ABSTRACT

The internet is a global, decentralized network which consists of many smaller interconnected networks. The networks are framed by many computing and routing devices. There are many paths available for information flow among the routers, in which a single path is chosen, depends on the routing policies and process. To locate appropriate host, routers and path selection are performed by routing protocols. The Border Gateway Protocol (BGP) is one among these routing protocols, which is used to exchange the routing information among the routers. BGP is the exterior gateway protocol (EGP), which is used to share the routing information among the routers in different Autonomous System (AS).

The AS is the interconnected network, which comes under a single administrative control. There are two categories of routing available in AS, which are intra (routing with in AS) and inter (routing between AS) domain routing. BGP is the most popular path vector inter domain routing protocol, which contains complete routing information to reach all destination.

The network reachability information of the BGP is maintained in database, which exchange information with other BGP systems. BGP uses this network reachability information to construct a graph of AS connectivity, thus allowing BGP to remove routing loops at the AS level and policy based routing.

Routing policies can be chosen among multiple paths to the destination and also to control distribution of routing information. Transmission Control Protocol (TCP) is used as a transport protocol for BGP and uses port number 179 to establish connections. Since TCP has reliable
transmission, it eliminates the need for BGP to implement updating of fragmentation, retransmission, acknowledgement and sequencing. More number of security issues arises, since BGP is responsible for exchanging routing information among different administrative control ASs.

One of the serious security issues in BGP is prefix hijacking attack. There are three possibilities of prefix hijacking attack, (i) the announcement of block holing unallocated space, (ii) announcement of a sub-block of existing allocation and (iii) competing announcement for exactly the same space as an existing allocation can be announced.

The main goal of this research work is to ensure attack less and reliable communication through BGP with high throughput, minimize the delay and also to improve the performance measure of each transaction. If an attack is detected on a node, then the route through that node becomes malicious, and that node is suspicious to deliver the packets between the nodes. Thus it directly affects its efficiency with respect to the route path distance. To mitigate Prefix Hijacking Attack on BGP, this research work proposes the technique like; Route Reliability Matrix (RRM) based Route Reliability Ranking Algorithm (RRR), Fast ReRouting technique and LifeSaver (LS) method. These techniques are used to authenticate the validation of routing update records in ASs.

Prefix hijacking attack is a category of path validation attack in BGP, hence a RRR algorithm is used to defence against it. This algorithm helps to authenticate the validation of a routing update, according to the common facts of the autonomous systems in the network. After RRR algorithm, a penalty based route selection mechanism is performed to identify suspicious candidates. Thus, it allocates a penalty value for AS which appears on an invalid route, so that the route with the lowest penalty value for a destination is selected as the best route.
To ensure the quality communication among ASs, Fast ReRouting technique is used as the extension of RRT. Based on RRR and penalty based route selection mechanism, the RRT is performed and reliable routes are identified. The primary link failure and untrustworthiness of the links are the major issues of BGP. Based on the primary link failure on a transaction, the alternative link has to be identified with the help of FRR technique. The main advantage of this research work is to find the alternative path with the lowest post failure, traffic load across all the links, which are taken into account to decrease the packet loss.

BGP is one of the critical protocols that provide security and stability to the internet. To avoid conflicts between routes, the concept of Lifesaver is proposed in this research work. Ideally, all ASs participate in the internet, which act as lifesaver ASs to completely eliminate the bogus routes. The lifesavers ASs are typically large Internet Service Providers (ISPs) multi homed network path, which encourages for deploying security features. The mitigation actions executed by the lifesaver ASs remain effective, until the original bogus route is withdrawn. The mitigation system instructs the lifesaver ASs to revert the previous state before the prefix hijacking attack. On detecting a prefix hijacking attack, the detection system notifies the mitigation system about the hijack, which includes the attacker AS, the victim AS, and the victim prefix.

Finally, the implementation result of this research work uses the parameters for calculating the efficiency and performance evaluation of prefix hijacking routing attack analysis and its prevention methodology in BGP such as packet loss, overhead, throughput, and packet transmission delay and packet delivery ratio. The positive results have encouraged these three proposed research techniques to find the prefix hijacking attack, ensure quality communication and eliminate the bogus routes.