

# Analysis of SIP Traffic Behavior with NetFlow-based Statistical Information

Changyong Lee\*, Hwankuk-Kim, Hyuncheol Jeong, Yoojae Won

Korea Information Security Agency, IT Infrastructure Protection Division  
78, Garak-Dong, Songpa-Gu, Seoul, Korea, 138-803  
{chylee, rinyfeel, hejung, yjwon}@kisa.or.kr

**Abstract.** With the population of an internet telephony, the security issues of a SIP application service is focused on, currently. For example, VoIP is easier to access than existing PSTN, and more exposed at many security threats. However, there is not enough monitoring and attack detecting devices, yet. In this paper, we propose analysis factors, a detection example to use it and required collecting information for the detection to analyze and monitor SIP traffic. Basically, we use NetFlow format, for collecting SIP information that is commonly used for broadband traffic monitoring.

**Keywords:** SIP, abnormal traffic, behavior-based detection, NetFlow version 9

## 1 Introduction

SIP(Session Initiation Protocol)[1] is an application level signaling protocol that establishes, finishes and controls multimedia sessions, such as VoIP(Voice over Internet Protocol), internet conference and IM(Instant Messages) services. Recently, SIP protocol has become populated with VoIP service revitalization, and is expected to be used widely as a main call establishment protocol with its potential possibility.

However, new security threats are expected to be appeared with the new service. Basically, it is implemented over IP network, and it inherits every security threats of IP network. In addition, appearance of new security threats specified by VoIP characteristic is forecasted. Currently, most of VoIP service use SIP for call set up, and use RTP[2] for media transportation. Therefore, various security threats using characteristics of SIP and RTP are prospecting to be appeared.

DoS, scan and some other existing IP based network attacks can be detected and prevented by the existing network security solutions (e.g. firewall, IPS (Intrusion Prevention System)). Generally, they use 5-tuple information (source IP/port, destination IP/port, protocol) inside of IP headers. However, this way of measure is not appropriate to VoIP's case. SIP protocol uses an additional identifier, URI

---

\* Corresponding author

This work was supported by the IT R&D program of MKE/IITA. [2008-S-028-02, The Development of SIP-Aware Intrusion Prevention Technique for protecting SIP-base application Services]

(Uniform Resource Identifier), for user identification and application header is located in a payload of IP packet. Therefore, with existing solutions that check only IP headers, it is impossible to account SIP/RTP traffic

SIP-based application service uses more factors than IP header information for its service providing. It uses URI information for user identification and Call-ID for call identification. SIP proxy server forward every signaling messages for application level routing. Existing security devices, such as firewall and IDS(Intrusion Detection System), detecting and blocking network attacks based-on IP header information, cannot analyze and detect abnormal SIP traffic exactly, and efficiently.

NetFlow is the most popular flow data format usually used for IP traffic monitoring. Originally, it was proposed for efficient packet switching and traffic monitoring, but currently it is used for abnormal traffic detection and anti-DDoS solutions. Nowadays, NetFlow version 5 is the widely used format, but version 5 uses static template and it can contain only information of IP header. In early 2000s, NetFlow version 9 has been proposed, and it has an extended header and configurable template idea. Therefore with NetFlow version 9, it has become to be able to analyze and detect abnormal SIP traffic.

In this paper, we describe characteristics of SIP traffic behavior and propose some analysis factors and detection examples for analysis of SIP traffic behavior.

The remainder of this paper is organized as follow. In Section 2, we give related work. We describe characteristics of SIP traffic and NetFlow version 9. And introduce some pre-proposed works. In Section 3, we propose scheme for SIP traffic analysis. We conclude the paper in Section 4.

## 2 Related Work

In this section, we describe characteristics of SIP traffic, and introduce NetFlow version 9. Additionally, we introduce some previous works about NetFlow and SIP traffic analysis.

### 2.1 Characteristics of SIP protocol

SIP based application service is based on IP network, and the traffic pattern at L3 layer is not so different from the other network services' traffic pattern. However, SIP based service uses additional L7 information for its routing, and

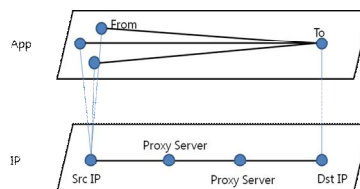


Fig. 1. The shape of traffic patterns at IP and application layer

Fig. 1 is an example of difference between L3 and L7 level SIP traffic pattern analysis. In the case, that an attacker performed attack by spoofing From URI information, it's L3 level pattern looks like a normal communication between two terminals. However, it shows a different pattern at L7 layer level.

Especially, SIP services uses URI for user identification and all SIP signaling traffic is sent to the destination via SIP proxy server. Every SIP signaling messages are sent to a proxy server, and the proxy server matches From/To URI and their real IP address. In this process the proxy server changes SIP packet's destination IP address each time, and it is not possible to find out the packets' final destination only with IP/port information.

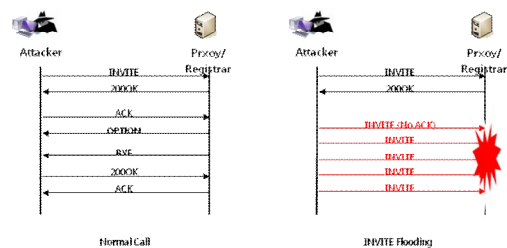


Fig. 2. INVITE Flooding

The abnormal pattern of SIP traffic can be characterized by type of transmitted messages. SIP session is established by transaction of SIP request and response messages, such as INVITE, 200OK, ACK. In normal condition of calls, the ratio of SIP messages is maintained as designated value. For example, normally, REGISTER method is the most frequently sent method, and ratio of INVITE and BYE is almost same. However, in abnormal condition, the shape of the ratio is different. Fig. 2 is very simple INVITE flooding attack. In INVITE flooding attack, the attacker overwhelms INVITE messages to a proxy server in a short time, and the ratio of INVITE messages increase instantly.

## 2.2 NetFlow version 9

NetFlow[3,4] is a traffic statistical information format that is developed by Cisco. Originally, the purpose of this format was adding efficiency to traffic switching by monitoring traffic volume of each network nodes. Existing network switches implemented based on packet-unit treatment, and it could not treat a huge of packets. NetFlow.

Nowadays, NetFlow version 5 is most widely used in industry. It has static header structure and can contain only 5-tuple information (source and destination IP/port, protocol). However, NetFlow version 9 is designed with extended and dynamic header idea. User can design the template of NetFlow and it can contain various types and contents of information. With this flexible structure, NetFlow version 9 can be applied various traffic monitoring, and so can SIP traffic monitoring and analysis. Currently, it is not the most common flow format at industry, yet. However, IETF has

chosen it as IPFIX standard flow format, and it is expected to be used widely for IPv6 or Layer-7 application service traffic management.

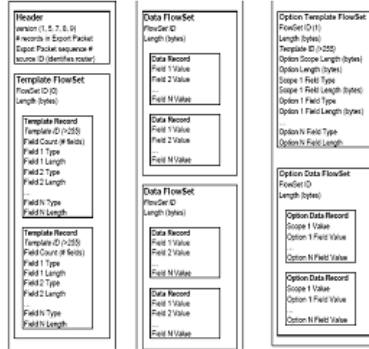


Fig. 3. The format of NetFlow version 9

### 2.3 Previous Proposals

Open source software, Nprobe[5] has supported generating NetFlow version 9 that containing some of SIP/RTP traffic information with SIP/RTP plug-in. However, its basic NetFlow export key depends on IP header information(5-tuple info.) And its developed as a IP level flow probe that has additional function to collect SIP information. As it is said above, SIP application services routes its signaling messages based-on URI information at layer 7 level, and NetFlow version 9, generated by Nprobe plug-in is not suitable for exact SIP traffic analysis. Table 1 shows the metrics of Nprobe plug-in. The scope of metrics is not enough to analyze SIP. In 2007, Romad et al proposed enhanced template of NetFlow version 9 to extent its usage, and it contains some SIP traffic information. However, it used export keys based-on IP header information, too. And collected information was almost same as Nprobe's collection information.

Table 1. VoIP metrics that can be measured by nProbe

SIP	RTP
SIP_CALL_ID	RTP_FIRST_SSRC
SIP_CALLING_PARTY	RTP_FIRST_TS
SIP_CALLED_PARTY	RTP_LAST_SSRC
SIP_RTP_CODECS	RTP_LAST_TS
SIP_INVITE_TIME	RTP_IN_JITTER
SIP_TRYING_TIME	RTP_OUT_JITTER
SIP_RINGING_TIME	RTP_IN_PKT_LOST
SIP_OK_TIME	RTP_OUT_PKT_LOST
SIP_ACK_TIME	RTP_OUT_PAYLOAD_TYPE
SIP_RTP_SRC_PORT	RTP_IN_MAX_DELTA
SIP_RTP_DST_PORT	RTP_OUT_MAX_DELTA

### 3 Proposed scheme

#### 3.1 An Assumption of the scheme

To implement the proposed NetFlow based SIP traffic behavior analysis, the following should be assumed.

- All the traffics of the network should be collected by SIP-based NetFlow generator with port mirroring or network tapping.
- All the traffics of the network should be transmitted as plaintext, without any encryption process.

#### 3.2 Collecting Information for SIP traffic behavior analysis

SIP-based NetFlow version 9 should satisfy the following requirements for SIP traffic behavior analysis.

- The flow should be generated based-on SIP session.
- Application service user and session identifier, URI, Call-ID, SSRC information should be collected.
- Main methods (e.g. INVITE, REGISTER, OPTION, BYE, CANCEL,) and Status code information should be collected.

As Fig. 4 shows, SIP traffic has characteristics at 3 aspects, user behavior, call behavior, server and network status.

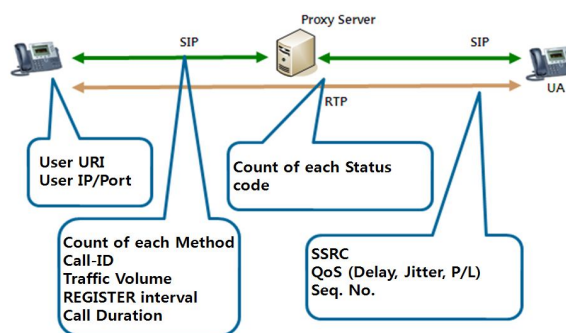


Fig. 4. Characteristics of SIP traffic

- User behavior
  - In general IP traffic behavior analysis, IP/port information is used as a main analysis factor. SIP application service uses URI for user identification, and it should be additionally considered URI information.
- Call behavior
  - Every calls has its unique signaling identifier, Call-ID, and media identifier, SSRC.
  - Normal calls are established by transaction of INVITE, 200OK, BYE messages. Generally, in normal situation, sending ratio of each method is maintained as a designated value.
  - REGISTER methods are sent every 3,600 seconds in general.
- Server and network status
  - As RFC 3216, proxy servers return corresponding status code such as 200OK, 403 Not Found, for each method that is sent from the others. Therefore, by analyzing sent status code, network or server status can be monitored.

### 3.3 Analysis and Detection of abnormal SIP behavior analysis

In this paper, we propose analysis factors to analyze SIP application traffic in 3 aspects, user behavior, call behavior, server/network status.

**Table 2.** VoIP metrics that can be measured by nProbe

	Analysis factor
User behavior	<ul style="list-style-type: none"> <li>• From/ To/ Call-ID ratio</li> <li>• Top N traffic user report</li> <li>• interval of REGISTER</li> </ul>
Call Behavior	<ul style="list-style-type: none"> <li>• ratio of Call-ID/SSRC</li> <li>• ratio of Req/Res</li> <li>• ratio of methods</li> <li>• ratio of IP and URI of REGISTER messages</li> <li>• Randomness of RTP Seq. No. for each SSRC</li> </ul>
Server/Network Behavior	<ul style="list-style-type: none"> <li>• changes of SIP/RTP traffic volume</li> <li>• ratio of status code for each server</li> <li>• changes of QoS</li> </ul>

With above factors, it is possible to define patterns of abnormal SIP traffic. And with appropriate threshold adoption, it can be used to detect abnormal SIP traffic.

For example, in INVITE Flooding situation, attackers normally duplicates INVITE messages for fast attack. So at the factor, 'From/To/Call-ID ratio', the number of Froms should be much bigger than the number of Call-IDs. And there should be no RTP traffic corresponding SIP messages. Therefore, as a characteristic of call behavior, the ratio of Call-IDs should be much bigger than the ratio of SSRCs. Additionally, SIP traffic volume should be increase instantly, and ratio of INVITE

messages should be bigger instantly. For the threshold value for each factor, we recommend to use the average value of 3 months' traffic information for same day of the week and same time.

## **4 Conclusion and Future Works**

In this paper, we describe layer-7 characteristics of SIP traffic and analysis factors to analyze its behavior. Existing traffic monitoring and analysis schemes were simply used to monitor highly loaded traffic node, source and target. However, the proposed scheme can be used to detect abnormal SIP traffic behavior, and with this scheme, more exact and efficient service traffic management can be expected to be implemented.

The detail detection algorithm is not established yet. And we are on the process to implement abnormal SIP traffic detection system now. Therefore, we are going to detail the algorithm and update it, and derive experimental result to verify this scheme. This is our future work.

## **References**

1. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002
2. H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January, 1996
3. Cisco Systems "NetFlow Services and Applications", White Paper, July 2002.
4. Cisco Systems "Cisco IOS NetFlow version 9 Flow-Record Format", White Paper, 2004.
5. L. Deri, "nProbe: an Open Source NetFlow Probe for Gigabit Networks", TERENA Networking Conference, 2003.