International Journal of
Computer & Software Engineering

Original Article Open Access

Special Issue: **Computational Analysis and Modeling**

On Vulnerability of the Longest Prefix Matching Rule to the IP Classless Subnetting

Yao Tong and Shigeo Akashi*

Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan

Abstract

The more commonly the Internet is used among the nations in the world, the more diversified is the way of cyber attacks. This fact implies that it is more difficult for the network administrators to develop generic countermeasures against various kinds of cyber attacks and malwares. Therefore, network theoretic classification of cyber attacks may play so important roles in constructing versatile countermeasures in the future. In this paper, network theoretic comparison of several cyber attacks with each other is discussed for the purpose of deriving the way of developing the generic conutermeasures against diversified malicious use of network theoretic skills.

Publication History:

Received: November 05, 2021
Accepted: November 16, 2021
Published: November 18, 2021

Keywords:

Cyber attacks, Malwares, Subnetting, Prefix matching, Gateway

Inroduction

As various kinds of cyber attacks have been diversified, it has become important for the network administrators to specify the skills which have been applied maliciously to cyber attacks and to develop versatile countermeasures against them. This is the reason why we had better investigate the network theoretic classification of cyber attacks and the mutual relations among them.

1. Whether cyber attacks are carried out intentionally or brought about spontaneously: For example, as for the network traffic congestions, we cannot easily discriminate the traffic congestions whch are brought about intentionally from the traffic congestions which happen spontaneously.
2. Whether or not the geogrpahic distance between the network segments where cyber attacks happen are apart from the network segments where cyber attackers exist: For example, it is maliciously convenient for the cyber attackers to commit their cyber attacks from the network segments which is far from the network segments where the victims suffering from the attacks exist.
3. Whether cyber attacks are scalable or not: For example, Denial-of-Service attacks are infamous for the reason why the generic countermeasures against the Distributed Denial-of-Service attacks have not been developed yet because the network theoretic skills which have been abused for these attacks are being diversified.
4. Whether the network theoretic skills having been used by the cyber attackers can be replaced with some other safer ones or not. For example, since the modern e-mail delivery system is based on the rule that only the receivers' e-mail addresses should be referred while the e-mails are forwarded, the malicious e-mails whose senders' addresses are falsified cannot be removed from the Internet before they reach the receivers.

The purpose of this paper is to prove that the longest prefix matching rule is not always compatible with the IP classless subnetting and that the simultaneously combined use of the longest prefix matching rule and the IP classless subnetting is likely to bring about several cyber attacks such as the ICMP packet interception, the ICMP reflection attack, the HTTP synflood attack and the HTTP reflection attack. In the first part of this paper, we introduce a generic network model which enables us to see that the network theoretic skills which have been applied to the ICMP packet interception is almost the same as applied to the ICMP reflection attack. In the second part, we discuss the problem asking whether the HTTP synflood attack and the HTTP reflection attack can be realized simultaneously or not.

As for the mathematically basic skills which can be used for analyzing network structure, we can refer to Knuth [2]. As for the foundation of cyber security, we can refer to Santos and Muniz [1]. As for the countermeasures against the Distributed Denial-of-Service attacks, which are based on packet filtering, we can refer to Chen, Hwang and Kwok [4]. As for another vulnerability of modern network structures to the Distributed Denial-of-Service attacks, we can refer to Ben-Porat, Bremler-Barr and Levy [5].

The Simplest Network Structure showing the ICMP Packet-Misforwarding

In this section, we introduce an example illustrating that a router misforwards a certain packet to some other network segment which does not contain the destination of the packet, if the router observes the longest prefix matching rule.

As shown in Figure 1, let Gateway router, Left-hand side route and Right-hand side router be three routers, moreover, let Path-12 (resp. Path-13) be two routing paths connecting Gateway router with Left-hand side router (resp. Gateway router with Right-hand side router). Here, if we assume that there exists Left-hand side PC whose IP address is 192.168.0.2/22, on the oppsite side of Gateway router beyond Left-hand side router and that there exists Right-hand side PC whose IP address is 192.168.1.2/23, on the opposite side of Gateway

***Corresponding Author:** Prof. Shigeo Akashi, Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan; E-mail: akashi@is.noda.tus.ac.jp

Citation: Tong Y, Akashi S (2021) On Vulnerability of the Longest Prefix Matching Rule to the IP Classless Subnetting. Int J Comput Softw Eng 6: 170. doi: https://doi.org/10.15344/2456-4451/2021/170

router beyond Right-hand side router, then Gateway router does not relay any packet that is bound for 192.168.0.2/22 to Left-hand side router, but relays it to Right-hand side router, because Left-hand side router advertises that there exists the network segment whose network address is 192.168.0.0/22 and Righthand side router advertises that there exists the network segment whose network address is 192.168.0.0/23. Such packet-misforwarding as is carried out by Gateway router results from the observance ot the longest prefix matching rule by Gateway router. More exaclty speaking, in Figure 1, the network segment including 192.168.0.0/23 is geographically disjoint from the network segment including 192.168.0.0/22, though all the IP addresses belonging to 192.168.0.0/23 are strictly included by all the IP addresses belonging to 192.168.0.0/22. Needless to say, the routing table of Gateway router proves that 192.168.0.0/22 and 192.168.0.0/23 corespond to Serial 0/0/1 and Serial 0/0/0, respectivly as the following Figure 2 shows:

As Figure 2 shows, RIP is used for the purpose of dynamically designing the network structure in Figure 1. Since this packet-misforwarding results from the fact that the set inclusion of 192.168.0.0/22 and 192.168.0.0/23 is inconsistent with the geographical correspondence between the network segment including 192.168.0.0/22 and the network segment including 192.168.0.0/23, in order to remove the difficulty accompanying packet-misforwrding, the network address registered with Left-hand side router should be replaced with 192.168.2.0/22, and moreover, the gateway IP address assigned for the gateway interface of Left-hand side PC and the IP address assigned for Lefthand side PC should be replaced with 192.168.2.1/22 and 192.168.2.2/22, respectively.

The following Figure 3 shows that the interface of Gateway router, namely Serial 0/0/1, thruogh which the ICMP echo-requests originating from Left-hand side PC come in is different from the interface of Gateway router, namely Serial 0/0/0, through which the ICMP echo-replies originating from Web server go out:

A Relation between the ICMP Packet Interception from Remote Network Segments and the ICMP Reflection Attack

In this section, we discuss a relation between the ICMP packet-interception and the ICMP reflection attack.

The ICMP packet-interception is defined as the malicious cyber attack that a large part of the ICMP packets commuting between two authenticated network users are intercepted by another network user who is located apart from the route connecting two authenticated

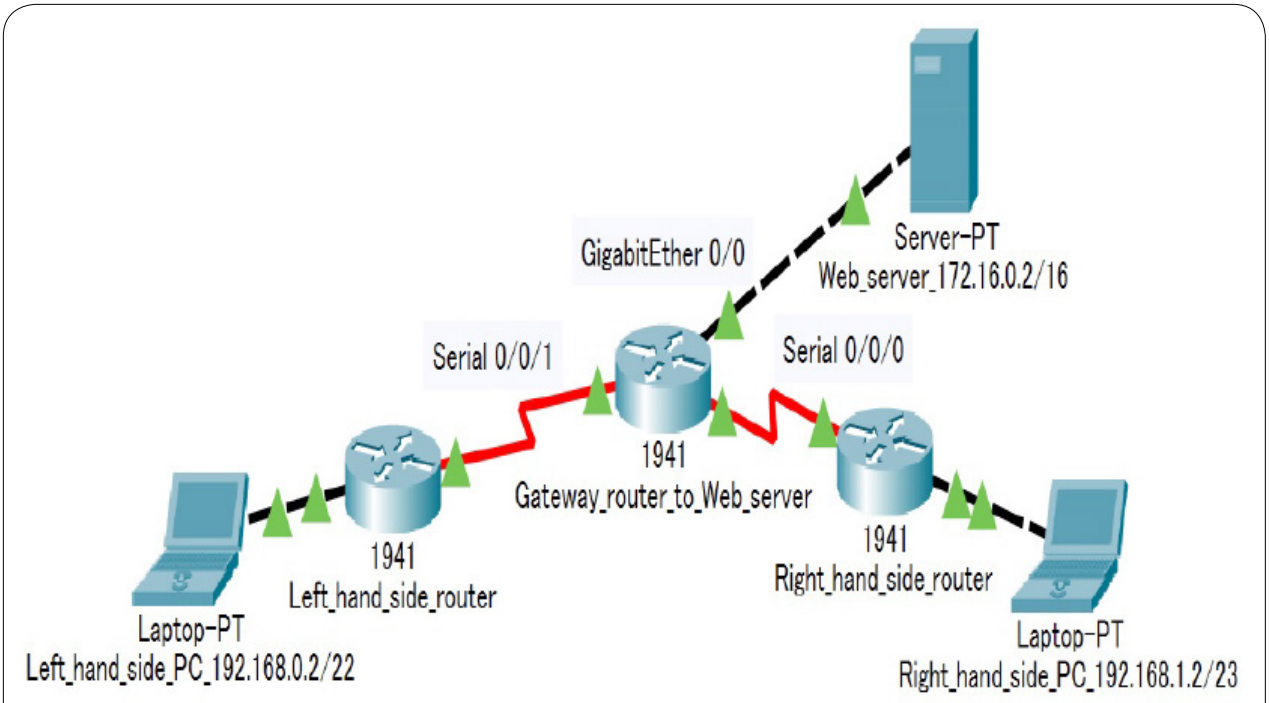

Figure 1: Incompatibility of the longest matching prefix rule with IP classless subnetting.

```
Gateway_router#
Gateway_router#show ip route rip
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.0.0/22 [120/1] via 10.1.2.2, 00:00:04, Serial0/0/1
R       192.168.0.0/23 [120/1] via 10.1.1.2, 00:00:04, Serial0/0/0
```

Figure 2: The routing table of Gateway router.

network users. For example, in Figure 1, if Left-hand side PC sends ICMP echo-requests to Web server whose IP address is 172.16.0.2/16, then Web server responds with as many ICMP echo-replies whose destination IP address is 192.168.0.2 as this web server has received. Actually, none of the ICMP echo-replies originating fromWeb server are able to reach Left-hand side PC, and all of them flow into Right-hand side router, because the destination IP address assingned for the ICMP echo-replies is 192.168.0.2 and Gateway router forwards all of them not to Left-hand side router but to Right-hand side router according to the longest prefix matching rule.

The ICMP reflection attack is defined as the malicious cyber attack that a malicious network user forces such a server as an open DNS resolver to send a large number of unnecessary ICMP echo-replies originating from the server used frequently by the victim and which are bound for the victim. In the ICMP reflection attack, the malicious network user targets the victim not directly but indirectly, because, in case that the server receives these unnecessary ICMP echo-requests originating from the malicious network user, it responds with the ICMP echo-replies which are not bound for the malicious network user but bound for the victim. Eventually, this is the reason why the victim has come to suffer from the arrival of a large number of unexpected ICMP echo-replies which have been sent by the server used frequently by the victim. Exactly speaking, the ICMP packet reflection attack can be classified into two cases, namely, the ICMP packet reflection attack from remote network segments and the ICMP packet reflection attack from local network segments. The former case is the cyber attack under the condition that the network segment where a malicious network user exists are separated from the network segment where the targeted victim exists, while the latter case is the cyber attack under the condition that a malicious network user shares the same network segment as the targeted victim exists. For example, in Figure 1, Right-hand side PC has come to suffer from the arrival of a large number of unexpected ICMP echo-replies having originated from Web server. We can call this case the ICMP packet reflection attack from remote network segments, because the network segment where the malicious network user exists are disjoint not only from the network segments where Left-hand side router and Web server exist but also the routing path connecting the authenticated network users with each other.

Such consideration as stated above concludes that, when the ICMP packet interception is compared with the ICMP reflection attack, the network structure where the former cyber attack is brought about intentionally is exactly the same as the latter cyber attack is brought about, and that what is different between the ICMP packet interception and the ICMP reflection attack consists in the difference betwen the role which Left-hand side PC plays and the role which Right-hand side PC plays. In other words, the ICMP packet interception can be brought about in case that Left-hand side PC plays the role of the victim and Right-hand side PC plays the role of the malicious network user, while the ICMP reflection attack can be brought about in case that Left-hand side PC plays the role of the malicious network user and Right-hand side PC plays the role of the victim. The comparison of these attacks with each otehr can be summarized as the following Table 1:

ICMP	packet interception	reflection attack
purpose	Wiretapping	Denial-of-Service
cyber attacker	smaller segment	larger segment
victim	larger segment	smaller segment

Table 1: ICMP packet interception and ICMP reflection attack.

Simultaneous Feasibility of HTTP Synflood Attack and HTTP Reflection Attack

In this section, we discuss the maliciously synergistic effect which has been brought about by the intentional HTTP reflection attack. In Figure 1, if Left-hand side PC is in charge of the website visitor and Right-hand side PC is in charge of the victim, then the HTTP synflood attack from which Web server suffers and HTTP reflection attack from which Right-hand side PC suffers can be brought about simultaneously.

If we assume that there exist neither Right-hand side router nor Right-hand side PC in Figure 1, then Left-hand side PC can visitWeb server and see the web contents published by Web server after TCP connecton of Left-hand side PC with Web server has been established. On the contrary, when Left-hand side PC begins to connect itself with Web server under the condition that both Right-hand side router and Right-hand side PC exist, Left-hand side PC and Web server cannot

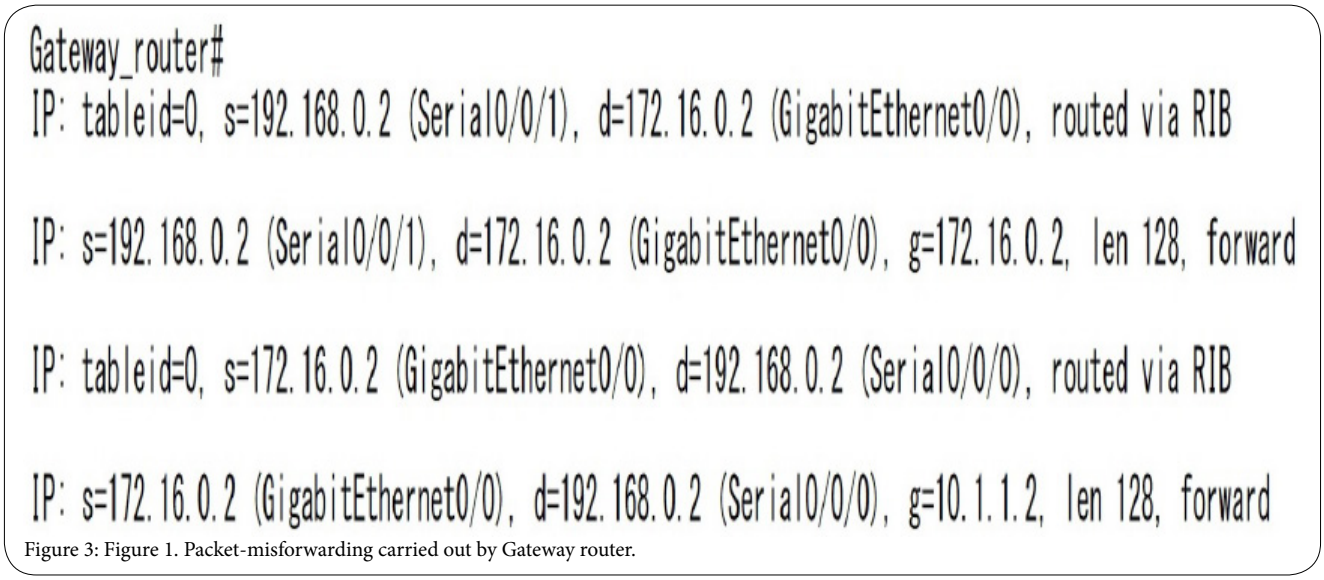

Figure 3: Figure 1. Packet-misforwarding carried out by Gateway router.

establish TCP connection of them with each other, Eventually, Left-hand side PC cannot display the contents of Web server according to the failure of TCP three-way handshake which can be decomposed into the followiing three sequential procedures:

1. In the first procedure, Left-hand side PC sends a SYN packet to Web server, and it reaches Web server.
2. In the second procedure, as soon as the SYN packet reaches Web server, Web server sends the SYN-ACK packet back to Left-hand side PC. Actually, Gateway router would not forward the SYN-ACK packet sent by Web server to Left-hand side router beyond which Left-hand side PC exists, on the opposite side of Gateway router, but forwards it to Right-hand side router beyond which Right-hand side PC exists, because Gateway router observes the longest prefix matching rule.
3. In the final procedure, though Left-hand side PC is ready for replying with the ACK packet which is bound for Web server as soon as the SYN-ACK packet originating from Web server reaches, it cannot receive the SYN-ACK packet originating from Web server. This packet-misforwarding follows that the ACK packet, which is expected to be sent by Lefthand side PC, keeps staying in the inside of Left-hand side PC and thatWeb server waits for the ACK packet originating from Left-hand side PC to reach. This is the reason why TCP three-way handshake does not hold successfully, regardless of whether Left-hand side PC visits Web server with malicious purpose or not.

This consideration follows that the Denial-of-Service attack can be classified into the following two cases:

1. If Left-hand side PC sends a large amount of the renewal request of web contents without changing the sender's IP address which has been assigned for Lefthand side PC, then this attack is called the Denial-of-Service attack targeting Web server.
2. If Left-hand side PC sends a large amount of the renewal request of web contents after having changed the sender's IP address which has been assigned for Left-hand side PC for the IP address which has been assigned for Right-hand side PC, then this attack is called the HTTP synflood attack targeting Web server.

The following Figure 4 shows that TCP session between Web server and Right-hand side router has been established sucessfully, while TCP session between Web server and Left-hand side router has not been established:

If Left-hand side PC imposes a large amount of the renewal request of web contents repeatedly onWeb srver, not for the purpose of displaying the latest version of the web contents but also for the purpose of making Web server busy then the HTTP synflood attack against Web server is much more malicious than the Denial-of-Service attack, because the former attack does not only keeps some of Web server's ports open for a long time, but also brings about the Denial-of-Service attack against Right-hand side PC with a large number of SYN-ACK packets simultaneously. The comparison of these attacks with each otehr can be summarized as the following (Table 2):

the sender's IP address	not falsified	falsified
primary target	Web server	Web server
how to attack	DoS	Synflood
involvd victim	none	another PC

Table 2: HTTP synflood attack and HTTP reflection attack.

Conclusion

In the former half of this paper, the network structure where the ICMP packet interception happens is the same as the ICMP reflection attack happens and the difference between these two attacks results from casting roles such as a cyber attacker and a victim in the networks, and in the latter half of this paper, while the ICMP reflection attack can be brought about by the same way as the HTTP reflection attack, the ICMP reflection attack does not bring about any other attack such as the HTTP synflood attack, which is induced by the HTTP reflection attack.

Competing Interests

The authors declare that they have no competing interests.

References

1. Santos O, Muniz J (2017) CCNA Cyber Ops Secfnd 210-250. Cisco Press, Indianapolis, 1st edition.

```
C:¥>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.0.2:80          192.168.1.2:1028       CLOSED
C:¥>
C:¥>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.0.2:80          192.168.0.2:1027       SYN_RECEIVED
C:¥>
```

Figure 4: The HTTP synflood attack recorded in Web server.

2. Knuth DE (1973) The Art of Computer Programming. Addison-Wesley Publishing Company, Massachusetts, 2nd edition.
3. Loukas G, Oke G (2010) Protection against Denial of Service Attacks: A Survey. Comput J 53: 1020-1037.
4. YChen Y, Hwang K, Kwok YK (2005) Filtering of shrew DDoS attacks in frequency domain. The IEEE Conference on Local Computer Networks 30th Anniversary.
5. Ben-Porat U, Bremler-Barr A, Levy H (2013) Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks. IEEE Transactions on Computers 62: 1031-1043.

This article was originally published in a special issue:

Computational Analysis and Modeling

Handled by Editor:

Prof. Shigeo Akashi
Department of Information Sciences
Tokyo University of Science
Japan