A NOVEL APPROACH FOR SECURE ROUTING THROUGH BGP USING SYMMETRIC KEY

Divan Raimagia, Shraddha Singh and Sameena Zafar

Department of Electronics and Communication Engineering, PIES College, Ratibad, Bhopal, India

Divan_ec@yahoo.com, shraddhasingh5@gmail.com, sameena_zafar82@yahoo.com.

ABSTRACT

The Border Gateway Protocol (BGP) is the path vector routing protocol that connects different autonomous systems.. These ASes have unique integer numbers which assign by IANA organization. The traditional BGP protocol is not sufficient to provide security and authentication for AS path and verification of AS number ownership as well as network IP prefix. The BGP remains vulnerable to various types of misconfiguration by users and attacks. Many secure BGP algorithms have been proposed but complexity of algorithm and attack on that models still remain open problem. In this paper, we propose an efficient model for SBGP; initially establish trust relationship between BGP peers. In this process BGP use TCP protocol for reliable communication. The BGP routers will attempt to create secure BGP session by exchanging BGP Open messages. During this Open messages master BGP router generate private key with help of cyclic shifting of ASCII of password called cyclic shift algorithm. Then hash of this private key send towards neighbour. Instead of key exchange, we use hashing algorithm, we generate hash of only key through SHA-1. This hash code for private key sent with Open messages during session establishment. When this Open messages receive by neighbor BGP routers, first it generate key using same password with same algorithm & generate hash code for same and then compare both hash code. If it matches then establish secure session with master BGP router & accept the Autonomous system number which is sent by master router during Open Messages. In this manner both BGP speakers make trust relationship between each other & then exchange route UPDATE within secure channel. If hash code at receiver end does not match then simply receiving BGP router discard Open messages and does not make connection with unauthorized AS number. If malicious router wants to inject false route or false ip prefix then it does not create secure session by lack of secure private key. So malicious router does not participate in above BGP routing process.

KEYWORDS

BGP Protocol, Symmetric Key, SHA-1, hashing.

1. INTRODUCTION

This Routing involves two main activities, first find the shortest path and second transport of packets through internetwork. One of the protocols called Border Gateway Protocol (BGP) performs these both activities. BGP works in interdomain routing in TCP/IP network [1]. BGP is exterior routing protocol which means that it performs routing between various autonomous systems. BGP is also called path vector routing protocol. Routers who run BGP protocol are called BGP speakers. The BGP is only deployed exterior routing protocol connecting different IP networks and ASes to make the whole internet. Every autonomous systems announces its route update or route information with different IP prefix. Neighboring ASes update own routing table

DOI : 10.5121/ijnsa.2013.5513

with new arrival IP prefix as well as AS path without verify autonomous system ownership as well as IP prefix ownership. So in ordinary BGP routing protocol has several weaknesses. There is no mechanism to verify ASes ownership and IP prefix ownership. In simple BGP protocol there is no rule for check integrity and authentication of both IP prefix and autonomous system number. One serious problem is that misconfiguration of BGP router and false BGP route with same ip prefix propagates across the Internet. Malicious BGP speaker may poison the routing tables of many other well-behaved BGP speakers by injecting wrong route or wrong ASes numbers in internet. This has the potential to down the internet infrastructure as traffic can easily be redirected to unintended networks and cause slow down network. These false UPDATE generated by configuration errors or malicious attacks, can cause WAN or Internet connectivity problems or slow down the network.

In order to remove false update and improve the security of BGP, numbers of proposals have been submitted towards these operations. But only SBGP is effective contribution to date and implemented by Cisco in Cisco routers. In this paper, we focus on reduce the number of signature generation as well as verification. Existing approach use cryptography mechanism and also use distributed and centralized key distribution mechanism. But using above approaches require a large amount of processing and memory power, which result in a significant degradation of the performance of routers and internet that create a high volume of BGP traffic. So in our approach we simply use symmetric key only for secure session establishment between BGP speakers, not for encrypt whole route UPDATE. We does not use any usual unsecure approach for symmetric key generation, instead of that we use cyclic shifting method for key generation. In this method first both BGP speakers agree on large prime numbers and using complex operation on prime numbers generate symmetric private key. So in our approach we use two algorithms: first cyclic shifting for key generation and SHA-1 (secure hash algorithm) for hash generation of key.

2. Background & Overview

The Internet is a group of interconnected autonomous systems. Each AS manage by single administrative domain and require individual unique AS number from IANA. Main operation of the internet to perform routing within different autonomous systems. This routing operation between different ASes performs by BGP exterior routing protocol which is widely implemented in internet. In internet each AS has one or more than one BGP speakers which perform routing operation. There are two types of BGP speakers, iBGP and eBGP peers. In iBGP peer, each iBGP speaker must link with other iBGP speaker within AS. Whereas in eBGP peer, each eBGP speaker must link with other eBGP speaker in different AS. Each AS has unique AS number as well as IP prefix. Both AS number and IP prefix provide by IANA organization.

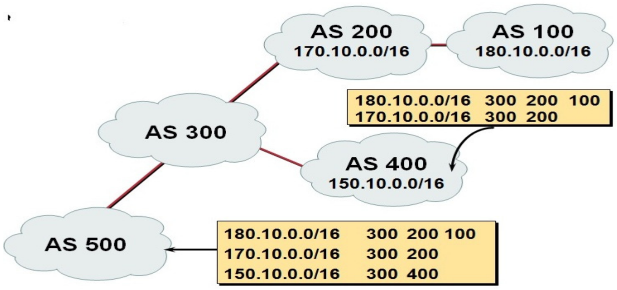

Fig 1: Sequence of ASes thorough which route has traversed and working of BGP.

In Fig 1, show that five autonomous systems linked together like AS 100, AS 200, AS 300, AS 400, and AS 500. AS 100 have 180.10.0.0 /16 ipprefix. Similarly AS 200 has 170.10.0.0 /16 ipprefix and AS 400 has 150.10.0.0 /16 ipprefix. In BGP routing each AS pass route update and AS path to neighbor AS and neighbor AS update his route table with add its own AS number and pass this AS path to neighbor AS. For example in fig 1, AS 100 advertises its ipprefix 180.10.0.0 /16 with AS number 100 to neighbor AS 200. When AS 200 receive this information form AS 100, its update own routing table as well as add own AS number with 180.10.0.0 /16 ipprefix and pass to AS 300 and so on. So for AS 400 and AS 500 receive route update of 180.10.0.0 /16 from AS 300 with AS path 300 200 100.

So in today internet connects several ASes and several IP prefixes but simple BGP provide weak internet structure and unreliable connection between BGP speakers. There is no mechanism in BGP to verify AS and IP prefix ownership.

BGP attacks with IP prefix hijacking

Prefix hijacking is a serious BGO security therat by which attackers steal IP addresses belonging to other netwoks [13]. Malicious AS injects false route into global routing table by advertising another network's IP prefix. This stolen IP prefix can be used for unauthorized or malicious activities like slow down internet, spread virus, denial of service (DoS attack), and spamming. In prefix hijacking the attacker announces exactly same IP prefix already announce by victim. Other AS will select one such route to adopt and forward all packets towards attackers' router as well as attacker router forward unwanted packets towards other AS with victim IP prefix and slow down other AS BGP router performance.

In Fig 2, four ASes are linked together like AS 100, AS 300, AS 150, AS 200, and AS 160. Now AS 100 is actual owner of IP prefix of 9.0.0.0 /8 with router 0. Neighbor of AS 100 are AS 300 and AS 200 with different IP prefixes. AS path for 9.0.0.0 /8 for AS 200 is <200 100>, similarly for AS 150 is <150 200 100> so when pc 2 (source) transmit packet with destination IP 9.0.0.2 /8 then it traverse from AS 150 200 100 and reach to actual destination. But AS 160 is attacker and advertises its own IP prefix as 9.0.0.0 /8 to neighbor AS 150. But actual owner of 9.0.0.0 /8 is AS 100. Now AS 150 update its routing table for IP prefix 9.0.0.0 /8 with new AS path <150 160>. So now when pc 2 (source) try to communicate with pc 0 (9.0.0.2 /8) then data traverse from AS 150 160 and towards from router 4 which is malicious router and finally reach at pc 1 not to pc 0. This type of attack is call IP hijack attack.

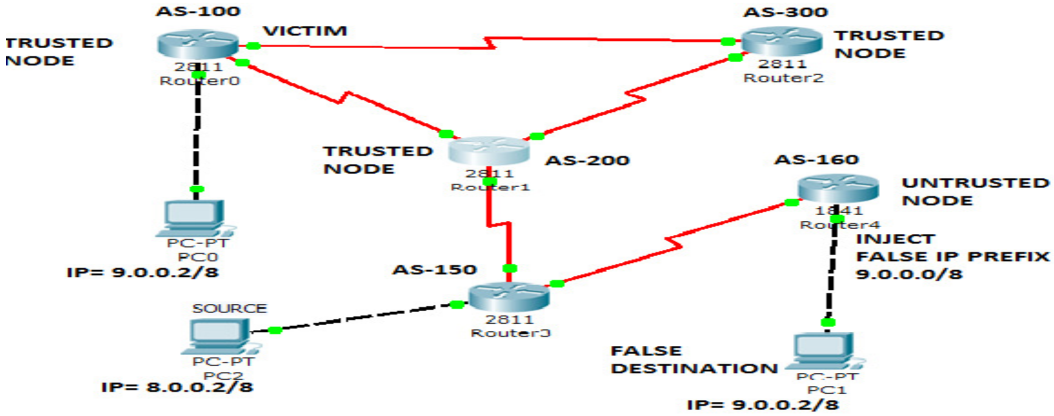

Fig 2: IP hijack attack with malicious router announce false or stolen IP prefix.

The following formatting rules must be followed strictly. This (.doc) document may be used as a template for papers prepared using Microsoft Word. Papers not conforming to these requirements may not be published in the conference proceedings.

2.1. BGP attack with false AS advertise

Another attack called false AS advertise, in this type of attack attacker router establish session with neighbor routers using TCP protocol. So during OPEN message each AS share its own AS number with neighbor AS and through handshaking establish session between neighbors AS. But in this process malicious AS announce other stolen AS number. Sometimes misconfiguration BGP router injects false AS number.

In fig 3, Router 4 establishes TCP connection with neighbor AS 150 through handshaking with OPEN message. During session establishment Router 4 send own AS number as 100 with OPEN message. But actual owner of AS 100 is router 0. Now neighbor AS 150 find shortest path for IP prefix 9.0.0.0 /8 and when OPEN message receive from router 4, AS 150 assume that router 4 is owner of AS 100 because its direct neighbor of AS 100. So AS 150 update its routing table with false AS Path and all packets for 9.0.0.0 /8 travel through AS <150 100> directly instead of AS path <150 200 100>. Therefore malicious router 4 spread unwanted packet towards AS 150 through internet and slow down performance of BGP router as well as internet called DoS attack.

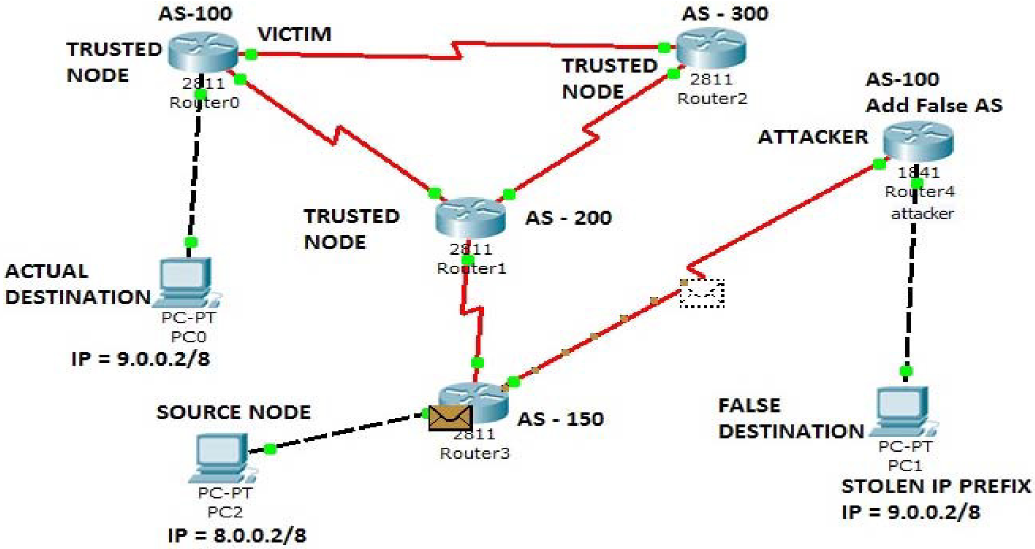

Fig 3: BGP attack with false AS number and inject false AS path.

Standard A4 (210mm x 297mm) portrait page set-up should be used. The left, right, top and bottom margins should be 30mm. Do not use any headers, footers or footnotes. No page numbers. Single column. All main text paragraphs, including the abstract, must be fully (left and right) justified. All text, including title, authors, headings, captions and body, will be Times New Roman font.

3. RELATED WORK

Secure Border Gateway Protocol (S-BGP) [9] is the first effective framework for securing BGP. But in SBGP extensive use of asymmetric cryptography and certificates, SBGP is costly in storage, computation, and timing of key generation as well as verification. However, due to public key cryptography, SBGP has high sign verification cost and an additional the cost of storing the topology information.

Secure Path Vector (SPV) [6] is based on Merkle hash tree. The design of SPV is vulnerable truncation attack, in which a single-ASN private key obtained from a shorter ASPATH can be used to truncate a longer ASPATH from the same origin. To counter such an attack, SPV introduces an additional level to the ASPATH authenticator, and degrades private values to semi-private values gradually along the path. Obviously, this induces design complexity and extra performance overhead to SPV. Moreover, the fairly complicated design makes it challenging to implement and deploy SPV in practice.

KC-X ALGORITHM [4] uses hybrid cryptosystem. In this approach use of KC-RSA based on RSA and KCMT based on Merkle hash tree**.** But KC-X requires signature for each route update and KC-X use same RSA alogirhtm in SAS-V. Due to use of RSA, KC-X require public key for each route update. Using PKI (Public Key Infrastructure) requires more time for sign generation and sign verification. However, building such an infrastructure is challenging. Some efforts have been made to address this issue, and they are complementary to our approach.

ID-based Aggregate Path Verification protocol (IDAPV) [14] to provide authenticity for route announcements in the Border Gateway *Protocol (BGP).* In such cryptosystems, the public key of a user is derived from his identity information, and his private key is generated by a trusted third party called Private Key Generator (PKG). The ID-based cryptography has an inherent weakness: PKG has the knowledge about the system master key and private keys of all users in the system. In practice, this is very risky. As a result, this key escrow problem must be addressed when the ID-based cryptography is applied in the real world.

Pretty Secure BGP (psBGP) [7] represents a new solution for prefix authentication via the construction of a decentralized authentication system, rather than a centralized infrastructure employed by S-BGP. Each AS maintains a *prefix assertion list* (PAL), which includes the address ownership assertions of the local AS and its peers. The prefix information is validated by checking the consistency of PALs of the peers around the origin.

soBGP [2] is another lightweight protection scheme: its essence is to detect suspicious advertisements using historical hints, and delay the propagation of them. Suspicious origin ASes are temporarily assigned a low preference, and suspicious sub-prefixes are temporarily ignored.

Symmetric Key Approaches to Securing BGP [1] that use two types of approach the centralized as well as distribution key approach. In the centralized key approach improve the sign generation cost but takes too much time for the sign verification. Combine of centralized and distribution overall degrade the performance of secure routing and additional computational cost and overheads.

4. PROBLEM IDENTIFICATION

Use of PKI to solve security issues in routing has been proposed for almost twenty years. However, there are still two main problems to solve for production routers: oversubscription of router resources and inter-AS PKI creation.

In SPV [6], each originating routers needs to generate a onetime signature that will be verified by its downstream routers. The one-time signature is the root of a merkle hash tree generated using the as_path field and a secret key held by the sender. This structure is called an as_path protector and is built over the number of ASes that need to be protected. For example, if security is required over 15 ASes then the as_path protector contains the one-time signatures of the 15 ASes. Hence, **in SPV, each node needs to generate and verify several hash values**. Thus, for SPV, the cost of signature generation and verification are comparable although verification is slightly smaller than signature generation. For comparing SPV, we chose concept of trusted Autonomous system, in this concept first autonomous system gets master certificate from central KDC server and become trusted ASes. After that each BGP speaker sign UPDATE from last trusted AS to it. As show in fig-4 use HASH code for complete route and address prefix generate by each router then they define only one router is enough for trust as they generate HASH CODE so it requires more computational task and burden on router as well as require more time. As well as they use both algorithm for key distribution central key distribution and distributed key distribution.

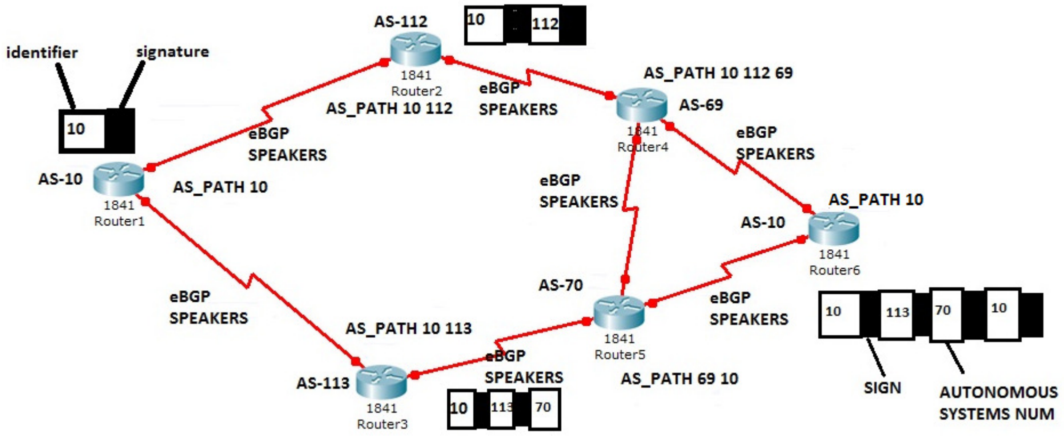

Fig 4: HASH generates at each Route UPDATES.

The paper "**Analysis of Impact of Trust on Secure Borde Gateway Protocol"**[8] shows that only 20% of *trusted* nodes in the network can reduce the number of AS-path verifications by almost 50%. Similarly, the average number of IP prefix validations is reduced by 80% when 20% of the ASes are *trusted*. Also, the average number of public keys is reduced by 67% when 20% of the ASes are *trusted*.

From above discussion we conclude that main problem is for route encryption, AS_PATH verification and prevent false route injection either use hash code or use cryptosystems. Recently in Symmetric Key Approaches to Securing BGP [1] introduce hash code with key send in plain text so when receiver router receives route update and ip prefix with key in plain text they decrypt route update and again generate hash code for that and compare with hash code send by sender or neighbor router. So they require more computational time and storage requirement.

The above attestation does not prevent a malicious router from claiming to own a particular AS number and generating forge routes. In order to verify the owner of an AS number and the authorization of using it, each route update is digitally signed by the attestation service upon the successful attestation challenge. A router is authorized to use its own private key to sign any valid announcement only when routes are successfully attested in OUT filters. The signature is then verified by its neighbors via their own attestation service. In our contribution we only use one time authentication during connection establishment. During connection establish with help of OPEN message we send secure hash code for only key. We do not generate hash code for each and every route so we require less computation cost and less time for hash verification. After one time authentication, make trust relationship between BGP peers and then each route update transmits on secure communication channel without burden of overheads and hash codes.

5. PROPOSED WORK

In previous work used either cryptography methods or hashing method for security reasons in BGP routing. In SBGP use so many signatures for attested each and every routes UPDATES. In SBGP requires more time for sign generation as well as sign verification for each route. But in our work we only use one time attestation during connection establishment, i.e. make trust between BGP peers during connection setup. As shown in fig-5, we use cyclic key shifting algorithm for key generation and SHA-1 for hashing of key only. We only use one time hash for making trust relationship between BGP speakers. A BGP peer use a simple FSM (finite state machine) that consist of six states: idle; Connect; Active; Open sent; Open confirm and establish. During Open sent state, BGP neighbor listen for an OPEN message from BGP speaker. Once the OPEN message has been received, BGP router check version of BGP and AS number. First both BGP speakers agree with key generation algorithm and hashing algorithm. Then during connection establishment, each BGP speaker generates secure key with the help of cyclic shifting algorithm and add this secure key with OPEN message. Only BGP speaker generates secure key which has authorize AS certificate id. Each BGP speaker uses certificate id to generate secure key with the help of several computational operations of cyclic shifting algorithm. This secure key sent with OPEN message during initial connection establishment. This secure key can’t transmit in plain text so we use SHA-1 hashing for generate hash value of only secure key and this hash value send with OPEN message.

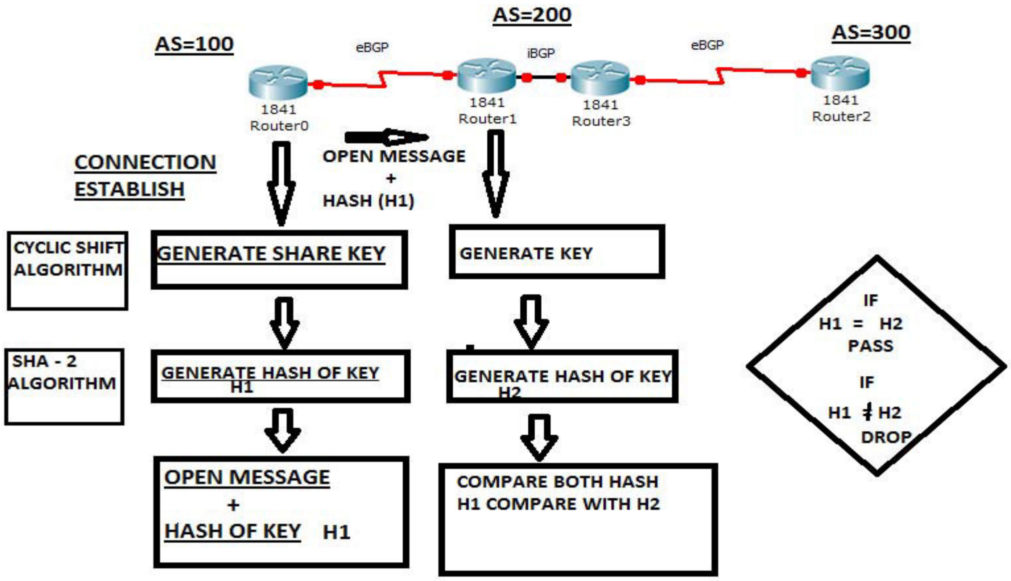

Fig 5: Establish trust relation between BGP peer.

In previous work hashing use for each route update and making secure AS_PATH. But in our work we use hashing for only one time authentication. Each BGP speaker generate hash value of secure key and at other end of BGP receiver again generate hash value of key which generate by same algorithm. After generation hash value, compare both receiving and generating hash value. If both hash values are match then accept OPEN message and establish trust relationship. If hash values are not match then simply discard OPEN message. The sender and receiver use same large prime numbers and unique certificate id for generate secure key and use same algorithms for generate secure key and hash of particular key like cyclic shifting of prime number and SHA-1. Once secure session establish each route update travel on secure channel. During session, false route update can't inject by attackers and attackers can't behave as owner of fake AS. In duration of secure session attacker can't hijack AS_PATH. When session is terminate between BGP peer and at that time of new session establish each BGP speaker requires secure private key and hash value for same so attacker can't entertain in BGP routing process. We don't use so many signs and hash codes for each route update so less time require for one time hash generate and verification.

As shown in fig 5, BGP Router-0 connected in AS-100, Router-1 and Router-2 connected in AS-200, and Router-3 connected in AS-300. Router-0 and Router-1 establish e-BGP peer. Router-1 and Router-2 establish i-BGP peer. Router-0 in AS-100 first establishes connection with Router-1 in AS-200 through passing OPEN message. Before transmit OPEN message Router-1generate secure key with help of cyclic shifting algorithm, then find hash code for secure key (H1). OPEN message and H1 (hash code of key) transmit to neighbor BGP router in another autonomous system AS-200. In AS-200, first Router-1 generate secure key with help of same cyclic shift algorithm, then generate hash code (H2) for same. Finally compare both hash code H1 and H2. If H1 match with H2 then establish secure connection between BGP speakers and make trust between BGP peer. After making trust relationship between BGP peer, route update and AS_PATH transmit on secure channel.

As show in fig-6, there are five autonomous systems interconnected like AS- 100, 200, 300, 150, 160. Each AS has own IP_PREFIX and address pool. Real owner of 9.0.0.0/8 is AS-100, but attacker AS-160 try to announce 9.0.0.0/8 is own IP_PREFIX. But due to lack of the secure private key and hashing of key, attacker can't inject stolen IP_PREFIX.

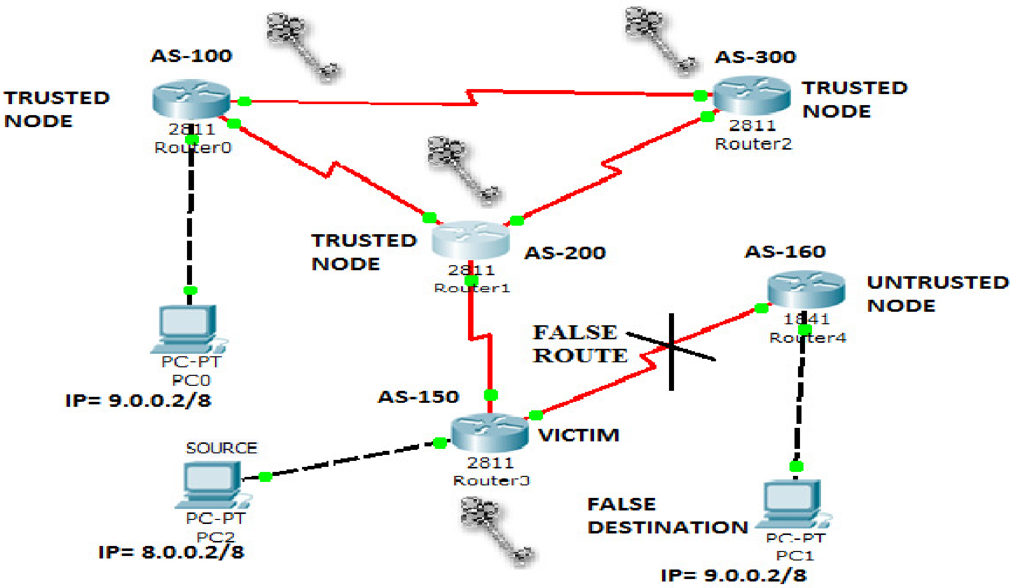

Fig 6: Secure communication between two ASes with help of symmetric private key generate by each authorized Autonomous System.

We use NS-2 simulator for design, analysis and simulate our algorithm. Using NS-2 we can simulate our protocol graphically and another tool is C-Language but in C-Language we can't simulate our Protocol so we worked on a TCL language of NS-2 Simulator. In real time routers have fewer memories so each route update cause burden on router performance. In our approach initially use secure key and hash code for make trust relationship between BGP speakers. In real world all BGP routers first establish secure connection then further there is no requirement of attested routes and AS_PATH.

5.1 Cyclic shifting Algorithm:

Here we generate symmetric key using password is case sensitive and depend on each byte of password.

If [A1A2A3…An] be the password, where 1, 2, 3...n = length of password and an ASCII value of each password multiply by 2^i where i= position of each byte of password. Keep doing above process until we have finished this method for all bytes of password. Then we add all this values which is generate unique code. During next key generation we cyclic shift all bytes of password and perform same operation on all bytes of PASSWORD.

For example Password is 'BcDe'

A1 = B A2= c A3= D A4= e
N = 66*2^1 + 96*2^2 + 68*2^3 + 101*2^4
N = 2676

Symmetric Key = 2+6+7+6 = 21

5.2 SHA-1: Secure Hash Algorithm

It is a algorithm that is used in cryptography to make information confidential. It produces a 160-bit digest from a message with a maximum size of 2^64 bits. For example, the hash of the zero-length string is:

SHA1 (" ") = da39a3ee5e6b4b0d3255bfef95601890afd80709

A **hash function** takes a long string (or message) of any length as input and produces a fixed length string as output as shown in fig.7.

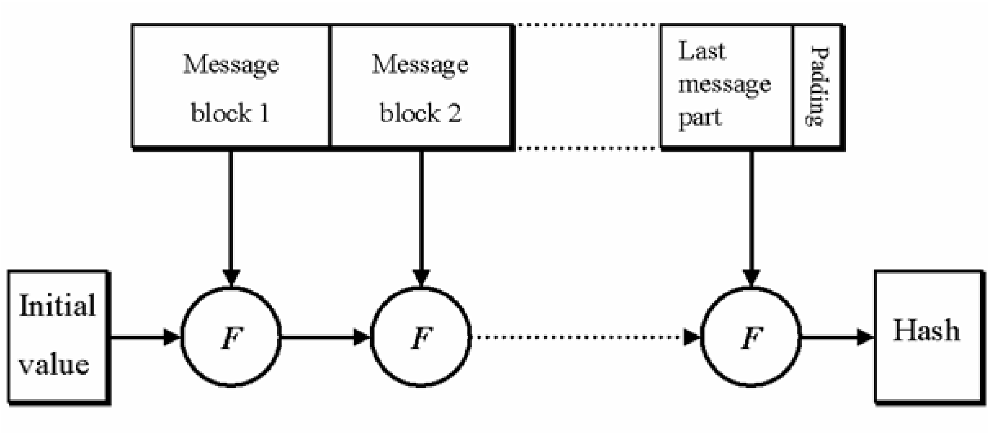

Fig 7: Hash generation from long string message.

We use SHA1 algorithm for generate hash of only symmetric key instead of long string message. Fig-8 shows the function of SHA1, it uses five 32 bits initial buffer like A, B, C, D, and E. and use left shifting operation and finally generates 160 bit hash value of symmetric key.

The SHA 1 hash algorithm generates a fixed-length hash value of 160 bits (20 bytes). The SHA1 digest message is usually represented as a 40 character hexadecimal value. This function is used in security. SHA1 is mostly used to secure protocol as SSH, TLS, SSL, PGP, and IPsec.[15]

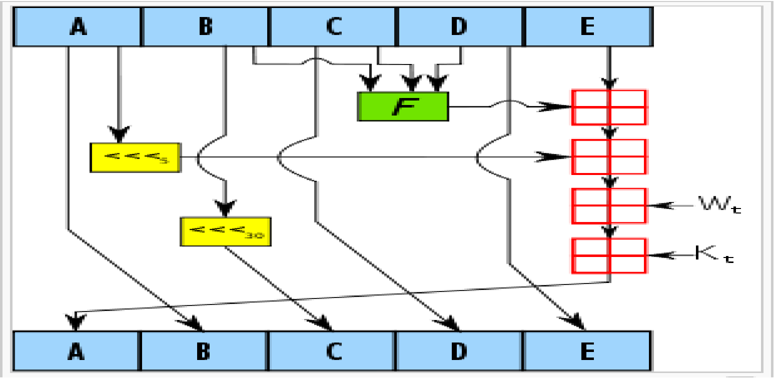

Fig 8: SHA 1 function for generate 160 bits hash code

6. RESULTS:

6.1 Time Analysis:

As Fig-9 shows results under heavy work load and x-y geometry base on time. In SBGP with simple encryption takes too much time for routing because each route UPDATE require authentication so we get periodic variation in time, whereas using one time authentication require less average time and it require only one time variation in time then after get less constant time for route UPDATES. Previous algorithm with each time encryption and authentication shown by red line and modified one time authentication shown by green line in graph. According to our algorithm, we require slide more time during initialization for connection establishment of BGP speakers then after we get constant less time for each route UPDATE transaction. Whereas in previous SBGP algorithm require variable more time for routing.

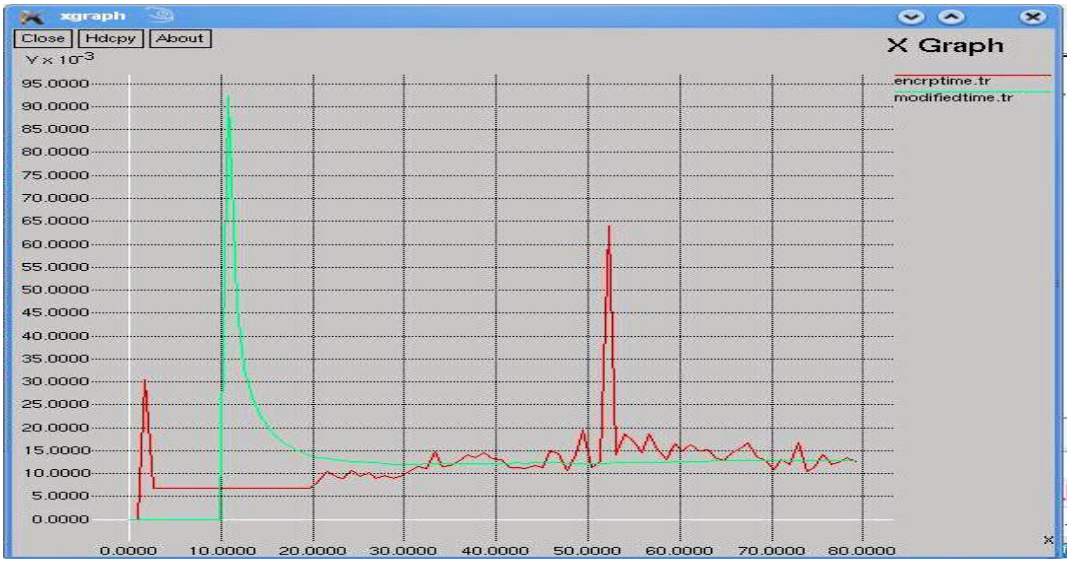

Fig 9: Encryption and Authentication time in traditional algorithm and our approach

6.2 Memory Consumption:

As shown in fig-10, in real time BGP routers have less memory space either DRAM or NVRAM. A Routing security algorithm yields large signature cost so router memory is another parameter which should be consider in algorithm. In previous work require memory up to 135 MB because each route UPDATE generates a signature. In our algorithm we reduce requirements of Router memory cost up to 120 MB because we generate signature during session establishment only.

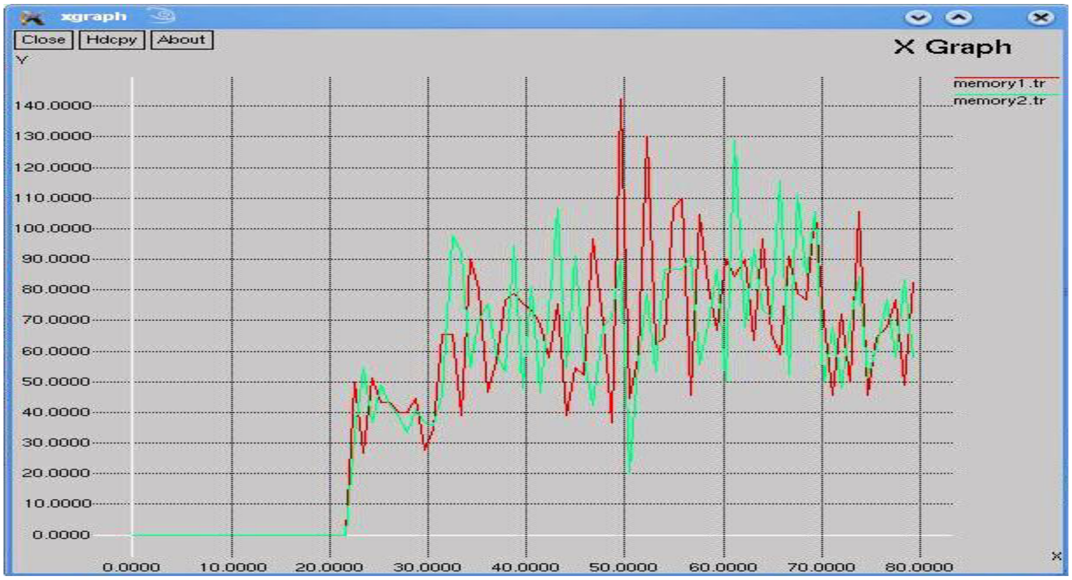

Fig 10: Memory Utilized for encryption key in traditional algorithm and our approach.

6.3 Traffic Analysis:

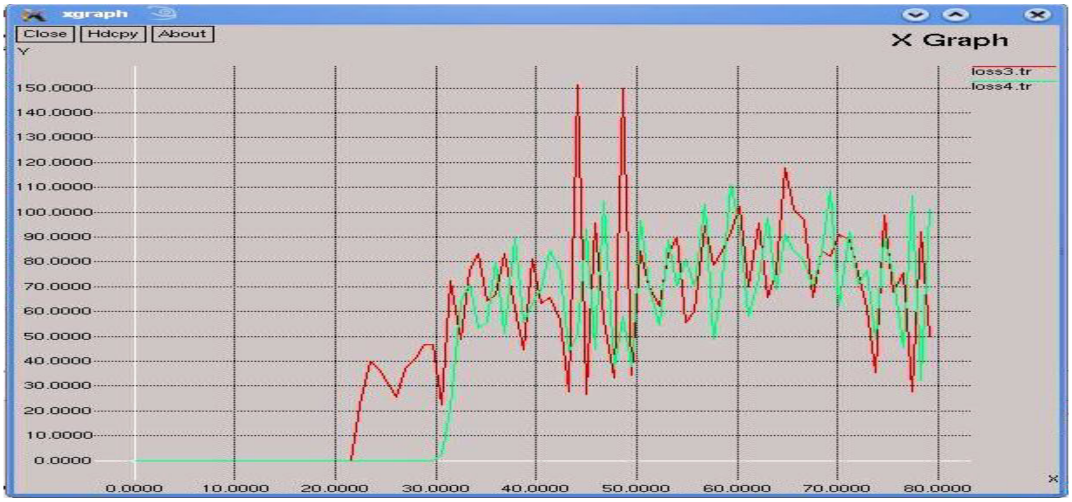

Fig 11: Traffic Analysis for both traditional algorithm and our algorithm

As shown in fig.11, the traditional SBGP is vulnerable to attack and has high loss of packets during routing process. In our algorithm provide high security mechanism and reduce loss of packets during routing process.

7. CONCLUSION

We make such key contribution in this paper. First, we show that efficiency and security for BGP could be achieved by adding trust on BGP routers. So that we require less number of keys for attested the route. Second, for confidentiality we use symmetric approach for one time authentication. In this approach we provide security at time of initial connection establish and use of OPEN message of TCP for transmission of secure key. We generate authentication key using secure cyclic shift algorithm and hash of the particular key using most secure SHA-1 algorithm. We only make trust between BGP peer during connection establishment process. Our main purpose is generate less number of keys for encryption as well as attested complete route and less time require for verification of digital signature. So we make all autonomous systems become trusted at initial time of routing. The false AS can't establish connection with BGP neighbors, due to lack of secure private key and hash values for same. Each authorizes autonomous system only generates secure private key and hash value for establish trust relationship between BGP peers. So using this approach overall performance of internet is improve and require less memory of BGP routers as well as reduce packets loss.

REFERENCES

[1] Bezawada Bruhadeshwar, Member, IEEE, Sandeep S. Kulkarni, Member, IEEE, and Alex X. Liu," Symmetric Key Approaches to Securing BGP—A Little Bit Trust Is Enough"In SEPTEMBER 2011

[2] R. White and B. Akyol, "Deployment considerations for Secure Origin BGP(soBGP)," Internet Draft, Internet Engineering Task Force, June 2003.

[3] CCNA STUDY GUIDE, PHI publication 7th edition by TODD LAMLE.

[4] Heng Yin, Member, IEEE, Bo Sheng, Member, IEEE," Keychain-Based Signatures for Securing BGP",in OCTOBER 2010.

[5] www.iana.org/numbers

[6] Yih-Chun Hu, Adrian Perrig, and Marvin Sirbu, "SPV: Secure path vector routing for securing BGP," in Proc. ACM SIGCOMM 2004, September 2004.

[7] ao Wan, Evangelos Kranakis, and P.C. van Oorschot, "Pretty secure BGP (psBGP)," in Proc.Network and Distributed System Security Symposium (NDSS 2004), February 2004.

[8] Junaid Israr, Mouhcine Guennoun, Hussein T. Mouftah," Analysis of Impact of Trust on Secure Border Gateway Protocol" in 2011

[9] Stephen Kent, Charles Lynn, and Karen Seo, "Secure border gateway protocol (S-BGP)," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp.582–592, April 2000.

[10] Qi Li, Student Member, IEEE, Mingwei Xu, Member, IEEE, Jianping Wu, Member, IEEE "Enhancing the Trust of Internet Routing with Lightweight Route Attestation".

[11] www.cisco.com

[12] Cryptography and Network security by atul kahate, second edition,McGraw Hill publication.

[13] Ying Zhang, "HC-BGP: A Light-weight and Flexible Scheme for Securing Prefix Ownership", IEEE 2009.

[14] Na Wang, Yingjian Zhi, Binqiang Wang, "A New Path Verification Protocol for Securing BGP", IEEE 2008.

[15] http://en.wikipedia.org/wiki/SHA-1