CoISM: Improving Security and Accuracy of BGP through Information Sharing

Ning Hu* and BaoSheng Wang

College of Computer National University of Defense Technology
ChangSha, Hunan, China
ning_hu@163.com, bsw@nudt.edu.cn
http://www.nudt.edu.cn

Abstract. Ensuring the authenticity of BGP routing information is a challenge problem of Inter-domain routing security. Due to lack of global information view, is it difficult to single autonomous system to detect bogus BGP routing information. A method for cooperative BGP validation based on self-organizing information sharing is presented in this paper. Cooperative validation gives a more comprehensive route view by sharing information among autonomous systems. It loosens the constraints from the autonomy and improves the security and accuracy of BGP. By leveraging the characteristics of locality and relativity, which is caused by routing policy, cooperative validation drives autonomous systems to cooperate independently and share information on-demand. More specifically, our method has incentive effect and supports incremental deployment.

Keywords: routing security, route validation, BGP monitoring, information sharing, coordination.

1 Introduction

Internet is comprised of thousands of Autonomous Systems (ASes), which exchange routing information with Border Gateway Protocol (BGP) and transmit traffic according to the routing information. Because it was designed for a trusted environment, BGP is vulnerable to routing attacks[1]. Recent studies and security incidents show that Inter-domain routing system is facing serious security challenges and the need to secure BGP has become increasingly pressing [2–4]. Many BGP security enhanced solutions based cryptographic authentications uses digital signatures and associated public key certificates to validate path attributes in BGP UPDATE messages passed among ASes[5–7]. All of these solutions provide an absolute security protection to routing information, but none of them has been deployed in Internet. The major obstacle includes: 1)lack of Internets global PKI infrastructure, 2)the high computational overhead caused

* Supported by Foundation of Science and Technology on Information As-surance Laboratory(No.KJ-12-07), Program for ChangJiang Scholars and Innovative Research Team in University(No.IRT1012), Light-weight algorithm and protocol for secure data transmission in RFID sensor networks(61070201).

J. Su et al. (Eds.): ICoC 2013, CCIS 401, pp. 256–265, 2013.

by calculating digital signatures, 3)the requirement to change BGP, 4) lack of incentive effect. Since there is no practically deployed security routing protocol, routing monitoring system is designed and deployed to offset the security vulnerability of BGP as a mitigation solution. BGP monitoring system improves the security and accuracy of routing information through collecting and validating BGP data from BGP router [8, 9]. However, most routing monitoring systems need a schedule or management center and do not consider the requirement of autonomy and incentive.

In this paper, we designed a cooperative method for BGP route validation which is based on information sharing. The basic principle of cooperative validation is as follows: multiple autonomous systems (ASes) deploy monitoring service and check the credibility of BGP route in a self-organized way to achieve the ultimate security together. By means of sharing the monitoring information among multiple autonomous systems, cooperative validating BGP provides a more comprehensive routing view, overcomes information unavailability and locality constraints and enhances the ability of autonomous system to detect false routing information. In this paper, we also consider two important factors which include incentive and deployment. For convenient, our method is names as CoISM.

This paper is organized as follows: Section 2 described our motivation and objectives. Section 3 describes the algorithm for cooperative route validation. Section 4 gives experiment and result analysis. Section 5 is an overview of related work. Finally, Section 6 concludes the paper.

2 Motivation and Objective

2.1 Motivation

Ensuring the authenticity of routing information is the key issue of routing security. Route monitoring system increase the security and accuracy of BGP routing information through route validation. But, due to lack of global information view, it is difficult to single BGP monitor to identity false BGP route. For example, due to lack of enough information about IP prefix ownership, single AS can not identify a prefix hijacking advertise. To implement cooperative BGP monitoring among ASes, we need more efficiency information sharing mechanism. Based on this purpose, we noticed two characteristics of monitoring information: local validity and relative validity.

When an AS (such as X) received a BGP route, it might do not select the route as the best route for some reasons. Hence, any monitoring information about this route is invalid to X. This characteristic is called local validity. Obviously, if a piece of monitoring information is invalid to AS X, it is not necessary to send this information to it. According to local validity, all of the internet ASes can be classified into three subsidiary sets which are infection set, immunity set and isolate set. For any AS node, if it selects the false route as the best one, it belongs to the infection set. If an AS node can identify the false route, it belongs to the

immunity set. If an AS node does not receive or use the false route according to its routing policy even it is true, it belongs to the isolate set.

For an example, as shown in Fig.1, suppose AS E is a malicious node and try to hijack prefix P_1 of AS F. When AS E advertise a NLRI for prefix P_1 to AS A, both A and B will select this bogus route as the best route according to rule of shortest path first. In this case, AS A and B are infection nodes. AS C is an immunity node, because C is the owner of prefix P_1, when it receives NLRI advertised by AS E, it detects it is a prefix hijacking. At last, AS D is C's customer and C will not advertise false routing information to AS D, so AS D is an isolated node.

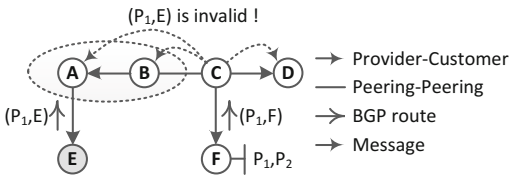

Fig. 1. Local validity of monitoring information

Most routing policies are designed oriented AS without diffusing prefixes owned by the same AS. Since routing hijacking attack is based on routing policy breaches, if an AS is under routing attack, all of its prefix might be under attack too. So, if monitoring information about prefix P_1 is valid to an AS (such as Y), information about prefix P_2 which is owned by the same AS is probably valid to Y. This second characteristic is called relative validity. According to relative validity, all of the monitoring information about prefix owned by the same AS might cause the same infection, immunity and isolation node classification.

Therefore, we realizes it is possible to implement monitoring information sharing on-demand.

2.2 Objective

For the sake of further argument, we explained the special meaning of some terms, which appeared in the following description.

Term 1: ***Monitoring Information***. Monitoring information refers to route validation request and acknowledge.

Term 2: ***Monitor***. Monitor collects BGP route from AS BGP router, validates the authenticity of BGP route according to local knowledge. To simplify description, we denote AS node as monitor. A monitor can be defined by a tuple $= (M_{ID}, I_M, K_M)$. M_{ID} is a unique identity of monitor. I_M represents set of local monitoring information which is produced or received by monitor. K_M is the local knowledge database which is composed of BGP routing table, routing policy, prefix ownership, anomaly detection rules, blacklist of false route and

so on. The local knowledge is used to produce, identify and deliver monitoring information.

Term 3: ***Information Coverage***. Given a monitor M and a piece of monitoring information I_i, if I_i is included in the I_M of M, M is covered by I_i.

Term 4: ***Effective Coverage/Ineffective Coverage***. Given a monitor M_I, and a piece of monitoring information I, if M_I receives I and benefits from it, it is an effective coverage, nor it is an ineffective coverage.

Term 5: ***Maximum Effective Coverage***. Given a piece of monitoring information I and a monitor set $S = M_1, M_2,, M_n$, if and only if every monitor of S is effective covered by information I, it is a maximum effective coverage.

Term 6: ***Routing Correlative***. Given two BGP routes R_A, R_B and corresponding monitoring information I_A and I_B, if any condition as follows is satisfied, I_A and I_B are routing correlated.

a) The IP prefix of R_A and R_B belong to the same AS;

b) The AS-PATH property of R_A and R_B share the common sub-path;

Being similar with the topology of Internet, all of the AS monitors are widely distributed and lacking of global view for information requirement, monitor only coordinates closely with a subset of the rest monitor.Considering these characteristics,the key issue of node coordination is how to share information. The objective of CoISM can be described as follows: For a given monitor set $S_M = \{M_1, M_2,, M_n\}$ and a series of information $S_I=\{I_1,,I_m\}$, how to realize maximum effective coverage for S_I with low computing and communication cost.

3 Cooperative Validating BGP

3.1 Algorithm

Geoffrey G. proposed an origin and path validation method IRV [15]. In their study, BGP monitor sends query message to other ASes monitor one by one which are included in AS-PATH. Geoffreys method proposed a cooperative monitoring method but did not consider blind spot and linearity increasing communication cost.

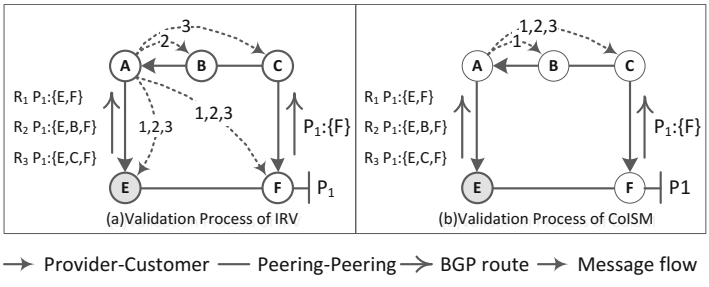

Fig. 2. Route validation process of IRV and CoISM

Fig.2 (a) demonstrates the validation process of IRV. The dotted line denotes validation message sent by AS A. In this scene, AS A, B and C deploy IRV services. These three ASes monitoring their native and customers IP prefix. E is a malicious AS and advertises three false BGP routes R_1, R_2 and R_3 for prefix P_1 to AS A. In the first loop, AS A sends a validation message to F when it receives R_1 from AS E because only AS F is included in AS-PATH property of R_1. Unfortunately, AS A does not get confirmation message because AS F does not deploy IRV service. In the second loop, AS A will send validation message to F and B when it receives R_2 from AS E. Again, AS A does not get confirmation message because AS B cannot identify whether R_1 is a false route. Only when AS A sends AS C a validation message for route R_3, it will receive a notification because AS C knows that AS F is the actually owner of prefix P_1. In this example, AS A is a blind spot for R_1 and R_2. In addition, IRV does not make use of relativity of monitoring message. For every BGP route, AS A sends message to all AS nodes included in AS-PATH. As the count of routing increasing, the communication cost increases linearly.

According to the analysis of local validity and relative validity, we propose a coordination model which is called CoISM. Fig.2 (b) demonstrates the route validation process of CoISM. When AS A receives R_1, it sends validation request to AS B and C which has deployed BGP monitoring service. In the first loop, only AS C replies a notification. In the second loop, AS A does send request to AS B because AS B does not reply in the first loop. Instead, AS A sends request to AS C, because these three routes are routing correlative. Contrasting with Fig.2 (b), our method removes blind spot and decreases communication cost. we designed CoISM algorithms which are described in algorithm1 and algorithm2.

3.2 Implementation

We implement a cooperative routing monitoring system which is composed of route monitor and CoISM registry. There are three functions of route monitor. First, monitor establishes dumb iBGP session with ASs router to collect BGP routing. Second, monitor exchanges routing monitoring information with other monitor. Last, monitor sends notification to other monitor when false route is detected. CoISM registry provides access information of AS which deploys monitor service.

In our cooperative routing monitoring system, each ASs routing monitoring service is deployed on PC server and exchanges monitoring information with other ASs monitoring service through TCP connection. Each AS sends registration information to CoISM registry when monitoring service is deployed. Small size AS can consign monitoring service to its provider. The architecture of CoISM is illustrated as Fig.3.

Due to lacking of schedule center, AS cannot sense whether other AS deploys monitor. Hence, an important issue of CoISM is how to locate monitor for AS. To resolve this question, we build a CoISM registry web site to store and provide all monitors contact information. CoISM registry only store monitor location

Algorithm 1. Produce and send route validation request

```
1: if Validate(R ,K_M) is VALID or INVALID then
2:    return;
3: end if
4: if Validate(R ,K_M) is UNCERTAIN then
5:    Initialize newM and add it into I_M;
6:    for I∈I_M do
7:       if I.Route is routing correlative with R then
8:          Add validator of I into authSet;
9:          Add producer of I into applicantSet;
10:      end if
11:   end for
12:   if authSet and applicantSet is NULL then
13:      Add monitor in R.AS-PATH into authSet;
14:   end if
15:   for all monitor in authSet and applicantSet do
16:      if newM.TTL equal THRESHOLD then
17:         break;
18:      end if
19:      Send newM to the monitor;
20:      emphnewM.TTL++;
21:      if ackM.result is VALID or INVALID then
22:         Update K_M and newM;
23:         return;
24:      end if
25:      if emphackM.suggestedList is not NULL then
26:         Add suggested monitor into authSet; goto 12;
27:      end if
28:   end for
29: end if
30: return;
```

Algorithm 2. Receive and reply route validation request

```
1: newM = Listen();
2: if Validate(newM.Route,K_M) is VALID or INVALID then
3:    Add newM into I_M;
4:    Update fields of newM and reply ackM;
5:    return;
6: end if
7: if auth(newM ,K_M) is UNCERTAIN then
8:    Search I_M for validation request which is routing correlative with R;
9:    Add requests validator into ackM.suggestedList;
10:   Add requests producer into ackM.suggestedList;
11:   Update fields of newM and reply ackM;
12: end if
13: goto 1;
```

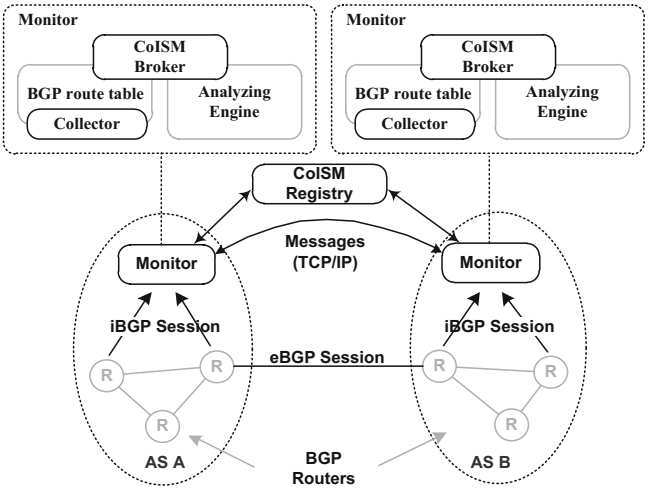

Fig. 3. Deployment and implementation of CoISM

information (e.g., IP addresses) for each AS. AS can get the monitor deployment view through CoISM. Be different from IRR, CoISM registry only provides the distribution view of BGP monitor and does not strive AS submit their monitoring information.

4 Simulations and Analysis

In this section, we define several indicators to evaluate the efficiency of CoISM.

1. **Effective Coverage Ratio**

Effective coverage ratio is used to assess whether CoISM implements information on-demand. In equation 1, function $Cover(I_i,\ M_j) \rightarrow \{0,1\}$ indicates whether monitor M_j is covered by message I_i. Function Valid($I_i,\ M_j) \rightarrow \{0,1\}$ indicates whether message I_i is effective to monitor M_j.

$$\sum_{j=1}^{n} \left(\frac{\sum_{i=1}^{m} (Cover(I_i, M_j) * Valid(I_i, M_j))}{\sum_{i=1}^{m} Cover(I_i, M_j)} \right) \tag{1}$$

2. **Profit Ratio**

Profit ratio is used to indicate the incentive effect of CoISM. Function $Imp(I_i,M_j)\rightarrow\{0,1\}$ indicates whether message I_i is received from other monitor. Function Exp(I_i,M_j)$\rightarrow\{0,1\}$ indicates whether message I_i is exported by entity M_j.

$$\sum_{i=1}^{m} \frac{Import(I_i, M_j) * Valid(I_i, M_j)}{Exp(I_i, M_j) + Imp(I_i, M_j) * Valid(I_i, M_j)} \tag{2}$$

3. **Communication Cost**

To simplify analyze, we use count of information transmission to evaluate the communication cost when effective coverage ratio reach threshold value t.

$$\sum_{j=1}^{n}(Cover(I_i, M_j)) \tag{3}$$

To simulate the real inter-domain routing system, we select a BGP snapshot from RouteViews on May 20, 2012 [10]. In this experiment, we first construct a network according to BGP data of RouteView. Then we sorted AS node according to the degree in descending order and select the first K(K=200,400,600,800, 1000) nodes to construct monitor community M.

We adopt round-robin model to execute this experiment. In each loop, every monitor randomly received 10 hijacking route which shared prefix with one of other monitor. When any monitor receives a new BGP route, it produces and sends validation request according to algorithm1. This procedure repeats 10 loops. We calculate and record three indicators defined upon when every loop is finished and get the experiment result which are shown in Fig4.

In Fig.4(a), the horizontal represents the number of loop, and vertical represents the valid coverage rate. From Fig.3(a), we get following conclusions: For a specific AS set, valid coverage ratio approaches to 1 in a limited time. Due

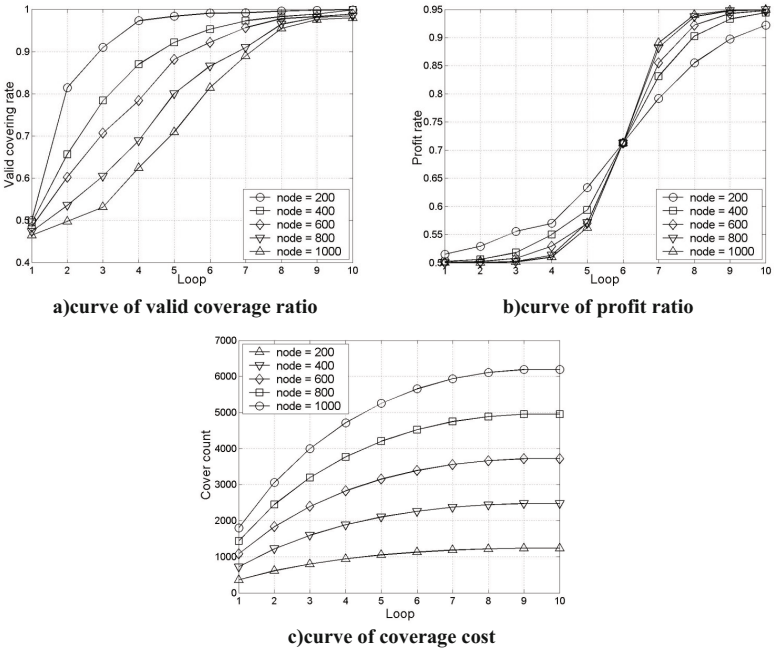

Fig. 4. Curve of valid coverage ratio

to lack of enough elicitation information in the initial phase, the valid covering rate increases slowly. This phenomenon is more obvious when the count of node is large.

Fig.4(b) shows the change of average reward. From this result we get following conclusions: The profit of monitor depends on valid coverage rate. At beginning, valid coverage rate is lower and profit rate of monitor increase slowly. Monitors profit rate increases quickly when the valid coverage is large than threshold value. This is because valid information causes more valid feedback. Due to transmission control and loops avoid mechanism, profit rate of monitor increases slowly when it approaches 1.

Fig.4(c) shows the change of communication cost when valid coverage arrives 0.9. From this result, we get two conclusions: The communication cost nonlinear increase with the iteration times and amount of monitoring information. This is better than IRV. After several loop iterations, CoISM slows down the increasing speed of communication cost. This is benefited from valid coverage increasing.

5 Related Work

Most route monitoring systems adopt two category information sharing model, which are centric model and distributed model.

In centric model, there is an information center which is in charge of collecting, storing and querying information from all the AS. For example, IRR (Internet Routing Registry) uses a centralizing model to store routing policy of AS. IRR allows ISPs to publish high-level specifications of their policies, and analyze the effects of their policies on Internet routing [11]. Some BGP routing monitoring project also adapts centralize model to implement information sharing, such as Looking Glasses [9], MyASN of RIPENCC [12] and Gradus of Renesys[13]. Centric model has some limitations. First, the cost of data storage and communication are huge. Second, the efficiency of information sharing is low, because every AS must search some information on demand from the massive database. Last, because the information provider does not know who their information customers are and what the purposes of them are. For protecting their security, the accuracy of the registered data is uncertain [14].

In distributed model, ASes directly exchange and share routing validating and monitoring information each other without a third party. Goodell et al. provide a solution to validate BGP routes which is called IRV (inter-domain route validation)[15]. Pei et al. provide an active query based method to validate a BGP route which is called Diagnosis through Root Cause Notification, topology Accumulation, and Query (DRAQ)[16]. Yu et al. [17] proposed a novel distributed reputation protocol to make assure the trustworthy of BGP route.

6 Conclusion

How to sharing information among AS nodes is the crucial issue of cooperative inter-domain routing monitoring. CoISM proposes a heuristic information sharing method which makes using the local validity and relativity of monitoring

information. Being contrasted with flooding or IRV, CoISM has higher information transmission efficiency and lower communication cost. Additionally, CoISM is incentive and builds ASs reward on its invocation.

References

1. Murphy, S.: BGP Security Vulnerabilities Analysis. RFC 4272, IETF (2006)
2. Ola, N., Constantinos, D.: Beware of BGP Attacks. Computer Communication Review 34(2), 1–8 (2004)
3. Butler, K.: A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE 98, 100–122 (2010)
4. Rensys Blog, `http://www.renesys.com/2008/02/Pakistan-hijacks-youtube-1/`
5. Stephen, K., Charles, L., Karen, S.: Secure Border Gateway Protocol (S-BGP). IEEE Journal on Selected Areas in Communications (JSAC) 18(4), 582–592 (2000)
6. Cisco, `ftp://ftp-end.cisco.com/sobgp/presentations/BCR-soBGP.pdf`
7. Van, P.C.O., Wan, T., Evangelos, K.: On Interdomain Routing Security and Pretty Secure BGP (psBGP). ACM Transactions on Information and System Security 10(3), 1–41 (2005)
8. Yan, H., Oliveira, R., Burnett, K.: BGPmon: A real-time, scalable, extensible monitoring system. In: Cybersecurity Applications and Technologies Conference for Homeland Security (CATCH), pp. 212–223. IEEE Computer Society Press, Los Angels (2009)
9. Looking Glasses, `http://www.traceroute.org`
10. University of oregon route views project, `http://www.routeviews.org/`
11. Internet Routing Registry, `http://www.irr.net/index.html`
12. The RIPE NCC MyASN service, `http://www.ris.ripe.net/myasn.Html`
13. GRADUS, `http://www.renesys.com/index.shtml`
14. Georgos, S., Michalis, F.: Analyzing BGP Policies: Methodology and Tool. In: IEEE INFOCOM, pp. 1640–1651. IEEE Society Press, New York (2004)
15. Goodell, G., Aiello, W., Griffin, T.: Working around BGP: An incremental approach to improving security and accuracy of inter-domain routing. In: ISOC NDSS, pp. 75–85. National Security Agency Press, San Diego (2003)
16. Pei, D., Lad, M., Massey, D., Zhang, L.: Route Diagnosis in Path Vector Protocols. Technical Report TR040039, UCLA CSD (2004)
17. Yu, H., Rexford, J., Felten, E.W.: A distributed reputation approach to cooperative Internet routing protection. In: Secure Network Protocols, pp. 73–78. IEEE Society Press, New York (2005)