

A method for Real-time Detecting and Responding to Harmful Traffic

Eun Joo Kim

Network Architecture Research Team, Future Network Research Department
Electronics and Telecommunications Research Institute
138 Gajeongno, Yuseong-gu, Daejeon, 305-700, KOREA
E-mail : ejkim@etri.re.kr

Abstract—By rapid development and growth of the Internet, communications has developed into IP-based converged network, based on individual media convergence, such as broadcast, communications, Internet, etc.

With the development of network, security issues are very important in managing the network, especially defence against a distributed traffic attack causing traffic congestion can be called essential. In a distributed traffic attack, security management on the new unknown pattern of hazardous traffic as well as the defence against well-known patterns of hazardous traffic is necessary.

It is possible to block Internet attacks using defense technology including the sinkhole tunnelling, but real-time detection and response methods are not defined on the unknown traffic patterns, which do not require the sinkhole router.

In this paper, the authors propose real-time detection and counter-measures on harmful traffic such as a distributed attack traffic, viruses, etc.

Keywords- harmful traffic, DFI, DPI, DDoS

I. INTRODUCTION

Surge in demand for Internet services has made information and communications service providers give a lot of effort to provide a guaranteed network quality. The current security system has many problems, which can not provide to the user guaranteed network services that can quickly adapt at the time of DDoS attacks. Particularly as a large scale of decentralized network is becoming very close to users' lives, the need to protect these networks is increasing.

In recent years, various kinds of damages over the Internet have continued to occur. Especially in July of 2009, the severity of DDoS is widely recognized in society due to DDoS attack. The ministry of Public Administration and Security soon revealed its plan to invest 200 billion won in order to establish an emergency response system as part of countermeasures of distributed attack traffic.

In addition, according to data submitted from the Korea Communications Commission last October, 46% of all providers of Internet phone, 73% of special category of operators turned out to have very inadequate response capabilities in the event of a distributed service denial of attack (DDoS).

As response to harmful traffic is highlighted as an important social issue, proper responses to ongoing security problems are essential to meet the rapid evolution of the network.

II. RELEVANT RESEARCHES

In order to detect and prevent a Distributed Denial of Service (DDoS) attack, methods such as pattern-based filtering techniques or queue management techniques are typically used. In most cases, these typical methods observe traffic on a network and detect a DDoS attack, however, they have limitations in that only known patterns are detected and prevented.

In order to solve this limitation, there has been proposed a sinkhole tunneling technique in which data is caused to pass through a predetermined tunnel without changing the next hop address of a destination address, required operations such as access control list (ACL), rate-limit or analysis are performed in the tunnel, and then the data, when determined to be normal data, is let out of the tunnel such that the data can be sent to an original destination. This attack prevention method requires a sinkhole router connected to analysis modules, and needs to generate a tunnel that introduces packets from a router into the sinkhole router

However, no sinkhole tunneling techniques according to the related art define a method of detecting and responding to harmful traffic of unknown patterns is real time, without using a separate sinkhole router.

In this paper, we classify harmful traffic by 4 types, and suggest an effective method for detecting harmful traffic in IP network.

III. SYSTEM FOR DETECTING TO HARMFUL TRAFFIC

In this chapter, we suggest an effective method for classifying, detecting, and responding harmful traffic in IP network.

A. System

Proposed system provides a method and system for detecting and responding to harmful traffic, which can detect and respond to harmful traffic even of an unknown pattern, without using a separate sinkhole router.

Also it provides a method for detecting and responding to harmful traffic, which can detect and respond to harmful traffic infected with a virus containing an unknown signature, by using a pattern analyzer of a policy & resource control entity.

Also, it can detect and respond to harmful traffic including attack traffic and virus traffic by using the policy routing function of a router and a policy & resource control entity

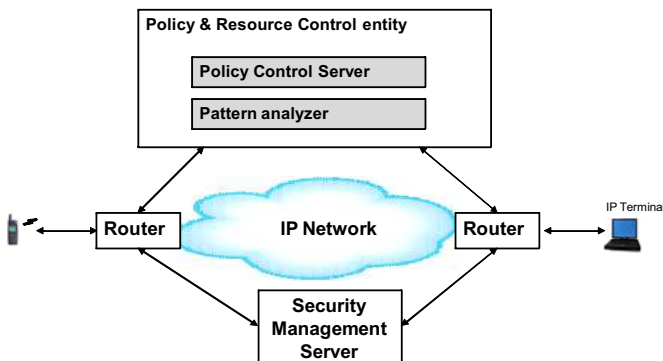


Fig. 1 System for detecting and responding to Harmful traffic

Fig.1 is a block diagram for explaining a method and system for detecting and responding to harmful traffic.

Referring to Fig 1, proposed system includes a router, a policy & resource control entity, and a security management server.

A transmission terminal and a reception terminal have IP addresses, and are capable of providing Voice over Internet Protocol(VoIP) services and Multi-Media over IP (MMoIP) services. Examples of the transmission and reception terminals may include cellular phones, portable digital assistants(PDAs) and smart phones.

- Router

The router has a policy routing function. The router determines whether or not received data is harmful traffic including a known pattern of signature by using a dynamic flow identification (DFI) function and a deep packet inspection(DPI) function. Simultaneously, the router sends Cflowd information of the received data to a pattern analyzer of the policy & resource control entity. The Cflowd information includes a source IP address, a destination IP address, a next-hop IP address, a packet, a byte, a flow start time, a flow end time, a source port, a destination port, and an IP protocol.

That is the router detects harmful traffic relevant to a distributed attack with a known pattern by using a DFI function, and detects harmful traffic relevant to a known virus by using a DPI function.

In addition, the router encapsulates data determined to be harmful traffic, by using an IP encapsulation function, adds a header, which designates the IP address of the security management server as a receiver, to the encapsulated data, and sends it to the security management server.

The major functions of the router for detecting harmful traffic are as follows.

- ✓ DFI(Dynamic flow identification)
- ✓ DPI(Deep Packet Inspection)
- ✓ Cflowd
- ✓ Policy Routing
- ✓ IP Encapsulation function

- Policy & Resource Control entity

The policy control & resource control entity exists in a transport stratum, and includes a policy control server and a pattern analyzer.

The policy control server sends DFI information and DPI information to the router so that the router can perform a DFI function and a DPI function. The DFI information includes ranges regarding duration, an average packet size, an average transfer rate, and a byte count. When data is out of such ranges, the router considers the corresponding data to be harmful traffic.

The Pattern analyzer determines whether or not received data is harmful traffic including an unknown pattern or signature by using Cflowd information received from the router, and sends the result of determination to the router.

The policy control & resource control entity for detecting harmful traffic must have a function and information as follows.

- ✓ Detecting function harmful traffic for pattern analyzer
- ✓ DFI, DPI, Cflowd information

- Security Management Server

The security management server receives encapsulated data from the router, and reconfirms whether or not the

encapsulated data is harmful traffic. When the encapsulated data is not harmful traffic, that is, when the encapsulated data is normal traffic, the security management server decapsulates the encapsulated data by using an IP decapsulation function, removes a header containing the IP address of the security management server, and then sends it to the router.

When encapsulated data is harmful traffic, the security management server stores a source IP address of the encapsulated data, deletes the encapsulated data, and sends information relevant to the source IP address to the policy control server.

B. Classification of harmful traffic

Harmful traffic includes distributed attack traffic, a virus and the like. The types of harmful traffic are as follows.

- Type of harmful traffic
 - ✓ Known pattern
 - ✓ Unknown pattern
 - ✓ Known Signature
 - ✓ Unknown Signature

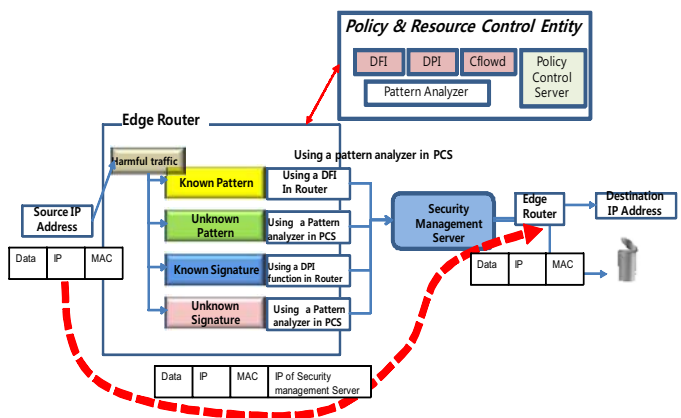


Fig. 2 Detecting method of harmful traffic

Pattern Search use detecting harmful traffic for distributed attack traffic and Signature Search use detecting harmful traffic for Virus.

C. Method of detecting and responding to harmful traffic

Fig. 3 is a flowchart showing a method of detecting and responding to harmful traffic, applied when the harmful traffic includes an unknown pattern or signature.

Referring to Fig. 3, the pattern analyzer receives Cflowd information of data received from the router , and determines, using the Cflowd information, whether or not the received data is harmful traffic including an unknown pattern or signature.

When the corresponding data is determined to be harmful traffic, the pattern analyzer sends the result of determination to the router, and the router encapsulates the data by using an IP encapsulation function. The router adds a header, designating the IP address of the security management server as a receiver, to the encapsulated data, and sends it to the security management server.

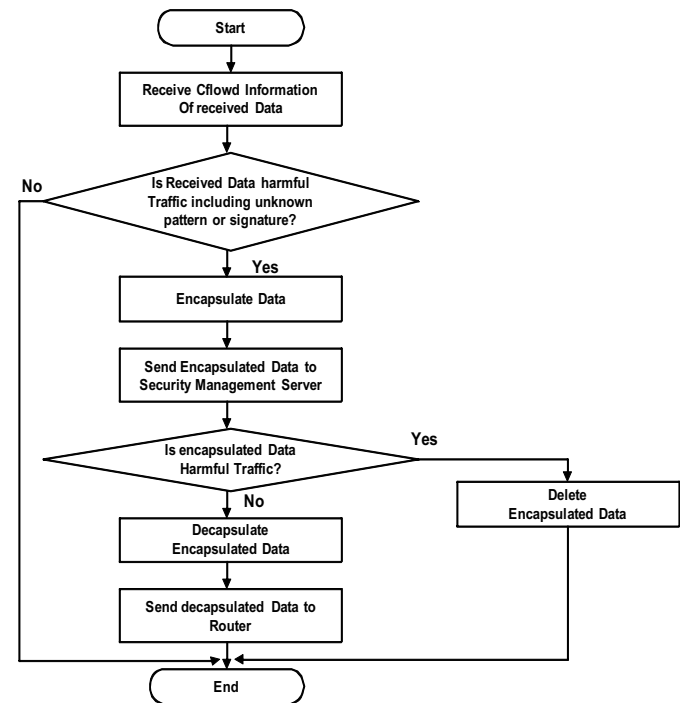


Fig. 3 Flowchart I (unknown pattern or signature)

The security management server reconfirms whether or not the encapsulated data is harmful traffic , and deletes the encapsulated data when the encapsulated data is confirmed to be harmful traffic.

When the encapsulated data is not harmful traffic, the security management server decapsulates encapsulated data, removes the header containing the IP address of the security management server, and then sends it to the router.

Fig. 4 is a flowchart illustrating a method of detecting and responding to harmful traffic, applied when the harmful traffic includes a known pattern or signature

Referring to Fig. 4, the router receives DFI information and DPI information from the policy control server in order to perform a DFI function and a DPI function, and determines, using the DFI function and the DPI function, whether or not received data is harmful traffic including a known pattern or signature.

The router encapsulates the data using an IP encapsulation function. The router adds a header, designating the IP address of the security management server as a receiver, to the encapsulated data, and sends it to the security management server.

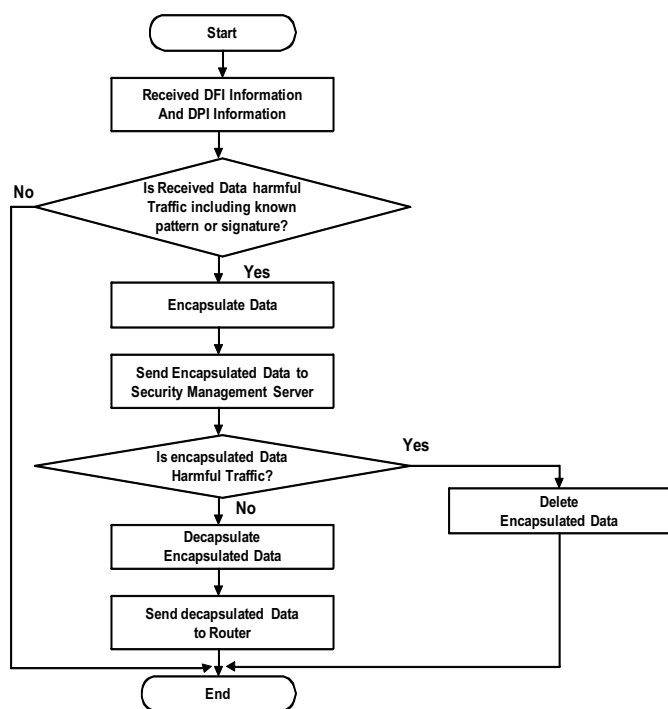


Fig. 4 Flowchart II (known pattern or signature)

Fig. 5 is a flowchart illustrating a method of responding to harmful traffic.

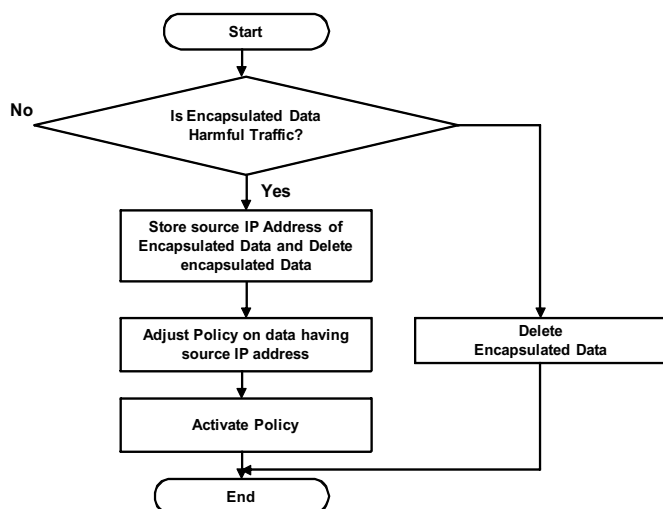


Fig. 5 Flowchart III (example)

Referring to Fig. 5, the security management server receives encapsulated data from the router and reconfirms whether or not the encapsulated data is harmful traffic.

When the encapsulated data is harmful traffic, the security management server stores the source IP address of the encapsulated data, and deletes the encapsulated data.

Thereafter, the security management server sends the source IP address to the policy control server. Then, the policy control server adjusts the policy on data having the source IP address, and activates the policy by sending it to the router. That is, the policy control server causes the router to manage the QoS(E.g., rate limit or the like) of data having the source IP address and to control a data flow from a user using the source IP address.

When the encapsulated data is not harmful traffic, the security management server decapsulates the encapsulated data, and sends it to the router.

IV. CONCLUSIONS

As the communication network is evolved dramatically, the need for establishing secure communication increases responding the cyber terrorism.

This paper relates to a method and system for detecting and responding to harmful traffic in real time in an All-IP convergence network, and more particularly, to a method and system for detecting and responding to harmful traffic, capable of facilitating the implementation of a sinkhole tunnel technique even in the case of an unknown pattern of harmful traffic, which includes a distributed attack and a virus, by using the policy routing function of a router and a policy & resource control entity.

REFERENCES

- [1] Internet Security System (ISS) White Paper "Distrubuted Denial of Service Mitigation", 2002
- [2] Byung-Hak Song Seung-Yeon Lee Choong Seon Hong Eui-Nam Huh Seongwon Sohn, "Anomaly Detection Mechanism against DDoS on BcN, Internet Information Conference, Vol 8 No.2, 2007.04
- [3] Chan Kyou Hwang, Jong Kyu Seong, Min Hyung Lee, Jae Hyung Yoo, "Design of Implementation on real-time Anomaly Traffic Lookup & Analysis System", KNOM Review, Vol. 10, No.1, August 2007