ROUTE RELIABILITY RANKING ALGORITHM FOR PREFIX HIJACKING ATTACKS IN BORDER GATEWAY PROTOCOL

C. Siva[1] and S. Arumugam[2]
[1]Department of Information Technology, Nandha Engineering College, Erode, Tamil Nadu, India
[2]Nandha Educational Institutions, Erode, Tamil Nadu, India
E-Mail: csivaphd@gmail.com

ABSTRACT

Prefix-hijacking attack offers malicious parties to gain access to untraceable IP addresses in Intenet. Border gateway protocol (BGP) is the dominant inter domain routing protocol used in Internet. In this paper, to defend against Prefix Hijacking Attack on border gateway protocol (BGP), we propose to design a route reliability ranking (RRR) algorithm. The algorithm is used to authenticate the validation of a routing update based on the common facts of the autonomous systems (AS's) in the network. After RRR, an incentive based route selection mechanism is performed to identify the suspicious candidates and avoid routes propagated by them. By simulation results, we show that the proposed algorithm is efficient defensive technique for prefix hijacking attack in Internet.

Keywords: hijacking, border gateway protocol, IP addresses, authentication.

1. INTRODUCTION

1.1 Border gateway protocol

The internet is a universal, decentralized network which constitutes many smaller interconnected networks. Network consists of hosts and routers. On the availability of many paths, the information flows through a single path chosen according to routing process. The ways to locate other hosts and routers and path selection are performed by routing protocol. The autonomous system (AS) is the network which is under the control of a single organization. The two categories of routing available in AS are intra domain (routing within an AS) and inter domain (routing between ASs) routing. Border gateway protocol (BGP) is the dominant inter domain routing protocol. It has been deployed since the commercialization of the internet, and version 4 widely exists for a decade. Due to practical simplicity and resilience, BGP plays a major role in global internet. Moreover BGP offers security guarantees.

As internet is intended for communication between largely trusted parties, BGP was designed to enable inter domain routing within and between trusted networks. [1]

The drawbacks related to BGP and the inter-domain routing environments are

1. The techniques to protect the reliability, freshness and source authenticity are not available.
2. The mechanism involving verification of authenticity of an address prefix and an AS and origination of this prefix in the prefix in the routing system is not present
3. The strategy to verify genuineness of attributes of a BGP update messages is not available
4. The technique to verify whether local cache RIB information is reliable to the existing state of the forwarding table is not present.

1.2 Prefix hijacking attack

The attack that offers malicious parties to gain access to untraceable IP addresses is prefix-hijacking attack.

Prefix hijacking occurs in one of the three ways

1. The announcement of block holding unallocated space.
2. The announcement of a sub-block of an existing allocation.
3. Competing announcement for exactly the same space as an existing allocation can be announced. [17]

1.3 Existing secure BGP protocols

Secure BGP (S-BGP): The first wide ranging routing security solution aimed specifically for BGP is secure BGP (S-BGP). The key element of S-BGP is that it employs public key certificates for communicating authenticated data. The security is implemented in this protocol by validating the data passed among AS's using public key certificates [10]

Secure origin BGP (soBGP): In comparison to S-BGP, soBGP defines a PKI for authenticating and authorizing entities and organization. The three types of certificates managed by PKI are as follows. Certificate 1: It binds a public key to each soBGP speaking router. Certificate 2: It offers details regarding policy along with selected protocol parameters and local network topology. Certificate 3: It is similar to S-BGP's address attestations. It represents address ownership or delegation. [11].

Inter Domain Route Validation (IRV): IRV service is a receiver-driven protocol. Its operation is independent of the routing protocol. Each AS in IRV has an IRV server. On receiving an update message, a receiving BGP speaker will demand to local speaker to indicate regarding the correctness of received information. The limitation of IRV is that it requires a functioning network to be useful. [12]. Pretty Secure BGP (psBGP): The introduction of address origin authentication service within a large comprehensive architecture for BGP security is done by pretty secure BGP (psBGP). Here, the

AS's are validated with the help of PKI and path authentication is done by optimized version of S-BGP [13].

Secure Path Vector Protocol (SPV): The implementation of path validation using a string of one-time signature is performed by SPV. This approach is extended by SPV to allow a single off-line signature to generate potentially many signatures. The merit is that the operation of SPV is extremely lightweight and hashing is used as the primary cryptographic mechanisms [14].

Aggregated path authentication: The authentication of path information in BGP route announcements by blending of two efficient cryptographic techniques such as signature amortization and aggregate signatures is done by aggregated path authentication techniques. This method reduces the number of stored signatures effectively use hardware acceleration to considerably speed up signature verification required for path authentication. [15]

Idealized Secure BGP: Idealized Secure BGP utilizes the oracle to filter malicious routes. Following the filtration of a route, the next finest route (if any) is used. Idealized Secure BGP provides the greatest possible security benefit among all secure protocols. [16] In this paper, to defend against Prefix Hijacking Attack, we propose a reliability ranking algorithm for BGP.

2. RELATED WORKS

Junaid Israr *et al.* [4] proposed an easy to deploy protocol to validate BGP routing updates. CBGP modifies the current BGP selection algorithm by adding an extra check of the validity of the origin IP prefix and the AS path. In the future, they are planning to investigate the overhead and cost associated with the deployment of CBGP protocol on the current Internet infrastructure. Since the proposed validity state factor will override other criteria for BGP decision process, the network routing table with the validity state factor considered will appear very different from when the validity state factor is not considered.

Fernando Sanchez *et al.* [5] developed a light-weight region-based BGP announcement filtering scheme (RBF) to improve the BGP security. In contrast to existing solutions that indifferently prevent or detect prefix hijacking attacks, RBF enables differentiated AS and prefix filtering treatment and blends prefix hijacking prevention with deterrence. Hexing Wang *et al* [6] proposed the BGP security configuration framework based on currently available technologies to improve the security of BGP routers. The framework is made up of three layers. In each layer, specific guidelines according to configuration commands are described. The deployment of the framework doesn't rely on public key infrastructure or other central authority. So it can be easily deployed in ISP networks without additional costs.

Bezawada Bruhadeshwar *et al.* [7] addressed the problem of securing routing protocols in the control as well as data plane. They have presented symmetric key based solutions that can work at the control plane and can be reused for securing the data plane. Moreover, compared to existing approaches, their solutions can handle collusive attacks among routers more effectively. Currently, they are working on the practical issues such as implementation and deployment of their protocols on the Internet. Jian Qiu *et al.* [8] proposed a lightweight hijack-proof BGP proposal and its transition scheme. The design goals and the techniques adopted offer the distinguished features such as: 1) the system is able to prevent prefix hijacking, which utilizes the route validation information of prefix ownerships, AS links, and AS relationships of the entire Internet to prevent the origin-AS, AS-Path and redistribution hijacking respectively and 2) transition scheme, which introduces an independently operated verification server to protect the BGP system against prefix hijacking during the transition period, ensures the seamless deployment of Hi-BGP and finally we combine the advantages in the existing BGP security solutions to ensure the simplicity and efficiency of their system.

Francesco Palmieri [9] focused on the impact of worm spreading events on BGP inter-domain routing dynamics on time scales that are long enough to have the potential to increase route convergence times and impact the network behavior. In future, they plan to build even greater resiliency and adaptive containment countermeasures into the Internet infrastructure operating real-time smart checks on the network stability to prevent such events from recurring with even more impact. Zhenhai Duan *et al.* [19] have proposed an algorithm for mitigating the attacks on Denial of service attacks based on IP spoofing. Their algorithm used inter domain packet filtering (IDPF). IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. A key feature of their scheme is that it does not require global routing information. Their algorithm is applicable only for a small number of candidate networks. Their IDPF architecture is efficient for counter attack of DDOS. In their work, the attacker can be easily traced. Further, their architecture can easily be deployed for the currently based BGP architecture.

3. ROUTE RELIABILITY RANKING (RRR)

3.1 Overview

To defend against Prefix Hijacking Attack which is a category of path validation in BGP, we propose to design a Route Reliability Ranking (RRR) algorithm. To authenticate the validation of a routing update, the algorithm is based on the common facts of the ASs in the network. The algorithm verifies the accuracy of AS path when a BGP update message is received, by looking up the path details from other autonomous systems in the network. Each AS constructs a Route Reliability Matrix (RRM) based on its received BGP routing update messages. The reliability of a received path can be checked by the RRM.

In addition to route reliability testing, we also provide an incentive based route selection mechanism to identify the suspicious candidates and avoid routes propagated by them. In this mechanism, a penalty value is assigned for the AS which appears on an invalid route. A router maintains a counter in each destination to count the occurrence of suspicious AS. As the number of destinations that are affected by the attacking AS increases, the number of penalty increases for the AS. Then the route with the lowest penalty value for a destination is selected as the best route. Since the RRR algorithm does not require the modification of existing routing protocols, and does not use cryptography calculation; it is cost effective and less complex.

3.2 Prefix-hijacking attack

We assume that AS's prefer shortest path routes. Hence, if an adversary is able to falsely advertise a shorter path to the prefix to any AS on the legitimate path, then it is able to divert the legitimate path to itself. This can be performed by prefix hijacking. Figure-1 explains the prefix hijacking process.

The circle represents AS's
AS_d - destination
AS_s - source.

AS_m - malicious node and it performs the attack at some given AS in the path denoted as AS_p. AS_p could be any AS along the path.

AS_m is illegally originating AS_d's prefix. In the absence of authenticating information, AS_p is unable to determine which originator is genuine, and so we assume it simply chooses the closer AS in terms of hops. This attack succeeds whenever one or both of AS_d or AS_p have not deployed origin authentication, and dis (AS_m, AS_p) < dis (AS_d, AS_p).

To defend against Prefix Hijacking Attack which is a category of path validation in BGP, we propose to design a Route Reliability Testing (RRR) algorithm.

3.3 Route reliability ranking (RRR) algorithm

Route Reliability Ranking (RRR) algorithm is designed to tackle the BGP vulnerabilities. The RRR algorithm does not require the modification of existing routing protocols, and does not use cryptography calculation, making it both deployment and resource friendly. This algorithm is based on the common views from the AS's in the network to verify the validation of a routing update. i.e., if one receives an update about the path P from AS_k, it calculates to see if other AS's (except AS_k) in the network have the same information about P as that just received from AS_k.

In RRR algorithm, the steps handled are as follows

1. Each AS constructs a route reliability matrix (RRM) based on its received BGP routing update messages.

2. The reliability of a received path can be checked using RRM

3. If conflict exists, the RRR algorithm launches another process to find out the actual path.

The reliability check in step2 is based on the previous hop information stored in the RRM. As can be seen in step3, the RRR algorithm not only provides the validation of a path to a destination, but also be able to identify the actual connection of that path.

3.3.1 AS-path pool

Figure-2 shows an example of BGP network linking nine autonomous systems. Considering the network G in the example, as BGP routers advertise their path to network G by BGP update messages, after receiving the messages from AS_J and AS_L, AS_K will have the AS-path pool of network G.
For the network G

Case-1
Path = {J, I, H, G}
Next hop assigned will be AS_J

Case-2
Path = {L, M, N, O, G}
Next hop assigned will be AS_L

From the above cases, there are two paths for network G, and the path [J, I, H, G] is selected since it is shorter.

3.3.2 Route reliability matrix

RRR algorithm, RRM is built, which are based on the AS-path pools. RRM is the 10×4matrix, where row denotes the number of AS and column constitutes the values of destination, length, previous hop and penalty values. Figure-3 shows the Route Reliability Matrix (RRM).

Column-1: It indicates the destination ASs in the network.
Column-2: It indicates the number of hop from the origin AS to the destination ASs.
Column-3: It indicates the predecessor of the destination AS in the path to the origin AS.
Column-4: The process of assigning penalty value is described in the next section 3.4**.** Initially the penalty values are assigned as zero in RRM.

The steps involved in construction of RRM are explained as follows.

1. Since AS_K is the owner of the table, on the entry of AS_K, the length and predecessor values are zero and itself respectively.

2. Since AS_J and AS_L are the neighbors of AS_K, the length from them to AS_K is 1, and their predecessor is AS_K.

3. Based on the selected path [J, I, H, G] in the AS-path pool of network G, AS_I and AS_J are in the middle of the path from AS_H to AS_K. Therefore, for the entry of AS_H, the length is 3, and the predecessor is AS_I; whereas for the entry of AS_I, the length is 2 and the predecessor is AS_J.

It is important to note that the selected (best) path is used to calculate the length value, even though there is more than one path available.

4. Similarly, based on another AS path {L,M,N,O,G} shown in the AS path pool of network G, the entries of ASs M, N, and O in the RRM can be filled.

3.3.3 Verifying reliability for declared as path

After receiving a new BGP, AS_K can validate the AS path claimed in that update by checking the corresponding RRM. Figure-4 shows an example of an attack. AS_L has a malicious router that advertises to AS_k a BGP update containing a false AS path {L, O, G} to the prefix G.With the RRR algorithm, when AS_K receives the claimed AS path to the prefix G from AS_L, it asks for the "network G RRM" from other involved ASs to validate the claimed AS path in the update.

In this case, since the claimed path is {L, O, G}, excluding the announcer, other involved ASs are AS_G and AS_O. Suppose that AS_K first check the AS_G's RRM. By tracing the destinations in the matrix, AS_K finds that AS_G is the neighbor of AS_O This relationship (O-G) matches part of the claimed AS path (L, O, G). However, as AS_G's RRM does not contain any information of AS_L, AS_K checks AS_O 'RRM. After tracing the destinations in the table, AS_L finds that only AS_G and AS_N are directly connected to AS_O. It is inconsistent to what the AS path claimed in the BGP update (which claims AS_L is directly to AS_O). Therefore, AS_K identifies that this update is suspicious.

The purpose of this method is to check the reliability of a claimed AS path. However, if contradiction occurs, it is only able to identify that the update is suspicious, but not able to Figure out the correct AS path.If a path to a given prefix is correct, the ASs in the network should have the consistent knowledge about that path. Therefore, by checking more RRR algorithm from other ASs, it is able to Figure out the correct AS path which is common to other ASs in the network.

3.4 Penalty based route selection

As per section 3.3, RRR only provides the ability to trigger alarms whenever a node propagates invalid route announcements. In this section we add penalty based route selection along with reliability testing so that suspicious candidates is identified and routes propagated by these candidates can be avoided. In RRR, the path will be traced back to the each destination in the RRM. If conflict exists, AS_K can discard the update and label the advertiser as suspicious, thus assigning a penalty value. After that, ASK can find out the actual path to the claimed prefix in that update, by checking more RRM from other ASs.

The process involved in penalty based route selection is as follows. Each time AS appears on an invalid route, router starts counting across destination and assigns this count as a penalty value for the AS. As adversary at the destination is increased, the penalty value for AS is also increased. Thus the route selection strategy helps in choosing the route to a destination which as the lowest penalty value.

Consider the example of an attack in Figure-4. As per RRR described in the previous section, AS_L is found to be a malicious node. So the penalty value of the AS_L is increased. In the same way, there can be many malicious AS in a route with increased penalty value. By choosing the minimum penalty route, the analyzer G can avoid the invalid routes through AS_L since they have higher penalty value. One key assumption used in this technique is: The identity of AS propagating invalid routes is always present in the AS path attribute of the routes. The identity of every AS is verified by the neighboring AS which receives the advertisement.

4. SIMULATION RESULTS

AS_L has a malicious router that advertises to AS_k a BGP update containing a false AS path {L, O, G} to the prefix G.With the RRR algorithm, when AS_K receives the claimed AS path to the prefix G from AS_L, it asks for the "network G RRM" from other involved ASs to validate the claimed AS path in the update.

In this case, since the claimed path is {L, O, G}, excluding the announcer, other involved ASs are AS_G and AS_O. Suppose that AS_K first check the AS_G's RRM. By tracing the destinations in the matrix, AS_K finds that AS_G is the neighbor of AS_O This relationship (O-G) matches part of the claimed AS path (L, O, G). However, as AS_G's RRM does not contain any information of AS_L, AS_K checks AS_O 'RRM. After tracing the destinations in the table, AS_L finds that only AS_G and AS_N are directly connected to AS_O. It is inconsistent to what the AS path claimed in the BGP update (which claims AS_L is directly to AS_O). Therefore, AS_K identifies that this update is suspicious.

The purpose of this method is to check the reliability of a claimed AS path. However, if contradiction occurs, it is only able to identify that the update is suspicious, but not able to Figure out the correct AS path.

If a path to a given prefix is correct, the ASs in the network should have the consistent knowledge about that path. Therefore, by checking more RRR algorithm from other ASs, it is able to Figure out the correct AS path which is common to other ASs in the network.

4.1 Simulation setup

This section deals with the experimental performance evaluation of our algorithms through simulations. In order to test our protocol, the NS2 [20] is used. NS2 is a general-purpose simulation tool that provides discrete event simulation of user defined networks. We have used the ns-BGP extensions 2.0 for ns-2.33 [21] for simulating the BGP architecture. The experimental setup is similar to Figure-5. In our simulation topology 10 AS nodes are connected to each other. Each AS having separate network prefix addresses ranging from 10.0.0.1 to 10.0.9.1. The link bandwidth is 10Mb and link delay is 20ms. BGP agent is attached to each AS connected with neighbor AS as shown in the Figure. CBR traffic is used with packet size 100 bytes. We consider AS5, AS6, AS7, AS8, AS9 as attackers which performs prefix hijacking attack. The proposed Route Reliability Ranking (RRR) is compared against inter-domain packet filter (IDPF) [19] technique. The results are presented in the next section.

4.2 Results

The number of attackers performing Prefix-hijacking attack is varied from 1 to 5. The packet loss, packet delivery ratio, overhead and fraction of affected communications are measured for the two techniques. Figure-5 shows the Simulation Topology. Figure-6 show that packet loss increases when the attackers are increased. From the Figure, we can see that the RRR has 15% lesser packet loss when compared to normal IPDF. Figure-7 shows the overhead in terms of computation and communication for the two techniques represented in Mb/s. From the Figure, we can observe that, when the attackers increase, the overhead also increases and the overhead of RRR is 55% less than IPDF. Figure-8 shows the packet delivery ratio for the two techniques. As the packet loss increases when the attackers are increased, the delivery ratio decreases as depicted by the Figure. But RRR has 17% higher delivery ratio, when compared to IPDF. Figure-9 shows the fraction of affected communications when the attackers are increased. Similar to the other metrics, the affected communications for RRR is 19% less than IPDF.

5. CONCLUSIONS

In this paper, we have proposed route reliability ranking algorithm to defend against Prefix Hijacking Attack on border gateway protocol (BGP). The algorithm verifies the accuracy of AS path when a BGP update message is received, by looking up the path details from other autonomous systems in the network. In addition to route reliability ranking, we have also provided an incentive based route selection mechanism to identify the suspicious candidates and avoid routes propagated by them. It allocates a penalty value for AS which appears on an invalid route so that the route with the lowest penalty value for a destination is selected as the best route. By simulation results, we have shown that the proposed algorithm provides efficient defense against prefix hijacking attack on BGP.

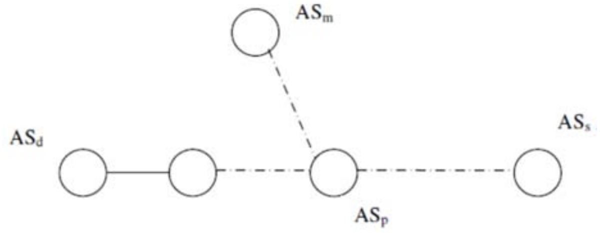

Figure-1. Prefix hijacking attack.

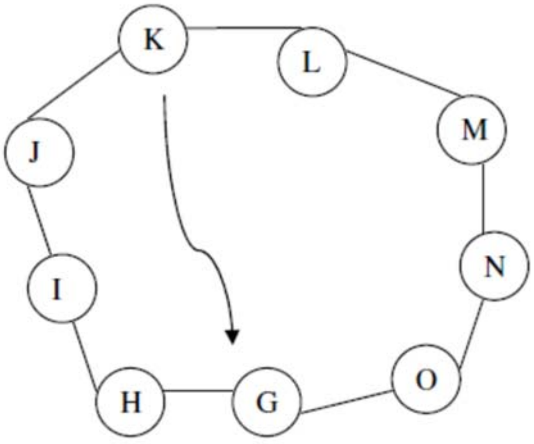

Figure-2. The BGP network.

$$\begin{bmatrix} K & 0 & K & 0 \\ L & 1 & K & 0 \\ J & 1 & K & 0 \\ I & 2 & J & 0 \\ M & 2 & L & 0 \\ H & 3 & I & 0 \\ N & 3 & M & 0 \\ G & 4 & H & 0 \\ O & 4 & N & 0 \\ G & 5 & O & 0 \end{bmatrix}$$

Figure-3. Route reliability matrix (RRM).

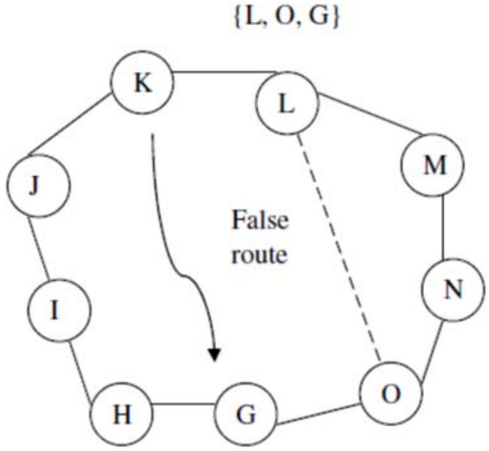

Figure-4. An example of an attack.

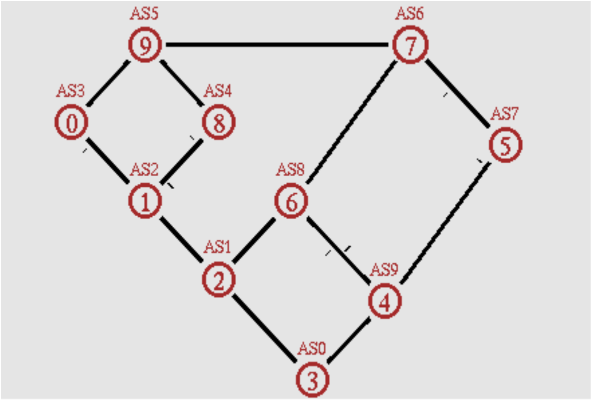

Figure-5. Simulation topology.

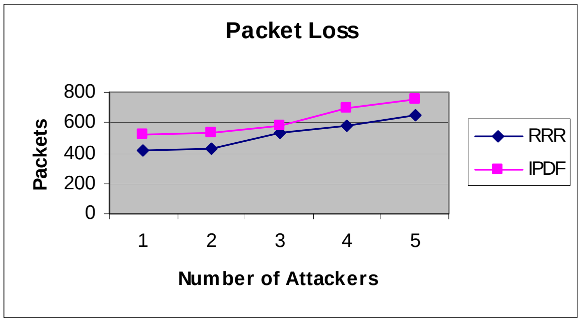

Figure-6. Attackers vs. packet loss.

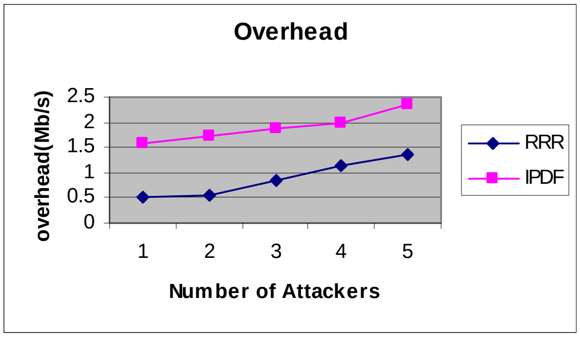

Figure-7. Attackers vs. overhead.

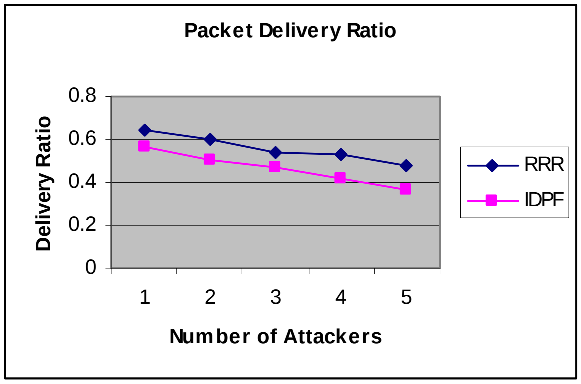

Figure-8. Attackers vs. delivery ratio.

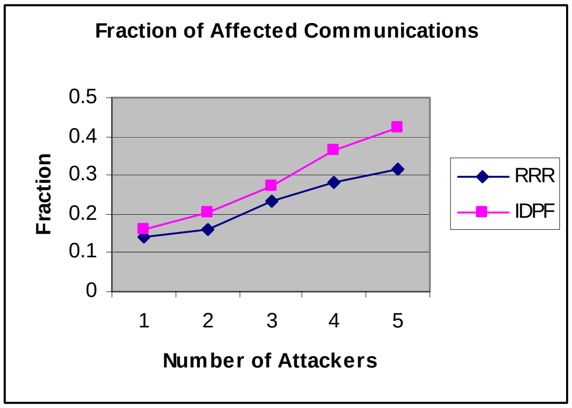

Figure-9. Attackers vs. fraction of affected communications.

REFERENCES

[1] K. Butler, T. Farley, P. McDaniel, and J. Rexford, "A survey of BGP security", Technical Report TD-5UGJ33, AT and T Labs, June 2004.

[2] Geoff Huston, Mattia Rossi, Grenville Armitage, “Securing BGP - A Literature Survey”, IEEE Communications Surveys and Tutorials, 2010.

[3] Kevin Butler, Toni R. Farle, Patrick McDaniel and Jennifer Rexford “A Survey of BGP Security Issues and Solutions” Proceedings of the IEEE Vol. 98, No. 1, January 2010.

[4] Junaid Israr, Mouhcine Guennoun and Hussein T.Moufiah “Mitigating IP Spoofing by Validating BGP Routes Updates” IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No. 5, May 2009.

[5] Fernando Sanchez, Zhenhai Duan. “Region-based BGP announcement filtering for improved BGP security”, ACM Symposium on Information, Computer and Communication Security (ASIACCS), pp 89-100, 2010.

[6] Hexing Wang, Cuirong Wang and Ge Yu,” BGP Security Configuration in ISP Networks”, PIERS, pp. 700-704, 2009.

[7] Bezawada Bruhadeshwar, Kishore Kothapalli, M. Poornima, M. Divya: “Routing Protocol Security Using Symmetric Key Based Techniques”, ARES 2009: 193-200.

[8] J. Qiu and L. Gao, “Hi-BGP: A lightweight hijack-proof inter-domain routing protocol,” Department of ECE, University of Massachusetts, Tech. Rep., 2006.

[9] Francesco Palmieri, “Inter-domain Routing Stability Dynamics during Infrastructure Stress Events: The

Internet Worm Menace", International Journal of Network Security, Vol.6, No.1, pp. 6-14, Jan. 2008.

[10] Stephen Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo, "Secure Border Gateway Protocol (S-BGP) - Real World Performance and Deployment Issues", IEEE Journal on Selected Areas in Communications, February 2000.

[11] Russ White," Securing BGP through Secure Origin BGP (soBGP)", Business Communications Review Article, May 1, 2003.

[12] Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel and Aviel Rubin, "Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing", in proc. of NDSS, San Diego, CA, USA, February 2003.

[13] T. Wan, E. Kranakis, and P. van Oorschot, "Pretty secure BGP (psBGP)," in Proc. of Network and Distributed System Security, 2005.

[14] Yih-Chun Hu, Adrian Perrig and Marvin Sirbu, "SPV: Secure Path Vector Routing for Securing BGP", ACM SIGCOMM Computer Communication Review, vol. 34, no. 4, pp. 179-192, October 2004.

[15] Meiyuan Zhao, Sean W. Smith, David M. Nicol, "Aggregated Path Authentication for Efficient BGP Security", 12th ACM Conference on Computer and Communications Security, November 2005.

[16] Martin Suchara, Lannis Avramopoulos, Jennifer Rexford, "Securing BGP Incrementally", Association of Computing Machinery, 2007.

[17] http://www.cs.uoregon.edu/Activities/poster_contest/2005/boothe-hijacking.pdf.

[18] Haowen Chan, Debabrata Dash, Adrian Perrig, Hui Zhang. "Modeling adoptability of secure BGP protocols", In Proceedings of SIGMETRICS/Performance'2006, pp. 389~390.

[19] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, "Constructing Inter-Domain Packet Filters to Control IP Spoong Based on BGP Updates", IEEE Info Com, 2006.

[20] Network Simulator, http://www.isi.edu/nsnam/ns.

[21] http://www.ensc.sfu.ca/~ljilja/cnl/projects/BGP-ns-2.33/ns-bgp.html.