Pakistan Journal of Engineering and Technology, PakJET
Multidisciplinary | Peer Reviewed
Volume: 04, Number: 01, Pages: 97- 105, Year: 2021

PHDS: IP Prefix Hijack Detection System

Muhammad Usman Ghani[1], Akmal Khan[2], Shabir Hussain[3], M. Zeeshan Jhandir[2], Rafaqat Kazmi[2], Imran Sarwar Bajwa[2]

[1]National College of Business Administration & Economics Rahim Yar Khan
[2]Department of Computer Science, The Islamia University of Bahawalpur, Pakistan
[3]School of Information Engineering, Zhengzhou University, Henan, China

Corresponding author: Akmal Khan (e-mail: akmal.shahbaz@iub.edu.pk).

Abstract- **Border Gateway Protocol (BGP) is the routing protocol for routing information between autonomous systems (AS) on the Internet. Back in 1989, BGP was not developed with a security perspective. Therefore, there are many security concerns regarding BGP, and it is highly vulnerable to malicious attacks. Due to rapid development in Internet technology, the Internet is filled with malicious users. It is not challenging to hijack someone's address space and use it for malicious activities such as denial-of-service attacks (DoS attacks) and spamming. Our aim behind this research work is to figure out and discuss all the techniques regarding BGP prefix hijacking and design a system that can be used to detect IP prefix hijacking attacks and facilitates mitigation. In this type of hijack attack, to avoid Multiple Origin AS (MOAS) conflicts, the attacker announces a hijacked prefix with AS number belongs to victim AS; this creates the illusion that BGP speaker has a direct connection with victim AS. To accurately detect IP prefix hijack attacks, we design a system called Prefix Hijack Detection System (PHDS). To test our system, we have collected all the Autonomous Systems (ASes) of Pakistan and their prefixes using RIPEstat API. PHDS collect BGP updates for every prefix using RIPEstat API. To monitor all 5,845 prefixes of Pakistan, we have collected 3.35 million BGP updates; all this data is collected from November 03, 2018, to November 20, 2018. We have monitored these prefixes through PHDS and found our system correctly detecting all types of IP prefix hijacks. Therefore, this system is useful for early detection of IP prefix hijack attacks. PHDS detects 47,223 malicious updates out of 3.35 million BGP updates. PHDS detected 983 unique IP prefix hijack attacks from 47,223 malicious updates. Hijack, a prefix, and it's AS is the most common type of attack; PHDS detected 983 prefix hijack attacks, and out of these, 898 are hijacked a prefix, and its AS**.

***Index Terms*—**Border gateway protocol (BGP), autonomous system (AS), internet protocol (IP) prefix.

I. INTRODUCTION

BGP is the primary routing protocol that is used for routing information through the backbone of the Internet. With BGP's help, various Internet Service Providers (ISPs) and organizations communicate effectively in a cost-efficient manner. However, back in 1989, BGP was not developed with a security perspective [2]. Due to a lack of security measures, BGP is highly vulnerable to malicious attacks. The rapid development in Internet technology and network applications leads to serious concerns about the data's security and privacy transferred over the Internet. It is not tricky to hijack someone's IP address space and use it for malicious purposes, such as DoS attacks or spamming.

A BGP hijack can be described as stealing IP address space or even Autonomous System Number (ASN) that belongs to some other network. To accomplish the BGP hijack attack, attackers advertise hijacked address space to neighboring routers from the network they control to send and receive information through stolen address space [3]. Attackers can use hijacked address space to conduct malicious activities such as denial-of-service attacks (DoS attacks) and spamming without disclosing their identity. The unintentional network misconfiguration is another reason due to which BGP prefix hijacking can also occur.

In this research work, we described all types of IP prefix hijacking attacks and designed a Prefix Hijack Detection System (PHDS) system for accurate early detection of prefix hijacking attacks. To test the working of PHDS, we have monitored all the prefixes of Pakistan. PHDS has accurately detected all types of prefix hijack attacks.

II. BACKGROUND

A. AUTONOMOUS SYSTEM (AS)

The collection of routers under a single administrative authority is called an Autonomous System(AS). Each AS has a unique number. Autonomous System uses interior gateway protocol (IGP) to determine the route on which packet is transferred within the AS, and uses an inter-AS routing protocol to determine which packet is transferred to other Autonomous Systems [2]. An Autonomous System globally unique number is called Autonomous System Number (ASN); this number is used to identify AS in the world uniquely and transfer the exterior routing information between Autonomous Systems (ASes)

Internet Assigned Numbers Authority (IANA) authority assigns Autonomous System Number (ASN) to Autonomous Systems (ASes). AS numbers with Internet-wide scope and

available range from 1 to 64511, each number should be assigned to a single Autonomous System. Only public AS numbers can appear in the BGP update message advertised by the BGP speaker in the AS-PATH attribute of the BGP advertised message. Autonomous System does not require a unique AS number if connected to a single upstream network provider responsible for this ASN's connectivity to other networks. In this case, AS can be assigned a private AS number, which is in the range of 64512 to 65535 for communication with its provider through the Border Gateway Protocol (BGP). The provider's router is responsible for the advertisement of BGP routes on behalf of AS that have assigned a private AS number. The service provider doesn't include a private AS number in the path. In this way, the service provider uses the same AS number for its customers [4].

B. CLASSLESS INTER-DOMAIN ROUTING (CIDR)

As the Internet has evolved and overgrown in the last couple of decades and faces several scaling problems, including the exhaustion of the address space of class B network and the routing table's size increases so significantly that it was difficult for hardware, software, and people to manage it effectively [5]. Classless Inter-Domain Routing (CIDR) was designed and deployed to solve these major problems. CIDR provides a mechanism that can reduce the consumption rate of IPv4 address space and slow down global routing tables' growth. In CIDR notation, a block of IP addresses is called prefix consisting of two groups of bits; most significant bits are used to identify a network or a sub-network (subnet), and the least significant bits are used as host identifier. An IPv4 address in CIDR notation looks like 145.92.0.0/16, "/16" indicates 16 most significant bits are used to identify network and least 16 bits used as host identifier. A subnet is a small portion of a specific prefix; for example, 192.168.74.12/26 is a subnet from prefix 192.148.0.0/16.

C. C. BGP SECURITY ISSUES

Back in 1989, BGP was not developed with a security perspective. Therefore, there are many security concerns regarding BGP, and it is highly vulnerable to malicious attacks. It is not tricky to hijack someone's IP address space and use it for malicious purposes, such as DoS attacks or spamming. There are several reasons why BGP is highly vulnerable to malicious attacks cite{butler2010survey}.

- BGP requires peering between different Autonomous Systems (ASes) to deliver routing information between different administrative domains. By default, there is no authentication mechanism used between peeringrouters.
- By default, BGP not performs any verification on receiving prefix announcements from the peering router. Moreover, BGP does not verify that the advertised prefix is owned by the advertiser or not.
- By default, no validation was performed on the received prefix information. The original prefix advertisement can be easily disrupted by changing the path attribute of the received prefix.

D. PREFIX HIJACKING

BGP prefix hijacking occurs when a BGP speaker claims a prefix or sub-prefix from address space; some other AS. Attackers hijack prefixes to perform malicious activities such as denial of service (DoS) attacks and spamming [6]. An Autonomous System (AS) can advertise prefix from some other AS address space, this action known as prefix hijacking. Neighboring Autonomous Systems that receive this announcement might select the announced route as the shortest route and start directing traffic towards the wrong AS. This announcement might propagate through the entire routing system as BGP doesn't perform any validation [4].

a) PREFIX HIJACKING TYPES

IP prefix hijacking can be categorized into five types; for these five types of IP prefix hijacking attacks, we used the following terms to refer to these attacks.

b) HIJACK A PREFIX

In this type of hijack attack, the BGP speaker announces a prefix that belongs to another AS address space.

c) HIJACK, A SUB-PREFIX

In this type of attack, the BGP speaker announces a sub-prefix from some other AS address space. The most widely propagated type of attack because the BGP speaker selects a more specific route.

d) HIJACK, A PREFIX AND ITS AS

In this type of hijack attack, to avoid MOAS conflicts attacker announce the hijacked prefix with AS number belongs to the victim AS; this creates the illusion the BGP speaker has a direct connection with the victim AS.

e) HIJACK, A SUBNET AND ITS AS

In this type of attack, the attacker announces a prefix sub-prefix with AS number that belongs to victim AS. The detection of this type of attack is the most difficult.

f) SUPERNET HIJACK

In this type of hijack attack, the BGP speaker announces a larger prefix of a prefix that belongs to another AS address space.

E. BGP MISCONFIGURATION

The unintentional misconfiguration of BGP speakers by network operators is another reason due to which IP prefix hijacking can also occur. If misconfigured BGP speakers start announcing used prefixes, this causes IP prefix hijacking because they belong to the address space of some other AS. If misconfigured BGP speaker starts announcing unused prefixes, this caused by leaked routes, this might cause blackhole to some other ASes. For example, in 2008, Pakistani Telecom accidentally started to announce a subnet of prefix owned by YouTube and started causing availability issues for YouTube all over the world [7]. In another incident, one of the major ISP in Turkey, Turk

Telekom, accidentally hijacked the IP address of some popular DNS to censor twitter.com in response to orders from the government [8].

Some tools have been developed to help network operators resolve faults due to BGP misconfiguration, such as BGP Visibility Scanner [9] and router configuration checker [10]. The Configuration of BGP policies is complicated because network operators consider many factors, such as traffic engineering, scalability, business relationships, and security-related policy [11]. BGP misconfiguration can be categories into export misconfiguration and origin misconfiguration. Export misconfiguration occurs when network operators accidentally configure BGP policies to block some legitimate routes, creating the DoS situation for blocked prefixes. Origin misconfiguration occurs when a misconfigured BGP speaker starts announcing prefixes that belong to the address space of some other AS. These two types of misconfiguration have different effects; due to origin misconfiguration, significantly dangerous fluctuations in BGP routes can occur, and export misconfiguration can create problems in BGP routing convergence.

F. BGP DATA SOURCES

IP prefix hijacking detection techniques used various types of BGP data sources to detect IP prefix hijack. Different data sources are: route registries database, BGP raw data, and some other type BGP data sources are also available [12]. Different BGP features are derived from these data sources, which can be useful for detecting prefix hijack. BGP raw data can be classified into two types: the control plane and data plane. Control plane information includes BGP update message exchange between BGP routers, and data plane information is collected from the live host is monitored network [13]. Two well-known repositories from where Control plane data can be freely downloaded are Reseaux IP Europeens (RIPE) Network Coordinate Centre (NCC) [14] and RouteViews project [15]. RouteViews project provides a BGP routing table every 2 hours and BGP updates every 15 minutes. RIPE provides a BGP routing table every 8 hours and BGP updates every 5 minutes. RIPE and RouteViews repositories provide data in MRT (Multi-Threaded Routing Toolkit) format, which is not human readable. Different tools are available to convert it to a human-readable format, such as a bgpdump and pybgpdump.

Both the control plane and data plane information have advantages and disadvantages. IP prefix hijack detection techniques such as [16], [17] that uses control plane information are scalable and easy to deploy but can be inaccurate. While prefix hijack detection techniques such as [18], [19] that use data plane information are more accurate in detection but not scalable. Techniques such as [20], [21], [13] that used both control plane and data plane information are more accurate, but they are challenging to deploy. Internet Routing Registry (IRR) is a distributed database established to share routing-related information between network operators. Autonomous systems (ASes) store their routing policies in the IRR database. These routing policies are expressed in Routing Policy Specification Language (RPSL). Internet Routing Registry database provides information that can configure backbone routers, debug routing problems, and address and engineer Internet routing. Information in the IRR database is used in many research works to validate the BGP update's origin. Other sources of BGP Data that can be helpful in IP prefix hijack detection techniques include bogon prefixes and IP geolocation Databases. Bogon prefixes is a list of IP addresses reserved by IANA or within private address space [22] or not allocated by any RIRs; these IP addresses should not appear on the Internet. Bogon prefixes list is not static; IP addresses are added and removed to this list regularly.

Some sources published regularly updated the Bogon prefixes list, such as the CIDR report, which provides a daily updated list of bogon prefixes based on the RIR stats files, RIR whois data, and IANA registry files. ISP should have a mechanism to filter bogon prefixes. IP geolocation database provides the facility to map an IP address to its geolocation. Looking glasses, another BGP data source that can provide valuable information for the detection of prefix hijack. Almost 200 looking glass servers are available on the Internet that provides information related to backbone routing.

G. CONTRIBUTIONS

In this research work, we designed a system called Prefix Hijack Detection System (PHDS).

- To test the working of PHDS, we have collected all the Autonomous Systems of Pakistan and their prefix using RIPEstat API [1].
- To monitor all 5,845 prefixes of Pakistan through PHDS, we have collected 3.35 million BGP updates using RIPEstat API [1], processed all these updates by PHDS, and found PHDS correctly detecting all type of prefix hijacks attacks. PHDS detected 983 unique prefix hijack attacks from 47,223 malicious updates.
- Analysis performed on the detected hijacks reveals some interesting points are: PHDS detected 983 prefix hijack attacks, and out of these, 898 are (Hijack a prefix and its AS) attacks, and none of Autonomous System belongs to Pakistan, which is involved in this type of attack.
- Prefix Hijack Detection System (PHDS) provides the solution for the detection of possible prefix hijack attacks for both IPv4 and IPv6.

III. RELATED WORK

Different methods for prefix hijack alert can monitor the Border Gateway Protocol. Some solutions use control-plane information to detect IP prefix hijack, such as ARTEMIS [23], which uses control plane information to detect IP prefix hijack attacks. Other solutions use data-plane information for the detection of IP prefix hijack. Control plane information can be obtained through the BGP feed. Some existing tools used both control-planes and data-plane information for the detection of prefix hijack.

The method used by [24] uses control-plane information for prefix hijack detection and also utilizes data-plane information to verify the validity of suspected hijack. Different commercial web

services are available for monitoring of BGP prefix. For example BGPmon [25] and Dyn.com [26]. These web services don't provide the details of the methods they used to monitor prefixes.
Several methods are proposed for the detection of IP prefix hijack [3], [24], [27], [13] Xingang Shi et al. [20] propose an agile system named Argus for the detection of prefix hijack and for identification of the reason that causes route anomaly. Argus's concept is based on the control and data plane information collected by monitoring the Internet for more than one year.

They have identified 40k route anomalies during analysis. According to their findings, a more specific route is hijacked more frequently, and almost 20% of hijacking attacks last less than ten minutes. Some hijacking attacks propagate 90% of the Internet in less than two minutes. Argus uses both control and data plane information to detect prefix hijack attacks, which caused Argus to face scalability problems because a solution that uses data plane information is not scale-able.

A solution proposed by Hu et al. [3] uses both control-plane and data-plane information to improve the detection accuracy of prefix hijacking attacks. Their solution used control-plane information detection of prefix hijack; when hijack is detected, the algorithm uses data-plane information to validate hijack. However, this solution is not scalable because it needs a live client in monitored prefix and in-network that hijack the prefix. The solution proposed by Zheng et al. [24] utilizes data-plane information for the detection of IP prefix hijack. They place multiple monitoring nodes on a path that is traversed to AS. They collect information from monitoring nodes to detect prefix hijacking. However, the proposed solution is hardly scalable because the algorithm used data-plane information to detect prefix hijack.

BGP is the primary inter-domain routing protocol that is used to share Network Reachability Information between ASes. BGP prefix hijacking is one of the major concerns for both network operators and users. Several solutions and modifications to BGP have been proposed to protect the Internet against prefix hijacking. However, most network operators are reluctant to deploy these techniques [28]. Network operators often use proactive techniques to decrease prefix hijacking or use third-party services to detect prefix hijacking attacks.

To secure inter-domain routing, IETF introduces Resource Publication Infrastructure (RPKI). It provides the facility to identify the legitimate owner of the IP address space. However, according to Yossi Gilad et al. [29], the deployment of RPKI is limited. Most network operators have not deployed RPKI in their networks as a proactive technique against prefix hijacking. The reason for less deployment RPKI is, it increases cost, complexity, and processing overhead.

The solution proposed by M Lad et al. [17], namely Prefix Hijack Alert System (PHAS), is one of the earliest methods that provide actual implementations. They have collected BGP routing data from RIPE RIS and RouteViews project and examine this routing data to detect prefix hijack. They have maintained an origin set for monitored prefix; when a new origin associated with the monitored prefix is identified, a notification alert is sent to the prefix owner.

The owner then verifies the notification, whether it is a routine topology change or a hijack; if it is a hijack, the owner takes appropriate action to mitigate this hijack attack. However, their solution suffers from many false positives because using control-plane data makes it very difficult to distinguish whether MOAS conflict is legitimate or not [30] PHAS is also suffering from detection delays critical for mitigation of prefix hijack attempts.

Chaviaras et al. [31] proposed a tool named Automatic and Real-Time Detection and Mitigation System (ARTEMIS); network administrators can use ARTEMIS to detect and mitigate prefix hijacking attacks for prefix they own. ARTEMIS consists of three major components, which are detection, mitigation, and monitoring service. Detection service runs continuously for detection prefix hijack attack and collect real-time BGP data from Looking Glass (LG) servers, RIPE RIS [1], and BGPmon [32] projects.

ARTEMIS uses a mitigation service when prefix hijack is detected; this service announces the hijacked prefix sub-prefix. However, this requires permission must be granted to ARTEMIS for the advertisement of owned prefixes. ARTEMIS runs monitoring service parallel with mitigation service to monitor the mitigation process. ARTEMIS [23] 's main idea is to design a system that individual network operators can use to monitor their prefix against possible prefix hijack attacks. However, if the detection system is designed to monitor more than one Autonomous System prefixes, it gives more details to detect prefix hijack attacks and the reason behind these prefix hijack attacks.

For the early and accurate detection of all possible IP prefix hijack attacks, we design a system called Prefix Hijack Detection System (PHDS). To test our system, we have collected all the Autonomous Systems of Pakistan and their prefix using RIPEstat API [1]. PHDS collect BGP updates for every prefix using RIPEstat API [1]. To monitor all 5,845 prefixes of Pakistan, we have collected 3.35 million BGP updates; all this data is collected from November 03, 2018, to November 20, 2018. We have monitored these prefixes through PHDS and found PHDS correctly detecting all types of prefix hijacks attacks. PHDS detects 47,223 malicious updates out of 3.35 million BGP updates. PHDS detected 983 unique IP prefix hijack attacks from 47,223 malicious updates. Therefore this system is useful for early detection of IP prefix hijack attacks.

MOAS conflicts occurred if more than one autonomous system advertise the same prefix. Zhao et al. [33], First introduce the term MOAS and provide several reasons for MOAS other than network misconfiguration and hijacking attacks. Accuracy of the methods that use control-plane information to detect prefix hijack is degraded when Multiple Origin AS conflicts occur [24]. It is difficult to differentiate between prefix hijack and legitimate MOAS conflict, as the change of origin is observed in both cases.
Identification of MOAS conflicts plays a vital role in the detection of prefix hijack. MOAS conflicts are caused by multihoming or misconfiguration. To avoid valid MOAS

conflicts, PHDS get geolocation of upstream update providers using RIPEstat API [1] (Geolocation). This geolocation information is compared with geolocation of monitored prefix origin if corresponding geolocation information is matched. Then the update is considered valid.

IV. ARCHITECTURE OF PHDS

We build a web-based application called Prefix Hijack Detection System (PHDS) to monitor IP prefixes and detect IP prefix hijack attacks. The architecture of the PHDS is given in FIGURE 1. When a new prefix is added to PHDS for prefix hijack detection, all the prefix's valid information is collected using RIPEstat API [1]. This information includes the authorized origin AS of prefix, country code, upstream AS, and valid AS-PATHs. RIPEstat API [1] (RIS Peerings) is used to collect the information about the routes originated for a given prefix. This API provides the city or country name of the monitored prefix and provides latitude and longitude. RIPEstat API [1] (Looking Glass) is also used to collect the information about the routes originated for the given prefix; this API provides information from Looking Glass. RIPEstat API [1] (Geolocation) is used to collect the information about a given prefix's geolocation. The information provided by this API is based on GeoLite data created by MaxMind [34].

To monitor prefixes, a module of PHDS is running continuously; this module collects BGP update using RIPEstat API [1] for each prefix added to the database of PHDS. Every prefix included in the BGP update message is processed by the PHDS algorithm to check whether the update is valid. If the prefix update message is found malicious, then a hijack alert is raised, and corresponding information is stored in the database.

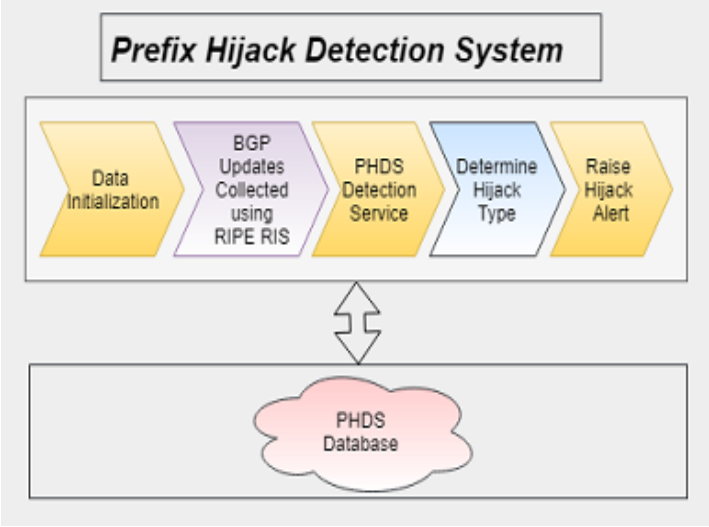

FIGURE 1. ARCHITECTURE OF PREFIX HIJACK DETECTION SYSTEM

A. ALGORITHM OF PHDS

In this section, we described the algorithm that PHDS uses for the detection of prefix hijack attacks. The pseudo of the PHDS algorithm is given below. For every prefix PHDS algorithm fetch BGP update using RIPEstat API [1] (BGP Updates). This API returns a BGP update for given prefixes that are observed over a certain period. When BGP updates are fetched, each update is checked, whether its announcement or withdrawal.

a) ANNOUNCEMENTS

If the BGP update that is fetched is an announcement, then origin AS information is getting from the update, and it is searched in the database for a match with an authorized origin AS of monitored prefix. If update origin is equal to monitored prefix origin, then AS-PATH of the update is search for a match with monitor prefix valid AS-PATH in origins_table. If corresponding AS-PATH matches, then the update is considered valid and advertised by authorized origin AS. Anyhow this announcement might be caused by cancel hijack because the BGP speaker only announces preferred routes or when a preferred route is invalidated.

Therefore hijacks_table is searched for any entry related to monitored prefix; if any entry exists, it marked clear; if no entry exists in hijacks_table update is discarded. If AS-PATH of and monitor prefix didn't match then upstream providers of update and monitored prefix is compared if corresponding upstream provider matched update is considered valid and hijacks_table is searched for any entry related to monitored prefix if any entry exists, it marked clear, if no entry exists in hijacks_table then update discarded.

Algorithm 1 Prefix Hijack Detection Algorithm

```
For every prefix
fetch update
        if (update_type = announcement) then
            if (update_origin = prefix_origin) then
        if (update_as_path = origin_as_path)
        then
        checkHijackedEntry()
    else
        if (update_upstream = prefix_upstream)
        then

        checkHijackedEntry()
        else
        Update_geolocation=get update upstream AS
        geolocation
        if (Update_geolocation = Origin_geolocation)
        then
                                checkHijackedEntry()
    else
        checkHijackType(prefix)
        addHijackAlertInfo()
    else
        AS_IRR=get lates IRR records of prefix
                                if (AS_IRR = Update_ASN)
        then
              update origin information of AS in
                                        database
    else
        checkHijackType(prefix)
```

```
            addHijackAlertInfo()
else if     (update_type = withdrawal)
            then
            For every entry in hijacks_table related
            to prefix
            clearHijack(prefix)
  else
            discard(update)
```

If corresponding upstream providers don't match, this might be occurred due to the announcement of legitimate AS from an upstream that might never be observed before. This might be due to legitimate MOAS conflict. PHDS get geolocation of upstream update provider by using RIPEstat API [1] (Geolocation). This geolocation information is compared with geolocation of monitored prefix origin if corresponding geolocation information is matched. The update is considered valid, and hijacks_table is searched for any entry related to monitored prefix; if any entry exists, it is marked explicit that no entry exists in hijacks_table update is discarded. If corresponding geolocation information doesn't match, then PHDS check prefix hijack type and hijack alert is raised. If update origin is not equal to monitored prefix origin, this might be due to the transfer of monitored prefix to another Autonomous System. PHDS uses RIPEstat API [1], which gets the latest IRR records to verify this. If the origin Autonomous System number in the update is equal to origin AS in update, then origin information is updated in the database. If corresponding information doesn't match, then the PHDS check prefix hijack type and hijack alert is raised.

b) WITHDRAWALS

If the BGP update that is fetched for the monitored prefix is found to be withdrawal, then PHDS checks hijack _table for hijacks that are related to monitored prefix; if any entry exists, it is marked clearly if no hijack found update is discarded.

B. DATA INITIALIZATION

During the initialization phase, all the required data is collected by using RIPEstat API [1] PHDS is first loaded with all the Autonomous Systems (ASes) of Pakistan. In Pakistan, there are 113 routed Autonomous System, and 45 are non_routed. After that PHDS collect all the announce prefix for each Autonomous System using RIPEstat API [1] 5,845 prefixes are announced by Pakistan routed Autonomous Systems.

C. AS TOPOLOGY OF PAKISTAN

To draw the AS topology of all the Autonomous Systems of Pakistan, we have drawn a graph between Origin ASes and Upstream ASes, as shown in FIGURE 2. As shown in FIGURE 2, AS17557 (PKTELECOM-AS-PK Pakistan Telecommunication Company Limited) has more connection with other ASes than by any other AS, and AS38193 (TWA-AS-AP Transworld Associates (Pvt.) Ltd.) is a second number that has more connection with other ASes.

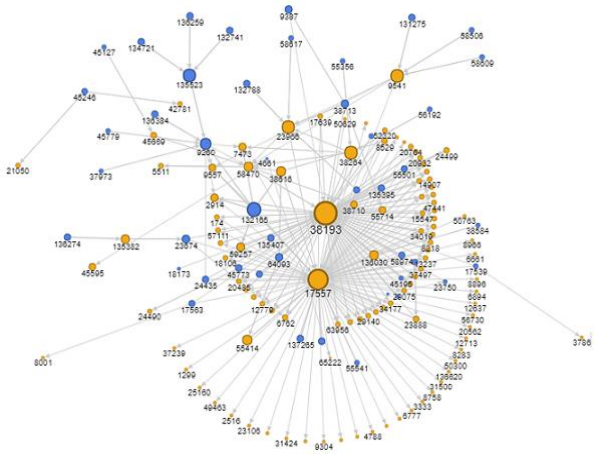

FIGURE 2: AS TOPOLOGY OF PAKISTAN AUTONOMOUS SYSTEMS

D. BGP UPDATE COLLECTION

For the prefixes entered in Prefix Hijack Detection System (PHDS) to monitor against possible prefix hijack attacks, PHDS collects BGP updates for every prefix using RIPEstat API [1]. To monitor all 5,845 prefixes of Pakistan, we have collected 3.35 million BGP updates. PHDS process every update to check whether the update is announced by authorized AS or not and verifies the AS-PATH containing an update message. If update message contains valid information, then PHDS discard that update, and if the update is found malicious, then PHDS determine the type of the prefix hijack and store all the details regarding prefix hijack in the database and raise the alert.

E. MALICIOUS UPDATES DETECTED BY PHDS

To test the working of the Prefix Hijack Detection System (PHDS), we have processed all the 3.35 million BGP updates by PHDS collected for 5,845 prefixes of Pakistan. During the detection process that is performed by PHDS, as shown in Table 1, we have found 47,223 malicious updates out of 3.35 million BGP updates. A graph is drawn between malicious updates and ASNs from which these updates are originated. As shown in FIGURE 3 large portion of malicious updates are from AS38713 (CONNECT2B-AS-PK Broadband ISP), AS38710 (WORLDCALL-AS-LHR World call Broadband Limited) is the second leading contributor to these malicious updates, and AS17557 (PKTELECOM-AS-PK Pakistan Telecommunication Company Limited) is the third main contributor to these malicious updates and. A large number of malicious updates from these three Autonomous Systems might be due to misconfiguration.

TABLE 1
TOTAL BGP UPDATES PROCESSED BY PHDS

NO. OF Prefixes Monitored	BGP Updates Processed	Malicious Update Found
113	3.35(million)	47,223

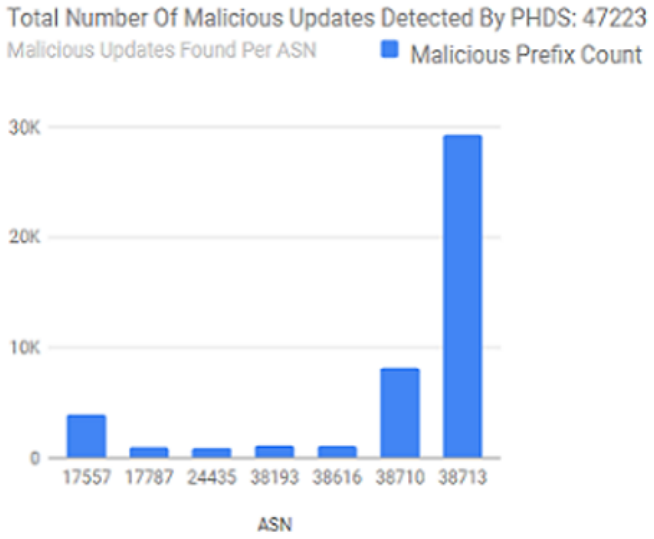

FIGURE 3. MALICIOUS UPDATES DETECTED BY PHDS

F. HIJACKS DETECTED BY PHDS

PHDS detected 983 unique prefix hijack attacks from 47,223 malicious updates. AS shown in FIGURE 4, these 983 unique attacks include Hijack Prefix, Hijack a prefix, and its AS and Supernet Hijack attacks.

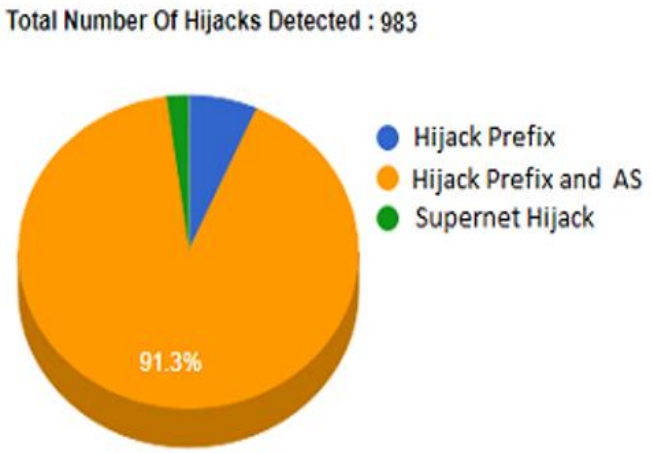

FIGURE 4. PREFIX HIJACKS DETECTED BY PHDS

a) HIJACK PREFIX

In this type of hijack attack, the BGP speaker announces a prefix that belongs to the address space of another AS. PHDS detects 983 unique attacks and out of which 65 are detected as Hijack Prefix attack. As shown in FIGURE 5, AS38710 (WORLDCALL-AS-LHR World call Broadband Limited) is involved in 43% of attacks. AS38713 (CONNECT2B-AS-PK Broadband ISP) is the second major contributor; it involved 26.2% of attacks, and AS23456 (AS_TRANS reserved by RFC6793) is involved in 13.8% of attacks.

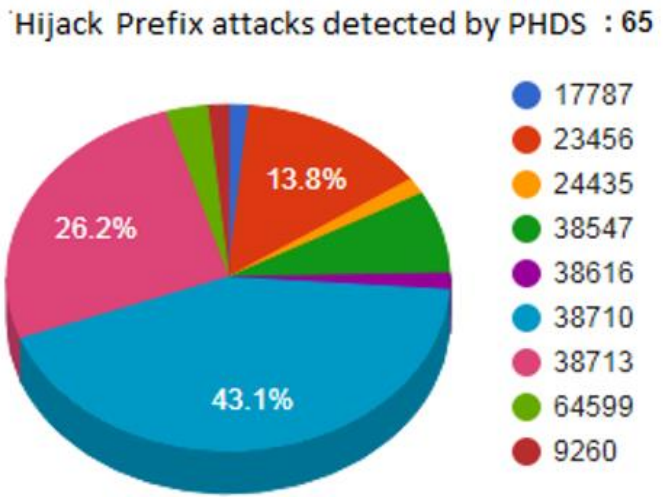

FIGURE 5. HIJACK PREFIX ATTACKS DETECTED BY PHDS UNITS FOR MAGNETIC PROPERTIES

b) HIJACK A PREFIX AND ITS AS

In this type of hijack attack, to avoid Multiple Origin AS (MOAS) conflicts attacker announces hijacked prefix with AS number belongs to victim AS; this creates the illusion that the BGP speaker has a direct connection with victim AS. PHDS detected 983 prefix hijack attacks, and out of these, 898 are of this type of attack, as shown in FIGURE 6. None of the Autonomous System belongs to Pakistan that is involved in this type of attack. In this type of attack, to avoid valid MOAS, the PHDS detection algorithm compares the country code of authorized ASN and upstream AS found in a malicious update; if both matched, the update is considered valid otherwise update considered a hijack.

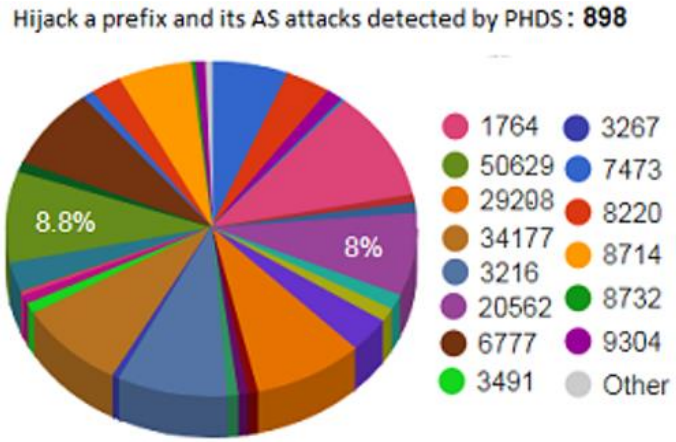

FIGURE 6. HIJACK, A PREFIX AND ITS AS ATTACKS DETECTED BY PHDS

c) SUPERNET HIJACK

In this type of hijack attack, the BGP speaker announces a larger prefix of a prefix belonging to the address space of another AS. PHDS detected 983 prefix hijack attacks; these 20 are supernet hijack attacks as shown in FIGURE 7.

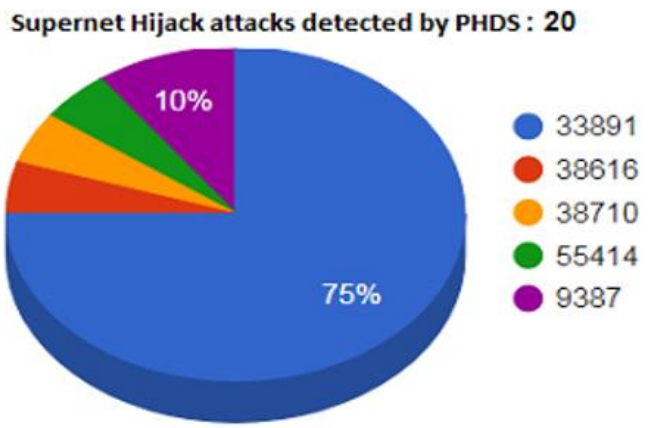

FIGURE 7. SUPERNET HIJACK ATTACKS DETECTED BY PHDS

d) HIJACK SUB-PREFIX OF A PREFIX

In this type of attack, the BGP speaker announces a sub-prefix from some other AS address space. This is the most widely propagated type of attack because BGP speakers select a more specific route. To test the working of PHDS for this type of attack, we feed a malicious update that contains this type of attack and process this update by PHDS and found system detection this type of attack successfully.

e) HIJACK A SUBNET AND ITS AS

In this type of attack, the attacker announces the prefix's sub-prefix with AS number that belongs to the victim AS. To test the working of PHDS for this type of attack, we feed a malicious update that contains this type of attack and process this update by PHDS and found a system detecting this type of attack successfully.

V. CONCLUSION

Border Gateway Protocol (BGP) is the primary routing protocol used for routing information between Autonomous Systems (ASes) on the Internet. Back in 1989, BGP was not developed with a security perspective. Therefore, there are many security concerns regarding BGP, and it is highly vulnerable to malicious attacks. Due to rapid development in Internet technology, the Internet is filled with malicious users. It is not challenging to hijack someone address space and use it for malicious activities such as denial-of-service attacks (DoS attacks) and spamming. Therefore, an accurate detection system is required that can be used for early detection of prefix hijacking attacks and to facilitate mitigation.

In this research work, we design a system called Prefix Hijack Detection System (PHDS). To test the working of PHDS, we have collected all the Autonomous Systems of Pakistan and their prefix using RIPEstat API [1]. To monitor all 5,845 prefixes of Pakistan through PHDS, we have collected 3.35 million BGP updates using RIPEstat API [1], processed all these updates by PHDS, and found PHDS correctly detecting all type of prefix hijacks attacks. PHDS detected 983 unique prefix hijack attacks from 47,223 malicious updates. Analysis performed on the detected hijacks reveals some interesting points are: PHDS detected 983 prefix hijack attacks, and out of these, 898 are (Hijack a prefix and its AS) attacks, and none of Autonomous System belongs to Pakistan, which is involved in this type of attack. Therefore, Prefix Hijack Detection System (PHDS) provides the solution for the detection of possible prefix hijack attacks for both IPv4 and IPv6.

VI. FUTURE WORK

The data that is processed by the Prefix Hijack Detection System for the detection of possible hijack attacks are collected for the prefixes of Pakistan using RIPEstat API [1]. But other information sources such as Route Views and Looking Glass Servers are also available, which can also be used to detect prefix hijack attacks. Looking at Glass can provide valuable information that can be used for accurate detection of prefix hijacks attacks; we leave these information sources for future work.

REFERENCES

[1] Khan, Muhammad Nasir, Syed K. Hasnain, and Mohsin Jamil. Digital Signal Processing: A Breadth-first Approach. Stylus Publishing, LLC, 2016.
[2] Weitz, Konstantin, Doug Woos, Emina Torlak, Michael D. Ernst, Arvind Krishnamurthy, and Zachary Tatlock. "Scalable verification of border gateway protocol configurations with an SMT solver." In Proceedings of the 2016 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications, pp. 765-780. 2016.
[3] Hu, Xin, and Z. Morley Mao. "Accurate real-time identification of IP prefix hijacking." In 2007 IEEE Symposium on Security and Privacy (SP'07), pp. 3-17. IEEE, 2007.
[4] Butler K, Farley TR, McDaniel P, Rexford J. A survey of BGP security issues and solutions. Proceedings of the IEEE 2010.
[5] Fuller V, Li T. Classless inter-domain routing (CIDR): The Internet address assignment and aggregation plan. 2006.
[6] Ballani, Hitesh, Paul Francis, and Xinyang Zhang. "A study of prefix hijacking and interception in the Internet." ACM SIGCOMM Computer Communication Review 37, no. 4 (2007): 265-276.
[7] Hijacking Y. A RIPE NCC RIS case study. 2008.
[8] Toonk A. Turkey Hijacking IP addresses for popular Global DNS providers. 2014.
[9] Lutu A, Bagnulo M, Maennel O. The BGP visibility scanner. In: IEEE. ; 2013.
[10] Feamster N, Balakrishnan H. Detecting BGP configuration faults with static analysis. In: USENIX Association. ; 2005.
[11] Caesar, Matthew, and Jennifer Rexford. "BGP routing policies in ISP networks." IEEE network vol. 19, no. 6 pp. 5-11, 2005.
[12] Sriram K, Borchert O, Kim O, Gleichmann P, Montgomery D. A comparative analysis of BGP anomaly detection androbustness algorithms. In: IEEE. ; 2009.
[13] Biersack E, Jacquemart Q, Fischer F, et al. Visual analytics for BGP monitoring and prefix hijacking identification. IEEE Network, vol. 26, no. 6, 2012.
[14] Réseaux I. Européens-Network Coordination Center (RIPE-NCC). URL: http://www. ripe. net/.
[15] RouteViews O. University of Oregon RouteViews project. Eugene, OR. [Online]. Available: http://www. routeviews. org.
[16] Chi YJ, Oliveira R, Zhang L. Cyclops: the AS-level connectivity observatory. ACM SIGCOMM Computer Communication Review 2008; 38(5).
[17] Lad M, Massey D, Pei D, Wu Y, Zhang B, Zhang L. PHAS: A Prefix Hijack Alert System.. In: 1. 2006.
[18] Zhang Z, Zhang Y, Hu YC, Mao ZM, Bush R. iSPY: Detecting IP prefix hijacking on my own. IEEE/ACM Transactions on Networking (TON), vol. 18, n0. 6, pp. 1815-1829, 2010.

[19] Fischer F, Fuchs J, Vervier PA, Mansmann F, Thonnard O. Vistracer: a visual analytics tool to investigate routing anomalies in traceroutes. In: ACM. ; 2012.
[20] Shi X, Xiang Y, Wang Z, Yin X, Wu J. Detecting prefix hijackings in the Internet with Argus. In: ACM. ; 2012.
[21] Schlamp J, Carle G, Biersack EW. A forensic case study on as hijacking: the attacker's perspective. ACM SIGCOMM Computer Communication Review 2013; 43(2).
[22] Cotton M, Vegoda L, Bonica R, Haberman B. Special-purpose IP address registries. tech. rep., 2013.
[23] Sermpezis P, Kotronis V, Gigis P, et al. ARTEMIS: Neutralizing BGP hijacking within a minute. IEEE/ACM Transactions
[24] Zheng C, Ji L, Pei D, Wang J, Francis P. A light-weight distributed scheme for detecting IP prefix hijacks in real-time. In: .37. ACM. ; 2007.
[25] bgpmon.net (bgp monitoring service). http://www.bgpmon.net/Accessed: 25-09-2018.
[26] Dyn.com/renesys (bgp monitoring service). http://dyn.com.Accessed: 25-08-2018.
[27] Park JH, Jen D, Lad M, Amante S, McPherson D, Zhang L. Investigating occurrence of duplicate updates in BGPannouncements. In: Springer. ; 2010.
[28] Sermpezis P, Kotronis V, Dainotti A, Dimitropoulos X. A Survey among Network Operators on BGP Prefix Hijacking. arXiv preprint arXiv:1801.02918 2018.
[29] Gilad Y, Cohen A, Herzberg A, Schapira M, Shulman H. Are We There Yet? On RPKI's Deployment and Security. IACR Cryptology ePrint Archive 2016.
[30] Vervier PA, Thonnard O, Dacier M. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In 2015.
[31] Chaviaras G, Gigis P, Sermpezis P, Dimitropoulos X. ARTEMIS: Real-time detection and automatic mitigation for bgp prefix hijacking. In: ACM. ; 2016.
[32] Khan, Muhammad N. "Importance of noise models in FSO communications." EURASIP Journal on Wireless Communications and Networking vol. 2014, no. 1, pp. 1-10, 2014.
[33] Zhao X, Pei D, Wang L, et al. An analysis of BGP multiple origin AS (MOAS) conflicts. In: ACM. ; 2001.
[34] Maxmind geoip. https://dev.maxmind.com/Accessed: 15-11-2018.