Securing BGP sessions through Peer Link Elliptic Curve Cryptography

Naasir Kamaal Khan[1] and Gulabchand K. Gupta[2]

[1]*J.J.T University,*
Rajasthan, India

[2]*Western College of Commerce and Business Management,*
Mumbai, Maharashtra, India

***Abstract* - Border Gateway routing protocol (BGP) is the de-facto inter-domain routing protocol. Threat vulnerabilities and security issues of BGP have been addressed various times by different researchers through different angles including its functionality, operations and mechanism. BGP security classification is broadly classified in two planes, control plane and data plane. Control plane deals with routing policies whereas data plane talks about secure data delivery. This paper advocates the BGP security in data plane believing in its security and efficiency. In this paper a BGP threat model is designed and an attack overcoming procedure is suggested using peer link elliptic curve cryptography (PLECC) algorithm and session key concept in the network. The design is further implemented using network simulator taking into consideration some of the major attacks associated with data delivery. The result thus obtained concludes that the opinion of securing data delivery instead of securing routing protocol is more effective, easier and robust to reduce performance overhead.**

***Keywords*- BGP, PLECC, Subverted Unauthorized, Misrounding, Power Control, Masquerading.**

I. INTRODUCTION

Tremendous growth of Internet usage worldwide and recent developments in the field of communication made ease of reachability between individuals, business professionals, educational Institutions, government and non-government organizations to access, share and communicate information. Routing in the Internet technically means receive, store and transmit the information using the best possible path. Routing table stores the information of all possible paths available to successfully transfer the data to the next router in the mesh. The Internet consists of independently administered networks, which are called autonomous systems (ASes). The Border Gateway Protocol (BGP) is the de-facto interdomain routing protocol that connects ASes together [1]. BGP provides two essential services: mapping IP prefixes onto the ASes that own them and the construction of source specific paths to each reachable prefix [2]. Every BGP router announces the IP prefixes that its AS owns in an update message and sends the message to its neighboring BGP routers. Received update messages are recursively concatenated with an additional AS number and propagated from AS to AS forming a routing path, which will be used to forward traffic. When a BGP router receives multiple paths for the same prefix, the router chooses the best path based on multiple criteria such as path length, routing policies, etc. Although one AS may have multiple BGP routers, all BGP routers within the same AS use the same AS number. Due to the lack of security mechanisms in the current BGP protocol, attackers may spoof or tamper BGP messages. Thus, it is critical for a recipient AS to validate the authenticity and integrity of update messages before making routing decisions. Several solutions for securing BGP have been proposed earlier including public and private key approach (e.g., [3], [4] - [8]). However, none of them have been adopted so far due to either high cost or high complexity. The increasing popularity of BGP depicts its broad ability to distribute reachability information by selecting the best route to each destination according to policies specified by network administrator. BGP is a critical component of the exponentially growing network of routers that constitutes Internet. Carrier networks, as well as most large enterprise organizations with multiple links to one or more service providers use BGP. A BGP session between peers is assumed to have some level of integrity at the session transport level. BGP assumes that the messages sent by one node are exactly the same messages as received by the other node, and assumes that the messages have not been falsified and reordered, have spurious messages added into the stream or have messages removed from the conversation stream in any way. As with any farsighted TCP session, the BGP peer session is vulnerable to eavesdropping, session readjust, misrounding, message alternation and denial of service attacks via conventional TCP attack vectors. In this paper we have proposed a BGP threat model in section II where major possible attacks and attack overcoming procedure are discussed. In section III we have introduced Peer Link Elliptic Curve Cryptography (PLECC), its key generation, key exchange and key management procedure. In section IV PLECC is implemented using network simulator and its implementation details are discussed. In section V results are obtained and output graphs with their throughput are discussed. In the last section our research is concluded which shows significant throughput as compare to attacker's path communication.

II. BGP THREAT MODEL

A. Threats at Session level

A threat at the session level is that a third party may attempt to break into the TCP session, and alter the BGP message flow. There are various forms of attacks at this level [9], one form is by injection, where an intruder eavesdrops on the conversation and injects unauthentic messages into the BGP session. Eavesdropping allows the attacker to have knowledge of the TCP sequence numbers. Another form of threat is by active intermediation where an attacker sits on the wire between the two BGP nodes and intercepts all traffic in both directions. In this case an attacker node has complete control of the BGP message stream and can perform any form of message alteration. A variation of this form of threat is by session hijacking, where an attacker wiretap upon an active BGP session and injects its own traffic into the message stream that allows the attacker to take over the session and masquerade as one of the parties to the BGP session. As the overall performance of BGP depends on timing another form of attack at this level is to delay messages. Here the content of the messages are unaltered, the timing signals within the message stream are altered by this form of interposition, potentially causing the local BGP speaker to behave differently and fall out of sync with its routing peers. For example, it is possible to exercise various forms of local inhibition of routes by altering the timing of propagation of BGP messages. Another form of attack is a replay attack, where older BGP messages are replayed into a hijacked TCP session. One form of this replay attack could be to replay a pair of messages that withdraw and then declare the same address prefix [10]. Selective dropping attack [11] has a feature of dropping malicious router from the network so that communication can be established without intervention of potential intruder; this type of attack is further explained and implemented [12] to demonstrate its severity.

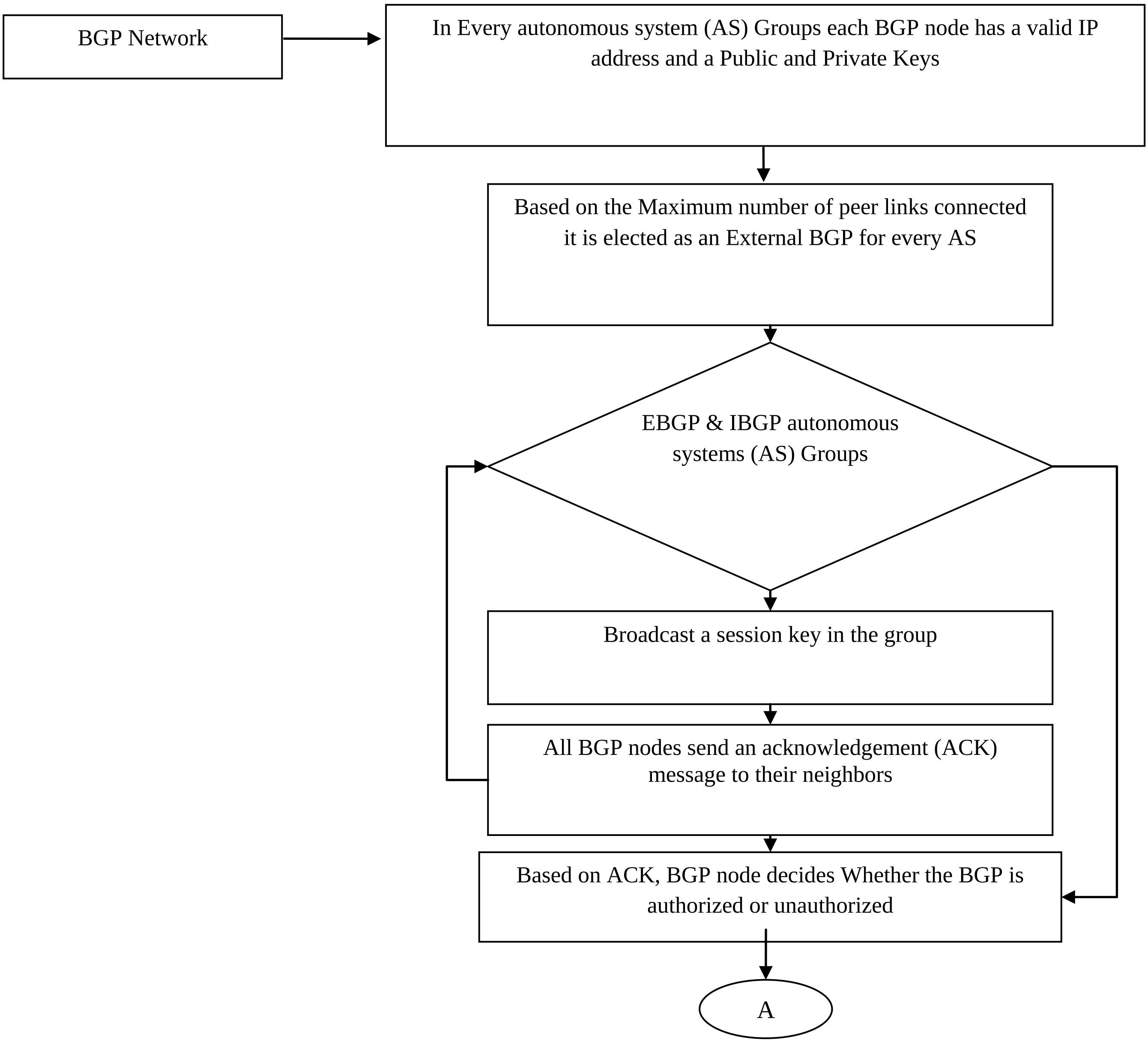

BGP Network
In Every autonomous system (AS) Groups each BGP node has a valid IP address and a Public and Private Keys
Based on the Maximum number of peer links connected it is elected as an External BGP for every AS
EBGP & IBGP autonomous systems (AS) Groups
Broadcast a session key in the group
All BGP nodes send an acknowledgement (ACK) message to their neighbors
Based on ACK, BGP node decides Whether the BGP is authorized or unauthorized
A

Figure 1: Threat model flowchart

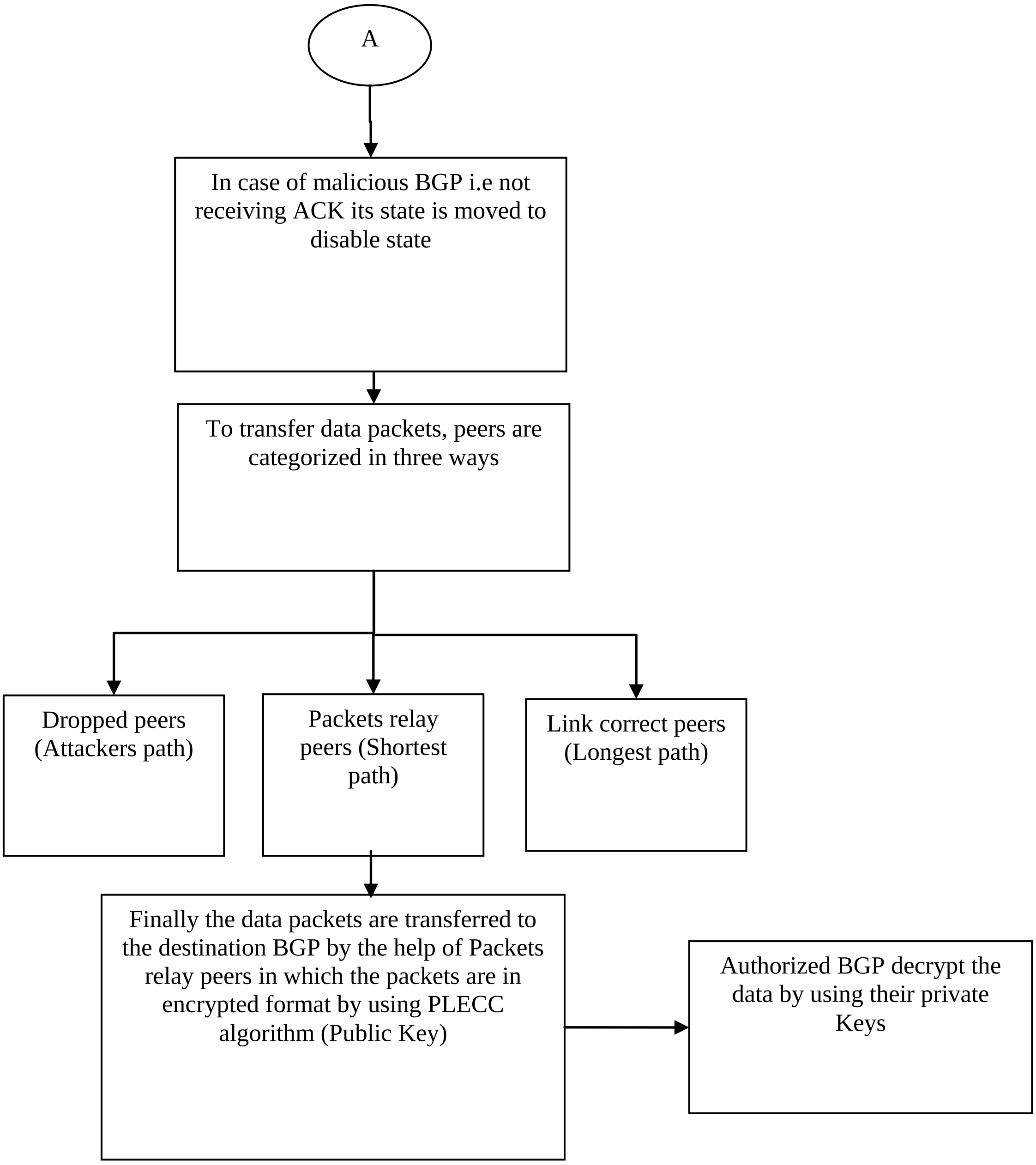

A
In case of malicious BGP i.e not receiving ACK its state is moved to disable state
To transfer data packets, peers are categorized in three ways
Dropped peers (Attackers path)
Packets relay peers (Shortest path)
Link correct peers (Longest path)
Finally the data packets are transferred to the destination BGP by the help of Packets relay peers in which the packets are in encrypted format by using PLECC algorithm (Public Key)
Authorized BGP decrypt the data by using their private Keys

Figure 2: Threat model flowchart (contd.)

B. Securing Data Delivery

Dependable Internet communication can be afflicted by attackers who compromise routers or by link failures and misconfigurations. In a conventional threat model, attackers can fiddle with data or portray identities, spy on traffic, or deny service. Off all, availability requires support from the routing infrastructure. Integrity can be provided end-to-end using long-familiar cryptographic techniques and hash functions along with shared secret or public key authentication systems. Data confidentiality is likewise easy to protect using encryption. This leaves availability as the remaining threat [13]. Unluckily, cryptography cannot get packets across a path that drops or misdirects all traffic. Communication security in both planes control and data, are compromised by control of a router, either lawful or unlawful. The link cut analysis explores the question of fortune-sharing, if one link is cut by physical means, others will be cut as well. The same issue applies to routers: in a war situation, the military may find it easier to destroy an entire POP, rather than just one or two routers [14]. Sometimes, an adversary would like to monitor traffic among three or more nodes. A more sophisticated algorithm would determine the link cuts that would satisfy multiple constraints simultaneously. Routing on the Internet is generally asymmetric; an adversary would generally want to monitor traffic in both directions of any peculiar path. As noted, the effect of attacker positioning is critical. It is interesting to design algorithm that placed desirable nodes to compromise for a given number of link cuts.

C. Proposed Threat Model

In our BGP Threat Model we have constructed three ASes comprising of various BGP nodes. The Internal and External BGPs are connected through various links based on their IP addresses. A TCP communication is exchanged between peers. Each BGP advertises their route information to the entire network. As soon as data packets are sent from source to destination via shortest path there might be two cases depending on whether BGP attack occurs or not and consequently packets are reached with or without loss. Major attacks which are taken into consideration in this model are masquerading, packet dropping, and subverted unauthorized and subverted link. Attack overcoming procedure of this design is shown in Figure 1 and 2. The main Idea is to incorporate public and private key for each BGP peer using PLECC algorithm. Based on maximum number of peer links a BGP is elected as EBGP. A session key is broadcasted in the group and an acknowledgement is expected from each BGP, based on this acknowledgement it is decided that whether it is authorized BGP or not. Finally bogus BGPs are dropped and data is transferred through shortest path with the help of packet relay peers where packets are in encrypted format. These packets can only be decrypted using private key of authorized BGP.

III. PLECC ALGORITHM

PLECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements. For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b,$$

Along with a distinguished point at infinity, denoted by ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.) This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

A. Peers links Elliptic Curve Cryptography Key Pair Generation:

The Peer links Elliptic curve key pairs are generated as follows:

Input: Valid Peer link elliptic curve domain parameters PL= PS, PE

Output: A Peer link elliptic curve key pair (PS, PE) Authorized to PL

Actions: Generate an elliptic curve key pair as follows:

1. Randomly or pseudo randomly select an integer d in the interval between PS, PE.
2. To check Peer links
Calculate key Peer links PS=PE
3. Output (PS, PE).

PL= Peers links, PS= Peer start, PE= Peer End

B. Peers links Elliptic Curve Public Key Validation

The Peer links elliptic curve public key validation primitive should be used to check an elliptic curve public key is valid as follows:

Input: Valid elliptic curve domain parameters PL= PS, PE and an elliptic curve public key PL= (PS U PE) associated with equals.

Output: An indication of whether the elliptic curve public key is valid or not—either ‘valid’ or ‘invalid’.

Actions: Validate the elliptic curve public key as follows:

1. Check that PS U PE = TRUE
2. If PL represents elliptic curve domain parameters over PS and PE, check that integers Public Key in the range or not
3. The data will be encrypted by using both PS and PE public key
4. Check that PL = integers values
5. If any of the checks fail, output ‘invalid’, otherwise output ‘valid’.

C. Encryption Operation

PS should encrypt messages to send to PE using the keys and parameters established during the setup procedure and the key deployment procedure as follows:

Input: A string S which is the data to be encrypted.

Output: A string S which is the cipher text corresponding to PE, or ‘invalid’.

Actions: Compute the cipher text PL as follows:

1. Convert string S based on PL keys values
2. Calculate the encryption in both PS and PE using the encryption operation and also scheme under the shared secret key K.
3. If the encryption operation outputs ‘invalid’, output ‘invalid’ and stop.
4. String transferred
5. End

D. Decryption Operation

PS should decrypt cipher text from PE using the keys and parameters established during the setup procedure and the key deployment procedure as follows:

Input: A encrypts string S which is the unreadable state.

Output: A Decrypts string S which is the decryption of PL, or ‘invalid’.

Actions: Decrypt PL as follows:

1. Convert readable state in string S by using the secret key K
2. Calculate the decryption String S using the decryption operation of the selected correct secret key or not
3. Based on condition return ‘invalid’, or output
4. End

IV. Implementation Using Ns2

Overall network creation is shown in following figure with different Autonomous systems and an external BGP is elected in each AS based on maximum number of links connected to it.

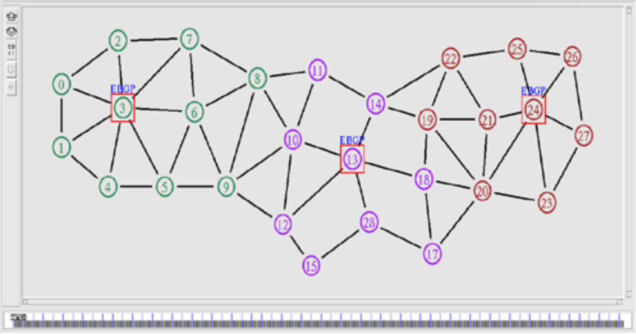


Figure 3: AS1 is shown as Green AS2 as pink and AS3 as Brown.

A Synchronization message is transferred between EBGP and IBGP followed by SYN message in whole group and further between all EBGPs as shown in following figures.

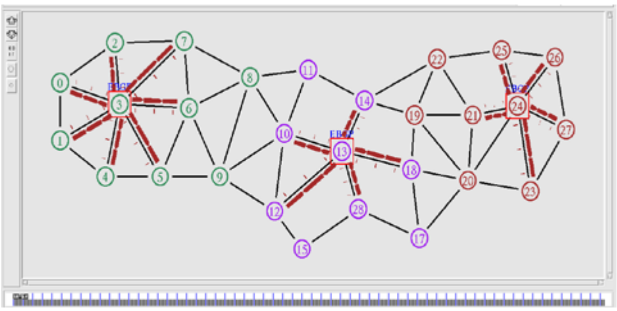
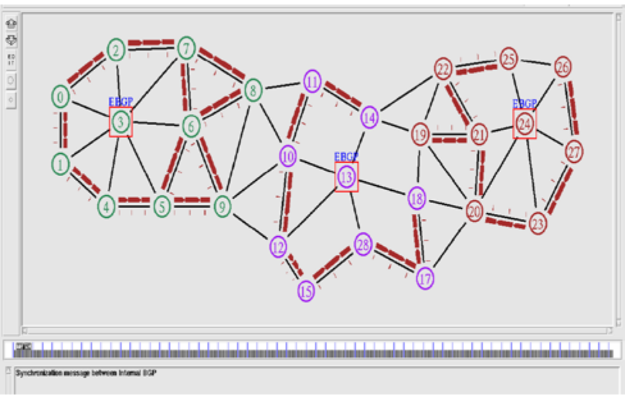
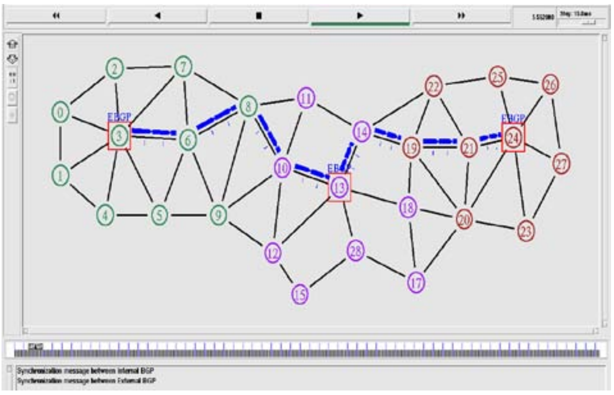


Figure 4: Transfer of synchronization message



Synchronization message between Internal BGP

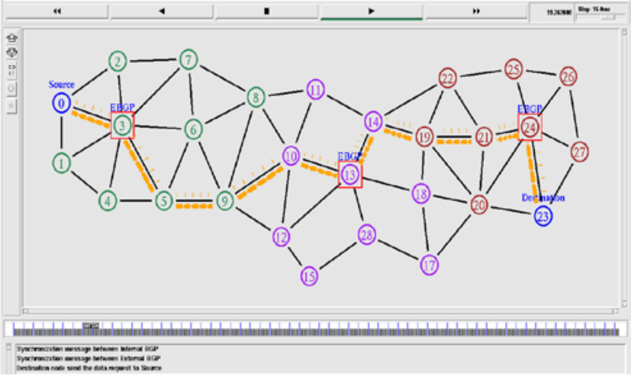
Figure 5: Transfer of synchronization to whole group



Synchronization message between Internal BGP
Synchronization message between External BGP

Figure 6: Transfer of synchronization message between the EBGPs

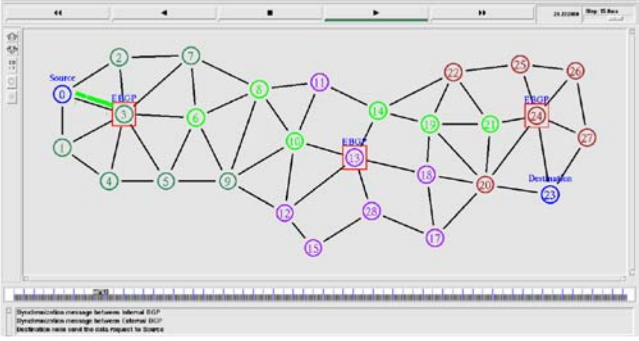
After SYN message has been transferred a data request has been sent to source node 0 from destination node 23 through EBGPs



Synchronization message between Internal BGP
Synchronization message between External BGP
Destination node send the data request to Source

Figure 7: Data request from node 23 to node 0.

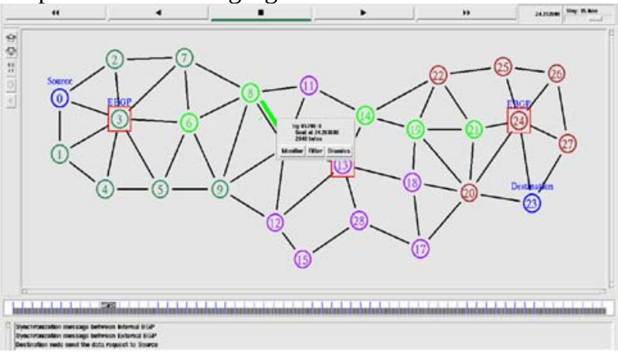
A path is chosen by source node to transfer the data is 0-3-6-8-10-13-14-19-21-24-23 as shown by green nodes



Synchronization message between Internal BGP
Synchronization message between External BGP
Destination node send the data request to Source

Figure 8: Path chosen by source node to send the data

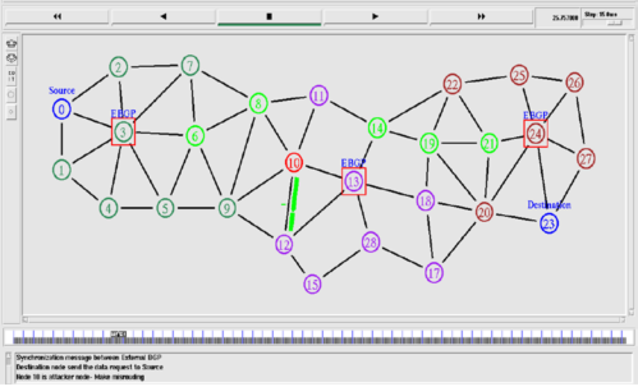
Case 1: Data is transferred without any attack i.e ideal case is depicted in following figure.



Synchronization message between Internal BGP
Synchronization message between External BGP
Destination node send the data request to Source

Figure 9: Data transferred in ideal case.

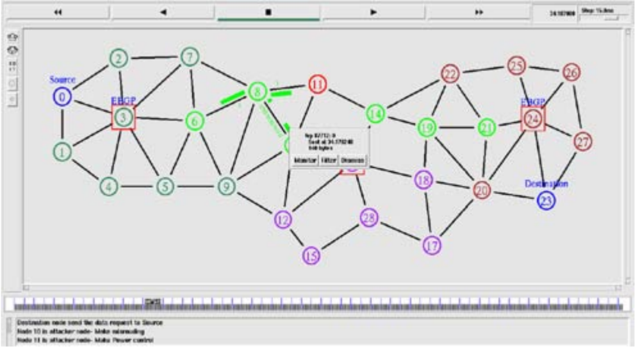
Case 2: Attack of misrounding by node 10 is shown in following figure.



```
Synchronization message between External BGP
Destination node send the data request to Source
Node 10 is attacker node- Make misrouting
```

Figure 10: Attack of misrounding by node 10

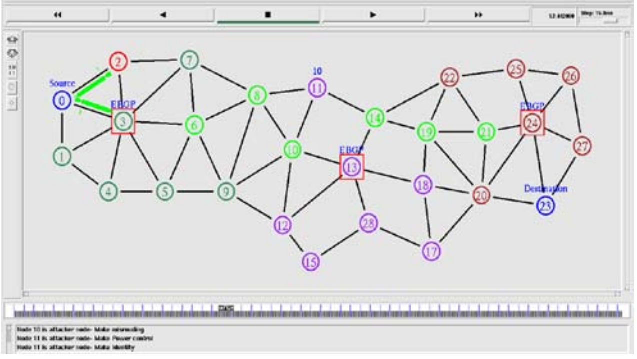
Case 3: Attack of Power control by node 11 is shown in following figure



```
Destination node send the data request to Source
Node 10 is attacker node- Make misrouting
Node 11 is attacker node- Make Power control
```

Figure 11: Power control attack by node 11

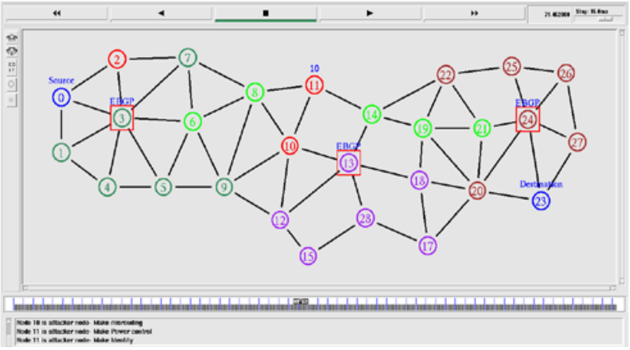
Case 4: Attack of masquerading by node 2 as shown in following figure.



```
Node 10 is attacker node- Make misrouting
Node 11 is attacker node- Make Power control
Node 11 is attacker node- Make Identity
```

Figure 12: Masquerading attack by node 2

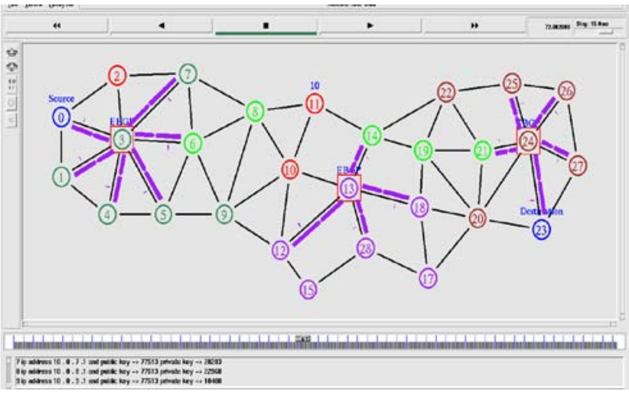
In the following figure all attackers node are identified and marked in red color that are node 2, 10 & 11.



```
Node 10 is attacker node- Make misrouting
Node 11 is attacker node- Make Power control
Node 11 is attacker node- Make Identity
```

Figure 13: Attackers are identified in red color

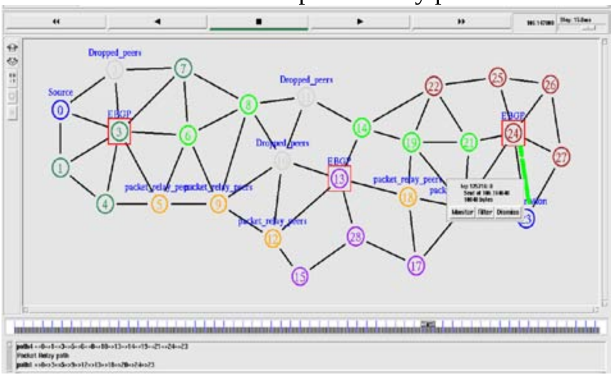
Now the ip-addresses and private keys are transferred in the group except the attacker's node as shown in following figure. Now whenever EBGP sends request message to its group a reply is received from all nodes except attacker nodes as they doesn't hold the appropriate key and thus can be dropped from the network for uninterrupted transfer of data.



```
7 ip address 10 . 0 . 7 .1 and public key -> 77513 private key -> 28283
8 ip address 10 . 0 . 8 .1 and public key -> 77513 private key -> 22968
5 ip address 10 . 0 . 5 .1 and public key -> 77513 private key -> 18408
```

Figure 14: Transfer of IP address and private key except attacker nodes

Attacker nodes are discarded from the network and a safe path is determined for successful transmission of message as shown in following figure. There may be several paths available out of which a best packet relay path is chosen.



```
path4 <-0<-1<-3<-5<-6<-8<-10<-13<-14<-19<-21<-24<-23
Packet Relay path
path1 <-0<-3<-5<-9<-12<-13<-18<-20<-24<-23
```

Figure 15: Destination node receives the data packets

V. Results And Discussion

In every simulation run, attacker node is changing based on "optimal power" range for each nodes, in our bgp.tcl file we have set different conditions such as if {3000 < $optimalpower(0)}, if {3000 < $optimalpower(0) && 4000 > $optimalpower(0)}….etc. Every node is generating public key, private key and ip address in the code as follows.

$ns_ at 73.0 "$ns_ trace-annotate \"17 ip address 10.1.17.1 and public key => $key(41) private key => $key(17) \""

$ns_ at 73.0 "$ns_ trace-annotate \"18 ip address 10.1.18.1 and public key => $key(41) private key => $key(18) \""

$ns_ at 73.0 "$ns_ trace-annotate \"28 ip address 10 . 1 . 28 .1 and public key => $key (41) private key => $key (28)\""

The program is written in such a manner that possible packet relay paths are changing in every simulation and the best path is chosen based on occurrence of attacker in the path, for examples if source is node 2 and destination is node 18, possible paths are:- Path 1: 2-3-4-11-16-18,Path 2: 2-3-5-10-13-18 and Path 3: 2-6-9-15-18 as attacker has been occurred in path 1, there are two alternatives to choose the best path, path 2 & path 3which does not have any attackers in those paths. By comparing those paths (2&3), path 3 is better than path 2 as path 3 is the shortest path.

Figure 16 is depicting the XGraph based on attackers BGP where x-axis represents type of attacker and y-axis represents attackers node ID.

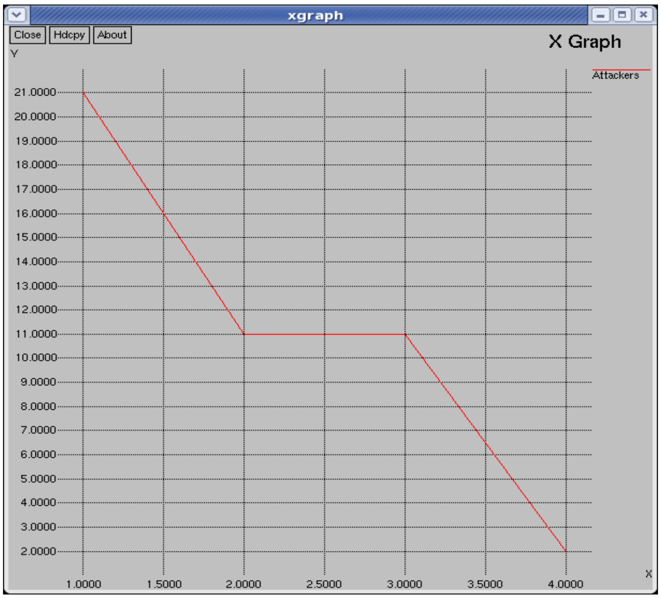


Figure 16: Graph based on Attackers BGP

Comparison of throughput rates between attacker path communication and the proposed system is shown in figure 17. In this figure comparison has been done between attacker path and normal path where x-axis represents number of packets delivered and y-axis represents total execution time of the program.

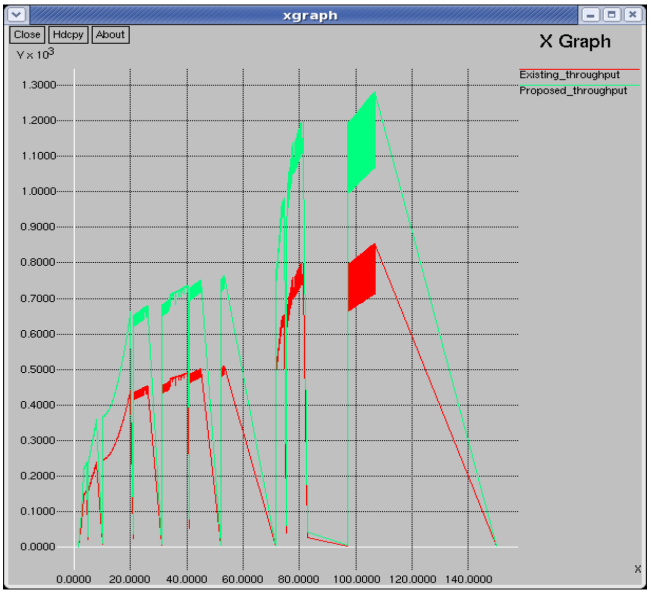


Figure 17: Throughput rates comparison

VI. CONCLUSION

Network layer security can be achieved without securing the routing protocols as the properties such as confidentiality and integrity can be provided end-to-end by applications requiring strong security. As far as availability is concerned it is better achieved by securing data delivery rather than routing protocol. By recognizing that many applications today already require and use end-to-end security, we present a novel and persuasive point in the routing security design space. PLECC provides strong protection from data-plane adversaries and failures; we believe its principles are a worthwhile addition to the routing security toolbox. In this paper we analyzed the security weakness of BGP and explored four major attacks subverted, unauthorized, masquerading and subverted links in detail, a BGP threat model is designed and an effective attack overcoming procedure has been proposed based on session key concept of network. A new algorithm named Peer link Elliptic Curve Cryptography (PLECC) is suggested and further implemented using ns-allinone-2.35. Here connections are established using asymmetric key approach in which malicious nodes are discarded from the network as soon as they are detected. Further these malicious peers are dropped from the network to assure safe packet relay path. The results thus obtained are compared with the attacker's path communication which shows tremendous increase in the throughput rate of the system.

REFERENCES

[1] Y. Rekhter, T. Li, and S. Hares, "*A border gateway protocol 4 (BGP-4),*" RFC 4271 (Draft Standard), Internet Engineering Task Force,Jan. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4271.txt

[2] Bezawada Bruhadeshwar, Sandeep S. Kulkarni, and Alex X. Liu "*Symmetric Key Approaches to Securing BGP—A Little Bit Trust Is Enough*". IEEE Transaction on PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, 2011

[3] B. Smith and J. Garcia-Luna-Aceves, "*Securing the border gateway routing protocol,*" in Global Telecommun. Conf., 1996. GLOBECOM '96. 'Commun.: Key Global Prosperity, Nov 1996, pp. 81–85.

[4] R. Mahajan, D. Wetherall, and T. Anderson, "*Understanding BGP misconfiguration,*" in SIGCOMM '02: Proc. 2002 Conf. Appl., Technol., Architectures, Protocols Comput. Commun.. New York, NY, USA: ACM, 2002, pp. 3–16.

[5] J. Qiu, L. Gao, S. Ranjan, and A. Nucci, "*Detecting bogus BGP route information: Going beyond prefix hijacking,*" in Security Privacy Commun. Netw. Workshops, 2007. SecureComm 2007. Third International Conf., Sept. 2007, pp. 381–390.

[6] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin, "*Working around BGP: An incremental approach to improving security and accuracy of interdomain routing,*" in Proc. Internet Society Symp. Netw. Distributed Syst. Security (NDSS 03), Feb. 2003.

[7] Y.-C. Hu, A. Perrig, and M. Sirbu, "*SPV: Secure path vector routing for securing BGP,*" in SIGCOMM '04: Proc. 2004 Conf. Appl., Technol., Architectures, Protocols Comput. Commun.. New York, NY, USA: ACM, 2004, pp. 179–192.

[8] A. Heffernan, "*Protection of BGP sessions via the TCP MD5 signature option,*" RFC 2385 (Proposed Standard), Internet Engineering Task Force, Aug. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2385.txt.

[9] O. Nordström and C. Dovrolis, "*Beware of BGP attacks,*" SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 1–8, 2004.

[10] K. Sriram, D. Montgomery, O. Borchert, O. Kim, and D. Kuhn, "*Study of BGP peering session attacks and their impacts on routing performance,*" Sel. Areas Commun., IEEE J., vol. 24, no. 10, pp. 1901– 1915, Oct. 2006.

[11] K. Zhang, X. Zhao, F. Wu, "*An analysis of Selective Dropping Attack in BGP*", Proceedings of IEEE IPCCC, April, 2004.

[12] Lata L. Ragha, B. B. Bhaumik, S. K. Mukhopadhyay "*Malicious Dropping Attack in the Internet: Impacts and Solution*" IJCA Volume 2 – No.3, May 2010.

[13] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford, "*Don't secure routing protocols, secure data delivery,*" in Proc. 5th ACM Workshop Hot Topics Netw. (Hotnets-V), Irvine, CA, Nov. 2006.

[14] S. Bellovin and E. Gansner. (2003, May). "*Using Link Cuts to Attack Internet Routing*". [Online]. Available: http://www.cs.columbia.edu/smb/papers/reroute.pd

Naasir Kamaal Khan has received his B.E (Hons.), & M.Tech (IT) in 2002 & 2004 respectively. Presently he is Pursuing Ph.D. Over the span of 9 years of his teaching experience he has Published & Presented Several Research Papers in National & International Conferences, Delivered expert lectures in India & Abroad. He has supervised several student research projects. He is a Life Member of Indian Society of Technical Education (ISTE). His areas of interest are Cryptography & Network Security, Information & System Security and Computer Networks.

Gulabchand K. Gupta has received his M.Sc, Ph.D in Electronics and M.Tech in Computer Science and Engineering. Presently he is Principal at Western college of commerce and Business Management, Navi Mumbai and Research Guide at J.J.T University. Over the span of 30 years of his academic and research experience he has published and presented several research papers in national and international conferences and journals. He has supervised several Ph.D and M.Tech students for their research work. He is a senior member of computer society of India (CSI). His areas of interest are Solid state Electronics, Computer Networks, Mobile Ad-hoc and sensor Networks, Network Security and Wireless Networks.