Autonomous System Announce Forged Route in Secure BGP Proposals and Countermeasures

Divya. K
Department Of Computer Science And Engineering
M.A.M College Of Engineering
India.

Abinaya. T
Department Of Computer Science And Engineering
M.A.M College Of Engineering Siruganur, Trichy,
Siruganar, Trichy, India.

***Abstract*— BGP is used to allocate routing information between the autonomous systems; it is highly possible to have a malicious attack due to lack of secure, it can cause without delivery of packet or delay delivery of the packet to reach destination. They do not have a mechanism to verify route is genuine. In this paper, to test security of the path to launch a routing table poisoning attack it affects whole of the internet. Toward a new securing scheme has been proposed to identifying the routing table poisoning. In particular pure data plane technique are proposed to detect this attack. In pure data plane, it verifies the current BGP table with the original table. If the path details are changed, it sends alert to the neighbor node and change the data path in current table. Experimental results show that routing table poisoning attack affects the internet. Pure data plane can achieve full detection of this routing attack.**

***Keywords*— Border gateway protocol; routing table poisoning; pure data plane.**

I. INTRODUCTION

The internet connects thousands of autonomous system operated by different institutions, such as internet service providers (ISPs) companies, and universities. Routing surrounded by an AS is controlled by intradomain protocols such as IS-IS and RIP. ASes be integrated via dedicated link and exchange reachability information using the Border Gateway Protocol (BGP). However, up to date studies exposed that a collection of ASes might have differing BGP policies that guide to route divergence [4, 5]. Route divergence can result in route oscillation which can significantly corrupt end-to-end performance of the internet. Routing information is exchanged between ASes in BGP, but Border Gateway protocol has proven to be highly helpless to a variety of attacks. Each BGP speakers controls an entire routing table and sends its best route for each prefix to each neighbor speaker. Correct operation of BGP depends upon the reliability, accuracy, and timelines of routing information it distributes as well as each BGP speaker's processing, storing and allocation of this information.

The internet relies on the BGP to communicate routing information. However, if BGP provides incorrect routing information, packets may never reach the proposed destination. BGP views the internet as a collection of interconnected ASes, AS is a segment of the network, each AS connects to other ASes. Autonomous system BGP provides information for controlling the stream of packets between ASes, the protocol plays a critical role in internet, reliability and security. However real world incidents reveal [2, 7] the being of compromised routers in internet service provider and enterprise networks that current network is unexpectedly exposed to data plane attacks: a dishonest transit ISP can easily drop, delay, inject or modify packets on the forwarding path to increase Denial-of-service, man-in-the-middle attacks etc. Unluckily, the openly available BGP paths do not cover the entire Internet due to issues such as visibility constraints. However, all existing trace route-based projects are restricted by their limited number of VPs.

BGP has a number of recognized vulnerabilities, thus the BGP does not supply any way of detecting the source of worst data. Today's a routing system is still for the most part unguarded, we have quite a lot of incidents [7, 22] of disrupted network connectivity for many prefixes. To construct an entire internet, then the routing protocol connecting with different IP network or autonomous systems. Normally in BGP, all AS announces its routing information with their different prefixes, but its neighboring ASes cannot validate this routing information. Clearly, the hope model that allows forged route announcements then the BGP which has a security weakness. This forged route which can generate by malicious attack which can cause network connectivity issues to improve the security of BGP is to eliminate the false announcements.

In this paper, to propose Routing Table Poisoning (RTP) which aims to launch routing attacks even with fully employment of these "proven secure" BGP proposals. In Routing Table Poisoning attack which announces forged routing node that means that this attack that tunnel the node then reaching destination is failed or dropped. For example let us assume that A, B, C, D, E, F are the nodes connecting between different autonomous systems A be the source and F be the destination. Routing Table poisoning which aims to invalidate the existing BGP proposals thus it concealing the intermediate node to reach its destination. Existing only

tunneling intermediate path that only the path is tunneled, here we are tunneling the node to test the security of the internet. Existing anomaly detection schemes [16], [22], [30], [40], [41] also fail to identify this RTP.

To detecting this Routing Table Poisoning attack we propose Pure Data Plane which detecting against routing table poisoning. In this paper challenges to detecting RTP, first to identify what are the intermediate nodes and how the intermediate nodes are tunneled. In Pure Data Plane after identifying if attack is formed in this network it compare with an original routing table to check original routing updates. In pure data plane**,** it verifies the current BGP table with the original table. If the path details are changed, it sends alert to the neighbor node and change the data path in current table. In addition, for which identify the attack using pure data plane to detect the Routing Table poisoning attack. By using Pure Data Plane successfully identifying intermediate nodes and dropping or delaying packets successfully detecting by this Pure Data Plane it can accurately detect RTP attacks with 100 detection ratio still below these complicated attacks. Our contributions are summarized as follows:

To derive a new type of attack called Routing Table Poisoning where the autonomous systems collude to generate a forged routing path yet below full deployment of existing BGP proposals. To present a Pure Data Plane to detect against RTP it accurately identifying this attack, it compares current BGP update with original table.

II. RELATED WORKS

In existing work there are many papers that focus on the improvement of to avoid prefix hijacking and interception by many BGP proposals. There is also papers deal with to achieve high authenticity of internet routing with simple and light weight attestation mechanism. By using this protocol it verifies routing updates which avoid invalid paths.
Several techniques have been proposed.

In [8] Paul Francis et al. present a study of prefix hijacking and interception in the internet there are the many happenings of prefix hijacking. Prefix hijacking of autonomous system that can cause blackhole the hijacked interchange. Here interception methodology is presented and implemented and there is a detailed study to detect the interception. Here tier-1AS focus on hijacking and other tier-1ASes decide which traffic can be hijacked and intercept by tier-1 AS in the internet. In control plane normally consists of routing table that thus routing experience not captured in the next-hop calculations.

Geoffrey good ell et al. proposes a new protocol that combine to effort with BGP, which ASes will use to help and identify by mistake introduced fake routing information. Inter domain routing protocol can be used in this paper, by using this technique to replace and spread reach ability in sequence between the organizations. IRV are used to validate the BGP data and obtain extra routing information applicable to an AS then the main goal of IRV is used to validate and obtain both the static and dynamic routing information. IRV that maintains best interdomain routing information in Autonomous system by using single IRV cost is high it does not have an load balancing IRV in their own network does not yield greatly then the single IRV running by its own is not very useful in the Autonomous system.

Stephen kent et al. describes a secure, scalable for an authorization and authentication that shows most of the problems related with BGP. Mainly this paper discusses and addresses vulnerabilities and thus provides comparison of this architecture to other approaches. S-BGP is uses in this paper uses two PKI's that based on certificates to validate the identities and agreement of BGP also the owners of ASes. S-BGP using certificate and attestation that sending route information without modification in a secure manner from the source to destination it does not offers authentication and integrity on point to point origin.

Vijay Ramachandran et al. focus on the security goal here interdomain routing game technique are used in which the nodes of the AS graph are planned players. In each round, recent path announced from its neighbors is the graph processor in one node and this purpose that depends only on the straightforward data plane paths from other nodes. Interdomain routing game that is difficult to achieve truthfulness without resorting expensive data plane protocols.

Xinwen zhan et al. proposes TBGP abbreviated as trusted BGP which aims at high authenticity of routing also with a straightforward and lightweight attestation mechanism. Here interfaces are provided by router in the attestation check to verify it create relationship among all routers on the routing path, identity based signature algorithm identity-based cryptography which is an another to public-key cryptography, that uses user identity information as the public-key then the private-key is generated by private-key generator according to the user individuality information. It does not involve further infrastructure to manage and certificates this authorities are only generate by private-key with ASes there are two way attacks they are prefix hijacks and invalid path attacks these are the problems in this paper.

Dan Massey et al. present a new prefix hijack alert system (PHAS). PHAS is a real time announcement system that is if any changes in the BGP basis it send alert to the prefix owners. PHAS that are quickly and easily detect prefix hijacking in the prefix owners then it is in lightweight and easy to implement. Instantaneous origin changes each prefix had origin set, if any changes in the origin set it sends an announcement then the windowed origin changes introduce windowed origin set compare to instantaneous origin changes time window delay the notification. Mainly focus on this approaches is in identifying prefix hijacking, normally prefix does not deliver data to the actual prefix it can cause serious problem in the internet then the reaching destination is incorrect finally an incorrect routing information also provides in the internet.

Patrick tague et al. proposes an efficient fault localization protocol called Short MAC which installs authentication and achieves detection delay. In the previous work prefix hijacking

and interception are the major problems in the internet that sometimes cause rest of an internet. To overcome these challenges by using Pure Data Plane technique it can reach the destination accurate and maintain an original path.

III. PROPOSED WORK

A. *Basic Terminologies*

1) BGP: In the internet BGP is used to transfer the information among autonomous systems it is a path which maintains path to different hosts and network.

2) Routing table: Different sources are learned by BGP prefix it has one or more paths BGP track which is the best path changes of BGP prefixes.

3) Pure Data Plane: Comparing operation is done in this plane it compare current BGP table with original BGP table to check the accurate destination.

4) Encoding: If the message encoding that has full of production message it can send the message with images, signs and video.

5) Decoding: Decoding is the process of near reading and change of coded information into widespread form then the receiving message is in effective communication manner.

B. *Architecture*

The proposed work to avoid blackhole in the internet by using the technique NAG (Neighbor Autonomous Graph) construction and Direct sequence Spread Spectrum (DSSS). Here Border Gateway Protocol are used that can send the information from one autonomous system to other autonomous system. This process is done to finding intermediate nodes and reaches the destination accurate; first we are using NAG construction in this technique identifying their original intermediate path. Construct NAG tree then identifying total number of autonomous systems present in this topology by analyzing its neighbor ASes. After that NAG tree send the data transaction by sending the data through NAG it can be monitoring packets information service are provider, then it identifying how the attacker present in this network and detect the traffic path monitoring is nothing but analyzing number of nodes. Other technique are used in this paper is Direct Sequence Spread Spectrum in the TIGER attack network first identifying intermediate by identify packet delay or delay in time. By identifying tunneled intermediate path then communicate with intermediate nodes to alert from the attacker nodes message is sent by watermarking technique. By using watermarking technique it sends encode mark in certain time interval and it can only decoded in receiving node, if the encoding message has full of production message sent from one to another in decoding process the receiving message is in effective communication manner. After encoding and decoding operation is done, communicate with intermediate nodes by tracing the data path, if the data packets dropped or difference in time travelling path then the path is hijacked and set low priority for that hijacked path in autonomous system network. Set low priority for hijacked path after that to detect the TIGER attack and send the message in their original routing path and check the original path.

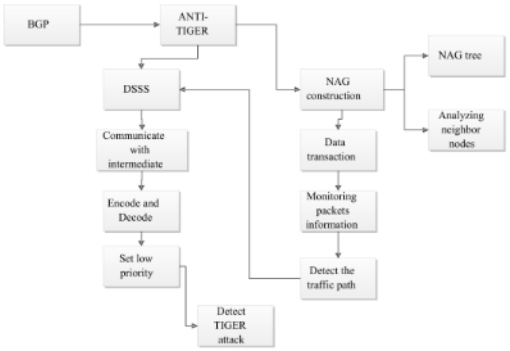

Fig. 1. System Architecture

Encrypts and decrypts operation is successful in this Direct sequence spread spectrum, this technique sends encode message to intermediate path in sequence order i.e. DSSS encrypts with an system and only decrypted by an receiving node to avoid blackholes and interceptions be because TIGER attack produce fake link by tunneling. After detecting TIGER attack by assigning low preference value to forged routing path in routing table, then the routing path updates its original data. Finally all the process is done to increase the security of the BGP proposals ANTI-TIGER is lightweight accurately identified TIGER attack.

C. *Detecting Tiger Attack: ANTI-TIGER*

1) *Tiger Attack Network*

The Network is formed with original routing path details. The AS can be registered and certificate is generated. When an AS send a message to another AS, it verifies with the certificate and receive the messages from AS. When the certificate match with the received AS the message cannot be received, hence it can send the data securely. Here TIGER attack network specific destination are tunneled by source ASes and then successfully hijacked by colluding ASes. Main goal of TIGER attack network is to create fake path that means it cannot reach the destination and store in the original BGP routing table.

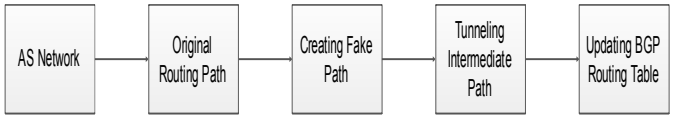

Fig. 2. TIGER Attack Network

When the path is tunneled in the network it creating fake path by tunneling intermediate path and the TIGER node assigns the path and update in BGP table. In BGP routing table the fake path is updated, if all modification update in routing table then the routing table that store in database for to refer their status. ANTI-TIGER use Direct Sequence Spread Spectrum to avoid Tiger attack network by constructing NAG and to transport encoding and decoding.

2) NAG Construction

In TIGER attack here using Neighbor Autonomous Graph (NAG) it constructs neighbor node for each AS with different prefixes, after that it can identify total number Autonomous systems in the network. NAG which comprise all ASes in the network colluding ASes may want to dropping routing updates or delaying routing updates to prevent the intermediate nodes by analyzing neighbor AS through NAG it know the tunneled path

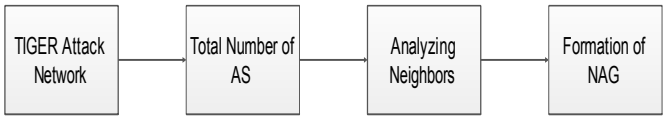

Fig. 3. NAG Construction

By using this technique intermediate ASes learn the original details of the source by learning routing updates from other Autonomous systems hence this is the way intermediate to identify the source ASes in the network.

3) Suspicious Traffic Detection

After NAG construction, the data are sending through the NAG by tracking the IP address with received routing updates, data transaction is mainly to identify the traffic between Autonomous systems. By send the data through NAG, it can monitor the packet information; it can monitor how the traffic is occurred and how they perform in the network. After monitoring is done through data transaction hence traffic path can be detected.

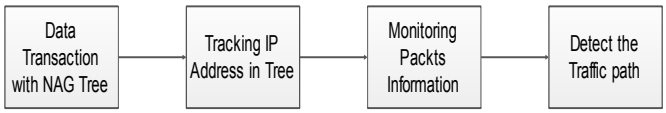

Fig. 4. Suspicious Traffic Detection

Once mistrustful traffic is known hence possible colluding Ases and victim Ases can be easily identified then TIGER can be detected in round of challenges and thus operation between intermediate and victim ASes and intermediate may need to communicate with all possible victim Ases to detect TIGER attack.

4) Tiger Detection Based On Watermarking

In TIGER attack network, it can identify the tunneled intermediate path by identify the packet delay or delay in time. After identify the tunnel intermediate path, communicate with them by water marking technique, through watermark the victim Ases send intimation to intermediate node if you are attacked by attacker it sends alert message to intermediate path. In water marking technique, it sends an encoded mark in certain time interval and it can be only decoded in receiving node.

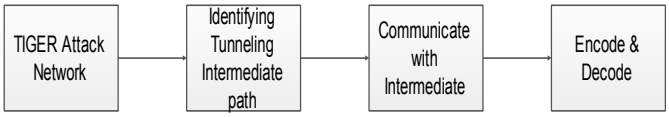

Fig. 5. Direct Sequence Spread Spectrum

By using watermarking technique intermediate finds their traffic is really tunneled, this watermarking uses three-way detection protocol i.e. intermediate, acknowledgement, and synchronization so that the intermediate Ases and victim Ases work together on accurate and strong TIGER detection.

5) Tiger Defense

Communicate with the intermediate node by tracing the data path, ANTI-TIGER service provides a routing update to the BGP router within the same AS. If data packets are dropped or difference in time travelling in path, then the path is hijacked. Set low priority for that hijacked path in Autonomous System network.

Fig. 6. Tiger Defense

TIGER detection is timely defends against the forged routing paths announced by AS, and triggers routing path reselection, e.g., by assigning low preference values to the forged routing path in its routing table. If the intermediate nodes tunneled by the tiger attack So that the anti-tiger communicate with intermediate nodes to alert that the path is tunneled then trace the data path there has been difference in time to receive the information, after that tiger attack is detected by constructing the NAG to analyze the neighbor number nodes are occurred and the hijacking path is to set low priority after setting priority there is no transfer of information through this path.

IV. CONCLUSION

In BGP security proposals vulnerable to have routing attacks, TIGER attack which is the main problem in the internet ASes this attack can be easily hijack in the network so this attack can affect the BGP security mechanisms several BGP scheme has been proposed also fail to detect this attack. To detect and defend against TIGER attack to proposed ANTI-TIGER which accurately identify the TIGER which identify total number of autonomous system and also find the intermediate nodes by using Direct Sequence Spread Spectrum to transport watermark technique

REFERENCES

[1] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P.McDaniel, and A. Rubin,(2003) "Working around BGP: An incremental approach to improving security and accuracy of interdomain routing," in Proc. ISOC Netw. Distrib. Syst. Security Symp, pp. 75–85.

[2] H. Ballani, P. Francis, and X. Zhang,(2007) "A study of prefix hijacking and interception in the internet," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun, pp. 265–276.
[3] K. Chen, D. R. Choffnes, R. Potharaju, Y. Chen, F. E. Bustamante, D. Pei, and Y. Zhao,(2009) "Where the sidewalk ends: Extending the internet as graph using trace routes from P2P users," in Proc. 5th Int. Conf. Emerging Netw. Experiments Technol., pp. 217–228.
[4] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang(2006) " PHAS: A prefix hijack alert system," in Proc. USENIX Secur. Symp, p. 12.
[5] Q. Li, M. Xu, J. Wu, X. Zhang, P. P. C. Lee, and K. Xu(2012) "Enhancing the trust of internet routing with lightweight route attestation," IEEE Trans. Inf. and Security, vol. 7, no. 2, pp. 691–703.
[6] S. Goldberg, S. Halevi, A. D. Jaggard, V. Ramachandran, and R. N. 7. Wright, (2008) "Rationality and traffic attraction: Incentives for honest path announcements in BGP," in Proc. ACM Conf. Appl., Technol., Archit., Protocols Comput. Commun, pp. 267–278.
[7] S. Kent, C. Lynn, and K. Seo,(2000) "Secure border gateway protocol," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 582–592.
[8] X. Zhang, Z. Zhou, H.-C. Hsiao, A. Perrig, and P. Tague, (2012) "Shortmac: Efficient data plane fault localization," in Proc. Netw. Distrib. Syst. Security Symp, p.1.