Inter-Domain Routing with Shielded Infrastructure and Buzzer Technique

Bhavneet Kaur
Department of Computer Science and Engineering
Guru Nanak Dev University
Amritsar, India

Karanjeet Singh Kahlon
Department of Computer Science and Engineering
Guru Nanak Dev University
Amritsar, India

Sandeep Sharma
Department of Computer Science and Engineering
Guru Nanak Dev University
Amritsar, India

ABSTRACT
In the internet, BGP is de-facto inter-domain routing protocol. It is unprotected against number of attacks such as prefix hijacking and traffic interference. There have been many incidents of prefix hijacking on internet. To protect BGP against these kinds of attacks several mechanisms exist but they are not implemented fully because it requires cooperation among tens of thousands of independent ASes. This paper proposes two mechanisms which will show that safety can be achieved by implementing these mechanisms on small group of ASes.

General Terms
Prefix hijacking, Autonomous systems, BGP.

Keywords
BGP, Prefix-hijacking, S-BGP, so-BGP

1. INTRODUCTION
Routing system on today's internet is excessively sensitive to attacks where the attacker network advertise routes for address block which it does not even own. The effect of prefix hijacking [1-6] and bogus route advertisements are very grave because data which was bound for victim prefix is instead delivered to the adversary who can misuse the crucial information contained in data. To enhance the safety of BGP, ASes should be formed in small groups and perform following action:

1) ASes must coordinate with each other so that they can exchange information about different paths which will result in checking validity of the route to destination.

2) Ases should be dedicated in encouraging the non-cooperating ASs ASes so that they can also help in selection of valid routes.

The above actions can be achieved with the help of 2 mechanisms:

1. Shielded superimpose routing
2. Buzzer: alarm against hijacker

2. PREFIX HIJACKING
On the internet, networks are under the control of a single entity which is known as Autonomous system (ASes). Each AS has a unique numerical ID assigned to it by its regional Internet Registry. Each AS has one or more routers on edge of its network which routes traffic to all of its peer ASes. ASes exchange this information with each other with the help of Border Gateway Protocol (BGP). It allows AS to make announcements about IP address space it controls.

Prefix Hijacking occurs when a malicious or mis-configured AS announces to its peer that a block of IP address space belongs to them, when in fact, it does not. Due to this false announcement other AS start sending data to malicious AS, thinking it as a valid original AS. Malicious AS can then misuse this information which can result in illegitimate network use.

Prefix Hijacking can be classified into 3 types:

- Regular prefix hijacking: In this malicious AS tries to hijack an exactly same prefix of the valid AS. Malicious AS announces invalid route by pretending that it is either owner of prefix or it is one of the transit ASes.
- Sub-prefix hijacking: In this malicious AS tries to hijack more specific prefix which is being announced by original AS. For example 'A' hijacks a /24 subnet, which is a subset of /16 prefix announced by original AS 'B'.
- Super prefix hijacking: In this malicious AS tries to hijack less specific prefix. This kind of hijacking is rarely used because it becomes effectives only when the route to valid prefix is withdrawn.

For this study cryptographically secured registry of routing information is considered. Set of ASes that broadcast information in the registry is known as cooperating ASes and all other are non-cooperating ASes. For each cooperating AS, registry consists of list of prefixes the as is permitted to originate along with a list of AS's neighbours. Other than having their information broadcasted, cooperating AS utilize registry to certify the BGP announcements. A cooperating AS abandon a route to a registered prefix if the origin AS number is not correct.

3. SHIELDED SUPERIMPOSED ROUTING
This section illustrates how a small group of ASes can help in increasing the security of inter-domain communication between its members. The group member s formulate a shielded superimpose network which

provides backup superimposed route which participating AS can use when no valid BGP route is usable. The network formed is known as shielded infrastructure (SI) which is described in detail in section 3.1 and in section 3.2, 3.3 simulations are performed on SI.

3.1 Shielded Infrastructure (SI)

Shielded Infrastructure (SI) is a superimposed network in which group members of cooperating ASes are associated with each other with the help of mesh of .

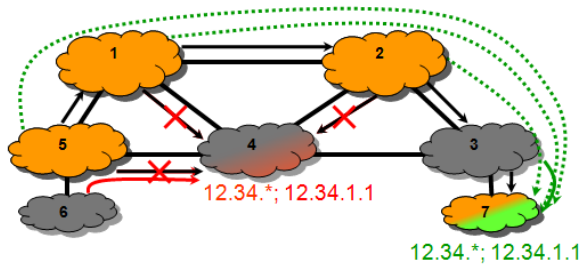

Fig 1: Shielded Infrastructure

Fig 1 shows the shielded infrastructure. Here node 1, 2, 5 and 7 are the cooperating ASes. Node 3 and node 6 are non-cooperating ASes. Node 4 is a hijacker. ASes 1, 2, 5 want to reach AS 7 which valid destination. But AS 4 makes a malicious announcement by advertising the prefix owned by AS 7. If there had been no SI then all traffic from AS 1, 2, and 5 would have been destined to AS 4. But due SI there is a superimposed network which can be used by AS 1, 2, 5 to send traffic to valid destination AS 7. The green dotted line in fig 1 represents the implicit channels formed by superimposed routing. Using these channels data can be transferred to valid destination.

The SI enhances stability in the following ways:

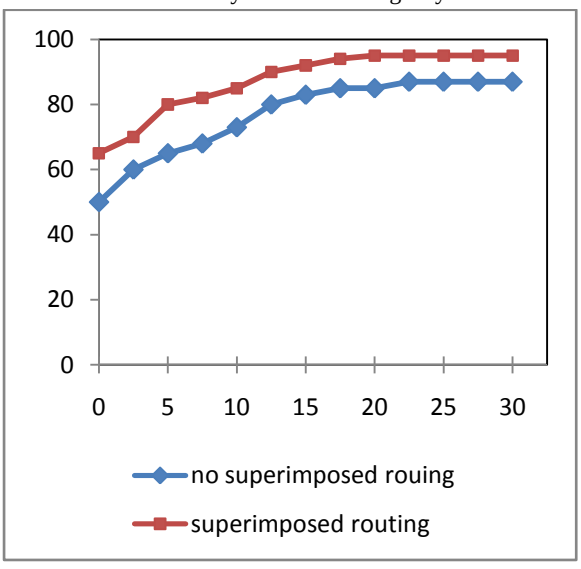

Fig 2: Percentage of ASes able to reach valid origin in contingent implementation

3.3 Support with the tier-1 Ases

In section 3.2, the cooperating ASes were contingently chosen from the set of all ASes. But in that case most of the ASes are remnant of bounded upstream connectivity which resulted in bounded path diversity which lead to cooperation of large group in order to gain significant security benefits.

To solve this problem, contingently chosen group of cooperating ASes are supported by tier-1 ASes which act as subordinates to help the group. Because subordinate ASes have rich connectivity, they give large exposure to rich path diversity which overcomes the above mentioned problem of section 3.2.In this experiment; it is shown that appointing one or more subordinate Ases in contingently chosen group can restrain the adversary's affect even if the overall size of the safeguard group which have subordinates is small.

Fig 3(a) shows the percentage of group members that are able to reach valid origin of a contingently chosen victim prefix. The subordinate ASes are prohibited from the set of possible origins and the adversary has also been chosen contingently. Suppose that adversary strikes both the cooperating AS's prefix and the channel endpoints of the superimposed network which is formed by the safeguard group. Both subordinate Ases and cooperating ASs are fitted with the filters which can detect bogus routes leading to adversary. Simulation is performed by considering 4 cases such that the group of subordinate ASes contains 0, 1, 3 and 5 members. Fig 3(a) shows that the percentage of cooperating ASs able to reach victim prefix is more than 95% if and only if subordinate ASes contains 3 or more members. Security is enhanced if the size of the group of subordinate ASes increases from 0 to

implicit channels which forms a superimposed network. SI is organized by the administrators of the cooperating Ases such that they have clarity in BGP routing.

The implicit channels are formed by associating members with IP channel that can enclose and enlarge the data packets. For each pair of group members A and B, two channels are created: one from A to B and other from B to A

- An SI node can change a virtual link from one underlying path to another, if it detects that there is some problem on the original path and it is not available.
- If all underlying paths are not available then SI node can move traffic through intervening SI node via the superimpose network.

3.2 Contingent implementation

Simulations are performed to check how competent SI is in preventing routing attacks. While performing simulation, it is supposed that participating AS are fitted with prefect filters which can detect bogus routes leading to the adversary. Simulation use BSIM [8] simulator. Data is taken from CAIDA [9] and route views [10].

The graph in fig2 shows the percentage of group members that are able to reach the authentic or valid origin AS, safeguard group and the adversarial AS are selected contingently from the set of all ASes. The size of safeguard group extends up to 30 members. Now examine a case 1st in which the group members are not able to choose the BGP path of a implicit channels i.e group members are superimposed owners that do not have clarity into BGP and in case 2nd group members have authority own BGP. Case 2 performs lot better than case 1st.

5 members. In fig 3(b), it is shown that if adversarial group consists of 5 members instead of 1 as in previous experiment. Fig 3(b) shows that large adversarial groups have more impact on the safeguard groups that do not support subordinate ASes. But effect of large adversarial group decreases us the number of subordinate Ases is increased. For example: in a safeguard group of 10 members that appoint 5 subordinate ASes, 90 % of the members are able to reach the valid origin of the victim prefix.

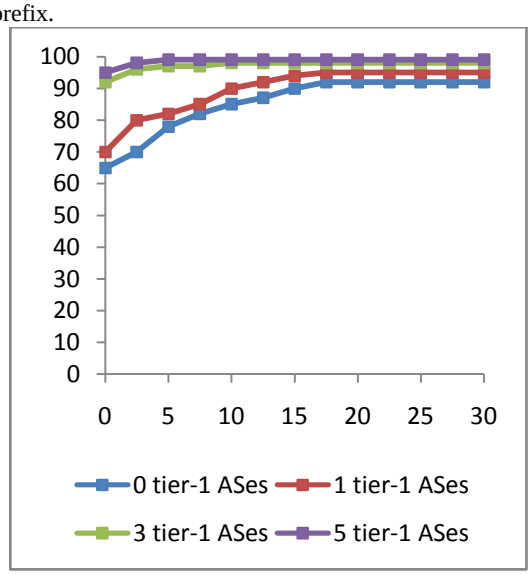

Fig 3(a): 1 Adversarial AS

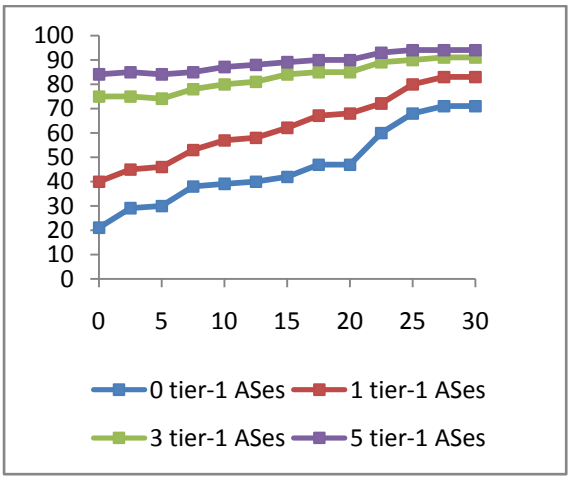

Fig 3(b): 5 Adversarial ASes

Fig 3: Percentage of group members that have superimposed route to victim prefix.

4. BUZZER: ALARM AGAINST HIJACKER

This section proposes another mechanism 'Buzzer' which the safeguard group can implement to safeguard traffic coming from non participating ASes that is destined to the participating ASes. Buzzer enhances the benefits of SI to non participating ASes which are not aware of the protection techniques that cooperating ASs use. To gain full benefits of SI, AS should be cooperating AS but SI targets the safety of non cooperating ASs and is destined for implementation during the brief period in which SI is building to include a target group of members.

4.1 Seize control of hijacker

Buzzer is a destination based technique that provides safety to non cooperating AS which are not aware of the various security mechanisms employed on system. Buzzer persuades non cooperating ASs to select routes which lead to nearby cooperating ASs instead of routes leading to adversarial ASes.

Buzzer challenges the adversary and attracts traffic from the non cooperating AS using the adversary own technique. Buzzer seizes control of hijacker by having the safeguard group of ASes at same time originating in BGP a cooperating AS's prefix. So even if adversary strikes the prefix receiving protection of the group, the non cooperating ASs will prefix the routes leading to the group members over the adversary's routes. Buzzer persuades non cooperating ASs to select routes leading to cooperating ASs and then it uses SI to transfer traffic to its destination.

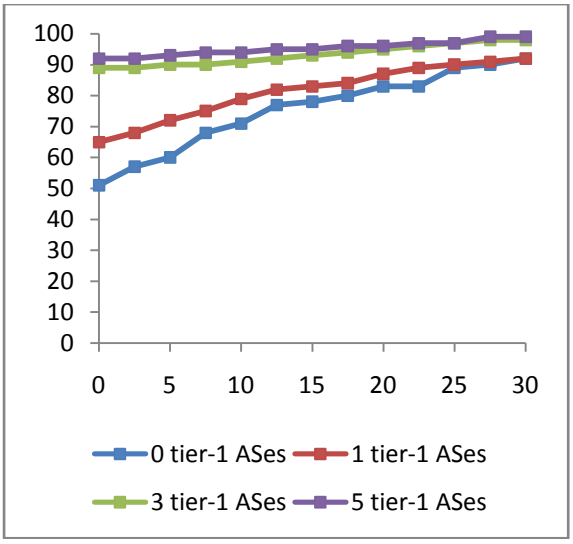

Fig 4(a): 1 Adversarial AS

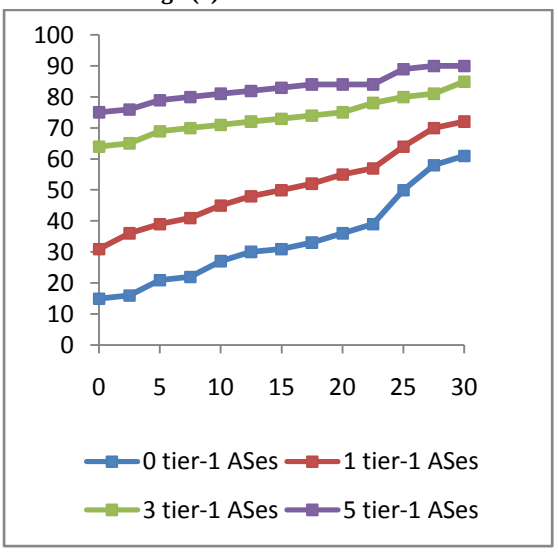

Fig 4(b): 5 Adversarial AS

Fig 4: Percentage of group members that have superimposed route to victim prefix

Fig 4 (a) shows the percentage of all ASes in the internet that are able to reach a cooperating AS's prefix. When cooperating AS and adversarial AS are chosen contingently. Suppose that the adversary strikes both the cooperating AS's prefix and the channel endpoints of the superimposed network created by safeguard group. Consider four cases in which 0, 1, 3 and 5 tier-1 ASes are appointed in safeguard group. If the group has 10 or more members and 3 or more tier-1 subordinates then more than 95% of the ASes in the internet are able to reach the victim despite the strike.

Fig 4(b) shows larger attack strike by adversarial group which consists of 5 members. As in the case of SI, large adversarial groups have more effect on those safeguard groups which do not appoint subordinate ASes and the effect of large adversarial group decreases as the number of subordinate ASes increases.

5. CONCLUSION

This study proposed and evaluated 2 mechanisms SSR, Buzzer which helps in securing interdomain routing. Both mechanisms achieve the following goals:

- They allow the coordination of the ASes so that they can have more exposure to path diversity.
- Helps non participating ASes to select valid routes
- As a small group provides more security, many other ASes tries to join the secure group.

Implementation of secure routing within a group, along with group's increasing size, gives a viable incremental implementation path for traditional cryptographic solutions.

6. REFERENCES

[1] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP misconfiguration," in *Proc. ACM SIGCOMM*, Aug. 2002.

[2] V. J. Bono, "7007 explanation and apology," Apr. 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html.

[3] P. Boothe, J. Hiebert, and R. Bush, \How prevalent is prefix hijacking on the Internet?," Feb. 2006.

[4] http://www.nanog.org/mtg-0602/boothe.html.

[5] R. Blog, \Con-Ed steals the 'net." http://www.renesys.com/blog/2006/01/conedstealsthenet.shtml.

[6] http://www.ietf.org/html.charters/rpsec-charter.html.

[7] http://www.nanog.org/

[8] J. Karlin, S. Forrest, and J. Rexford, *PGBGP simulator*. http://www.cs.unm.edu/~karlinjf/pgbgp/.

[9] http://as-rank.caida.org/data/.

[10] http://www.routeviews.org/.

[11] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, \PHAS: A pre¯x hijack alert system," in *Proc. USENIX Security Symposium*, Aug. 2006.