CHAPTER 1

PREFIX HIJACKING ROUTING ATTACK IN BORDER GATEWAY PROTOCOL

1.1 INTRODUCTION

The internetwork architecture which is partitioned into thousands of independently administered routing domains is called Autonomous System (AS). The collection of internet routers called as Autonomous Systems (ASs) has control over the central administrative point of the internetwork. ASs varies from one organization to another. Be contingent on the organization of connection based on Internet Protocol (IP), the ASs can be classified as multi-homed, stub, transit, Internet Exchange Point (IXP), etc. These ASs use the routing protocol that are relevant to the Border Gateway Protocol (BGP) for exchanging routes to reach destination address on the internet. On the blocks, the ASs is classified as inter-domain system which connects the ASs within and between the Internet Service Providers (ISPs). These connection criteria’s of routing protocols increasingly reduce the serious security problem on the internet.

To have control over very huge organization with independent connections to multiple networks of the internetwork, the ASs relevant to BGP routing protocol is not adequate for internet access in various domains.

By being compatible with the above process, this research work gives the main idea to fulfill the above-assigned problem, which can be
resolved by using different direction and different algorithms on the routing policy by applying various routing algorithms.

The algorithm used in this research work includes multiple organizations in BGP, with the help of multiple ASs of multi-homed ASs. The large domain connection inconsistency can be resolved in whole internetwork system with the help of this research proposal. These methods lead to compromise on all other ASs such as the stub, transit, Internet Exchange Point ASs, etc.

The inherent verification mechanism of BGP is based on inter-domain routing, which is useful to reduction of routing attacks such as prefix hijacking attacking in internetwork architecture by routers on the internet. BGP is used to share routing information among the ASs.

More than one AS produced in the internet with unique AS address prefixes of Internet Protocol number. This prefixes protocol number is used to exchange network information through BGP. This process runs by using route update with the announcements of known path and withdrawals of no longer reachable prefixes on the announcements. This announcements and withdrawals of prefixes of IP were occurring easily between the source and destination network prefix.

From this consideration of address prefixes of internet protocol number, the prefix hijacking routes are indentified as one of the fake routes. This fake route created by the misconfigured routing setup by using intent malicious attacks. These attacks are classified as the following types; depending on the behavior of the address prefixes namely duplicate prefix hijacking, sub-prefix hijacking, independent-prefix hijacking and super-prefix hijacking.
In this era, BGP has some drawbacks in providing better performance or security which can guarantee scalability, slow convergence, route stability and even prefix hijacking routes in the internetworking of ASs. It does not provide integrity, authentication, confidentiality, authorization and validation of the route. To overcome the above primary security-related limitations of BGP, Route Reliability Ranking Algorithm (RRR) is used. Fast ReRoute Technique and Mitigation System are based on Route Reliability Ranking Algorithm (RRR). This is vulnerable to eavesdropping, replay, message insertion, message deletion, message modification, man-in-the-middle and Denial of Service (DoS) attacks.

Prefix hijacking is based on the behavior of nodes that are malicious or misconfigured in ASs. To express opposition and reducing complexity of prefix hijacking attack on BGP, this research work introduces following general idea inferred like Route Reliability Ranking Algorithm (RRR) to authenticate the validation of routing update records in ASs in the network. In addition, penalty based route selection mechanism is used to identify the routes of suspicious nodes in the internetwork. To achieve more reliability, efficiency as well as to handle the issues of the BGP link failure and untrustworthiness of the link of ASs routing against the Prefix Hijacking Attack, this research work can put into proposed rerouting technique (not uncommon in routing protocol which avoids network faults, routing attacks and so on) that finds an alternate link to send the data. It is used to reduce the actual link failure and produce the lowest post failure, traffic load and decrease the data packet loss. The main goal of the rerouting technique is to restore the affected communications on the ASs. When managing the above constraints and developing the effective characterization of rerouting in the whole internet, the bogus routes have arisen highly desirable profile of rerouting. To avoid this conflict, the concept of Lifesaver is introduced to completely eliminate the bogus routes. Finally, the efficient technique for
prefix hijacking attack on internet is created and the rerouting technique is used to reduce the packet loss and also increases the throughput and reverts to the previous state before the attack by proposed research work.

1.2 AN OVERVIEW OF PREFIX HIJACKING ROUTING ATTACK

IP hijacking is prefix route hijacking technique on the internet which is routed by the IP addresses. Any host is identified and connected to unique IP address in internetworking, which is useful to communicate with each host devices with the help of IP address. The data transfer communications between the routers were monitored till the packet reaches the destination in secure manner. Group communication can be done by combining multiple IP address, which is intended to interact with the router. The process of grouping IP addresses is known as prefixes. This was owned by AS and also their lists of routing information in the BGP are originated in routing tables for each transformation. ASs defines the group of networks that operates under single external routing policy. BGP is the standard routing protocol used to exchange information about the IP routing between ASs. Thus, ASs uses BGP to advertise prefixes, through which it can deliver traffic.

In this occurrence of BGP session, the attacker creates the information as same as existing one from the routing table. This was the key aspect for prefix hijacking attack in BGP. So the IP information differs from other system's IP type and a session hijacking attack may be designed between BGP peers. This route causes eavesdropping, black holing and traffic analysis. Thus, BGP attempts to add all routes received by another peer into the routing table of the devices. This type of problem can be organized by prefixes announcement from one AS to another. Thus this problem can further
affect others peer with these two providers and also can cause anonymous systems to prefer the misconfigured link.

![Diagram](image)

**Figure 1.1 IP Prefix Hijacking Routing Attack**

The concept of BGP hijacking revolves around BGP session is susceptible to prefix hijacking attack. Once an attacker is found, any prefix can overload the Internet Service Provider (ISP). The attacker for infiltration or to perform a DoS or impersonation attack on the entity whose prefix is been advertised. It is not uncommon for an attacker to cause serious outages a complete loss of connectivity.

1.3 **PROBLEM CONTEXT**

Routing has witnessed a rapid growth in the number of host system availability in the past decades. The rapid increase in the number of the host system in internetworking leads to attacker finding process to be compelling
immediate action measures to deal with the resultant AS. Large denseness of AS like BGP AS is experiencing rapid growth and suspicious attacker issues have assumed critical importance. Improvement of BGP AS framework improves the route reliability ranking, route reliability matrix and its corresponding test with consistency check method to tackle immediate problems that will be able to address this issue comprehensively.

Internetwork AS plays a central role in quality of attacker reduction and well-defined communication. In addition to this reduction, the router, BGP and its infrastructures are responsible for the progress and the development of the efficient route selection as well as for data transmission. In this research work, the importance of prefix hijacking attack reduction is having superior power and influence, because it constitutes conflict in the routing between the two successful routers.

Prefix hijacking attack is a common attack in BGP based on internetworking. It was created due to the unmatched prefix in the routing table. Sharing of data between the two routers takes place using the nearby neighbor router. It is complex to minimize the attack in this path. In BGP system, examining of Prefix Hijacking routing attack and precluding methodology can be resolved with secure routing system. This enhances the performance of an existing system and remits the interruption.

1.4 RESEARCH PROBLEM STATEMENT

In an internetwork domain, many routers are used to communicate with one another, especially in BGP. This protocol uses specific type of attack like Prefix Hijacking Attack. It causes authentication validation of a routing and avoids routes propagation by the suspicious candidates. Based on the potential route in the network, the path between routers may cause link failure and untrustworthiness of the link. When the primary link fails, the data will not be reaching to its destination, which results in congestion. It also increases
the load on the network that is possible to increase the data packet loss. This conflict between routes and attacks create the bogus routes in BGP. The prefix hijacking is raised to detect the prefix hijacking attack events location (Qiu et al. 2009), which is a very challenging one. To reduce the above conflicts and problem, none of the existing works have fulfilling scheme for reducing the attacks and route failure in internetwork domain.

1.5 OBJECTIVE OF THE RESEARCH WORK

The objectives of this research work are to bring out prefix hijacking attack which is unpleasant to internetwork, to highlight different mitigating techniques used to avoid fulfilling routing attacks, to illustrate the procedure of implementing the best security practices and to extend the practices into the network of AS. The current challenges and internal attacks will be discussed in the forthcoming chapters. The objective of this research work is to protect route transmission from intra and inter routing attacks. The investigation on prefix hijacking routing attack analysis and its prevention methodology in BGP has to be designed and implemented and should have flexible mechanisms for efficient and convenient use. Hence, design architecture goals should be considered. The prominent role of this study is to enhance the network monitoring and also to analyze process by providing a secure routing between the ASs, which is easy to interact.

The important objectives of this research work are as follows.

- Route Reliability Ranking (RRR) algorithm authenticates the validation of a routing update and also verifies the accuracy of ASs path
- Route Reliability Matrix (RRM) is used to verify the received path of checked routing update messages
Fast ReRoute Technique and Mitigation System are based on Route Reliability Ranking Algorithm (RRR).

Consistency check (CC) is performed by RRR algorithm on RRM to verify the values of a routing table.

Penalty based route selection along with reliability testing is used, so that a suspicious candidate is identified and routes are propagated by these candidates, which can be avoided.

Finally, the route with the lowest penalty value for a destination is selected as the best route based on the RRR and RRM.

Fast ReRoute (FRR) technique, which is based on both intra and inter-AS link failures protects, by avoiding unexpected BGP routing disruptions due to hot potato routing effect.

Fast ReRoute technique is used to detect the primary link failures and also to find an alternate link for the data communication.

Lifesaver is used to avoid conflicts between routes which are completely eliminating the bogus routes.

### 1.6 RESEARCH METHODOLOGY

To overcome the problems of prefix hijacking attack, detecting the suspicious candidates, link failure and untrustworthiness of the link and also attacks between peers, larger scale attacks, DoS (Biersack et al. 2012), misconfiguration attacks and its conflicts and to find the bogus route in the network communication, the route reliability ranking algorithm and penalty based route selection mechanism is used. These algorithm and mechanism are used against prefix hijacking attack. To improve the quality communication on the route without attacks, Fast ReRouting technique, which is based on
Route Reliability Ranking (RRR) algorithm, is used. A new method named Lifesaver based Mitigation System is proposed, which is more efficient to reduce prefix hijacking attack (Schlamp et al. 2012). In case if any attacks arise in BGP, the following contributions are taken into the solution of such attacks and it is efficient to defense against the attacks.

1.6.1 Route Reliability Ranking Algorithm for Prefix Hijacking Attacks in Border Gateway Protocol

In phase I contribution, many routers are used to communicate with each other especially in BGP, which has the specific type of attack like Prefix Hijacking Attack. It causes authentication and validation of a routing and avoids routes propagation by the suspicious candidates. To resolve these constraints, the Route Reliability Ranking algorithm is used to authenticate the validation of a routing. Thus, a penalty based route selection mechanism is performed to identify the suspicious candidates and avoid less propagation of routes.

1.6.2 Fast ReRoute Technique in BGP with Secure Route Reliability Testing

In phase II contribution, BGP has lot of paths between the router, which causes link failure and untrustworthiness of the link, based on the potential route in the network. When the actual link fails, the data will not be sent to its destination and hence results in congestion. It also increases the load on the network, which results in the increase of data packet loss. To resolve those constraints, the Fast ReRoute (FRR) technique is used to find and reduce the primary link failure, by finding an alternate link for the data. An alternate link is used to find the lowest post failure, traffic load across all the links into the account. ReRouting technique (Yujing Liu et al. 2013) reduces the packet loss and increases the throughput.
1.6.3 Detection and Mitigation System for Routing Attacks in BGP

In phase III, contributions are performing to avoid the attacks and conflicts between routes, which create the bogus routes in BGP (Jian Qiu et al. 2007).

**Figure 1.2 Proposed Research Methodologies**
The prefix hijacking is raised to detect the prefix hijacking attack events location, which is a very challenging one. The number of false alarm and the number of legitimate objects were misidentified. To reduce the above conflicts and problems, the following solution is proposed. The concept of Lifesaver is introduced to completely eliminate the bogus routes. It has more incentives in deploying security features for mitigation actions executed by the lifesaver.

1.6.4 Simulation Setup for Performance Evaluation

In phase IV, it describes the simulation setup for performance evaluation which discusses the performance measure of the various techniques as follows,

- Inter-Domain Packet Filters (IDPF) are used to control IP spoofing based on BGP updates
- Heterogeneous Technologies Routing (HTR) is a new access technique that uses wireless technologies with soft-state framework suitable for interconnecting devices in a heterogeneous network
- Multiprotocol BGP (MP-BGP) configuration supports IPv4 unicast, IPv4 multicast, IPv6 unicast and IPv6 multicast. MP-BGP is used for MPLS VPN where MP-BGP is used to exchange the VPN labels. For each different “address” type, MP-BGP uses a different address family
- Route Reliability Ranking (RRR) algorithm is designed to tackle the BGP vulnerabilities such as eavesdropping, replay, message insertion, message deletion, message modification, man-in-the-middle, Denial of Service attacks arise in BGP especially in prefix-hijacking attacks
- The Fast ReRoute technique (FRR) in BGP is helping to find alternate route instead of failed routes by Fast ReRoute technique in BGP with Secure Route Reliability testing

All these techniques are compared and efficient results are pointed out in the graphs with respect to the evaluation criteria such as packet delivery ratio, packet lose, packet delay, overhead and throughput that are calculated using density of nodes based on their performances.

1.7 SCOPE OF THE RESEARCH WORK

In this research area of internetworking, many methodologies produce the secure communication between the nodes through the gateway router. To make these communications effective and also to achieve the following goals in internetworking, the following techniques is been developed.

- To reduce the BGP router attack
- To overcome post link failure, traffic load and packet loss
- To overcome the Attacks between Peers, larger Scale attacks, Denial of Service and Miss configuration
- To eliminate the bogus routes on internetwork routing

1.8 RESEARCH CONTRIBUTIONS

The contributions of this research work results from the following features:

1. Well-structured framework and flow of process are given for
   - Prefix Hijacking Attacks in BGP
   - Improve Security in BGP
• Routing Attacks in BGP Detection and Mitigation

2. By using Route Reliability Ranking Algorithm, prefix hijacking attacks are removed.

3. By using Fast ReRoute Technique, the shortest route selection is performed for the best route without interruption of the external router.

4. A new Detection and Mitigation System for routing attacks in BGP achieves bogus routes elimination and the problems of peer to peer interruption, denial of service and misconfiguration can be sought out.

5. Routing security takes place in Route Reliability Ranking Algorithm and an alternate link is used for lowest post failure, traffic load and packet losses with high throughput designs, which are given against the prefix hijacking attack in internetworks.

6. The dependent physical property of three existent techniques regarding Prefix Hijacking Routing Attack Analysis and its Prevention Methodology in BGP against the prefix hijacking routing attack was studied. Depending on the quality of service requirements such as routing, packet delivery, packet delay, overhead and throughput were evaluated.

The effectiveness of rate limiting in mitigating Prefix Hijacking Routing Attack against BGP was evaluated. These efficient technique is used to remove prefix hijacking attack in Internet BGP, which reduces the packet loss (378 packets out of 10000 packets), overload (0.573 Mb/s), packet delay (0.000314 sec) and increases the packet delivery ratio (0.784667) and throughput (5.4373). It also reverts to the previous state, before the attack reflects to the fraction of affected communication (0.15867), which is
detected based on the transmission time comparing it with the Inter-Domain Packet Filters (IDPF), Heterogeneous Technologies Routing (HTR) and Multiprotocol BGP (MP-BGP) configuration.

1.9 STRUCTURE OF THE THESIS

The overall structure of the thesis is as follows. In chapter 1, the overview of prefix hijacking routing attack is defined with its problem context and statements. The scope of this thesis includes the problem statement and research methodology. In Chapter 3, 4 and 5, the proposed methodology and the contributions of this research were given. Chapter 6 discusses the performance result and contribution comparison of this work with the existing work. Finally, Chapter 7 concludes this research work with future research direction.

This thesis starts out with an introduction of prefix hijacking routing attack which is given in Chapter 1. The motivation and problem statement is defined in this chapter. The detailed description of related review of this research was discussed in Chapter 2.

Chapter 3 provides a Route Reliability Ranking Algorithm for prefix hijacking attacks in BGP. These techniques resolve the issues involved in the internetwork and also discuss about BGP routing protocol with security model.

Chapter 4 provides the Fast ReRoute technique in BGP with secure route reliability testing. This chapter describes Route Reliability Ranking Algorithm and Fast ReRoute technique for selecting the alternate link used for lowest post failure and also to reduce the traffic load, packet loss with high throughput.
**Chapter 5** is based on Detection and Mitigation System for Routing Attacks in BGP, which is based on the problem of routing in BGP networks. This problem is resolved by Lifesaver and Mitigation System.

**Chapter 6** discusses the simulation setup for performance evaluation. This chapter shows the comparison of different methods related to the BGP routing.

**Chapter 7** discusses future enhancement of this research work. Finally, the summary section encourages networking router attack to use and make further recommendation on the practices.

### 1.10 SUMMARY

This chapter deals with the introduction about the investigation on prefix hijacking routing attack analysis and its prevention methodology in BGP. Many research paradigms were discussed in this chapter. Especially the introduction and overview of prefix hijacking routing attack terminology were illustrated. The research problem context and their respective problem statement were discussed. Chapter 3 describes the objective of this research work and explains this research methodology with illustration of the proposed methodology. There are three methodologies explained in this research work namely 1.Route Reliability Ranking Algorithm for prefix hijacking attacks in BGP, 2.Fast ReRoute Technique in BGP with Secure Route Reliability testing and 3.Detection and Mitigation System for routing attacks in BGP along with simulation overview, which is described in chapter 5. The Scope of this research is given in chapter 6 and research contributions are discussed in chapter 7.