Building Formal Model of the Internet Routing for Risk Evaluation of Cyberattacks on Global Routing

© Vitalii Zubok

Pukhov Institute for Modelling in Energy Engineering
National Academy of Sciences of Ukraine, Kyiv, Ukraine
vitaly.zubok@gmail.com

Abstract. One of the most significant problems deriving from the Border Gateway Protocol (BGP) weaknesses is route leaks and route hijacks. Estimating the risks of route interception requires quantitative measurement of the impact of an attack on the routing distortion, and therefore, the loss of information security breach. This offers a way of exploring the topology of connections between autonomous Internet systems to further formulate the risk management task as a topology problem. One of the most important steps in modeling the impact of routing attacks is to build a formal model of global Internet routing. In this paper we offer to provide formal description for objects, relations and processes of the Internet routing.

Firstly we postulate the Internet as a set of IP addresses, grouped to address prefixes in routing tables. Prefixes are announced by autonomous systems with BGP protocol. Prefixes are aggregated and incapsulated one to another using subnet mask and this affects the accessibility of IP addresses in prefix. The set of routes to each prefix can be represented as directional graph, and combination of all that graphs built as routes to all announced prefixes can be used as representation of the Internet at global routing level. We provide a formal description of global routing objects and their relationships, as well as the process of route selection. All formulations are equally applicable to both IPv4 and IPv6 types of prefixes. Therefore, a formal description of the two components of the routing process is provided: the calculation of the IP prefix and path selection. These steps are an important in formulating the route hijack risk management problem as a task for researching effective link topology.

Keywords: Global Internet Routing, Route Hijacking, Routing Model, Cybersecurity.

1 Introduction

Autonomous Systems (AS) use the Border Gateway Protocol (BGP) to exchange routes to their IP prefixes and set up cross-domain routes on the Internet. BGP is a distributed protocol that lacks route validation and authentication. As a result, AS may promote illegitimate routes for non-IP prefixes. These illegal route announcements spread and "pollute" the Internet, affecting service availability, integrity and

Copyright © 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-2577/paper24.pdf

privacy of communications. This phenomenon, called BGP hijack hijacking, can be caused by incorrect router configuration or malicious attacks. Because any route can be originated and announced by any random network, independent of its rights to announce that route, there needs to be an out-of-band method to help BGP manage which network can announce which route. There are proposed proactive mechanisms such as Resource Public Key Infrastructure (RPKI) [1]. It's part of the Internet Routing Registry system. This service provides a collective method to allow one network to filter another networks routes. Method begins with cryptographic signing the route origin. A Route Origin Authorisation (ROA) is a cryptographically signed object that states which AS is authorised to originate a certain prefix. A ROA contains three informational elements: the AS Number that is authorised, the prefix that may be originated from the AS, and the maximum length of the prefix.

However such techniques are fully effective only in global deployment, and operators are reluctant to deploy them because of the associated technical and financial costs. For example, Telia, one of the Tier-I Internet backbone operators, announced that it's using RPKI for security in its internet routing infrastructure since only September, 2019.

Anti-hijack protection consists of two steps: detection and mitigation. An analysis of the mechanisms of the attack, depending on its objectives and options for its implementation is described in detail in [2]. Detection is mainly provided by third-party services such as BGPMon. They notify the network administrator of suspicious events related to their prefixes based on routing information. They track worldwide routes by tracing and keep track of route announcements in BGP. In the event of an incident, the affected networks begin to mitigate the consequences of the event, for example by announcing more specific prefixes to their networks or by requesting other ASs to filter out false announcements.

However, due to the combination of technological and practical deployment issues, existing reactive approaches are largely inadequate. In particular, the most advanced technologies have the following major problems:

- the variety of types of routing attacks and combinations of methods lead to *the lack of a reliable method* for detecting route interception;
- operators *should be informed in advance of legitimate changes* to their routing policy (new interactions between AS, announcement of a new prefix, etc.) so that such changes are not considered suspicious events for conditional third party detection systems. Otherwise, adopting a less rigorous policy to compensate for the lack of updated information and reducing the number of false positives carries the risk of neglecting real events and not detecting false negatives;
- only few minutes of unauthorized traffic diversion can result in heavy financial losses due to unavailability of service or security breaches. At the same time, the response time to incidents is slow in any case, as current practice requires the need to manually check alerts coming from monitoring systems and third-party services. The duration of widely known incidents ranged from several hours to months [3].

In the risk assessment process, specific requirements for the quality of information are raised at the risk identification stage. The highest possible level of completeness,

accuracy and conformity at the time of its receipt is required. Quality requirements are also raised to the quality of information sources [3,4]. The outcome of a risk identification should be structured and encompass four elements: the sources of the risk, the immediate events of the realization of the threats, the causes of these events and the expected consequences. Building a formal model of Internet routing will help solve the problem of predicting the consequences of events.

2 Graph Approach to the Internet Modelling

The telecommunication network is an integral part of the information and telecommunication systems and is characterized by different forms of communication and different types of interaction. Often a graph can serve as a mathematical model for such networks. A graph can be thought of as a set of points called vertices or nodes, joined by lines called arcs or bonds. Each link and graph node can be matched by a number of parameters that characterize natural constraints. For example, a telecommunications network may be represented as a graph in which the edges correspond to the communication channels and the vertices to the switching nodes. Important parameters can be included in the model in the form of numbers or weights assigned to the arcs and vertices of the graph. These scales can be fixed and random. Thus, for a network, typical vertex representing a switching node may have the following weights: maximum bandwidth, storage capacity etc. A typical edge is a communication line and may have the following weights: maximum bandwidth, average transmission delay over the communication channel, reliability of the communication channel, and so on.

The feasibility of constructing and using a network model as a graph depends on the physical nature of the network we study. The most obvious advisability of using the graph model in solving problems related to connectivity. In usual cases we may be interested in the task of delivering information from anywhere to anywhere. This is a structural task in which at least one path from any vertex to any other path must be established. Another important task is to find the shortest path between two, several, or all vertices of the graph, as well as find the shortest path with different constraints. Using graphs, we can also solve the problem of synthesis of network topology, that is, building an optimal system. One of the possible optimality criteria may be the survivability or reliability of the telecommunication system. Since the telecommunication networks tend to damage and failure (resulting in a breach of communication), a possible task may be to build a system in which the consequences of malfunctions are minimal under the specified operating conditions.

Mathematical apparatus of graph theory, and later - complex network theory, in application to the global telecommunication network topology allows to analyze a single nodes degree, the degree distribution, the shortest path between a pair of nodes, the average shortest path in the network, the clustering, betweenness and many other factors and characteristics. Currently, in many studies, the graph is used to build a model of the Internet at the level of autonomous systems [5,6]. In those studies the Internet is represented as a graph $G := (V, E)$ where V is a set of autonomous sys-

tems, and E is their connections formed by the BGP-4 routing protocol. In this case, the bandwidth of the connections between the nodes of the Internet is not taken into account and does not affect the weight of the edges, thus the graph is unweighted. Node relationships between offline systems on the Internet were explored. Several types of relationships were identified, including “customer-provider”, “peer-peer”, and others. In the case of the interaction of two equal status operators, they announce to each other their own preferences and network prefixes of their customers. In the case of provider-customer interaction, the provider announces to the client all the prefixes available to him, and the client announces the prefixes of his own networks. Thus, the connections between the autonomous systems appear to be bidirectional, so the edges of the graph are undirected.

Using the mathematical apparatus of graph theory, we have proposed a metric distance function on the Internet for such a graph and proved its correspondence to the metric axioms of minimality, symmetry and the triangle inequality [7].

3 Formal Description of Global Internet Routing Objects and Their Relations

We come again with thought that in order to detect route hijcks and route leaks, investigate the extent of the impact on the topology, and to further assess the risks, it is necessary to have a global routing model of the Internet, that is, a BGP-based model. The first difference from the approaches presented in the previous section is that the routing process itself is inextricably linked to the choice of destination. Therefore, when investigating routing interference (when tampering results in unauthorized change of direction), we will not be able to use an undirected graph as a model. To determine the required qualities of the new model, it is proposed to formalize the concept of routing.

Let’s formulate the initial data. There is an address space of Internet A - a set of unique IP addresses a, which are grouped into IP prefixes p (hereinafter simply "prefixes"):

$$A = \{a_1, a_2, a_3, ...a_{|A|} : a_i \neq a_j, \{i, j\} \leq |A|\};$$
$$a \in p \subset A.$$

Prefixes, in turn, are grouped (often the term "aggregated" is used) from more specific to less specific, as defined in [8] and shown in Fig. 1. For a complete list of prefixes, see the CIDR documentation. From the illustration it is clear that any IP address belongs to 32 prefixes that are "encapsulated", i.e. include each other by changing the network mask. So the entire address space A can be described by one prefix with the length of the network mask 0, or by combining two prefixes with the netmask length 1, or four with the netmask length 2, and so on:

$$p_3 \subset p_2 \subset p_1 \subset p_0;\ |p_0| = 2|p_1| = 4|p_2| = 8|p_3|.$$

Prefix notation	Network mask bit length	Number of IP addresses	Number of such prefixes in the addrss space
x.x.x.x/32	32	1	4294967296
x.x.x.x/31	31	2	2147483648
x.x.x.x/30	30	4	1073741824
x.x.x.x/29	29	8	536870912
…..			
x.x.x.0/24	24	256	16777216
x.x.x.0/23	23	512	8388608
x.x.x.0/22	22	1024	4194304
…..			
x.x.0.0/17	17	32768	131072
x.x.0.0/16	16	65536	65536
x.x.0.0/15	15	131072	32768
…..			
x.0.0.0/9	9	33554432	512
x.0.0.0/8	8	16777216	256
x.0.0.0/7	7	8388608	128
…..			
x.0.0.0/3	3	536870912	8
x.0.0.0/2	2	1073741824	4
x.0.0.0/1	1	2147483648	2
0.0.0.0/0	0	4294967296	1

Fig.1. Aggregation of the IPv4 prefixes according to RFC 4632.

In the general case, we can thus express the relation between the subsets of IP addresses defined by the prefix prefixes in the set of all IP addresses:

$$\begin{cases} p_i = 2^{j-i} p_j; \\ i \le j; \\ 0 \le \{i, j\} \le \log_2 |A| \end{cases} \quad (1)$$

Prefixes are announced by autonomous systems (the term "originating" is used in the literature), so each prefix has its "origin" - an autonomous system that announces it. An example of AS interaction is shown in Fig. 2.

In the normal state, each prefix is announced by only one autonomous system and there is at least one route for each prefix

$$m(p) := (v_p, e_p), \quad (2)$$

which consists of directional edges e_p that correspond to the announcement of the perfix between vertices v_p (autonomous systems). There are no routes to the unannounced prefix, and it cannot be considered a member of the Internet.

A set of routes m_p to a specific prefix p can be represented as a ring-bound, oriented graph without loops:

$$M_p := (V_p, E_p), \tag{3}$$

where V_p - connections between autonomous systems that receive the announcement of the prefix p, and E_p - autonomous systems that have routes to the prefix *p*.

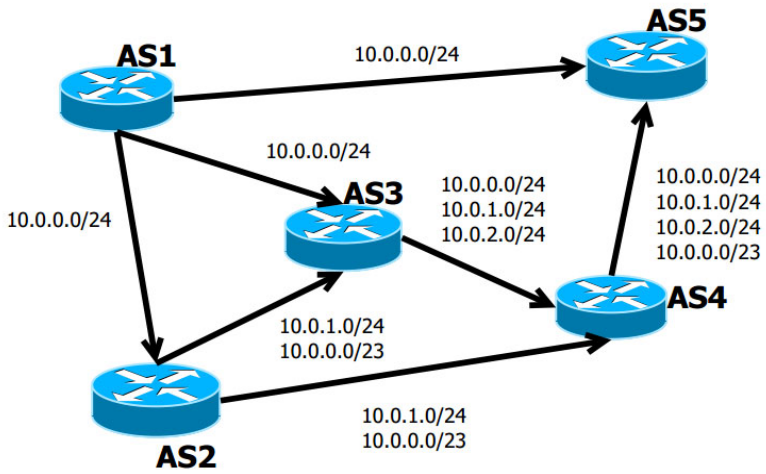

Fig.2. An example of exporting announcements of IP-prefixes in the process of interaction of autonomous systems.

The vertices of the graph on the inbound edges receive prefix announcements, and on the outbound edges they relay them to other vertices (whether or not relayed, depending on the routing policy or channel status). One of the vertices has only the outbound edges, and it's origin AS. Other vertices must have inbound vertices (because they accept announcements) and may have output ribbons (if they relay announcements).

The combination (ensemble) of all graphs is the set of all routes to all prefixes. It forms a graph:

$$G := (V, E) : V = \bigcup_p V_p \; ; \; E = \bigcup_p E_p \; .$$

This graph that can be interpreted as an Internet network represented at the global routing level.

Let's delve into the routing process. If the prefix p_j is a subset of the prefix p_i, that is $p_j \subset p_i$, it does not mean that they necessarily have the same origin, in general the prefix has origin regardless of the nesting. Example: a portion of a large ISP's prefix may be assigned to one of the ISP's clients and authorized to be announced by a client to other ASs. On the other hand, if there is no announcement for a prefix p_j in a certain autonomous system, it does not mean that it is unreachable through it: the presence at some node of the announcement p_i also means the possibility of routing to p_j (this is a unilateral statement):

$$p_j \subset p_i \Rightarrow m(p_j) \subset m(p_i). \quad (4)$$

A prime example of this is an edge network device connected to the network with its single network interface. Its routing table can only contain a route to the general prefix 0.0.0.0/0 (see Figure 1), which is also called the default route. It should be noted that the prefix 0.0.0.0/0 is only announced in BGP for participants who use equipment that cannot handle the full view - a complete routing table (usually end users - small ASs that are not transitors) .

4 A Formal Description of the Route Selection Process

The task of finding the best route is complicated. To solve this, the network topology, communication bandwidths, average message length should be known. This is a non-linear programming problem for which no algorithms exist, even with polynomial complexity. Only heuristic algorithms are known, which allow us to obtain only an approximate solution to the optimization problem. Therefore, the TCP/IP stack has adopted the so-called one-step approach to optimizing the packet route (next-hop routing) - each router and destination node only have to choose one step forward of packet transmission. A one-step approach means a distributed computation of the task of route selection, and this is an advantage that underlies the virtually endless scalability of the Internet.

The first step in choosing a delivery destination is choosing a prefix. The most specific prefix must be selected in the routing table, taking into account (1):

$$p(a) = \{\min_j(p_j) \ : \ a \in p \subset A, \ 0 < j \leq |A|\}. \quad (5)$$

As explained in the previous paragraph, the subject of route selection in global routing is the graph node, that is, the autonomous system. The prerequisite for starting the selection process is that there is more than one route to the same prefix *p*. One of the available routes can be defined as the path between two nodes of graph (2), where the initial node is the autonomous decision system and the final node is the autonomous system, which is the origin for the prefix *p*. Omitting specific local route attributes and administratively set routing rules, the only one factor that is taken into ac-

count is the network topology image "captured" at the time of the routing decision. The common criterion for choosing a path is path length (best path) - the number of transit nodes between the start and end nodes. Given (2) and (3), the route to the prefix will be this route $\pi_v(p)$:

$$\pi_v(p) = \{\min_v(m_v(p)) \ : \ \pi \in M_p, \ v \in V_p\}, \tag{6}$$

where *v* stands for outbound node in which desicion is made.

Therefore, there are two components of the routing process - prefix calculation (5) and path selection (6). A formal description is provided for them.

5 Relationships Between Global Routing Objects and Different Types of IP Addresses

To the date, there are two types of IP address that are different in bit rate on the Internet. The traditional IP address consisted of 32 bits. This limited the number of possible addresses to 2^{32} = 4294967296. The growth of the Internet, despite the introduction of economical allocation of address space, led to a lack of addresses. A modern IP address, commonly referred to as an IPv6 address (unlike the traditional IPv4 address), is 128 bits long. This difference affects the operation of the link layer and network layer according to the OSI model. However, the principles of CIDR and routing have generally not been changed by IPv6 implementation.

From a CIDR perspective, the difference IPv6 from IPv4 is this:

- the IPv6 address space consists of 2^{128} addresses;
- the maximum length of the network mask is 128 bits instead of 32;
- every network address in IPv6 address space is included in 128 IPv6 prefixes, incapsulated in each other.

Multiprotocol BGP is the supported exterior gateway protocol (EGP) for IPv6. Multiprotocol BGP extensions for IPv6 supports many of the same features and functionality as IPv4 BGP. IPv6 enhancements to multiprotocol BGP include support for an IPv6 address family and network layer reachability information and next hop (the next router in the path to the destination) attributes that use IPv6 addresses [9].

So the BGP-4 protocol for IPv4 and IPv6 is no different - BGP speakers use the same protocol messages, path attributes, route selection criteria for both the IPv4 address space and IPv6 address space. Therefore, the description of the global routing model proposed in the previous section, including expressions (1), (4) - (6), is the same regardless of the type of IP prefixes.

6 Conclusion

An important step towards assessing the risk posed by attacks on global routing is to predict the impact of the attack, namely to assess the scale of the attack (distribu-

tion routes, impact area, number of "damaged" routes). The routing process is inextricably linked to the choice of direction, so it is obvious that the routing attack affects direction change. When investigating routing interventions that result in an unauthorized change of direction, we must have adequate routing model. In this paper we offer to provide formal description for objects, relations and processes of the Internet routing. Firstly we postulate the Internet as a set of IP addresses, grouped to address prefixes in routing tables. Prefixes are announced by autonomous systems with BGP protocol. Prefixes are aggregated and incapsulated one to another using subnet mask (1) and this affects the accessibility of IP addresses in prefix. The set of routes to each prefix can be represented as directional graph (3) and combination of all that graphs built as routes to all announced prefixes can be used as representation of the Internet at global routing level.

The TCP/IP stack uses the so-called one-step approach to optimizing next-hop routing - each router and terminal node only have to choose one step (next step) for packet transmission. The first step in choosing a delivery destination is choosing a prefix. The most specific prefix must be selected in the routing table (5). The actor in the process of choosing a route in global routing is a graph node, that is, an autonomous system. The prerequisite for starting the selection process is that there is more than one route to the same p prefix. One of the available routes can be defined as the path between two graph nodes. The general criterion for choosing a path is its length, that is, the number of transit nodes between the start and end nodes (6). All formulations are equally applicable to both IPv4 and IPv6 types of prefixes.

Therefore, formal descriptions of global routing objects - autonomous systems, IP prefixes, BGP announcements, and relationships between them - are offered. A formal description of the two components of the routing process is identified and provided: the calculation of the IP prefix, and path selection. These steps are an important step towards modeling cyberattacks on global Internet routing such as route hijacks in order to formulate the risk management task for a particular node as a task for searching its most effective communications topology.

References

1. G. Huston, G. Michaelson et al.: Resource Public Key Infrastructure (RPKI) Validation Reconsidered. https://tools.ietf.org/html/rfc8360, last accessed on 209/10/29.
2. Zubok, V.: Metric Approach to Risk Evaluation of Cyberattacks on Global Routing: Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018). Vol-2318 urn:nbn:de:0074-2318-4.
3. Zubok V., Mokhor V.: Exploring the relations between topology and security risk of cybernetic attacks on global Internet routing]. // Modelyuvannya ta informaciyni technologii, vol. 85, pages 23-26.
4. Risk Management – Vocabulary (ISO Guide 73:2009, IDT) : DSTU ISO Guide 73:2013. – [Valid since 2014–07–01] . – Kyiv : Minekonomrozvytku Ukrainy, 2014.

5. IPv4 and IPv6 AS Core: Visualizing IPv4 and IPv6 Internet Topology at a Macroscopic Scale : http://www.caida.org/research/topology/as_core_network/, last accessed on 2019/10/29.
6. Pavlos Sermpezis, Vasileios Kotronis et al.: ARTEMIS: Neutralizing BGP Hijacking within a Minute : https://arxiv.org/abs/1801.01085 , last accessed on 2019/06/25.
7. Mokhor, V., Zubok, V.: Interconnection of the Internet nodes using methods of the complex networks theory. Kyiv : «Prometheus», 2017. – 175 pages.
8. Fuller, V., Li, T.: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan : https://tools.ietf.org/html/rfc4632, last accessed on 2019/10/01.
9. Marques, P., Dupont, F.: Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing : https://tools.ietf.org/html/rfc2545 , last accessed on 2019/10/12.