International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.1 (2016), pp.11-22
http://dx.doi.org/10.14257/ijmue.2016.11.1.02

Policy-Based AS Path Verification with Enhanced Comparison Algorithm to Prevent 1-Hop AS Path Hijacking in Real Time

Je-Kuk Yun[1] and Jin-Hee Song[2]
[1]Towson University, Towson, Maryland, U.S.A
[2]School of IT Convergence Engineering, Shinhan University, South Korea
jyun4@students.towson.edu, jhsong@shinhan.ac.kr

Abstract

The Border Gateway Protocol (BGP) is the routing protocol that enables large IP networks to form a single Internet. The main objective of BGP is to exchange Network Layer Reachability Information (NLRI) between Autonomous Systems (ASes) so that a BGP router can announce their IP prefix and find a path to the destination of packets. As the number of IP hijacking incidents has increased, a number of solutions are created to prevent IP hijacking. However, few studies have been researched about an AS path hijacking. We proposed a novel methodology of preventing AS path hijacking by comparing live BGP streams to our policy-based database that collected from RIPE NCC repository. As the number of ASes increases, our method for comparing live BGP streams to our policy-based database have to be enhanced to validate AS path in real time. We enhanced the main comparison algorithm and the performance result indicates that the enhanced algorithm is on average 1.45 times faster than the existing algorithm.

Keywords: *BGP, border gateway protocol, inter-domain routing, network security, networks, AS path hijacking*

1. Introduction

The Border Gateway Protocol (BGP) is an Inter-domain routing protocol that has gradually evolved over the past few decades. The initial design of BGP was a fully trust-based system. So, BGP itself does not have mechanisms to check whether a route is valid or not because BGP routers completely trust other BGP routers. This lack of consideration of BGP vulnerabilities often leads severe failures of Internet service provision [1] or other problems [2]. If a hijacking BGP router announces bogus blocks of IP addresses to BGP peers, the BGP peers transfer Internet traffic to the hijacking BGP router if the destination IP address is matched and the number of hops is shorter than the others. We call this threat of failures IP hijacking.

Such a failure happened on the twenty fifth of April in 1997 by a misconfigured router that advertised incorrect prefixes and announced AS 7007 as the origin of them. As a result, it created a routing black hole for almost two hours [3]. Similar events happened on the twenty second of January in 2006, when Con Edison (AS 27506) stole several important prefixes by misconfiguring them [4]. On Christmas Eve, 2004, TTNet in Turkey (AS 9121) announced the entire prefixes on the Internet so that every route came to them rather than to correct destinations [5].

The most well-known IP hijacking is the YouTube hijacking by Pakistan Telecom (AS17557) on the twenty fourth of February in 2008 [6]. In response to a government order to block YouTube access within their ASes, Pakistan Telecom announced a more specific prefix than YouTube's prefix. Then, one of Pakistan Telecom's upstream

[2] Corresponding Author: Jin-Hee Song(Shinhan University), email : jhsong@shinhan.ac.kr

providers, PCCW Global (AS3491), forwarded the announcement to other neighbors. As a result, YouTube traffic from all over the world was misled to Pakistan Telecom (AS17557) for two hours. In addition, The Dell Secure Works Counter Threat Unit (CTU) research team discovered a repeated traffic hijacking to Bitcoin mining sites between February and May 2014. Compromised networks belonged to Amazon, Digital Ocean, OVH, *etc*. The attacker hijacked cryptocurrency miners' traffic and earned an estimated $83,000 [7]. Furthermore, AS 23274, owned by China Telecom, announced approximately 50,000 prefixes, which were registered to other ASes in 2010. The reason the incident was magnified is because China Telecom was the 11th largest Internet provider. If small ISPs hijack a large part of the Internet, they don't have the capacity to deal with a huge amount of traffic. China Telecom, however, has the capability to operate under such traffics, and redirect its desired destination. The incident was not recognized for 18 minutes [8]. In order to solve the IP hijacking, many studies were conducted, such as RPKI [9], BGPmon [10], Argus [11], and PHAS [12]. Some of them are available as a tool for network administrators to protect their networks [13, 10-11].

While there are many studies on the IP hijacking, few studies have been researched about an AS path hijacking. There was some misdirected network traffic that was suspected of the man-in-the-middle (MITM) attack in 2013 observed by Renesys. In February 2013, global traffic was redirected to Belarusian ISP GlobalOneBel before its intended destination and it occurred on an almost daily basis. Major financial institutions, governments, and network service providers were affected by this traffic diversion in several countries including the U.S. From the thirty first of July to the nineteenth of August in 2013, Icelandic provider Opin Kerfi announced origination routes for 597 IP networks owned by a large VoIP provider in the U.S through Siminn which is one of the two ISPs that Opin Kerfi has. However, this announcement was never propagated through Fjarskipti which is the other one of the two ISPs. As a result, network traffic was sent to Siminn in London and redirected back to its intended destination. Several different countries in some Icelandic autonomous systems and belonging to the Siminn were affected. However, Opin Kerfi said that the problem was the result of a bug in the software and had been resolved [14]. A root cause of BGP hijacking can be discovered by empirical data analysis using BGP updates from Routeviews, RIB from iPlane project, paths from traceroute, *etc*. However, proving a malicious intent is hardly possible. According to this research, China Telecom incident is most likely caused by a routing table leak [14].

In order to protect the AS path hijacking, the AS_PATH attribute should not be manipulated. However, the BGP itself cannot verify whether the AS_PATH attribute has been changed or not. If a routing hijacker manipulates the AS_PATH attribute in a BGP message that is sent by another router and forwards the manipulated BGP message to other neighbors, the neighbors who receive the manipulated BGP message can be a victim of AS path hijacking. Only Secure Inter-Domain Routing (SIDR) working group proposed the RPKI using BGPSEC to validate AS_PATH, but BGPSEC is currently a work in progress [15-16]. In addition, a study propounds that BGP armed with BGPSEC cannot be secured because of BGP's fundamental design [17-18].

We proposed Secure AS_PATH BGP (SAPBGP) [19-20] in which the SAPBGP constructs its own policy-based database by collecting RIPE NCC repository and checks the AS_PATH attribute in BGP update messages whether the ASes listed in the AS_PATH attributes are actually connected or not. Some studies are conducted to detect malicious data through machine learning [21-24] and we will adopt them into our system in near future. For the validation test with the real BGP messages, the SAPBGP receives live BGP streams from BGPmon project [25-26]. In addition, we conduct the performance test of the SAPBGP to measure the duration of the validation with the live BGP messages. When SAPBGP collects policy information from the RIPE NCC repository, export and import policies were stored in random order. So, SAPBGP should check policy information and the complexity was O(n) in worst case. However, our system is modified and the export and import policies are stored in order so that SAPBGP can check policy information with the binary search method.

2. Related Research

In order to validate BGP update message, origin information of a BGP update message needs to be checked whether authorized BGP router originated its prefixes or not, which is called origin validation. In addition, AS_PATH information in a BGP update message needs to be checked whether AS_PATH attribute has been changed or not, which is called path validation.

2.1. Origin Validation

An origin validation means to verify whether the originator of update message has been authorized to announce its prefixes. In order to validate originators, the Resource Public Key Infrastructure (RPKI) was proposed by SIDR working group on January in 2013 and is currently used for origin validation. RPKI is a Public Key Infrastructure (PKI) [27] where an organization called IANA manages officially verifiable Internet resources that are the allocation of hierarchy of IP addresses, Autonomous System Numbers (ASN), and signed objects for routing security. IANA is the trust anchor that allows third party to officially validate assertions according to resource allocations. The authorization is hierarchically assigned from IANA to the Regional Internet Registries (RIRs), Local Internet Registries (LIRs), National Internet Registries (NIRs), and Internet Service Providers (ISPs). There are five RIRs and they act as trust anchors like IANA. The RIR issues certificates to NIR, ISP and subscribers. NIR and ISP are allowed to issue certificates to downstream providers and to subscribers. IP address holders specify which ASes are authorized to announce their own IP address prefixes called ROA.

2.2. Path Validation

IP hijacking can be completely prevented by RPKI if every address is covered by the ROAs. However, even though all of the IP addresses are covered by the ROAs, hijackers can try an AS_PATH hijacking by changing the AS_PATH attribute in the update message. In other words, the origin validation cannot assure that the update message has been originated by the authorized BGP router. In order to prevent the AS_PATH hijacking, BGP routers should verify whether an incoming update message is changed or not. In addition, the BGP routers check whether the sequence of ASes in the AS_PATH attribute is the same as the actual propagation path of the BGP update message. Currently, a SIDR working group is designing BGPsec to cryptographically prevent the AS_PATH hijacking. In BGPsec, an optional and non-transitive path attribute, BGPsec_Path attribute, is included in BGP update messages. BGPsec depends on RPKI certificates and a BGP router that wants to send BGP update messages that includes the BGPsec_Path should have a private key associated with the BGP router's AS number. When the BGP router originates IP prefixes, the BGP router signs the update message with its private key so that any BGP router that receives the update message can check that the update message has been originated by the right BGP router by verifying the signature with the public key corresponding to the private key. In addition, BGP routers who receive the BGP update message sign the BGP update message with their private key and forward the BGP update message to neighbors. If every router that receives and forwards the BGP update messages signs the BGP update message, the BGP update message can be considered as the message that has not been illegally changed by hijackers.

In order to protect BGP update message, especially to protect AS_PATH attributes, the BGP update message should carry the secured information such as digital signature. We call the BGP update messages including a BGPsec_Path attribute BGPsec update messages. The AS_PATH attribute in BGP update messages is replaced with BGPsec_Path attribute in the BGPsec update messages. The BGPsec_Path attribute contains a Secure_Path attribute and sequence of one or two Signature_Blocks. Basically, the BGPsec_Path attribute is logically equivalent to the AS_PATH attribute, but the BGPsec_Path attribute includes signature blocks for security methods.

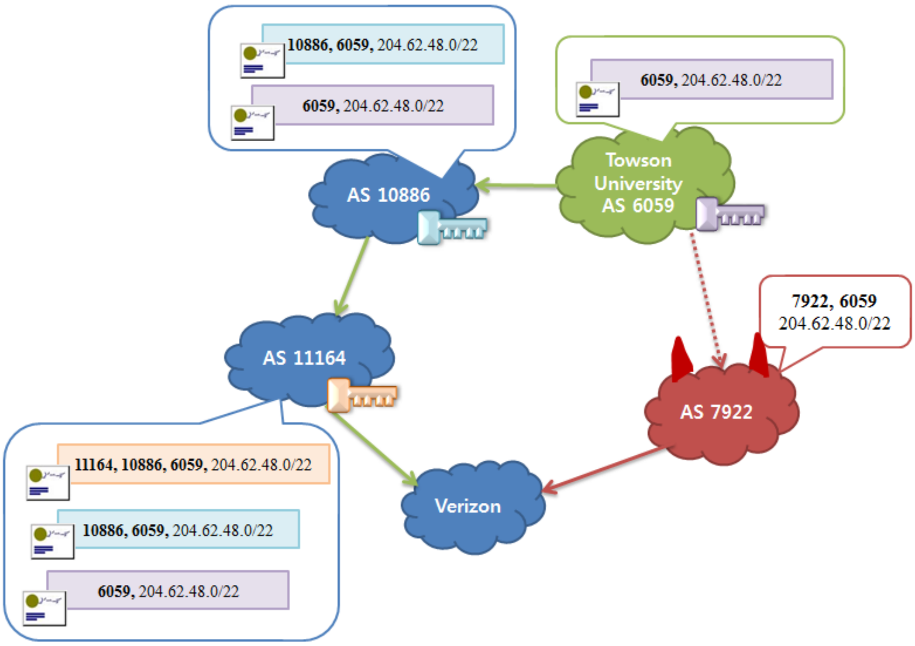


Figure 1. Protecting the 1-Hop Hijacking by BGPsec

Figure 1 depicts how the BGPsec update message works to protect the 1-hop hijacking. Verizon cannot protect the 1-hop hijacking, even though Verizon can conduct origin validation. In order to prevent 1-hop hijacking, every BGPsec router needs to use a BGPsec update message instead of a BGP update message and sign the BGPsec update message with its private key either when the BGPsec router originates or when the BGPsec router forwards it to neighbors.

3. BGP's Vulnerabilities

BGP is used to find the best path to reach the destination between the source AS and the destination AS. In selecting the best path, the length of prefix and the number of hops are considered. Hijackers use those two characteristics of BGP to illegally draw Internet traffic to their AS. First, a longer prefix has a higher priority. AS administrators can announce any prefixes, which means the AS administrator intentionally/unintentionally can announce others' prefixes, and it changes the destination of Internet traffic. Secondly, a shorter path has a higher priority. When a BGP update message is forwarded among ASes, each AS's ASN is added to the AS_PATH attribute. A hijacker can manipulate the AS_PATH attribute to change AS paths of the Internet package. In addition, hijackers can pretend their ASes are connected to other ASes, by manipulating the AS_PATH attribute in the BGP message, even though their ASes are actually not connected to each other. Therefore, when the best path is selected, illegal changes of AS_PATH attribute influence the process of the best path selection.

3.1. IP Hijacking

Once BGP routers are connected to each other, the BGP routers fully trust other routers. If a BGP router intentionally originates a bogus prefix to neighbors, the neighbors that receive the announcements trust the prefix and their traffic is hijacked by the hijacking router.

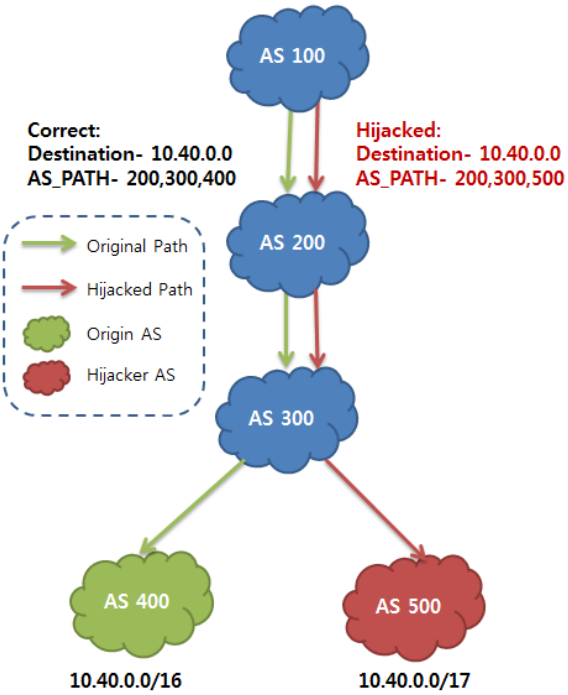


Figure 2. IP Prefix Hijacking

Figure 2 shows a scenario of IP hijacking. AS 500 is trying to hijack the Internet traffic heading for AS 400. AS 400 announces 10.40.0.0/16 to neighbors and traffic in AS 100 is going to 10.40.0.0. However, if AS 500 announces a bogus prefix, 10.40.0.0/17, to AS 100, then the traffic in AS 100 goes to AS 500 because 10.40.0.0/17 is more specific than 10.40.0.0/16. As a result, AS 100 takes the 10.40.0.0/17 as the destination.

3.2. AS Path Hijacking

AS path hijacking is the most severe problem that happens in BGP because it is hard to be detected [28]. AS path hijacking not only changes routes of Internet packets, but also sends the Internet packages to the right destination, which means victims of AS path hijacking hardly realize that their Internet packets are monitored or manipulated by AS path hijackers. Nowadays, there are many unknown BGP attacks [7-8] because victims of the hijacking cannot notice any changes except latency which is caused by the hijacker because the Internet packets traverse more AS hops.

A BGP router inserts its own ASN into the AS_PATH attribute in update messages when the BGP router receives the update message from neighbors. However, the BGP router can insert one or more ASNs into the AS_PATH attribute in update messages other than its own ASN. In addition, a BGP router might pretend as if the BGP router is connected to a certain BGP router by manipulating data contained in BGP updates. Figure demonstrates a scenario of manipulating BGP update messages.

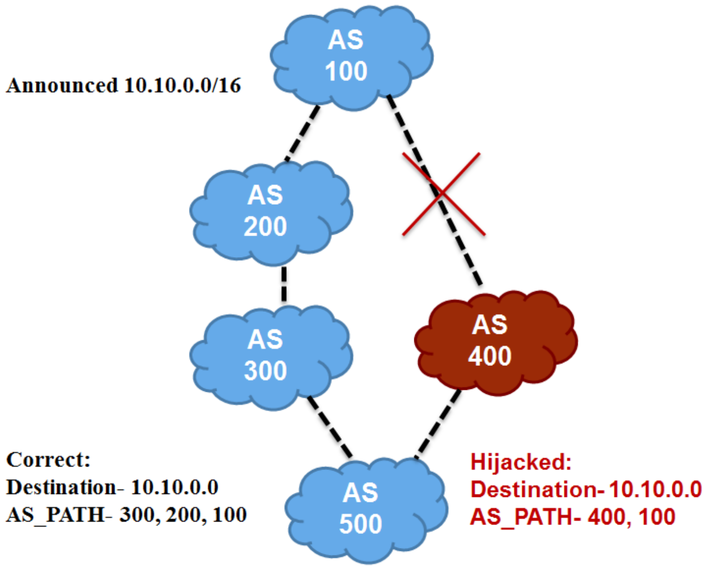


Figure 3. Manipulating AS_PATH Attributes

Suppose AS 400 has a connection to AS 500 and creates a fake BGP announcement to pretend that AS 400 received a BGP message originated by AS 100 and forwarded the update message to AS 500 even though AS 100 and AS 400 actually don't have a BGP connection. In terms of AS 500, the traffic heading for prefix 10.10.0.0/16 will choose AS 400 as the best path because AS 500 selects the shortest path and AS 400 is shorter than AS 300. Even if the AS 500 can conduct origin validation, the AS 500 cannot prevent this attack because prefix and ASN information is correct. As a result, AS 400 will have the traffic heading for prefix 10.10.0.0 and might start another attack using the traffic, such as a Man-In-The-Middle (MITM) attack.

4. Enhanced Secure AS Path BGP (SAPBGP)

In order to prevent AS path hijacking, SIDR working group is proposing BGPsec [29] but we approached differently from BGPsec to monitor and detect the AS path hijacking by using ASes connection information using BGP peer information through policy-based database peer information. RIPE NCC provides users with RIPE Data Repository that contains BGP peer information. Through this information, we can check whether ASes are actually connected to other ASes. This peer information has been collected by either Routing Information Service (RIS) or Internet Routing Registry (IRR). RIS has collected and stored Internet routing data from several locations all over the world since 2001.

4.1 Overview

We constructed our own policy-based database by using API provided by RIPE NCC. We have collected, every day, all of the AS imports and exports policies information since the eighteenth of February in 2014. In addition, we have separated tables in the database to keep the daily information as well as the accumulated routing policy information by adding new exports and imports to the existing exports and imports in the accumulate table. BGPmon is a monitoring infrastructure, implemented by Colorado State University that collects BGP messages from various routers that are distributed and offers the BGP messages as the routes for destinations are changed in real-time. Any BGP router can be a source that offers real-time update messages if the BGP router is connected to BGPmon.

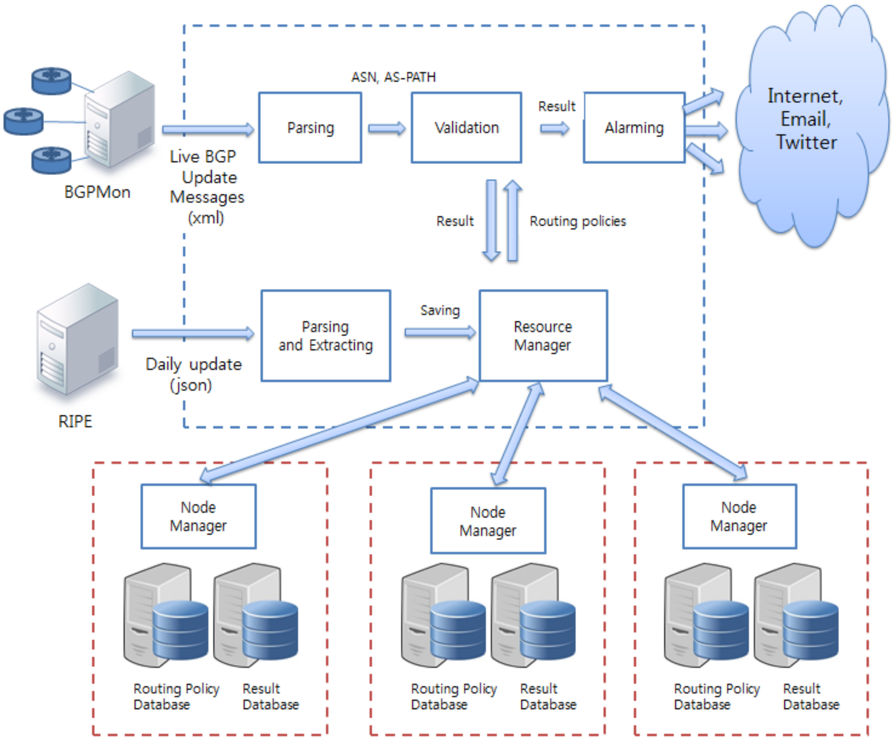


Figure. 4 Distributed Database for BGP Routing Policy Information

As shown in Figure 4, SAPBGP compares daily basis BGP update messages to our policy-based database. When SAPBGP collects policy information from the RIPE NCC repository, export and import polices are stored in random order. So, SAPBGP should check policy information and the complexity is O(n) in worst case. However, if the export and import polices are stored in order, SAPBGP can check policy information with binary search method and the complexity is O(log n). It takes time to keep managing policy information in order, but once the policy information is sorted, the comparison time is significantly reduced. In addition, local database of the SAPBGP will be distributed into multiple databases to stably manage policy information.

4.2 Constructing Database

We construct our own database by using API provided by RIPE. We have collected, every day, all of the AS imports and exports policies information since the eighteenth of February in 2014. In addition, we have separated tables in the database to keep the daily information as well as the accumulated information by adding new exports and imports to the existing exports and imports.

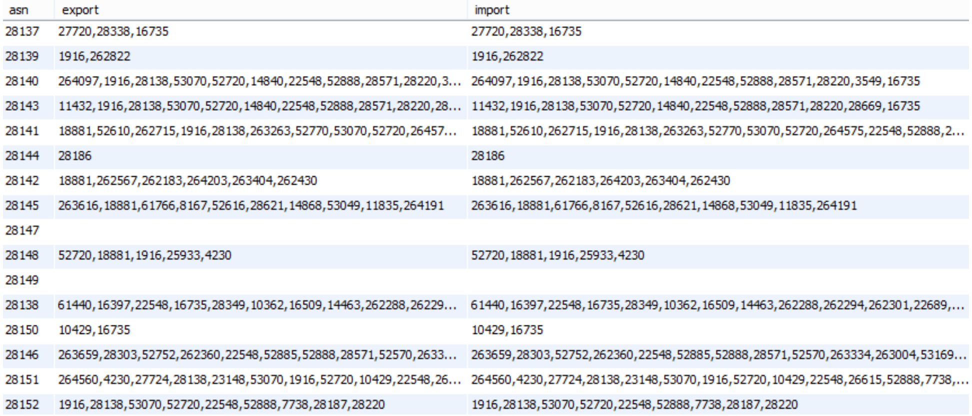
When the BGP was designed for the first time, the initial number of bits for the AS number was 16 bits, so AS number ranged from 0 to 65535. However, the number of bits for the AS number was changed to 32 bits. After that, each RIR reserves AS numbers as indicated in Table 1. We collected policy information from AS 1 to AS 394239 and skipped unallocated AS numbers that are not indicated in Table 1.

Table 1. 32 Bits AS Number Allocation Above 65535

	Allocation	*The number of ASes*
APNIC	131,072-135,580	4,509
RIPE NCC	196,608-202,239	5,632

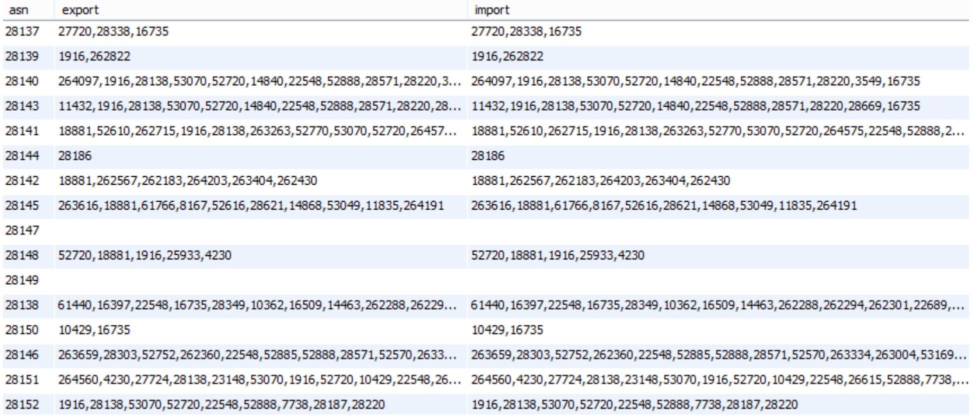
	Allocation	*The number of ASes*
LACNIC	262,144-265,628	3,485
AFRINIC	327,680-328,703	1,024
ARIN	393,216-394,239	1,024

We sent queries to RIPE NCC one by one. For example, if a query is related to AS 1 then the result includes AS 1's export policies, imports polices, and prefixes in the form of JSON. The SAPBGP parses the results so that the list of export policies and import policies can be stored to AS 1's record in the table. As a result, a new table is created every day to keep track of the daily policy information. In addition, the accumulated table is updated by adding new policies if AS 1 adds new policies against other ASes.



asn	export	import
28137	27720,28338,16735	27720,28338,16735
28139	1916,262822	1916,262822
28140	264097,1916,28138,53070,52720,14840,22548,52888,28571,28220,3...	264097,1916,28138,53070,52720,14840,22548,52888,28571,28220,3549,16735
28143	11432,1916,28138,53070,52720,14840,22548,52888,28571,28220,28...	11432,1916,28138,53070,52720,14840,22548,52888,28571,28220,28669,16735
28141	18881,52610,262715,1916,28138,263263,52770,53070,52720,26457...	18881,52610,262715,1916,28138,263263,52770,53070,52720,264575,22548,52888,2...
28144	28186	28186
28142	18881,262567,262183,264203,263404,262430	18881,262567,262183,264203,263404,262430
28145	263616,18881,61766,8167,52616,28621,14868,53049,11835,264191	263616,18881,61766,8167,52616,28621,14868,53049,11835,264191
28147		
28148	52720,18881,1916,25933,4230	52720,18881,1916,25933,4230
28149		
28138	61440,16397,22548,16735,28349,10362,16509,14463,262288,26229...	61440,16397,22548,16735,28349,10362,16509,14463,262288,262294,262301,22689,...
28150	10429,16735	10429,16735
28146	263659,28303,52752,262360,22548,52885,52888,28571,52570,2633...	263659,28303,52752,262360,22548,52885,52888,28571,52570,263334,263004,53169...
28151	264560,4230,27724,28138,23148,53070,1916,52720,10429,22548,26...	264560,4230,27724,28138,23148,53070,1916,52720,10429,22548,26615,52888,7738,...
28152	1916,28138,53070,52720,22548,52888,7738,28187,28220	1916,28138,53070,52720,22548,52888,7738,28187,28220

Figure 5 shows the records from AS 28137 to AS 28152 in the policy table.



asn	export	import
28137	27720,28338,16735	27720,28338,16735
28139	1916,262822	1916,262822
28140	264097,1916,28138,53070,52720,14840,22548,52888,28571,28220,3...	264097,1916,28138,53070,52720,14840,22548,52888,28571,28220,3549,16735
28143	11432,1916,28138,53070,52720,14840,22548,52888,28571,28220,28...	11432,1916,28138,53070,52720,14840,22548,52888,28571,28220,28669,16735
28141	18881,52610,262715,1916,28138,263263,52770,53070,52720,26457...	18881,52610,262715,1916,28138,263263,52770,53070,52720,264575,22548,52888,2...
28144	28186	28186
28142	18881,262567,262183,264203,263404,262430	18881,262567,262183,264203,263404,262430
28145	263616,18881,61766,8167,52616,28621,14868,53049,11835,264191	263616,18881,61766,8167,52616,28621,14868,53049,11835,264191
28147		
28148	52720,18881,1916,25933,4230	52720,18881,1916,25933,4230
28149		
28138	61440,16397,22548,16735,28349,10362,16509,14463,262288,26229...	61440,16397,22548,16735,28349,10362,16509,14463,262288,262294,262301,22689,...
28150	10429,16735	10429,16735
28146	263659,28303,52752,262360,22548,52885,52888,28571,52570,2633...	263659,28303,52752,262360,22548,52885,52888,28571,52570,263334,263004,53169...
28151	264560,4230,27724,28138,23148,53070,1916,52720,10429,22548,26...	264560,4230,27724,28138,23148,53070,1916,52720,10429,22548,26615,52888,7738,...
28152	1916,28138,53070,52720,22548,52888,7738,28187,28220	1916,28138,53070,52720,22548,52888,7738,28187,28220

Figure 5. A Screen Capture of the Policy Table

4.3 Monitoring Live BGP Stream

BGPmon provides live BGP streams through telnet to the public. So, whenever the routers that are connected to BGPmon receives BGP update messages, BGPmon converts BGP update messages to XML format messages and propagates the XML format messages to their clients. Apart from the BGP update message, the XML format message includes timestamp, date time, BGPmon id, BGPmon sequence number, and so on. Currently, there are 9 participants that are directly connected to BGPmon. We measured the number of update messages that BGPmon propagates for one day on February in

2014. Table 2 shows the minimum, maximum, and average number of update messages per 10 seconds.

Table 2. The Number of Update Messages from BGPmon

	The number of update messages per 10 seconds
Minimum	5
Maximum	1,321
Average	28.13

After parsing the live BGP message, the SAPBGP retrieves the ASN attribute and the AS_PATH attribute to check whether ASes in the AS_PATH attribute are connected to each other. Firstly, we compare the policy table in the database that is collected one day before. If we cannot find the pair, we compare the information from the accumulated table. If we cannot find the pair from the table, we consider the AS_PATH attribute as the suspicious AS_PATH attribute. If we find the suspicious AS_PATH attribute, we notify the AS network administrators of the suspicious AS_PATH attribute.

4.4 Experiments

In order to monitor AS path hijacking in the real world, we collected BGP live stream from the BGPmon project and compared the AS_PATH attribute to our policy-based database. The policy-based database is updated daily because BGP policy information changed whenever network operators wanted to change their BGP policies. Figure 6 shows the result of the AS_PATH monitoring experiment through the SAPBGP on the twenty-fourth of July in 2015. We conducted the experiment twice a month randomly during that period. Since original data contains a lot of duplicated information, we analyzed the result that does not contain duplications as well. Figure 6 shows the result of AS_PATH that does not contain the duplications. Our result shows 1.43% of the AS_PATH attributes are invalid and 98.57% of the AS_PATH attributes are valid.

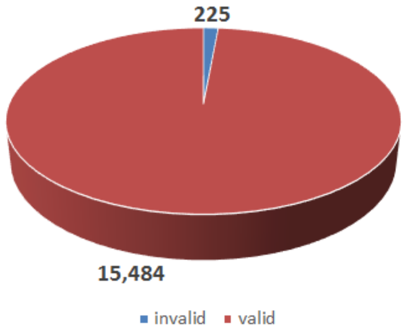


Figure 6. The Result of the AS_PATH Monitoring Experiment that does not Include Duplications

The SAPBGP runs on a 2.30 GHz i5-2415M machine with 16 GB of memory running Windows 8.1 MySQL Ver. 14.14 Distrib 5.1.41 is used for the database. We used JAVA to implement the SAPBGP that collects daily updates from RIPE NCC, receives live BGP streams from BGPmon, and validates the BGP stream by comparing the AS_PATH attribute to our database. The SAPBGP and database are located in the same machine to reduce the connection latency between them.

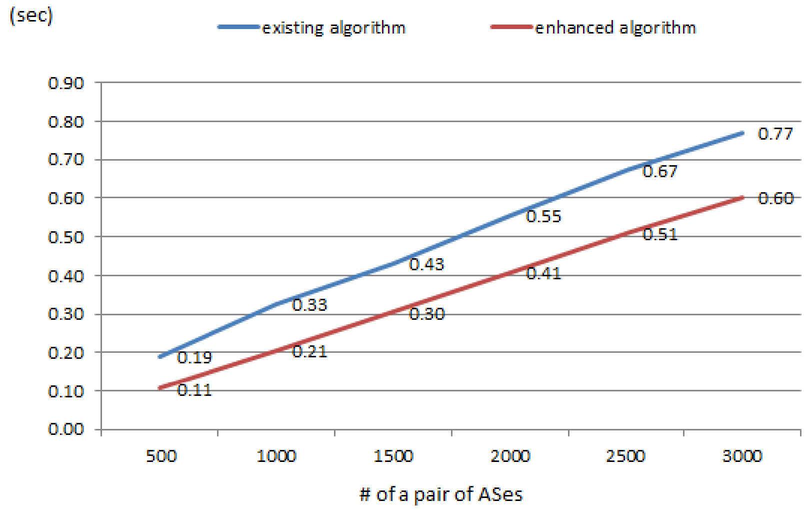


Figure 7. Comparison of the Two Results of the Performance Tests for the AS_PATH Validation

Error! Reference source not found.7 shows the AS_PATH validation time. The validation time includes accessing time to database, retrieving the specific AS record from a table, and comparing the AS_PATH attribute to the AS's record. The enhanced algorithm is on average 1.45 times faster than the existing algorithm.

5. Conclusions

Many solutions are proposed to prevent IP prefix hijacking, such as RPKI, BGPmon, Argus, and PHAS, but these solutions cannot protect the AS path hijacking except RPKI. SIDR proposed the RPKI using BGPSEC and BGPSEC is currently a work in progress. In order to monitor the AS path hijacking, we proposed Secure AS_PATH BGP (SAPBGP) that monitors the AS_PATH attribute in update messages whether each AS in the AS_PATH attribute is connected to each other based on our policy database collected from RIPE NCC repository. The result of the AS_PATH validation test shows 1.43% of the AS_PATH attribute is invalid and 98.57% of the AS_PATH attribute is valid on the twenty-fourth of July in 2015. In addition, the result of the performance test shows that the enhanced algorithm is on average 1.45 times faster than the existing algorithm.

References

[1] Murphy S., "BGP Security Vulnerabilities Analysis", RFC 4272, **(2006)**.

[2] F. Ying and Z. Hai, "Research on Characteristics of Internet Bottleneck Delay in AS Autonomous Domain and Analysis of Evolution", International Journal of Future Generation Communication and Networking, vol. 7, no. 2, **(2014)**, pp. 127-136.

[3] V. J. Bono, "7007 Explanation and Apology", http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html, **(1997)**.

[4] Renesys Blog, Con-Ed Steals the 'Net, http://research.dyn.com/2006/01/coned-steals-the-net

[5] Renesys Blog, Internet-Wide Catastrophe Last Year, http://www.renesys.com/blog/2005/12/internetwide_ nearcatastrophela.shtml

[6] Renesys Blog, Pakistan hijacks YouTube, http://www.renesys.com/blog/2008/02/pakistan_hijacks_ youtube_1 .shtml

[7] P. Litke and J. Steward, BGP Hijacking for Cryptocurrency Profit, http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit

[8] Renesys Blog, China's 18-Minute Mystery, http://research.dyn.com/2010/11/chinas-18-minute-mystery/

[9] Manderson T., Vegoda, L. and Kent S., "Resource Public Key Infrastructure (RPKI) Objects Issued by IANA", http://www.rfc-editor.org/rfc/rfc6491.txt, **(2012)**.

[10] D. Matthews, Y. Chen, H. Yan and D. Massey, "BGP Monitoring System", Available from: http://bgpmon.netsec.colostate.edu/

[11] X. Shi, Y. Xiang, Z. Wang, X. Yin and J. Wu, “Detecting Prefix Hijackings in the Internet with Argus”, In Proc. of ACM IMC, **(2012)**.

[12] Lad M., Massey D., Pei D., Wu Y., Zhang B. and Zhang L., “PHAS: A prefix hijack alert system”, In Proceedings of the 15th conference on USENIX Security Symposium - Volume 15 (USENIX-SS'06), vol. 15, **(2006)**.

[13] “Wireless Network Security: Vulnerabilities”, Threats and Countermeasures.

[14] Renesys Blog, Targeted Internet Traffic Misdirection, http://www.renesys.com/2013/ 11/mitm-internet-hijacking

[15] M. Lepinski, Ed., and BBN, “BGPSEC Protocol Specification,” Available: http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-08.

[16] IETF. “Secure Inter-Domain Routing (SIDR)”, Online, Sep. 2010. Available from http://datatracker.ietf.org/wg/sidr/

[17] Q. Li, Y. Hu and X. Zhang, “Even Rockets Cannot Make Pigs Fly Sustainably: Can BGP be Secured with BGP sec.?”, **(2014)**.

[18] R. Lychev, S. Goldberg and M. Schapira, “BGP Security in Partial Deployment”, **(2013)**.

[19] J. Yun, B. Hong and Y. Kim, “The Policy-Based AS_PATH Verification to Monitor AS Path Hijacking”, The Eighth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2014), Lisbon, Portugal, **(2014)**, pp. 16-20.

[20] J. Yun, B. Hong and Y. Kim, “The Policy-Based AS_PATH Verification to Prevent 1-Hop AS Path Hijacking by Monitoring BGP Live Streams”, International Journal on Advances in Security, vol. 8, **(2015)**, pp. 79-88.

[21] J. Juanchaiyaphum, N. Arch-int, S. Arch-int and S. Saiyod, “A Novel Lightweight Hybrid Intrusion Detection Method Using a Combination of Data Mining Techniques”, International Journal of Security and Its Applications, vol. 9, no. 4, **(2015)**, pp. 91-106.

[22] S. Divya and G. Padmavathi, “A Novel Method for Detection of Internet Worm Malcodes using Principal Component Analysis and Multiclass Support Vector Machine”, International Journal of Security and Its Applications, vol. 8, no. 5, **(2014)**, pp. 391-402.

[23] S. Z. Zhang, X. K. Qu and J. B. Sun, “Data Integration Mining based on Web Big Data”, International Journal of Multimedia and Ubiquitous Engineering, vol. 10, no. 6, **(2015)**, pp. 123-130.

[24] Z. Xu, Y. Gao and Y. Jin, “Application of an Optimized SVR Model of Machine Learning”, International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 6, **(2014)**, pp. 67-80.

[25] “The BGPmon project”, http://bgpmon.netsec.colostate.edu.

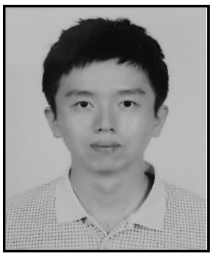
[26] “BGPmon live stream”, http://bgpmon.netsec.colostate.edu/join-the-peering.html.

[27] R. Housley, W. Ford, W. Polk and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC2459, **(1999)**.

[28] J. Schlamp, G. Carle and E. W. Biersack, “How to prevent AS hijacking attacks”, In Proceedings of the 2012 ACM Conference on CoNEXT Student Workshop (CoNEXT Student 2012), Nice, France, December **(2012)**.

[29] M. Lepinski, “Ed., and BBN, BGPSEC Protocol Specification”, http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-08.

Authors



Je-Kuk Yun, He received B.S. in computer science from National Institute for Lifelong Education in Seoul, South Korea, M.S. and D.Sc. degrees in computer science from Towson University, U.S.A. His research interests include network security, machine learning, image processing, and data mining.

Jin-Hee Song, She received B.S. degree in computer science from Seoul National University of Science & Technology, South Korea, M.S. degree in computer science from Hankuk University of Foreign Studies, South Korea, and Ph.D. degree in computer science from Soongsil University, South Korea. Currently, she is a professor at School of IT Convergence Engineering, Shinhan University, South Korea. Her research interests include parallel algorithms, distributed systems, embedded system, and data mining.