International Journal of
Advanced Science and Convergence

ISSN : 2619-8150
Volume 1, Number 4, December 2019
https://doi.org/10.22662/IJASC.2019.1.4.017

Research on Advanced Management of Network Traffic

Sunghyuck Hong[1]

[1]Division of Information & Communication Technology, Baekseok University, Cheonan, 31065, Republic of Korea

Abstract

Background/Objectives: Network traffic forms a lot in many modern server communication worlds. **Methods/Statistical analysis:** As a result, the network can exchange data with each other, and the sudden increase in trapping results in malfunction and communication error due to server overload. **Findings:** Traffic spikes can be attributed to scheduled backups within the LAN, remote backup programs, mail servers, software (SW) upgrades, malware generation and hacking attempts. In general, a small increase in traffic that is easily seen by everyone is likely to recover after a while. However, when traffic attacks coming from too much traffic and hacking intentions, fast network traffic detection, and responses are needed. **Improvements/Applications:** Therefore, the proposed proposal is proposed to maintain the causes of network traffic surges and countermeasures.

Index Terms

Network, Traffic, Bandwidth, IP, DDoS, UDP, TCP, PPS

Corresponding author : Sunghyuck Hong
shong@bu.ac.kr

• Manuscript received November 28, 2019.
• Revised December 19, 2019 ; Accepted December 20, 2019.
• Date of publication December 31, 2019.

I. Introduction

As the use of various services increases in modern society, network traffic usage is exploding. The network traffic analysis market is dominated by the rapid increase in data traffic caused by increased access to cloud computing, AI, IoT and global Internet. Figure 1 shows global IP traffic growth.

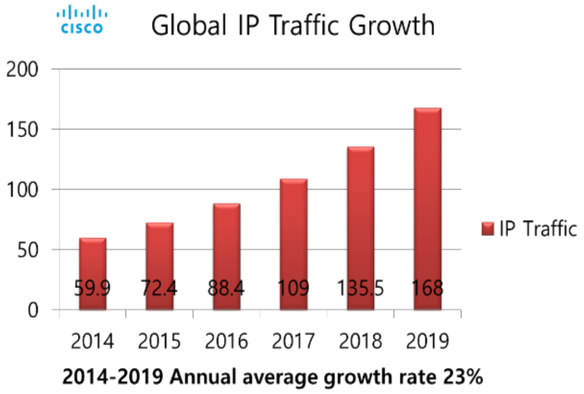


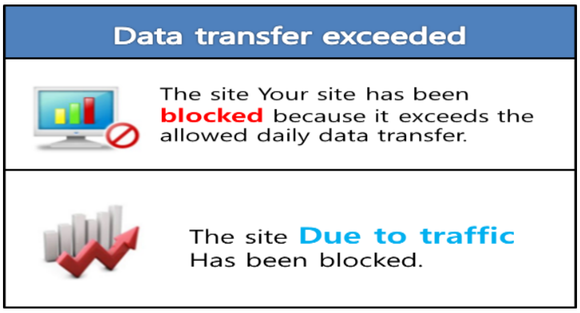
Fig 1. Global IP Traffic Growth

Data communications in telecommunications systems are developed and built by the International Systems Standardization (Open Systems Interconnection - OSI) seven-layer reference model and the International Organization for Standardization (ISO) [2].

In such a network, a network management system (NMS) plays a very important role. However, despite the ongoing management, there are too many to handle the communication of various servers and clients around the world, so perfect management is quite difficult. Thus, this report is organized as follows. First, Chapter 2 describes network traffic, Chapter 3 describes four cases of traffic spikes, and Chapter 4 describes traffic attacks and detection methods. Finally, we conclude with a summary of the contents of this report.

II. Network Traffic

Network is a compound word composed of Net which means network and work which means communication work, and functions that support connection including devices such as routers and hubs, and cables and connectors. It consists of. The types of networks are usually divided into sizes, including PAN, LAN, MAN, WAN, VAN, and Integrated Services Digital Network (ISDN). In addition, each network management system (Network Management System) exists for each network in scale and operates with five main functions: configuration management, fault management, performance management, account management, and security management [3].



Data transfer exceeded

The site Your site has been **blocked** because it exceeds the allowed daily data transfer.

The site **Due to traffic** Has been blocked.

Fig 2. Traffic Error

Networks are generally likened to telephones, couriers, and traffic so people can easily understand them. The most commonly used among them is to use the meaning of the same term in the network. Traffic is known as the word traffic, and it is so called because sending and receiving data via server communication is so similar to moving between highway cars. In practice, network traffic refers to the load on a communication system and the amount of data sent and received. For example, if 10 servers download 10MB of files, the traffic is 100MB. However, if there are various data in the world and many servers receive the same data at the same time, if the same data is received multiple times, each try to receive different data at the same time, the traffic increases too suddenly and exceeds the traffic usage. Do it. In general, you may have seen a lot of screens as shown in Fig. 2. Therefore, there is a need for solutions such as decentralizing traffic usage, checking traffic usage from time to time, or waiting for a user after a certain period of time[4].

III. Traffic spikes

A. *Increase in traffic*

Recently, internet traffic is increasing rapidly. The increase in the number of traffic starts with the widespread use of the Internet as the server communication network evolves and the technology for handling traffic and the development of various application services. However, this traffic surge overloads network servers of Internet Service Providers (ISPs) and restricts and blocks traffic on their own. As a result, the government is preparing a traffic management policy globally. In December 2013, the Korea Communications Commission decided to establish 'standards on rational management, utilization of network and transparency of traffic management'. According to traffic history, traffic management refers to the technologies that ISPs use when they determine that traffic needs to be restricted, distributed, or prioritized. As a result, traffic surges are increasing, and problems need to be prevented by analyzing the causes and solving them through management [4].

B. Causes of traffic spikes

Increasing network traffic has many causes, including large file sharing among research institutes, corporate applications, storage and computing moving to the cloud, as the number of IPs increases worldwide. If you are a competent system administrator, you must identify, identify, and resolve the root cause of the problem. Investigations by many network users have identified four major causes of traffic spikes.

(1) Scheduled backup job inside the LAN

Backup is to copy and save the original in case the original data is damaged or lost due to user's personal mistake, computer error or virus. Regular backups are insignificant in any way. In most environments, schedule backups to run at specific time intervals or time zones. Backup is usually a task that involves a significant amount of data and consumes a lot of bandwidth in such a short time. Therefore, if you plan to back up frequently or back up large amounts of data, you should prepare your backups at your leisure. [5]

(2) Remote backup program

Many networks use cloud-based systems to protect and manage their data. This applies more to external backups than to backups within a LAN. In most cases, it is added to a local backup. After all, uploading equally large amounts of data has a significant impact on bandwidth. Other web programs or applications slow down or stop working completely. Just like a regular LAN internal backup, you'll need to choose your time zone.

(3) Software Updates and Releases

Recently, as digital data such as financial and important documents increase, viruses also increase. Vaccine programs work for data integrity and protection by preventing and preventing the penetration of viruses. Thus, most programs repeat their updates to ensure the safety of the system against new security threats and intrusions. Vaccine program updates of computers in the network are distributed over the LAN to reduce bandwidth consumption. However, since the update size can also grow in some cases, traffic spikes can occur. If a computer updates its own software on the network, it can cause congestion on the Internet. Whenever possible, software and operating system updates should be distributed over the LAN. Otherwise, something that could be a simple update could affect the speed of the Internet and even interrupt it.

(4) mail server problems

Sending and receiving e-mail is the most common and basic task your network must perform. Emails with simple sentences or small files don't burden the network, even if you have a lot of users. However, if a problem occurs in sending and receiving mail, the mail server problem is persistent. Problems with traffic usually include sending a large file to an attached email or to many recipients. If there are other bandwidth spikes, there are three steps to find and correct the cause. First, watch the time when problems occur. If you see a certain pattern, look it up against the rest of the system. Then analyze the traffic with Packet Sniffer or Flow Monitoring tools. There are a few major causes of this, but with the opening of the Internet of Things and big data, the amount of data in the network has increased dramatically. This is the age of the Internet of Things (IOT), where all things are connected, but in the future, we are moving towards the age of the Internet of Everything (IEO), where everything can be acquired with data. As users service and receive all data on the network, traffic continues to increase and network efficiency decreases [6].

C. Traffic congestion attack

Traffic spikes may be a natural phenomenon in your business or in everyday communications, but sometimes intentional attacks. This is called a traffic attack. A traffic attack is a form of system resource exhaustion such as network bandwidth and processing power that prevents normal service activity. By collecting and analyzing the data that caused the traffic congestion, more accurate attacks can be detected. The most representative example of a traffic attack is a Distributed Denial of Service Attack (DDoS) attack, which is increasing every year as shown in Fig. 3.

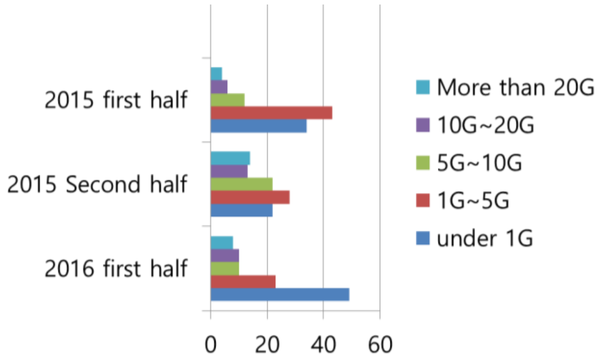


Fig 3. Semi-annual DDoS attack traffic volume

IV. DDoS

A. DoS/DDoS

As the use of the Internet increased rapidly, security investments were less than the structural stability of the system in the age of providing various services by general companies and public institutions. So hackers used it to attack using malicious hacking programs such as DoS / DDoS. DoS penetrates the network, causing massive data access, paralyzing the computer, and blocking it from other signals. DDoS is a way of seeing DoS as an extension and paralyzes service systems by generating massive access traffic at once. As shown in Figure 4, the attacker (Attacker) paralyzes the victim (Victim) at once with the distributed zombie (Zombie) evenly distributed through the master.

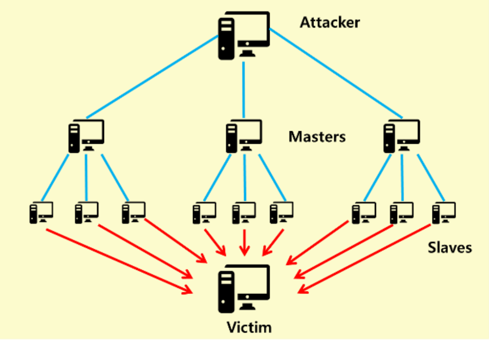


Fig 4. DDoS Attack

B. DDoS Attack

The biggest feature of DDoS attacks is that the attacker hides himself (IP Spoofing) and attacks with multiple agents. It is not easy for a target to trace back and know where the attack came from and how to block and defend it. Since DDoS is based on a distributed system, at its discretion, an infinite number of attack paths are possible, and other attacks can be exploited to proactively create damage. A new version of the DDoS program is emerging as a modified version. A recent variant of attack is distributed reflection denial of service. DDoS is a strongly applied type of attack because it can circulate a portion of a list of reflector servers and send traffic intensively and continuously to an attacker, and constantly use the attack route [7].

Table 1. DDoS Attack methods

Division	Bandwidth Consuming	PPS Consuming	HTTP Flooding
Protocol Using	UDP/ICMP	TCP Syn	HTTP
Attack PC Location	Domestic/ Overseas	Domestic/Overs eas	Domestic
IP Modulation	Modulation /Real IP	Modulation/Rea l IP	Real IP

Refer to Table 1 to see the attack methods. First, there is a bandwidth exhaustion attack using UDP and ICMP that exceed the bandwidth processing limit by transmitting a large amount of data using multiple PCs. In addition, there is a method of consuming PPS that increases CPU load of network equipment or servers by increasing packet per second (PPS) using TCP, and directly attacks through excessive web access [8].

C. DDoS Attack Detection and Countermeasures

DDoS attacks are indirect and remote, but they come in contact with the target. By detecting the network abnormality first through NMS and monitoring and analyzing the traffic as shown in Table.2, I can see the cause of the traffic surge [9].

Table 2. Traffic Monitoring and Analysis Tool

Traffic Analysis	NetFlow, cflowd, FlowScan, SnifferPro, I-Packet
Network Performance	ping, traceroute, Network Vantage, NetPerf
Network Monitoring	MRTG, RMON
Visualization	RRD

Traffic information can be obtained through SNMP, MIB, RMON MIB, tcpdump, etc. and detects DDoS traffic attack using Neflow or data mining technique. Host, web server, and broadband network-based detection technologies exist, respectively, and analyze traffic patterns or monitor and confirm malicious code (Zombie) infected systems [10].

Table 3. DDoS Attack Countermeasures

Division	**Role**
precautionary measure	Safety homepage operation
	DDoS Detection / Response
	Strengthen user PC security
	Establish monitoring world
	Security organization and personnel training
	International Cooperation System
Respond after an accident	Establishment of attack spread prevention
	Network block

Countermeasures against DDoS attacks can be largely prevented and dealt with immediately after an accident. The prevention side is to operate a safety homepage, detect and respond to DDoS, strengthen the security of the user's PC, establish a monitoring system, foster security organizations and manpower, and cooperate with the international cooperation system. Typically, after an accident, methods of preventing attack spread and blocking the network exist. See Table 3.

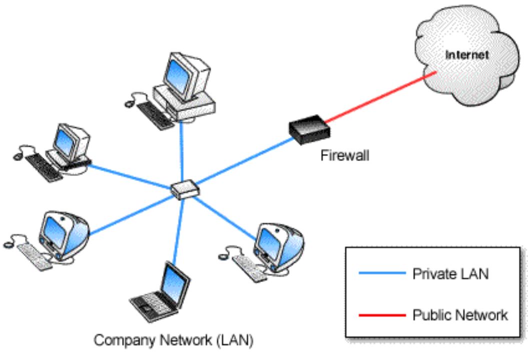


Fig 6. Configuration of Firewall

The common way everybody knows is a firewall. A firewall is a security system that monitors and controls network traffic. It works on the principle of creating a barrier between the internal network and the external network as shown in Fig. 6. Firewalls are devices that control network traversal and allow, deny, censor, and modify data as they are sent and received, depending on the level of trust [11].

V. CONCLUSION

Network traffic is becoming a very important figure in today's world. Many users are uncomfortable with this excess of traffic, and the causes are close enough to us and often happen. Network paralysis caused by traffic spikes can be intentionally created by attackers using hacking programs such as DDoS. Since DDoS attacks spread across multiple servers, it is not easy to trace back where the malware came from or who the attacker is. But countermeasures such as hardening PCs, blocking or monitoring the network continue to emerge, protecting our network from network traffic attacks.

ACKNOWLEDGMENT

This research is supported by 2019 Baekseok University Research Fund.

REFERENCES

[1] Hong, S., & Lopez-Benitez, N. (2006). Enhanced Group Key Generation Algorithm. 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006. doi: 10.1109/noms.2006.1687639

[2] Hong, S. (2015). Hybrid Routing Algorithm on Mesh Network Based on Traffic Records. *Indian Journal of Science and Technology*, 8(S7), 327. doi:10.17485/ijst/2015/v8is7/70441

[3] Hong, S. (2013). User Behavior Based Authentication on Mobile Network. *International Journal of Advancements in Computing Technology*, 5(11), 233–237. doi: 10.4156/ijact.vol5.issue11.25

[4] Zhao, G.-F., Lai, W.-J., Xu, C., & Tang, H. (2014). Revealing Service Visit Characteristics in Mobile Internet. *Chinese Journal of Computers*, 36(7), 1388–1398. doi: 10.3724/sp.j.1016.2013.01388

[5] Duffield, N. G., & Whitt, W. (n.d.). Network Design and Control Using On/Off and Multilevel Source Traffic Models with Heavy-Tailed Distributions. *Self-Similar Network Traffic and Performance Evaluation*, 421–445. doi: 10.1002/047120644x.ch17

[6] Lee, J.U. (2018). Reduction of tactical network traffic using radio access network caching Master`s Thesis. ChungAng University, Seoul

[7] Seo, D. H. (2009). An Efficient Dynamic Packet Filtering for Defense of DDoS Attacks. Master`s Thesis. Ajou University, Seoul

[8] Hong, S. (2016). Secure and Efficient Authentication Protocol on Cloud: Survey. *Indian Journal of Science and Technology*, 9(37). doi:10.17485/ijst/2016/v9i37/102544

[9] Bin, J. M. (2016). Study of the traffic management and virtualized IMS in the NFV/SDN, 10–18. Master`s Thesis. Korea Polytechnic University, Cheonan

[10] Yoon, Y.J. (2011). DDoS Attack Detection Method Using Average Rate of Change of Traffi Master`s Thesis. Chungbuk University, Cheongju

[11] Hong, S. (2015). Multi-factor User Authentication on Group Communication. *Indian Journal of Science and Technology*, 8(15). doi:10.17485/ijst/2015/v8i15/72941.