterson, T. Anderson, D. Culler, and T. Roscoe, "A blueprint for introducing disruptive technology into the Internet," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 1, pp. 59–64, 2003.

[44] L. Prehn and A. Feldmann, "How biased is our validation (data) for as relationships?" in *Proc. IMC*, 2021, pp. 612–620.

[45] Y. Rekhter, S. Hares, and T. Li, "A border gateway protocol 4 (BGP-4)," IETF, RFC 4271, Jan. 2006.

[46] R. Ricci, E. Eide, and C. Team, "Introducing CloudLab: Scientific infrastructure for advancing cloud architectures and applications," *Login Usenix Mag.*, vol. 39, no. 6, pp. 36–38, 2014.

[47] M. Saad, A. Anwar, A. Ahmad, H. Alasmary, M. Yuksel, and D. Mohaisen, "*RouteChain*: Towards blockchain-based secure and efficient BGP routing," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109362.

[48] R. R. Sambasivan, D. Tran-Lam, A. Akella, and P. Steenkiste, "Bootstrapping evolvability for inter-domain routing with D-BGP," in *Proc. SIGCOMM*, 2017, pp. 474–487.

[49] B. Schlinker, T. Arnold, I. Cunha, and E. Katz-Bassett, "PEERING: Virtualizing BGP at the edge for research," in *Proc. CoNEXT*, 2019, pp. 51–67.

[50] P. Sermpezis et al., "ARTEMIS: Neutralizing BGP hijacking within a minute," *IEEE/ACM Trans. Netw.*, vol. 26, no. 6, pp. 2471–2486, Dec. 2018.

[51] T. Shapira and Y. Shavitt, "AP2Vec: An unsupervised approach for BGP hijacking detection," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 3, pp. 2255–2268, Sep. 2022.

[52] K. Shrishak and H. Shulman, "Limiting the power of RPKI authorities," in *Proc. ANRW*, 2020, pp. 12–18.

[53] H. Shulman, N. Vogel, and M. Waidner, "Poster: Insights into global deployment of RPKI validation," in *Proc. CCS*, 2022, pp. 3467–3469.

[54] C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: A testbed for scientifically rigorous cyber-physical security experimentation," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 319–330, Dec. 2013.

[55] K. Sklower and A. D. Joseph, "Very large scale cooperative experiments in Emulab-derived systems," in *Proc. DETER*, 2007, pp. 1–7.

[56] B. R. Smith and J. J. Garcia-Luna-Aceves, "Securing the border gateway routing protocol," in *Proc. GLOBECOM*, 1996, pp. 81–85.

[57] B. R. Smith, S. Murthy, and J. J. Garcia-Luna-Aceves, "Securing distance-vector routing protocols," in *Proc. NDSS*, 1997, pp. 85–92.

[58] J. M. Smith and M. Schuchard, "Routing around congestion: Defeating DDoS attacks and adverse network conditions via reactive BGP routing," in *Proc. IEEE SP*, 2018, pp. 599–617.

[59] K. Sriram, D. Montgomery, D. R. McPherson, E. Osterweil, and B. Dickson, "Problem definition and classification of BGP route leaks," IETF, RFC 7908, Jun. 2016.

[60] T. Takemura, N. Yanai, N. Umeda, M. Okada, S. Okamura, and J. P. Cruz, "APVAS+: A practical extension of BGPsec with low memory requirement," in *Proc. ICC*, 2021, pp. 1–7.

[61] C. Testart, P. Richter, A. King, A. Dainotti, and D. Clark, "To filter or not to filter: Measuring the benefits of registering in the RPKI today," in *Proc. PAM*, 2020, pp. 71–87.

[62] M. A. To, M. Cano, and P. Biba, "DOCKEMU—A network emulation tool," in *Proc. WAINA*, 2015, pp. 593–598.

[63] J. Towns et al., "XSEDE: Accelerating scientific discovery," *Comput. Sci. Eng.*, vol. 16, no. 5, pp. 62–74, Sep./Oct. 2014.
[64] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A stealthier partitioning attack against Bitcoin peer-to-peer network," in *Proc. IEEE SP*, 2020, pp. 496–511.
[65] P.-W. Tsai, A. C. Risdianto, M. H. Choi, S. K. Permal, and T. C. Ling, "SD-BROV: An enhanced BGP hijacking protection with route validation in software-defined exchange," *Future Internet*, vol. 13, no. 7, pp. 1–16, 2021.
[66] N. Umeda, N. Yanai, T. Takemura, M. Okada, J. P. Cruz, and S. Okamura, "SQUAB: A virtualized infrastructure for experiments on BGP and its extensions," in *Proc. AINA*, 2021, pp. 600–613.
[67] K. van Hove, J. van der Ham, and R. van Rijswijk-Deij, "Rpkiller: Threat analysis from an RPKI relying party perspective," 2022, *arXiv:2203.00993*.
[68] P. Vervier, O. Thonnard, and M. Dacier, "Mind your blocks: On the stealthiness of malicious BGP hijacks," in *Proc. NDSS*, 2015, pp. 1–30.
[69] T. Wan, E. Kranakis, and P. C. van Oorschot, "Pretty secure BGP, psBGP," in *Proc. NDSS*, 2005, pp. 1–16.
[70] B. White et al., "An integrated experimental environment for distributed systems and networks," *SIGOPS Oper. Syst. Rev.*, vol. 36, pp. 255–270, Dec. 2003.
[71] R. White, "Securing BGP through secure origin BGP (soBGP)," *Bus. Commun. Rev.*, vol. 33, no. 5, p. 47, 2003.
[72] W. Xu and J. Rexford, "MIRO: Multi-path interdomain routing," in *Proc. SIGCOMM*, 2006, pp. 171–182.
[73] Z. Yan and J.-H. Lee, "BGPChain: Constructing a secure, smart, and agile routing infrastructure based on blockchain," *ICT Exp.*, vol. 7, no. 3, pp. 376–379, 2021.
[74] Y. Yang, X. Shi, Q. Ma, Y. Li, X. Yin, and Z. Wang, "Path stability in partially deployed secure BGP routing," *Comput. Netw.*, vol. 206, Apr. 2022, Art no. 108762.
[75] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. G. Andersen, "SCION: Scalability, control, and isolation on next-generation networks," in *Proc. IEEE SP*, 2011, pp. 212–227.

NAOKI UMEDA received the B.Eng. degree in engineering science and the M.S. Info. Eng. degree from the Graduate School of Information Science and Technology, Osaka University, Japan, in 2020 and 2022, respectively. His research interests include network security and machine learning.

TAIJI KIMURA received the B.E. degree from Shibaura Institute of Technology, Japan, in 1997, and the M.S.Eng. degree from the Nara Institute of Science and Technology, Japan, in 1999. He is currently a Researcher with Keio University Graduate School of Media Design and Japan Network Information Center, Japan. His research interest includes network security.

NAOTO YANAI (Member, IEEE) received the B.E. degree from The National Institution of Academic Degrees and University Evaluation, Japan, in 2009, and the M.S. Eng. degree from the Graduate School of Systems and Information Engineering and the Ph.D. degree in engineering from the Graduate School of Systems and Information Engineering, University of Tsukuba, in 2011 and 2014, respectively. He is currently an Associate Professor with Osaka University, Osaka, Japan. His research area is information security.