DOI: 10.2298/CSIS121108023Z

Evaluation on the Influence of Internet Prefix Hijacking Events

Jinjing Zhao[1,2], Yan Wen[1,2]

[1]Beijing Institute of System Engineering,Beijing, China
misszhaojinjing@hotmail.com

[2]National Key Laboratory of Science and Technology
on Information System Security,Beijing, China
celestialwy@gmail.com

Abstract. The inter-domain routing system based on the BGP protocol is a kernel establishment in the Internet. There have been many incidents of IP prefix hijacking by BGP protocol in the Internet. Attacks may hijack victim's address space to disrupt network services or perpetrate malicious activities such as spamming and DoS attacks without disclosing identity. The relation between prefix hijacking and the Internet hierarchy is presented in this paper. The Internet is classified into three tiers based on the power-law and commercial relations of autonomous systems. The relation between network topology and prefix hijacking influence is presented for all sorts of hijacking events in different layers. The results assert that the hierarchical nature of network influences the prefix hijacking greatly.

Keywords: IP prefix hijacking; Power law; BGP; Inter-domain routing system; Internet Service Providers

1. Introduction

The inter-domain routing system based on the BGP protocol is a kernel establishment in the Internet. It is not only the basic mechanism of exchanging the reachable information, but also the key way to inter-connect the autonomous systems and establish the policy control in ISPs. Unfortunately, the limited guarantees provided by BGP sometimes contribute to serious instabilities and outages. Prefix hijacking are probably the most straightforward type of BGP attack.

Prefix hijacking is also known as BGP hijacking, because to receive traffic destined to hijacked IP addresses, the attacker has to make those IP addresses known to other parts of the Internet by announcing them through BGP. Because there is no authentication mechanism used in BGP, a mis-behaving router can announce routes to any destination prefix on the Internet and even manipulate route attributes in the routing updates it sends to

neighboring routers. Taking advantage of this weakness has become the fundamental mechanism for constructing prefix hijack attacks. They occur when an AS announces a route that it does not have, or when an AS originates a prefix that it does not own. In the recent past, there have been many instances of prefix hijacking in the Internet wherein an Autonomous System hijacks routes simply by advertising the corresponding prefixes [1]. On January 22, 2006, a network (AS-27506) wrongly announced the IP prefix 65.173.134.0/24 representing an address block of 224 IP addresses, into the global routing system. This prefix belonged to another network (AS-19758) and because routers do not have a means to accurately verify the legitimate origin of each prefix, they accepted announcements from both the true origin (AS-19758) and the false one (AS-27506), and selected one of them based on the local routing policies and other criteria. As a result, some networks sent for data traffic destined to 65.173.134.0/24, to AS-27506 instead of the true owner.

Irrespective of whether it is caused by a misconfiguration or a malicious entity, the AS that hijacks a prefix can blackhole and intercept all the hijacked traffic and thus, cause a denial-of-service attack or a man-in-the-middle attack against the prefix owner [2, 3]. Because the current BGP protocol implements little authentication and often assumes a high level of trust to its neighbor routers, IP hijacking can easily succeed.

Previous efforts on prefix hijacking are presented from two aspects: hijack prevention and hijack detection. Generally speaking, prefix hijack prevention solutions are based on cryptographic authentications [4-8] where BGP routers sign and verify the origin AS and AS path of each prefix. While hijack detection mechanisms [9-15] are provided when a prefix hijack is going to happen which correction steps must follow.

Because there is a lack of a general understanding on the impact of a successful prefix hijack, it is difficult to assess the overall damage once an attack occurs, and to provide guidance to network operators on how to prevent the damage. Ballani et. al. [16] presents a study of Internet prefix hijacking and interception, which analyzes the probability of an AS hijacking the traffic to a prefix from another AS and the proposal of the prefix interception. Lad et. al. [17] estimate the resilience of Prefix hijacks through simulation across the Internet's AS-level topology.

In this paper, we conduct a systematic study on the impaction of prefix hijacks launched at different position in the Internet hierarchy. The Internet is classified into three hierarchies—core layer, forwarding layer and marginal layer based on the power-law and commercial relations between autonomous systems (ASes). Two impaction parameters—affected ASes set Nc and affected paths factor μ, are analyzed for typical nine types of prefix hijacking events in different layers.

The remainder of this paper is organized as follows: The section 2 descripts the hierarchy model of the Internet based on the power-law and relationships between ASes. Based on section 2, section 3 builds the attack model of IP prefix hijacks on a comprehensive attack taxonomy relying on the Internet hierarchy model and BGP protocol policies. The impaction

analysis of the prefix hijacks attack is also presented. The related works are discussed in section 4 and section 5 concludes the paper.

2. Internet Hierarchical Model

2.1. Internet Topology

The internet structure has been the subject of many recent works. Researchers have looked at various features of the Internet graph, and proposed theoretical models to describe its evolvement. Faloutsos et al. [18] experimentally discovered that the degree distribution of the Internet AS and router level graphs obey a power law. Opposite to negative exponential distribution, the curve of ASes' degree is declining very smoothly and heavy-tailed. So large numbers of ASes have little connections, but the ASes with rich connections are quite a few. The Internet AS structure is shown to have a core in the middle and many tendrils connected to it. A more detailed description is that around the core there are several rings of nodes all have tendrils of varying length attached to them. The average node degree decreases as one moving away from the core. We call these core nodes "hub" nodes, whose degree is very high. As a "storage-forwarding" network, the node degree is an important merit for evaluating a node's forwarding ability.

In order to consider the influence on the inter-domain system of the power-law nature, we classify the nodes by its forwarding ability. We build our model based on the traditional Transit-Stub model and also consider the power-law nature of the Internet. The Transit-Stub model [19] classifies ASes into two types, transit nodes and stub nodes. The transit nodes have the routing ability, but the stub nodes haven't. The transit nodes are interconnected into a core of the network, and the stub nodes connect to the core around. In order to emphasize the importance of the power-law, we classify the transit nodes into two kinds, hub nodes and middle nodes. So the whole inter-domain system can be classified into three layers, the core layer (hub nodes), the forwarding layer (middle nodes) and the marginal layer (stub nodes). We call this model power law-hierarchy model.

The power-law and hierarchy of the Internet fits each other very well. Generally, the nodes in the core layer have rich connections and the lots of the nodes in the marginal layer have few connections which need not forwarding for other nodes. The environment in the forwarding layer is more complex, but the node degrees are also decreasing with the hierarchy increased. A few nodes with high degree makeup the core layer, and a large numbers of node with few connections on the margin form the marginal layer, and between them is the most complex layer- forwarding layer.

2.2. Model Establishment

The main consideration of the power law-hierarchy model is to distinguish the performance of different layer nodes in the BGP convergence process. We build our model according to the hierarchy of the inter-domain system, and then, we testify it with the power-law rules. If the result is right, then the hierarchical model is also a power law-hierarchy model.

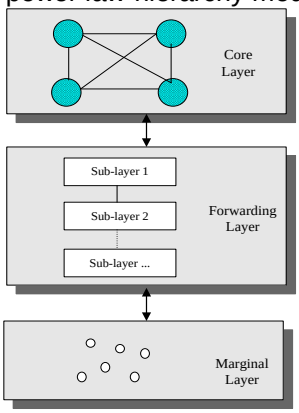

Fig. 1. Three Tiers Model Literature of Internet. a)The set of nodes who have no providers forms a clique is the core layer.b) If the nodes don't forward data for others, then it belongs to the marginal layer.c) The node that belongs to neither the core layer nor the marginal layer belongs to the forwarding layer.

The work in [20] presents a hierarchical formalization method for Internet. In [21], a five-hierarchy model of the Internet is presented based on the commercial relation between ASes. These models are too complex to analyze for BGP convergence. In [22], we build a three-hierarchy model of the Internet and give an efficient arithmetic for it. The model is organized as follows:

a) The set of nodes who have no providers forms a clique (interconnection structure), which is the core layer.

b) If the nodes don't forward data for others, then it belongs to the marginal layer.

c) The node that belongs to neither the core layer nor the marginal layer belongs to the forwarding layer. And the forwarding layer has several sub-layers.

By analysis on the number of nodes and connections of different layers which drawn from the route table data of RouteViews Project from 2005 to 2010, we can see that:

a) The average node degree of the core layer is about 880, however the one of the forwarding layer is about 7.4, and for the marginal layer, it's only 1.12, so the power-law is obeyed.

b) The proportion of the nodes number between forwarding layer and marginal layer is steady, which is about 1/6.

c) The number of the interconnections in the margin layer is zero, which means that its peer connections couldn't be observed by upper layers.

Table 1. Statistics of Connections of Layers.

	Core Layer	Forwarding Layer	Marginal Layer
Core Layer	78	2992	8374
Forwarding Layer	2992	7310	17699
Marginal Layer	8374	17699	0

In this way, we build the power law-hierarchy model of the inter-domain system based on the commercial relations between ASes, which also obey the heavy-tailed rule of power-law.

3. Prefix Hijacking Attack Model

3.1. Model Description

Prefix-hijacking occurs when a malicious or misconfigured AS announces to its peers that a block of IP-address space belongs to themselves, when, in fact, it does not. After a short delay, routes based on this bad announcement propagate through the internet at large and the malicious AS may be able to send and receive traffic using addresses it does not own. This hijacked space can be - and has been - used to send unsolicited mass e-mails, download copyrighted works, launch break-in attempts, or anything else generally considered to be illegitimate network use.

Prefix hijacking can happen in one of three ways - a block containing unallocated space can be announced, a sub-block of an existing allocation can be announced, or a competing announcement for exactly the same space as an existing allocation can be announced. Upon receiving these fabricated advertisements, other BGP routers may be fooled into thinking that a better or more specific route has become available towards the target prefix and start forwarding future traffic along the false path. As a result of the prefix hijacking, part (if not all) of the traffic addressed to the target prefix will be forwarded to the attacker instead of the target prefix.

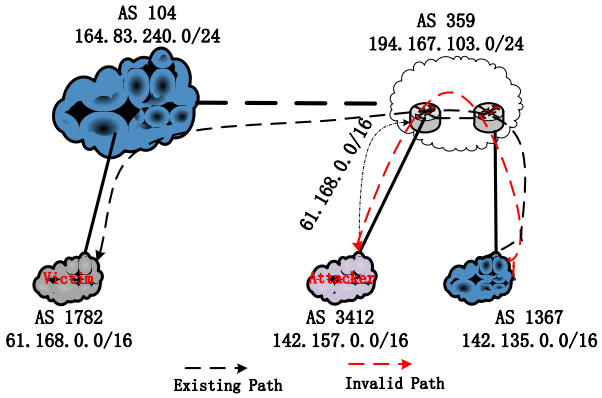

Fig 2. AS 3412 hijacks the prefix of AS 1782. AS 3412 has the IP prefix of 142.157.0.0/16 and AS 1782 has the IP prefix of 61.168.0.0/16. But AS 3412 in order to hijack the flow of AS 1782, it announces a BGP Update that it has the IP prefix 61.168.0.0/16. AS 1367 changes its path to the destination prefix 61.168.0.0/16, and its data to AS 1782 would be transmitted to AS 3412.

In Fig 2, Obviously, AS 1367's choice depends on both its existing route and the newly-received invalid route to 61.168.0.0/16. On the other hand, the success of the hijacking is also relies on its BGP routing policies. An AS will pick the shortest path to the destination in most cases, but the selected path must be valley-free and have no loops.

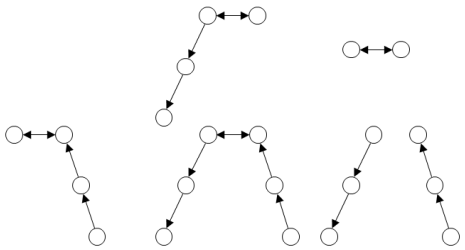

Fig 3. The Valley-free Path in BGP Policy. A valley-free path is a path has zero or several customer-provider sequences followed by one or zero peer-peer edge and then followed by zero or several provider-customer sequences.

Ballani et. al. [16] illustrated the influence of AS commercial relations between the prefix hijack path selections. Nine cases are analyzed according to different types of the existing paths and the hijacking invalid paths. Measurement studies in the past have shown that a large majority of ASes on the Internet tend to assign higher local-preference values to customer-routes than to peer-routes than to provider-routes. Since local-preference values are the first step of the BGP decision process, ASes prefer customer routes to peer routes to provider routes. In this paper, for the simpleness of our analysis, the ASes would not change their routes if the existing paths are the

same type and the same length as the hijacking invalid paths. The hijacking cases of different types if the existing paths and the invalid paths are summarized in Table 2

Table 2. Statistics of Connections of Layers.

Invalid Path / Existing path	Length	Customer	Peer	Provider
Customer	≤n	●	●	●
	>n	●	●	●
Peer	≤n	○	●	●
	>n	○	○	●
Provider	≤n	○	○	●
	>n	○	○	○

We model the Internet as a directed graph G= (V, E), nodes V represent the set of ASs in the Internet, links E are connections between them; a link e= (u, v) exists if node u will send update packets to v (but not vice versa). r = { v1,…,vk }is a simple path in G, for $\forall 1 \leqq i, j \leqq k$ and if i≠j, then vi ≠vj and e=(vi, vj) ∈E, the length of r is |r|=k. G is classified into three hierarchies according to the power law-hierarchy model in section 2, the core layer C, forwarding lay and the marginal layer S.

Definition 1 If vj is a provider of vi, then vj∈provider (vi), by the same token, customer(vi) and peer(vi) can be defined.

Definition2 Function h (vi) presents the layer level of vi, 1≤h(vi)≤3(1≤ i ≤n), n is the number of nodes.

vi belongs to the core layer,

iff $\{h(v_i) = 1 | \forall v_j \notin \text{provider}(v_i),\ 1 \leq i,j \leq n\}$

vi belongs to the marginal layer,

iff $\{h(v_i) = 3 | \forall v_j \notin \text{customer}(v_i),\ 1 \leq i,j \leq n\}$

vi belongs to the forwarding layer,

iff $\{h(v_i)=2 | v_i \notin C, \text{且} v_i \notin S, 1 \leq i \leq n\}$

Definition3 Function l(ej)presents the layer level of ej=(uk,um), 1≤l(ej)≤6 (1≤ j ≤m), m is the number of edges.

l(ej)=1, iff uk∈C and um∈C.

l(ej)=2, iff uk∈C and um∈T.

l(ej)=3, iff uk∈C and um∈S.

l(ej)=4, iff uk∈T and um∈T.

l(ej)=5, iff uk∈T and um∈S.

l(ej)=6, iff uk∈S and um∈S.

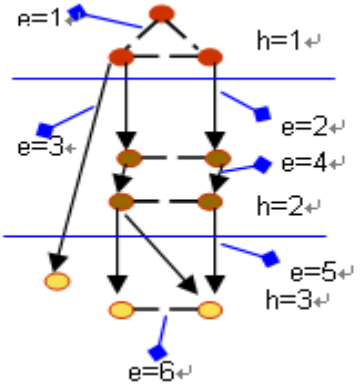

Fig 4. Hierarchy of the Nodes and Edges

To evaluate the influence if prefix hijacking events, two impaction parameters are introduced as follows:

Definition 4 Set of the affected nodes Nc: The set of nodes whose routing states might be changing because of the happening prefix hijacking event.

Definition 5 Affected path factor μ: The percentage of the paths might be changed because of the happening prefix hijacking event.

The affected path factor μ can be presented by an important parameter in graph theory, the betweenness centrality (BC) of a node.

Definition 6: Node BC $g(v)$: the BC of node v in the network is defined as: $g(v) = \sum_{s \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$.

Where σ_{st} is the number of shortest paths going from s to t and σ_{st} (v) is the number of shortest paths going from s to t and passing through e. BC gives in transport networks an estimate of the traffic handled by the vertices.

BGP does not always use the shortest path between two ASes however. And the affected paths factor μ is depend on importance of the path in the network. Because of this we use a definition of path betweenness:

Definition 7: Path BC $p(v)$: the path BC of node v in the network is defined as: $p(v) = \sum_{s \neq t \in N} Path_{st}(v)$.

Where pathst(p) is the number of BGP paths between IP blocks in s and t that use path p, N is the set of the nodes in the network.

3.2. Classification of Hijack

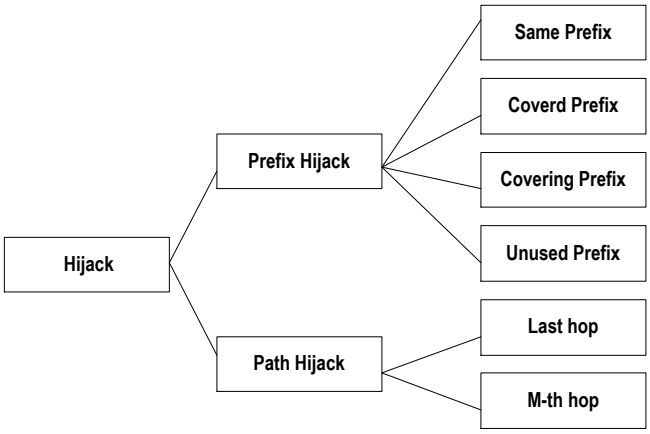

Fig 5. Types of prefix hijacks

The Hijack can be classified into two types by the way the attacker adopted, one is the node hijack and the other is the path hijack. The prefix hijack is done when an attacker announces an IP prefix which isn't belonging to him. And the path hijack is the way that the attacker announces a valid prefix, but reports an invalid path to a victim origin.

There are four types in the prefix hijack. An AS may pretend to be the owner of the same prefix of other's and originate the prefix resulting in a false origin hijack. If the attacker announces a sub-prefix of some valid prefix, termed as a covered prefix hijack, then routers in the Internet may contain routes to both the victim AS's prefix as well as the attacker's prefix. However, if the destination IP of a packet being routed, falls under the attacker's prefix space, then due to longest prefix match, the data would be forwarded to the attacker. An attacker AS may also announce a less specific prefix than a valid prefix, termed as a covering prefix hijack but will receive traffic, only when the route to the valid prefix is withdrawn. Finally, an AS may announce an invalid prefix that does not conflict with any used prefix space. For example, spammers are known to use unused prefixes for spam purpose.

To the path hijack, we separate the case of false last hop from false information on any other m-th hop in the path. The last hop hijack means that the hijacking AS announces a direct connection to the victim AS which is not existed. And m-th hop hijack is happened when the hijacking AS announces an m hops path to the victim AS, and the existing path is perhaps much longer than m or it even does not exist indeed.

The prefix hijacking events are illustrated in this paper, while the last two prefix hijacking types are not discussed. For the influence of hijacking a covering prefix hijack is the same as the hijacking the AS's prefix when the route to it is withdrawn. So the analysis to this type can be referenced to the same prefix hijack type. And the impact of the unused prefix hijack is not

determined by the hijacking event, but the activities after the hijacking, which is not focused in this paper.

3.3. Model Construction

The systematic study on the impaction of prefix hijacks launched at different position in the Internet hierarchy is descripted in this part, after the Internet hierarchy model and the prefix hijacking type are cleared.

For the simpleness of the description, the ASes whose prefixes being hijacked are expresses with V, and the hijack attack ASes are denoted by A. Furthermore, we suppose each AS only has one provider. The multi-home mechanism is not considered in this paper.

Firstly, the same prefix hijacking events are analyzed.

1. **V ∈ *Core Layer***

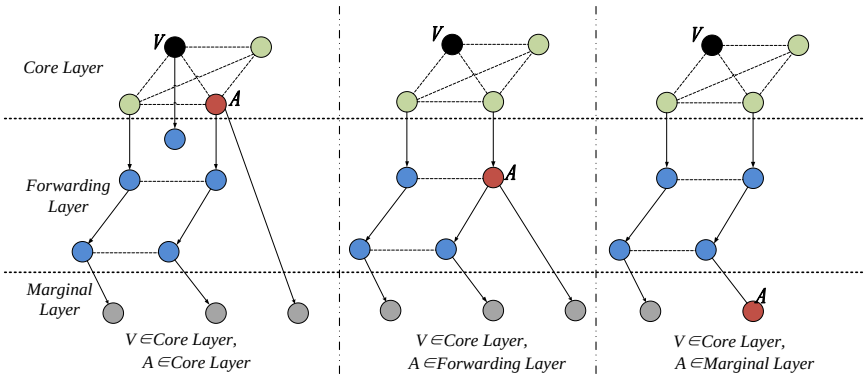

Fig 6. Hijacked AS in the Core Layer

1) A ∈ Core Layer

The hijacking and hijacked AS are both in the core layer.

Analysis:

All the ASes is the core layer are direct neighbors and they are peer nodes to each other. So, when the hijacking node A is trying to announce the same prefix of V to its neighbors, V will drop the update packet directly, and other ASes may find that they has a path to the prefix as {V} in their routing tables and they choose to ignore the announcement from A.

On the other hand, A will announce the same prefix to its customers. Its customer will accept the information and change their routing path to the prefix from {A,V} to {A}, and update the information to their customers. The update events will go on until the bottom nodes of the network who have the routes to the hijacking prefix receiving the update packets.

Parameters:

The set of the affected nodes Nc is:

$$Nc = \{A\} \cup \{\overset{\bullet}{Customer}(A))\}$$

2) A ∈ Forwarding Layer

The hijacked AS is in the core layer and the hijacking AS is in the forwarding layer.

Analysis:

If A hijacks the same prefix of V, it will announce the prefix to its providers, peers and customers. Because V is at the core layer, the routing information to it of the nodes in the forwarding layer must be received from its providers or peers before the hijacking event happening.

If A is the direct customer of an AS in core layer, its provider will ignore this announcement, because of the neighborhood between it and V. Otherwise, the provider of A will change their routing path to V, because the customer update has highest priority.

When A's peer nodes receive the announcement of hijacking prefix, they will judge where the existing route to V comes from. If the existing route is received from its providers, they will change the path to A. If the route is published by its peers, according to the rule of valley-free path, its peers can only announce the path from their customers. Because V is in the core layer, peers of A's peer could not get the path to V from their customers. So A's peer should accept he invalid path to the hijacking prefix.

When A's customers receive the announcement of hijacking prefix and the existing paths to V are coming from its providers, they will accept the update to V. If the existing paths to V are coming from its peers, they prefer to keep them, because the peer update has higher priority than the provider update.

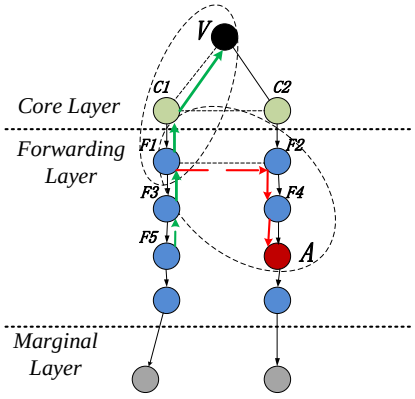

Fig 7. Existing paths compare with the invalidate paths

According to the valley-free rule of BGP path, after A's providers calculating there route to the hijacking prefix, they will announce the corresponding updates to their providers, peers and customers, while A's

peers or customers will announce updates to their customers. All the customers of A's providers or customers and their customers will changes their routing table. Whether the peers of A's n-th provider changing their routing tables or not depend on the length of their existing paths to V. In figure 7, AS F5 receives the update packets from its provider F3 to prefix which belongs to V before. The invalid path announced to F5 is {F3, F1, F2, F4, A}. And its existing path to the prefix is {F3, F1, C1, V}, which is shorter. So F5 would not accept the update event. The length of the invalid path is much correlated with A's hierarchy in the network. The higher it is, the larger hijacking impaction would be.

Parameters:

The set of the affected nodes *Nc* is in the range as:

$$\{\dot{provider}(A)\}\cup\{peer(\dot{provider}(A)\cup\{A\})\}\cup$$
$$\{\dot{customer}(\{A\}\cup(\dot{provider}(A)))\}\le Nc$$
$$\le\{\dot{provider}(A)\}\cup\{peer(\dot{provider}(A)\cup\{A\})\}\cup$$
$$\{\dot{customer}(peer(\dot{provider}(A)\cup\{A\}\cup(\dot{provider}(A)))\}$$

3) A ∈ Marginal Layer

The hijacked AS is in the core layer and the hijacking AS is in the marginal layer.

Analysis:

ASes in the marginal layer usually only have the provider relations. If A hijacks the same prefix of V, it will announce the prefix to its providers. If A is the direct customer of the core layer, its provider will ignore this announcement. Otherwise, the provider of A will change their routing path to V, and announce the update to its providers, peers and customers.

Parameters:

The set of the affected nodes Nc is in the range as:

$$\{\dot{provider}(A)\}\cup\{peer(\dot{provider}(A)\cup\{A\})\}$$
$$\cup\{\dot{customer}(\dot{provider}(A)\}\le Nc\le$$
$$\{\dot{provider}(A)\}\cup\{peer(\dot{provider}(A))\}\cup$$
$$\{\dot{customer}(peer(\dot{provider}(A))\cup(\dot{provider}(A)))\}$$

2. V ∈ *Forwarding Layer*

1) A ∈ Core Layer

The hijacked AS is in the forwarding layer and the hijacking AS is in the core layer.

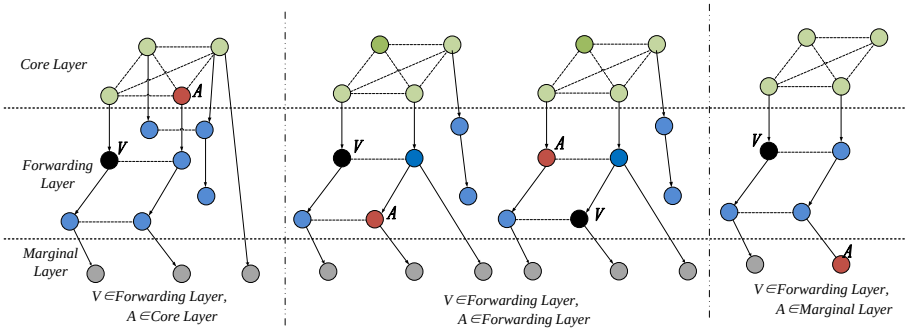

Fig 8. Hijacked AS in the Forwarding Layer

Analysis:

A announces the hijacked prefix of V to its peers. All the peers except the n-th provider of V in the core layer will update their path to V, because their existing path to V is announced by their peers and the invalid path is much shorter. The n-th provider of V would like to keep their existing path to V, because it came from their customers.

The peers, who accept the invalid path will update this information to their customers, withdraw the former paths and announce the new one. And their customers will do the update events to their customers. The procedure will going on. The ASes who is the peer of V's n-th providers or customers will reject, because their routes coms from the peer type update which has the high propriety than the provider type update.

Parameters:

The set of the affected nodes Nc is:

$$Nc = \{A\} \cup \{peer(A) - \{V\}\} \cup \{\dot{customer}(\{A\} \cup \{peer(A) - \{V\}\})\}$$
$$- \{peer(\dot{provider}(V) \cup \{V\} \cup \dot{customer}(V))\}$$

2) A ∈ Forwarding Layer

The hijacking and hijacked AS are both in the forwarding layer.

Analysis:

In the former case, if A hijacks the same prefix of V, it will announce the prefix to its providers, peers and customers.

There are three cases to analyze the peers of A: 1) the existing path is from their providers, the update from A has higher propriety; 2) the existing path is from their peers, the path length to V must be longer than one hop, so they will pick the path {A} to the hijacking prefix; 3) the existing path is from their customers, which is shown in Figure 9, they will keep their routing

information. If they change their routing table, their n-th customers will also do.

The customers of A will receive the withdraw update of their existing path to V through A and the new invalid path {A} to the hijacking prefix. And they do the same update events to their n-th customers.

The provider of A will change their routing path to V, because the customer update has highest priority. And the n-th provider of A will get the same decisions. But when they announce it to their peers, there are two cases, shown in Figure 9. When the peer of A's n-th providers is higher than V, they should not accept the update activity, because their existing path is announced by their customers. But when he peer of A's n-th providers is lower than V, they will update the paths.

To summarize the analysis above, the n-th providers of V would not affected by the hijacking events. To the n-th customers of V, if they has peer with other ASes they will accept the hijacking path. And if they has customer relations with other ASes and the path to A is shorter than the path to V, they will accept the hijacking path.

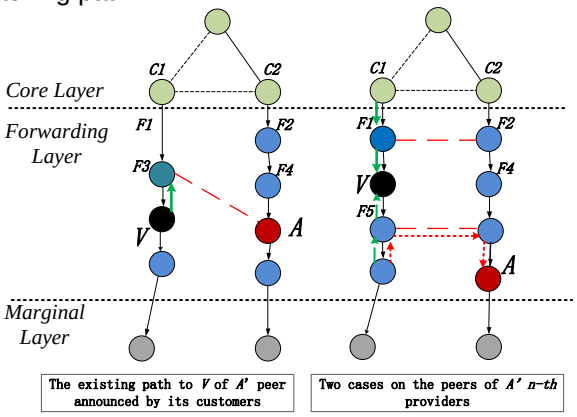

Fig 9. The hijacking and hijacked AS are both in the forwarding layer.

Parameters:

The set of the affected nodes Nc is in the range as:

$$\{\dot{provider}(A)\}\cup\{\dot{customer}(A)\}\le Nc\le\{\dot{provider}(A)\}\cup$$

$$\{peer(\{A\}\cup\dot{provider}(A))\}\cup$$

$$\{\dot{customer}(peer(\dot{provider}(A))\cup(\dot{provider}(A)))\}$$

3) A∈Marginal Layer

The hijacked AS is in the forwarding layer and the hijacking AS is in the marginal layer.

Analysis:

A in the marginal layer, it can only announce the hijacking update to its provider. The provider of A will change their routing path to V, because the customer update has highest priority. And the n-th provider of A will get the same decisions. But when they announce it to their peers, there are also two cases. When the peer of A's n-th providers is higher than V, they should not accept the update. But when he peer of A's n-th providers is lower than V, they will update the paths.

Parameters:

The set of the affected nodes Nc is in the range as:

$$\{\dot{provider}(A)\} \le Nc \le \{\dot{provider}(A)\} \cup \{peer(\dot{provider}(A))\}$$

$$\cup \{\dot{customer}(peer(\dot{provider}(A)) \cup (\dot{provider}(A)))\}$$

3. V ∈ *Marginal Layer*

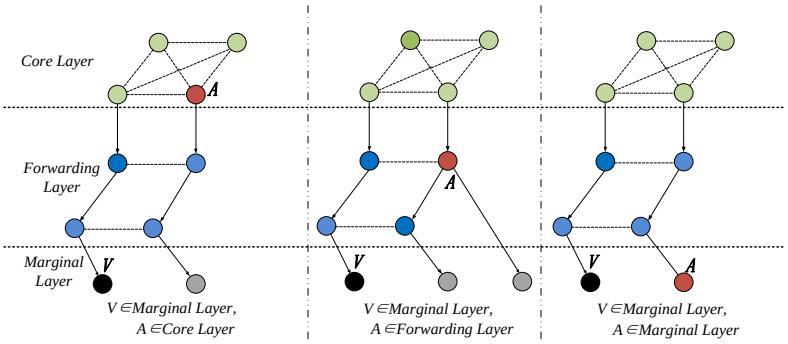

Fig 10. Hijacked AS in the Marginal Layer

1) A ∈ Core Layer

The hijacked AS is in the marginal layer and the hijacking AS is in the core layer.

Analysis:

A will announce the hijacking prefix to its customers and peers. Its n-th customer will accept the change unless its existing path to V is from its peers, which may be the providers of V. The peers of A except the n-th provider of V in the core layer will update their path to {A}. When they update the paths to its customers, if its customers are peers of V's n-th providers, they will reject the update. Otherwise, they will change the paths to the hijacking prefix.

Parameters:

The set of the affected nodes Nc is in the range as:

$$\varnothing \le Nc \le \{peer(A)\} \cup \{\dot{customer}(peer(A)) \cup \{A\})\}$$

2) A∈Forwarding Layer

The hijacked AS is in the marginal layer and the hijacking AS is in the forwarding layer.

Analysis:

When A announces the hijacking update to its providers, peers and customers, they will accept the path change to V, and send the update packets to its providers, peers and customers, unless their peers or customers are the V's n-th providers or their peers.

Parameters:

The set of the affected nodes Nc is in the range as:

$$\{\overset{\bullet}{provider}(A)\} \le Nc \le \{\overset{\bullet}{provider}(A)\} \cup \{peer(\overset{\bullet}{provider}(A))\}$$

$$\cup \{\overset{\bullet}{customer}(peer(\overset{\bullet}{provider}(A)) \cup (\overset{\bullet}{provider}(A)))\}$$

3) A∈Marginal Layer

The hijacking and hijacked AS are both in the marginal layer.

Analysis:

When A announces the hijacking update to its n-th providers, they will announce the updates to its peers and other customers. When they are the n-th provider of V, the hijacking attacks are successful to them.

Parameters:

The set of the affected nodes Nc is in the range as:

$$\{\overset{\bullet}{provider}(A)\} \le Nc \le \{\overset{\bullet}{provider}(A)\} \cup \{peer(\overset{\bullet}{provider}(A))\}$$

$$\cup \{\overset{\bullet}{customer}(peer(\overset{\bullet}{provider}(A)) \cup (\overset{\bullet}{provider}(A)))\}$$

To all the same prefix hijack types, the influenced ASes will change the paths to the hijacking prefix which is in the set of Nc. So, the affected path factor μ depends on proportion of Nc nodes in the whole network and the path BC of node V:

$$\mu = \frac{|Nc|}{N} \sum_{s \ne t \in N} Path_{st}(V)$$

N is the AS number of the network.

The covered prefix hijacking is much easier. Most all the ASes except for V will add a new path to the sub-prefix of V. So the set of the affected nodes Nc is all the ASes except for V.

$$Nc = All \setminus \{V\}$$

And the affected path factor μ is depends on the percentage of the sub-prefix hijacked in the prefix V assigned and the path BC of node V.

$$\mu = \eta \sum_{s \ne t \in N} Path_{st}(V)$$

η is the proportion of the sub-prefix in the prefix range of V.

From the analysis above, these results can be drawn:

1) The hijacked AS in the core layer is not the most awful thing. On the contrary, if the AS in the marginal layer being hijacked, the number of the affected nodes is the largest among the three levels;

2) The hijacked AS in the forwarding layer can affect more paths than the core layer or the marginal layer;

3) If the hijacked ASes are in the same level, the hijacking AS in the forwarding layer can affect more nodes than the core layer or the marginal layer, and the higher attacker is in, the larger its influence will be;

4) The sub-prefix hijack can affect more ASes than the same prefix hijack, and the lager sub-prefix range is, the bigger affected path factor μ will be.

4. Related Work

Various prefix hijack events have been reported to NANOG [23] mailing list from time to time. IETF's rpsec (Routing Protocol Security Requirements) Working Group provides general threat information for routing protocols and in particular BGP security requirements [24]. Recent works [3,25] give a comprehensive overview on BGP security. The prefix hijacking is one of the key problems being noticed to BGP in these papers.

Previous works on prefix hijacking can be sorted into two categories: hijack prevention and hijack detection. The former one is trying to prevent the hijacking in the protocol mechanism level, and the latter one is trying to find and alert the hijacking event after it happening. The methods can be categorized into two types: cryptography based and non-crypto based.

The cryptography methods, like [4-6, 27-31], imply that BGP routers sign and verify the origin AS and AS path of each prefix. Origin authentication [31] uses trusted database to guarantee that an AS cannot falsely claim to be the rightful owner for an IP prefix. However, the manipulator can still get away with announcing any path that ends at the AS that rightfully owns the victim IP prefix. Secure Origin BGP (soBGP) [30] provides origin authentication as well as a trusted database that guarantees that any announced path physically exists in the AS-level topology of the internetwork. However, a manipulator can still get away with announcing a path that exists but is not actually available. In addition to origin authentication, S-BGP [6] also uses cryptographically-signed routing announcements to provide a property called path verification. It effectively limits a single manipulator to announcing available paths. However, S-BGP does not prevent the manipulator from announcing the shorter, more expensive, provider path, while actually forwarding traffic on the cheaper, longer customer path. In SPV [32], the originator of a prefix establishes a single root value used to seed the generation of one-time signature structures for each hop in the PATH. However, the security of SPV is in some cases based on probabilistic arguments, which may be acceptable for some constrained environments, and it is unclear whether such arguments will be acceptable in the larger Internet. And it does not provide the requisite security to protect against path

modification. In addition to added router workload, these solutions require changes to all router implementations, and some of them also require a public key infrastructure. Due to these obstacles, none of the proposed prevention schemes is expected to see deployment in near future.

The non-crypto methods include [4, 9, 10, 12, 14]. PHAS [10] is predicated on the notion that a prefix owner is the only entity that can differentiate between real routing changes and those that take place as a result of a prefix hijacking attack. And if there are changes to the originator of a route, the owner of that prefix is notified through email. The system is incrementally deployable in that to join the system. A prefix owner need only register with the PHAS server; however, this server is also a single point of failure in the system, and if it is compromised, it could send out numerous false alarms to prefix owners. Additionally, the system relies on the validity of entities registering their prefixes; there is no protection against an adversary making a false registration. Hu and Mao examined prefix hijacking in greater detail and provided a mechanism for detecting prefix hijacking attacks in real time [14]. Their solution is based on fingerprinting techniques for networks and hosts. If there are conflicting origin ASes advertised, which is potential evidence of a prefix hijacking attack, the collected fingerprints are compared against probes sent to all origins. This approach relies on a real-time BGP UPDATE monitor, which sends differentiating probes if prefixes are advertised from multiple locations. The availability of the monitor is critical as, if updates are delayed, the ability to collect measures, such as probing and subsequent decision making, will be compromised. The Whisper protocol [4] is designed to validate the initial source of path information. The protocol seeks to alert network administrators of potential routing inconsistencies. A random value is initially assigned to each prefix by the originator. The value is repeatedly hashed at each hop as it is propagated from AS to AS. if the hash values are the same, then they must have come from the same source. Only the route originator can verify the route because of the non-invertibility of secure hash functions. Thus, the recipient would have to query the originator as to the veracity of the route, which is often outside of the purview of the originator's knowledge. Another recently-proposed alerting system is pretty good BGP (PGBGP) [12]. The key insight in this work is that misconfigurations and prefix hijacking attacks could be mitigated if routers exercise a certain amount of judgement with the routes that they adopt into their routing tables. MyASN[9] is an offline prefix hijack alert service provided by RIPE. A prefix owner registers the valid origin set for a prefix, and MyASN sends an alarm via regular email when any invalid origin AS is observed in BGP routing update.

5. Conclusion

This paper conducts a systematic study on the impaction prefix hijacks launched at different position in the Internet hierarchy based on the work in

paper [34]. The Internet is classified into three tiers—core layer, forwarding layer and marginal layer based on the power-law and commercial relations between ASes. Two impaction parameters—affected ASes set Nc and affected paths factor μ, are analyzed for the same prefix hijacking events and the covered prefix hijacking events in different layers. We studied nine type hijacking events based on the position of the hijacking ASes and the hijacked ASes.

The study shows that if the AS in the marginal layer being hijacked, the number of the affected nodes is the largest among the three levels. The hijacked AS in the forwarding layer can affect more paths than the core layer or the marginal layer. If the hijacked ASes are in the same level, the hijacking AS in the forwarding layer can affect more nodes than the core layer or the marginal layer, and the higher attacker is in, the larger its influence will be. The sub-prefix hijack can affect more ASes than the same prefix hijack, and the lager sub-prefix range is, the bigger affected path factor μ will be.

Acknowledgment. This research is supported by National Natural Science Foundation of China (Grant No. 61100223).

References

1 Mohit Lad, Ricardo Oliveira, Beichuan Zhang and Lixia Zhang ,Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks. pp.368-377, 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), 2007.
2 O. Nordstrom and C. Dovrolis, Beware of BGP attacks, SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, 2004.
3 Kevin Butler, Patrick McDaniel and Jennifer Rexford. A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE. Vol. 98, No. 1, January 2010
4 L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz. Listen and whisper: Security mechanisms for BGP. In Proceedings of ACM NDSI 2004, March 2004.
5 J. Ng. Extensions to BGP to Support Secure Origin BGP. ftp://ftp-eng.cisco.com/sobgp/drafts/draft-ng-sobgpbgp-extensions-02.txt, April 2004.
6 S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol (S-BGP). IEEE JSAC Special Issue on Network Security, 2000
7 S. S. M. Zhao and D. Nicol. Aggregated path authentication for efficient bgp security. In 12th ACM Conference on Computer and Communications Security (CCS), November 2005.
8 B. R. Smith, S. Murphy, and J. J. Garcia-Luna-Aceves. Securing the border gateway routing protocol. In Global Internet' 96, November 1996.
9 RIPE. Routing information service: myASn System. http://www.ris.ripe.net/myasn.html.
10 M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang. PHAS: A prefix hijack alert system. In 15th USENIX Security Symposium, 2006.

11 S. Qiu, F. Monrose, A. Terzis, and P. McDaniel. Efficient techniques for detecting false origin advertisements in interdomain routing. In Second workshop on Secure Network Protocols (NPSec), 2006.
12 J. Karlin, S. Forrest, and J. Rexford. Pretty good bgp: Protecting bgp by cautiously selecting routes. Technical Report TR-CS-2005-37, University of New Mexico, Octber 2005.
13 W. Xu and J. Rexford. MIRO: multi-path interdomain routing. In SIGCOMM 2006, pages 171–182, 2006.
14 X. Hu and Z. M. Mao, Accurate Real-time Identification of IP Prefix Hijacking, in Proc. of IEEE Security and Privacy (Oakland), 2007.
15 C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Realtime, in Proc. of ACM SIGCOMM, August 2007.
16 H. Ballani, P. Francis, and X. Zhang, A Study of Prefix Hijacking and Interception in the Internet. SIGCOMM Comput. Commun. Rev., vol. 37, no. 4, pp. 265–276, 2007.
17 M. Lad, R. Oliveira, B. Zhang, and L. Zhang, Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks," in Proc. of IEEE/IFIP DSN, 2007.
18 Michalis Faloutsos, Petros Faloutsos, Christos Faloutsos. On Power-Law Relationships of the Internet Topology.1999.
19 Zegura, Calvert and Donahoo, “A quantitative comparison of graph-based models for Internet topology”, IEEE/ACM Transactions on Networking, December 1997.
20 R. Govindan and A. Reddy. An Analysis of Internet Inter-Domain Topology and Route Stability. In Proc. IEEE INFOCOM ‘97, March 1997.
21 GE Z, FIGUEIREDO D, JAIWAL S, and et al. On the hierarchical structure of the logical Internet graph [A]. Proceedings of SPIE ITCOM[C]. USA, August 2001.
22 Peidong Zhu, Xin Liu. An efficient Algorithm on Internet Hierarchy Induction. High Technology Communication.14: 358-361, 2004.
23 The NANOG Mailing List. http://www.merit.edu/mail.archives/nanog/.
24 B. Christian and T. Tauber. BGP Security Requirements. IETF Draft: draft-ietf-rpsec-bgpsecrec-04, March 2006.
25 Sharon Goldberg, Michael Schapira, Peter Hummon, Jennifer Rexford. How Secure are Secure Interdomain Routing Protocols? in Proc. of ACM SIGCOMM, August 30–September 3, 2010, New Delhi, India.
26 Y. Rekhter, T. Li, and S. Hares. Border Gateway Protocol 4. RFC 4271, Internet Engineering Task Force, January 2006.
27 RFC 4271, Internet Engineering Task Force, January 2006. S. S. M. Zhao and D. Nicol. Aggregated path authentication for efficient bgp security. In 12th ACM Conference on Computer and Communications Security (CCS), November 2005.
28 B. R. Smith, S. Murphy, and J. J. Garcia-Luna-Aceves. Securing the border gateway routing protocol. In Global Internet’ 96, November 1996.
29 T. Wan, E. Kranakis, and P. van Oorschot, Pretty Secure BGP, psBGP, in Proc. of NDSS, 2005.
30 R. White, Architecture and Deployment Considerations for Secure Origin BGP (soBGP), draft-white-sobgp-architecture-01, Nov 2005.
31 W. Aiello, J. Ioannidis, and P. McDaniel, Origin authentication in interdomain routing, in Proc. of conference on Computer and communications security (CCS), 2003.

32 Y.-C. Hu, A. Perrig, and M. Sirbu, B. SPV: Secure path vector routing for securing BGP, in Proc. ACM SIGCOMM, Portland, OR, Aug. 2004.
33 J. Karlin, S. Forrest, and J. Rexford, B. Autonomous security for autonomous systems, Comput. Networks, Oct. 2008.
34 Zhao JJ, Wen Yan, Li Xiang, etc. The Relation on Prefix Hijacking and the Internet Hierarchy, The 6th International Conference on Innovative Mobile and Internet Services (IMIS'12), Italy, July, 2012.
35 Judanov, M., Jacko, O., Jevtia, M.: Influence of Information and Communication Technologies on Decentralization of Organizational Structure. Computer Science and Information Systems, Vol. 6, No. 1, 93-109. (2009)

Jinjing Zhao received her B.S., M.S. and Ph.D. degrees in School of Computer from National University of Defense Technology, Changsha, China. She is currently an associate professor at Beijing Institute of System Engineering. Her major research interests include computer networks, and information security.

Yan Wen received his B.S., M.S. and Ph.D. degrees in School of Computer from National University of Defense Technology, Changsha, China. He is currently an assistant professor at Beijing Institute of System Engineering. His major research interests include virtualization technology, operating system, and information security.

Received: November 08, 2012; Accepted: March 25, 2013