Copyright ⓒ 2009 KSII

Stateful Virtual Proxy for SIP Message Flooding Attack Detection

Ha-Na Yun[1], Sung-Chan Hong[2] and Hyung-Woo Lee[1]
[1] School of Computer Engineering, Hanshin University,
411, Yangsan-dong, Osan, Gyyunggi, Korea
[e-mail: ha1na11@nate.com, hwlee@hs.ac.kr]
[2] Div. of Information & Telecommunication, Hanshin University,
411, Yangsan-dong, Osan, Gyyunggi, Korea
[e-mail: schong@hs.ac.kr]
*Corresponding author: Hyung-Woo Lee

Received April 24, 2009; revised June 5, 2009; accepted June 8, 2009; published June 22, 2009

Abstract

VoIP service is the transmission of voice data using SIP protocol on an IP-based network. The SIP protocol has many advantages, such as providing IP-based voice communication and multimedia service with low communication cost. Therefore, the SIP protocol disseminated quickly. However, SIP protocol exposes new forms of vulnerabilities to malicious attacks, such as message flooding attack. It also incurs threats from many existing vulnerabilities as occurs for IP-based protocol. In this paper, we propose a new virtual proxy to cooperate with the existing Proxy Server to provide state monitoring and detect SIP message flooding attack with IP/MAC authentication. Based on a proposed virtual proxy, the proposed system enhances SIP attack detection performance with minimal latency of SIP packet transmission.

Keywords: SIP, SIP message flooding attack, attack detection, SIP state diagram, VoIP

This research was supported by the Ministry of Knowledge Economy, the Korean government, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2009-(C1090-0902-0016)).

DOI: 10.3837/tiis.2009.03.003

1. Introduction

VoIP (Voice over Internet Protocol) [1] service is a technology to transmit voice data through an IP network. VoIP provides various supplementary services with low communication cost. It can maximize the availability and efficiency of existing IP-based network resources. In addition, the users can use voice call service at any time and in any place, as long as they can access the Internet.

VoIP initially used the H.323 protocol [2] to provide such services. However, the H.323 protocol, which was developed to support multimedia communication in a LAN environment, is limited in building an expanded network and supporting a large number of users. In addition, the H.323 protocol has shortcomings in that the implementation of services is complex and compatibility is not guaranteed. SIP (Session Initiation Protocol) [3] was introduced recently to solve the shortcomings. It is growing rapidly as an alternative standard to H.323.

SIP is exposed to IP-based attacks and threats, since it also uses existing IP. Observed cyber threats to SIP services include wiretapping, denial of service, and service misuse, which are applicable to existing IP-based networks. These attacks are also applicable to SIP and continuously cause problems. Recently, various forms of attacks have been suggested as threats to SIP. However, most of them are formed by modifying or replacing messages transmitted through SIP or hindering call set-up.

The header and the body of a message are transmitted in the form of ordinary text in SIP. Thus, it is possible for attackers to make a malformed message attack by inserting different characters or modifying or deleting characters. In addition, a SIP message flooding attack sends abnormal SIP session packets continuously in the same process used by SIP users or service providers to provide normal services. When these SIP attacks are made, SIP service may stop or function abnormally and its quality is degraded. Accordingly, it is necessary to find active measures against attacks on the vulnerabilities of SIP.

Various studies have been made on how to cope with attacks on SIP including: (1) technique that use message authentication functions, such as HTTP authentication that prevents replay attacks, and provides the user authentication function [4]; (2) TLS technique that establishes a credible interval between hops and provides the confidentiality and integrity of SIP messages through encryption/decryption of SIP messages [5]; and (3) S/MIME (Secure/Multipurpose Internet Mail) technique that provides security functions to SIP users, and provides the confidentiality, integrity, and mutual authentication of messages [6].

However, these techniques have limitations in that they cannot cope with new attacks immediately and increase the delay and system load. Moreover, where attackers use various attacking tools (e.g. Sivus, Fuzzer, spitter, and redirect poison) they cannot detect and cope with them actively.

Currently, the proxy server executes the user registration process and each user (client) executes the SIP call connection process through the proxy server to provide SIP services. This process is a preparation step for using RTP (Real-time Transport Protocol) protocol [7]. RTP is a transmission service between users to support real-time data transmission. Using RTP, users can exchange data in real-time. SIP service is provided through these processes. When the call is terminated, the client terminates the call by exchanging session information with the proxy server.

Attacks on SIP are made by attacking messages transmitted between the SIP proxy server and users. Measures against these types of attacks should be developed, since attackers can perform sniffing and scanning attacks, MITM (Man In The Middle) and DoS attacks, etc. on SIP session information transmitted to the SIP proxy server [8][9][10].

We can encrypt/decrypt SIP session information transmitted between the proxy server and users, but this causes additional overload on the proxy server and transmission delay. Packets transmitted between the SIP proxy server and users should be classified and analyzed clearly to solve the vulnerabilities of existing SIP-based VoIP services. SIP attacks should be detected/blocked in advance based on the results.

This study proposed an attack detection/blocking method that adds a virtual proxy to the existing SIP proxy server to complement the insecure and vulnerable points of SIP services. This analyzes SIP sessions based on state information, and detects/blocks attacks through real-time analysis.

In the next section, we analyze related work on the SIP basic protocol and its vulnerable threats and possible attacks. In section 3, we propose a model to solve these problems. In section 4 and 5, we propose SIP attack detection methods based on the results analyzed in this study. We drew conclusions in section 6.

2. SIP and Its Threats

2.1 SIP protocol

SIP [3] is a signaling protocol in the application layer that specifies the procedure of creating, deleting or changing voice and multimedia communication sessions. This SIP protocol operates in both TCP and UDP, and is easy to implement. SIP provides flexibility and expandability in voice communication services. It has a more convenient protocol operation structure than existing H.323 [2].

The SIP session creation and communication process begins with the registration of the user in the proxy server. The SIP proxy server plays the role of requesting call connection and termination for the user. In **Fig. 1**, location server and proxy server run on the same physical server. The client SIP device provides its regional information to the location server. Location information includes the user's SIP address and IP address [3][11].

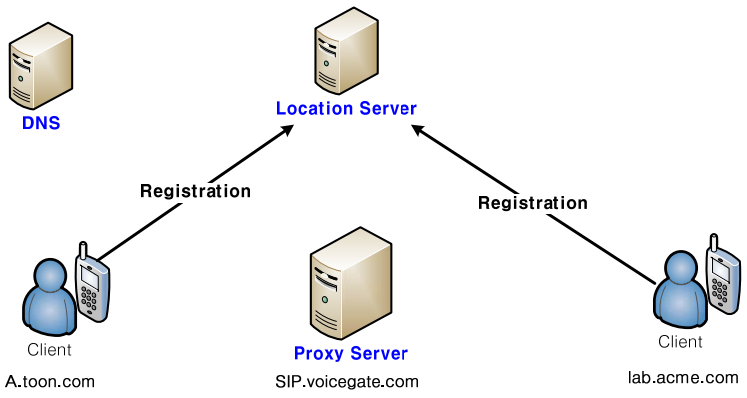

Fig. 1. SIP registration process

Each user and the server receive each other's accurate location information through DNS and Location Server. This helps a user invited for the first time acquire another user's location through the Location Server and set up a call between each other. **Fig. 2** shows a general SIP protocol based on the existing proxy server. SIP protocol is a text-based messaging system. Their content use a message structure in the form of existing HTTP language. The four message types are as follows.

- Register: SIP clients must provide their location information to the Registrar Server. They should register their SIP address and IP address.
- Invite: This message is sent by the user to the server when a SIP session starts when a call is created. In some cases, it may be sent directly to the opposite user (UAS).
- ACK: On receiving the final Response message for the Invite message, the user returs ACK for the response. Whether the response is Success or Fail, the final Response to the user's Invite should be replied to by sending ACK.
- BYE: When a client terminates a call, this message is used to inform the server that the call has been terminated.

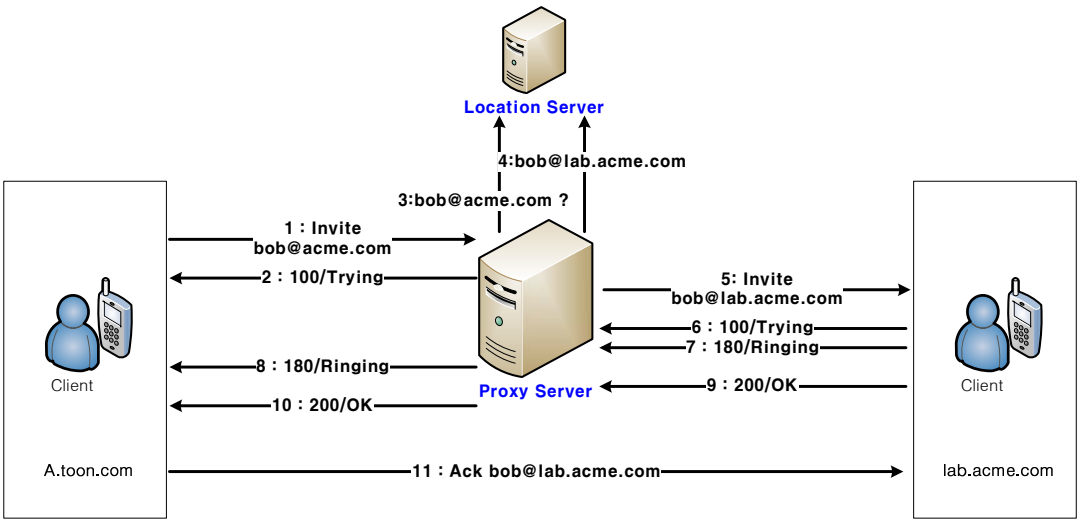

Fig. 2. SIP protocol

2.2 SIP message flooding attack

A hacker with access to the SIP signaling can impersonate signaling messages to perform various attacks. An attack is the attempt to impact infrastructure assets or operations. It is carried out by a threat agent. SIP threats and attacks can be categorized as active and passive attacks [12][13]. An active attack sends a large number of SIP messages, so that SIP users or service providers cannot use or provide normal services. For instance the message flooding attack is similar to DoS (denial of service) in ordinary networks. In this attack, the attacker sends a large number of messages, such as Invite and Register, which causes malfunctions or errors in the services of normal users or servers and make services unusable. A Message flooding attack is depicted in **Fig. 3**.

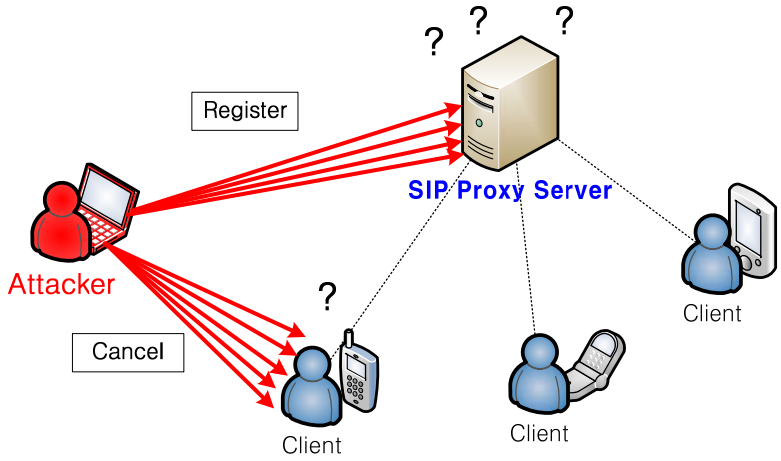

Fig. 3. SIP Message Flooding attack

- Register flooding attack: the attacker repeats registration and, by doing so, hinders other users from using the server and overloads the server. A representative type is server flooding attack.
- Invite, Cancel, RTP message flooding attack: this attack sends a large number of valid request messages (SIP Invite, Cancel) or RTP voice messages and makes the system prepare response messages. In doing so, it exhausts the system's CPU and memory resources. This causes all user services to be delayed or frozen.

2.3 Problems in the existing proxy server

SIP attacks are currently unpreventable, as the SIP proxy server cannot detect the message flooding attack. The main reason is to minimize its SIP service delay caused by SIP server overload. However, if the proxy server is modified to solve this problem, the server overload problem cannot be solved. In addition, this complicates SIP and there is still a problem with compatibility. These shortcomings are not resolved clearly [14][15][16].

We implemented a SIP virtual proxy additionally prior to the proxy server to analyze the state of the server and reduce existing proxy server overload to solve these problems in the SIP proxy server. We proposed the technique to maintain each user's state information and detect/block attacks based on the state information using the virtual proxy.

Additionally, previous research does not provide a function to detect/block these attacks accurately. Thus, this study proposes an algorithm to detect/block SIP attacks. We outline its module design. Finally, we proposed the implementation results.

3. Proposed SIP Virtual Proxy

3.1 SIP protocol state transition diagram

We suggest a SIP protocol state transition diagram, as in **Fig. 4**. The flow of messages can be described as a state transition diagram. It shows the entire process from the user registration step to final termination. Using this SIP state transition model, we can detect SIP flooding and malicious attack on each SIP call. We use both the IP/MAC authentication mechanism to filter

spoofed SIP traffic and the SIP State information to detect SIP attacks on each SIP transaction. This operational process can be divided into four steps as follows.

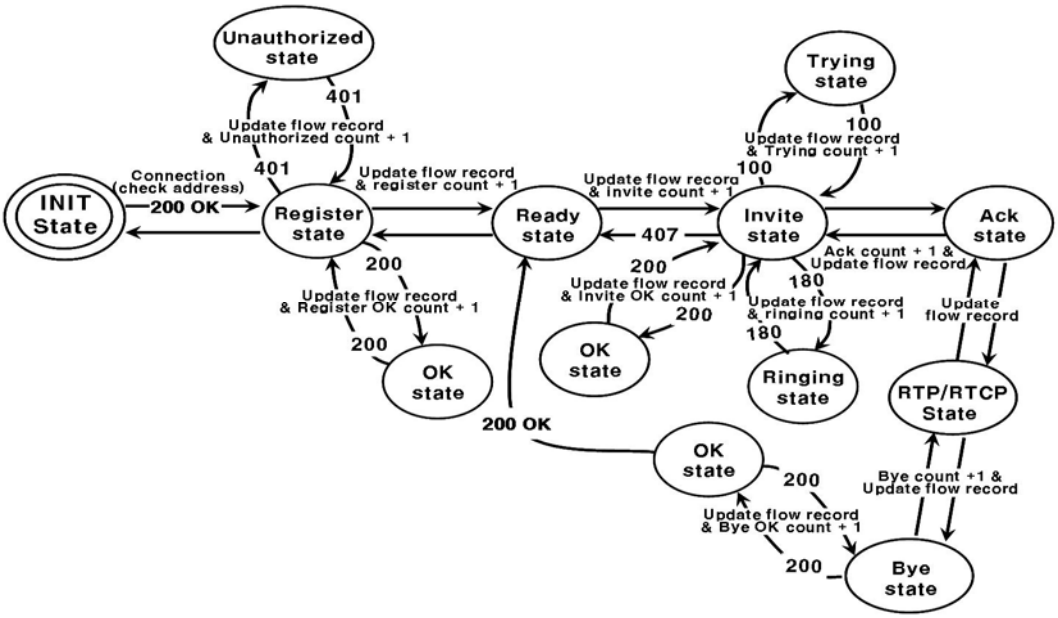

Fig. 4. SIP Protocol State Transition Diagram

- Step 1 : The user registers his/her own information to the proxy server.
- Step 2 : The user attempts call set-up through requesting the Invite and additional steps, such as Ringing, Trying, OK, and ACK to communicate with the SIP client.
- Step 3 : After the call set-up step has finished, the two users have bi-directional communication with each other through RTP/ RTCP.
- Step 4 : RTP communication is terminated, and the user enters into a waiting state through Bye and OK and maintains the state.

3.2 Proposed SIP attack detection mechanism

The state information-based virtual proxy for SIP communication stores state information for each session, and saves in/out information and important count information in the proposed SIP State table. The state information stored in the SIP State table is compared to rules and exceptions in the SIP formal model. Attacks are detected and dropped through this. **Fig. 5** shows the flowchart of the state information-based virtual proxy.

SIP attack detection based on the virtual proxy detects and blocks message flooding attacks that use messages, such as Register, Re-invite, RTP, Cancel and Bye. The proposed mechanism can detect a SIP message flooding malicious attacker, using the IP/MAC authentication and classification mechanism.

The proposed mechanism is initiated from the proposed IP/MAC authentication process. This process is reasonable when the virtual proxy and client are co-located in the same subnet. However, the virtual proxy and client can be located in different domains. Therefore, every source MAC address of SIP messages that the virtual proxy receives will be the MAC address

of the router to which the virtual proxy is directly connected. Thus, MAC authentication does not have any meaning in this case, because the virtual proxy will receive the MAC address of the router that it is directly connected.

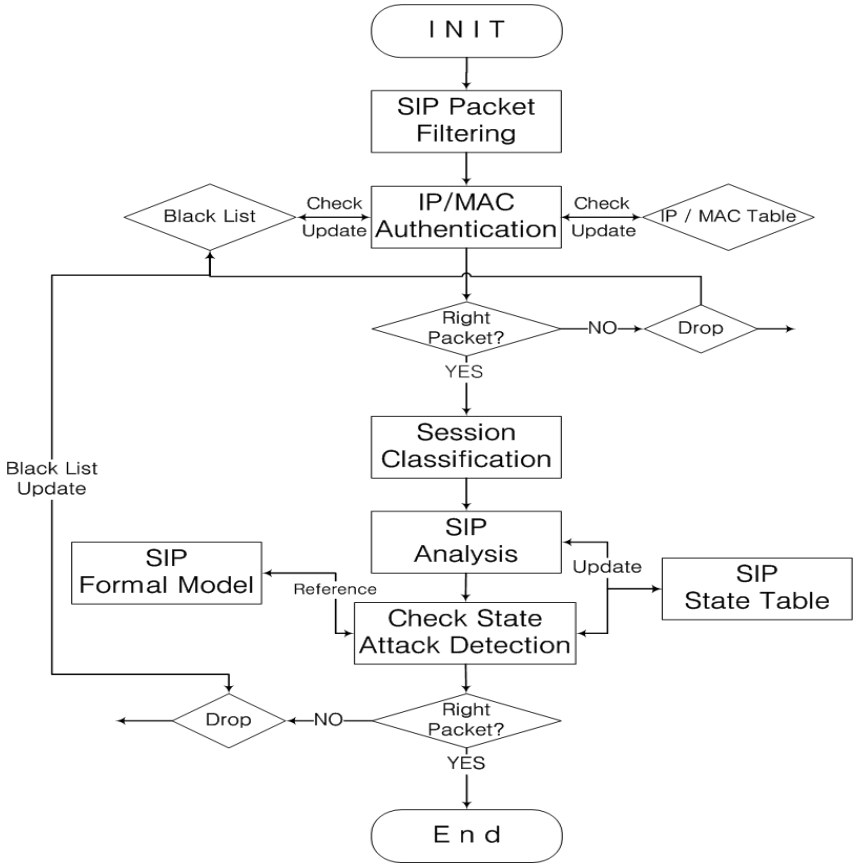

Fig. 5. Flow chart of the proposed virtual proxy for SIP attack detection

Therefore, we implemented the IP/MAC extraction module on each front end gateway, such as Access point, and gateway. The installed location of this IP/MAC extraction module will not be in the backbone router (gateway), but in the front end gateway, such as a wired/wireless gateway access point. The IP/MAC extraction module sends each SIP packet's IP/MAC address to the virtual proxy using UDP protocol.

The flow chart in **Fig. 5** determines whether to block a packet. Detected attacks are updated in the Black List. In addition, attacks can be detected in real-time, while the users' current state information is being updated continuously.

The system proposed in this study is mainly composed of three modules, as in **Fig. 6**: (1) SIP packet filtering module to capture the SIP session packet on the virtual proxy; (2) SIP IP/MAC authentication module to check for legitimate SIP packets; and (3) SIP state analysis module to detectattacks based on the previous SIP state information. Thus, this study implemented a state information-based virtual proxy. Additionally we implemented a SIP IP/MAC checking function to filter the attack packet and detected/blocked message flooding attacks based on the state information.

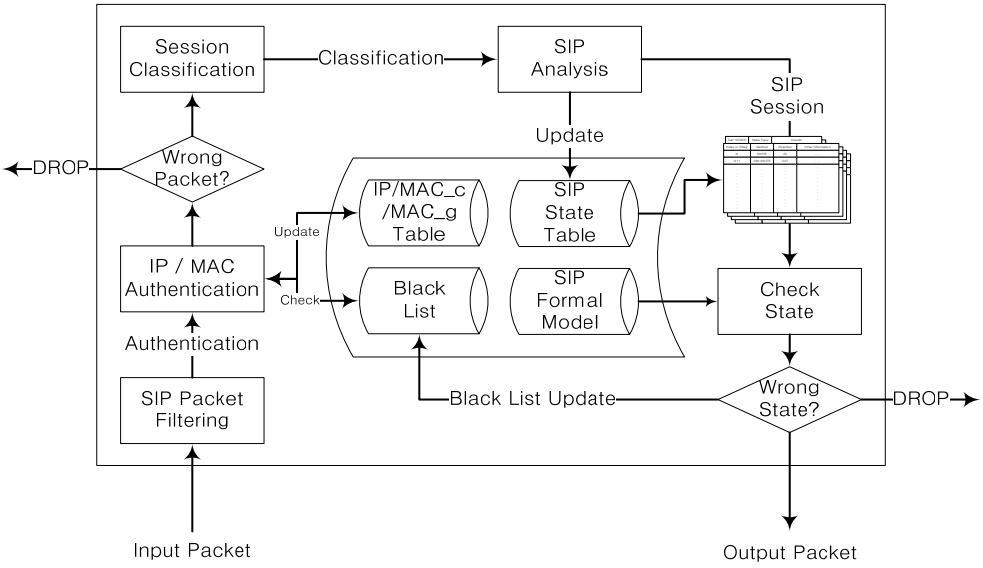

Fig. 6. Proposed SIP virtual proxy

4. Proposed SIP attack detection mechanism on virtual proxy

4.1 SIP packet filtering

This study proposes a state information-based technique to detect attacks and abnormal behaviors that threaten security by promptly analyzing state information. It is possible for us to establish and manage a safe SIP communication environment using the proposed schematic diagram of the virtual proxy.

The proposed virtual proxy captures the SIP packet from the network interface card (NIC) in front of the general SIP proxy server. Then we can only accept and filter the SIP packet. After this filtering process, we can authenticate the legitimate IP and MAC pairs based on the Blacklist Lookup Table. The Blacklist will be updated based on the state verification process checking its SIP state. Therefore, the list item on the Blacklist will be empty initially. It will be updated when it finds a new abnormal state SIP packet. We can authenticate the IP/MAC of the SIP packet based on this process.

When a user connects to the proxy server and attempts SIP communication, the virtual proxy receives the packet before the actual proxy server and executes steps as follows.

- Step 1: If the user attempts connection, the front end gateway checks if the packet is a SIP packet through the SIP packet filtering process. Then, it will extract the IP address stored in the IP header with the MAC address of the sender on the frame. The gateway sends these addresses to the virtual proxy with the SIP packet header using UDP protocol.
- Step 2: If a virtual proxy receives these data from the front end gateway, the SIP sender authentication step will operate using both Blacklist Lookup and the IP/MAC tables. The IP address of the SIP client(IP_c), MAC address of the client (MAC_c) and the MAC address of the intermediate gateway(MAC_g) will be stored in those tables.
- Step 3: Packets authenticated in Step 2 are classified through the Session Classification step.

- Step 4: The current state information for classified packets is added to the SIP State table and stored in the SIP Analysis step.
- Step 5: State information is compared and analyzed in the Check State step, based on the current state information and SIP Formal Model. If attacks are detected, the IP/MAC data will be updated as a new item in the Blacklist Lookup table.
- Step 6: Packets that have gone through all the steps are discarded and stored in the Blacklist, or pass and have normal communication.

The IP/MAC authentication process can work correctly in case of diverse SIP clients located in different networks, since the proposed virtual proxy can be implemented on the previous general proxy server or can cooperate as a additional module.

4.2 SIP IP/MAC authentication on virtual proxy

In this study, we used a black IP/MAC list lookup procedure on the proposed virtual proxy to block IP/MAC spoofing attacks. In **Fig. 7**, the IP/MAC checking process classifies a source IP and MAC address specified in SIP packets for accepting normal packets and rejecting abnormal SIP packets. We implemented the IP/MAC extraction module on the front-end gateway to obtain three address information, such as the IP address of the client (IP_c), the MAC address of the client (MAC_c) and the MAC address of the gateway (MAC_g). These three address items will be checked on the virtual proxy to authenticate the real sender. The IP/MAC checking module is formed by comparing data in the previously suggested IP/MAC matching table and checking the Blacklist Lookup Table stored in the previous SIP session.

First, we can extract both the IP address and MAC address from the SIP packet. Then, these addresses will be compared in the Blacklist lookup table. If these are not in these blacklists, proposed module additionally compares them on the IP/MAC table. If the current IP/MAC data of the SIP packet are not listed on the IP/MAC table, these paired data will be stored as a new instance or its MAC address updated as a new instance in the table. However, if the IP and MAC pair data were already in the blacklist table, then the SIP packet will be considered an attack packet.

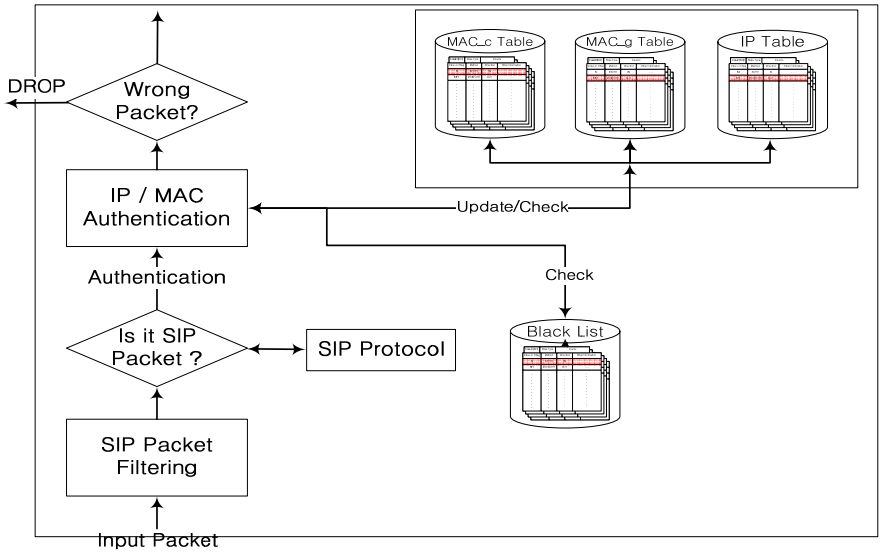

Fig. 7. SIP IP/MAC Authentication Module on the Virtual Proxy

Thus, spoofing attacks will be detected and blocked; passed SIP packets are transferred to the next Session Classification step. Therefore, this step compares the IP and MAC address with the lookup table, and blocks users with disallowed or unregistered IP and MAC addreses. This step is the authentication process for a user connected to the proxy server. The legitimacy of a client is determined using the IP address and the MAC address. Through this, the attacker's SIP packets are blocked by this module.

4.3 SIP state analysis on virtual proxy

After the authentication of IP and MAC information has been executed, the virtual proxy stores and manages the SIP state information. The module proposed in this study stores and manages clients' SIP state information to detect attacks more safely. Through this process, SIP server overload can be minimized. Abnormal behavior will be detected by blocking SIP attack packets. Each session classified in **Fig. 5** is updated in the SIP State Table through the SIP analysis process. In addition, abnormal SIP attacks are detected referring to the SIP formal model and a rule-based model[13] through the state checking process.

Fig. 8 shows the SIP state formal model based attack detection procedures using the SIP state diagram (**Fig. 4**). The virtual proxy proposed in this study uses a check list on each SIP packet after analyzing its state, and updating state information on each SIP transaction. Based on this process, we can classify its state on each SIP transaction.

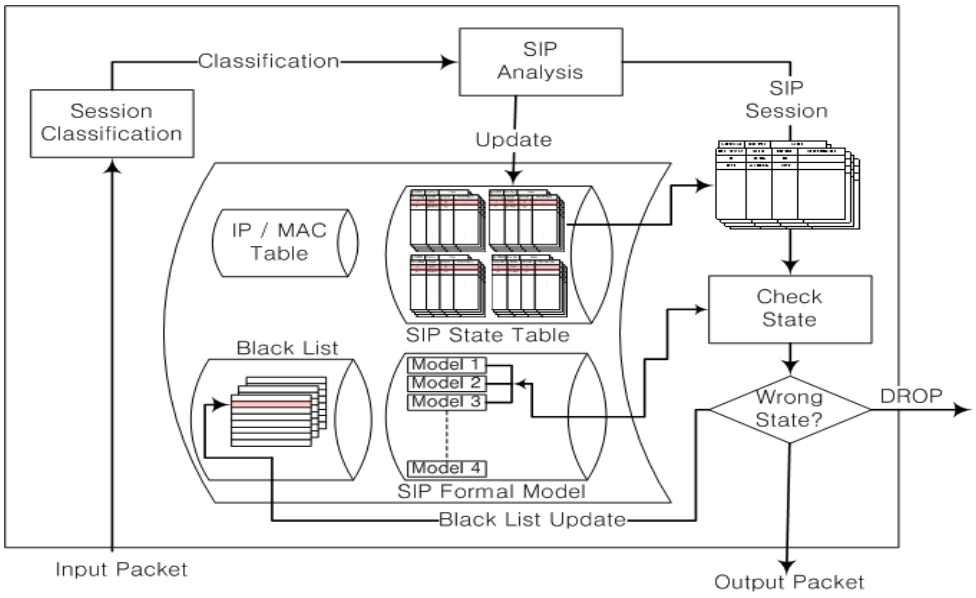

Fig. 8. SIP State Analysis Module on Virtual Proxy

In the SIP analysis step, packets are analyzed and needed items are stored as state information in the SIP State table. Attacks are detected by comparing the state information with the rule-based SIP formal model. Through this step, the virtual proxy detects and drops attacks on SIP communication. It provides a safe communication state in doing so.

In this study, attacks are detected accurately through the SIP State Table, the SIP formal model, and the blacklist. New attacks are detected/blocked promptly, as the SIP State Table and the Blacklist are updated in real-time. Safe SIP communication is guaranteed through the

attack detection process. Attacks that have not been previously detected can be controlled/analyzed.

5. Results of implementation and performance evaluation

5.1 SIP attack detection system

We implemented the proposed virtual proxy on wireless and wired networks to evaluate the performance of the system developed in this study. A proposed virtual proxy was installed in front of the SIP proxy server. The virtual proxy has functions for collecting, analyzing and comparing SIP packets, and detecting/blocking SIP message flooding attacks. In addition, it monitors and controls all SIP session packets based on the state transition diagram. Using this system, we measured the time to detect and block attacks. We use WireShark to verify the correctness of the proposed virtual proxy for packet statistics. **Fig. 9** shows the proposed architecture and installed location of the IP/MAC extraction module for authentication.

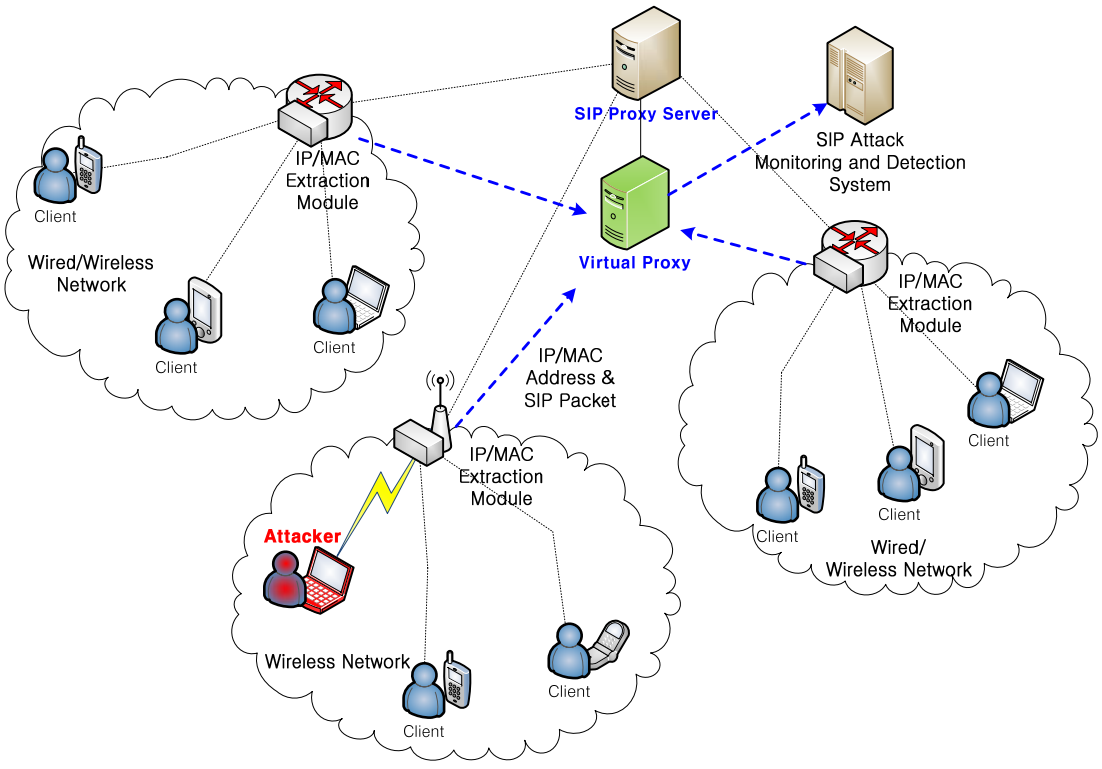

Fig. 9. System architecture on the proposed virtual proxy

First, the virtual proxy receives information on the SIP authentication protocol. The server checks a IP address of the received packet against the blacklist to authenticate the SIP information. Then, the virtual proxy inspects the possible state diagram based on the Client-Server transactions to detect and block the message flooding, as depicted in **Fig. 10**. The proposed system is implemented in Windows OS using Visual C++. Additionally, we implemented the SIP packet monitoring system combined with the virtual proxy.

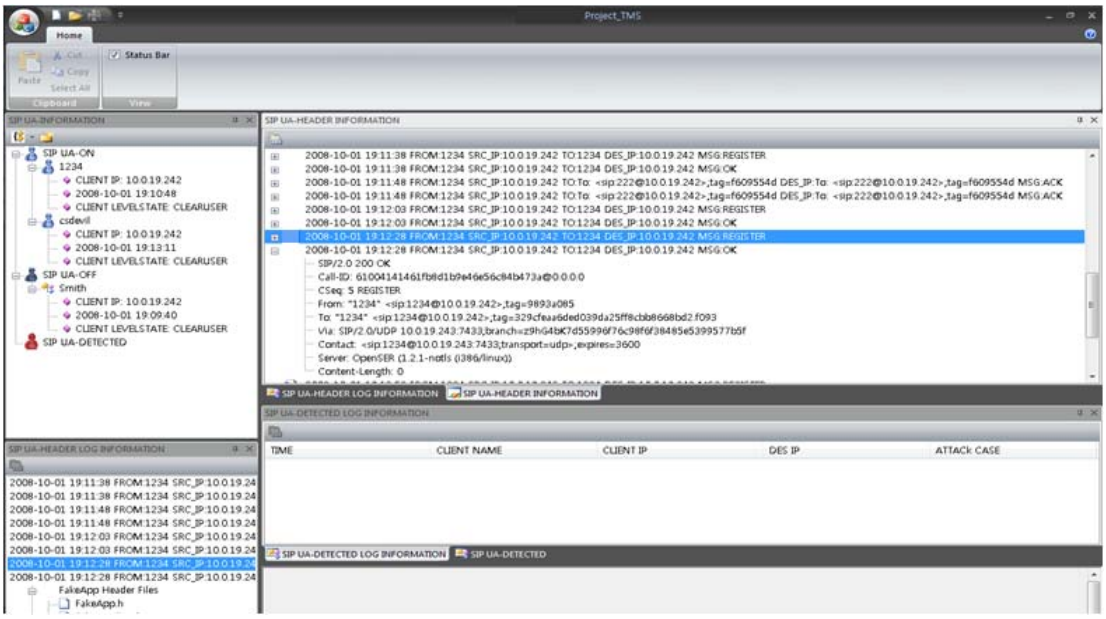

Fig. 10. SIP attack monitoring and detection system

5.2 Analysis of SIP attack detection

The clients' program using SIP sends the “REGISTER” packet continuously. Then, the proxy server sends the “200 OK” packet. Therefore, the virtual proxy processes “REGISTER” and “200 OK” separately, but “INVITE” is an infrequent packet. Accordingly, when the same packet is transmitted continuously, as in SIP attacks, the order of protocol should be ignored. Thus, it is possible to detect attacks through the SIP State Diagram. If the same packet is generated continuously for a SIP attack and the speed exceeds the processing capacity of the SIP proxy server, the virtual proxy proposed in this study can detect SIP attacks.

A process to identify packets to be blocked, using the IP address and the MAC address, should detect and cope with attacks. In this study, packets go through the process comparing IP address and MAC address, but this process should not affect SIP communication. Thus, in this study, information is only extracted from SIP packets and the process does not overlap the packet marking process explained earlier.

Based on the packet transmission time in **Fig. 11**, the transmission interval differs little when the virtual proxy module does not run (without) and when it runs (with). As demonstrated by the experiment, the SIP attack detection and coping module developed in this study does not affect SIP communication. This implies that the module does not seriously affect the overall transmission performance. Therefore, the proposed virtual proxy enables the administrator to monitor the SIP session in real-time with minor delay. Experimental results reveal a 1.3% additional overhead through the proposed virtual proxy. This does not degrade the overall performance of the SIP proxy system.

In addition, **Fig. 12** shows the results of traffic monitoring using the proposed technique when an attack was attempted while three SIP clients were connected and one client was transmitting SIP attack packets. The experimental shows that even when the number of SIP packets increased, abnormal SIP traffic was monitored and detected without notable delay by the proposed virtual proxy. It demonstrates the enhanced attack detection performance.

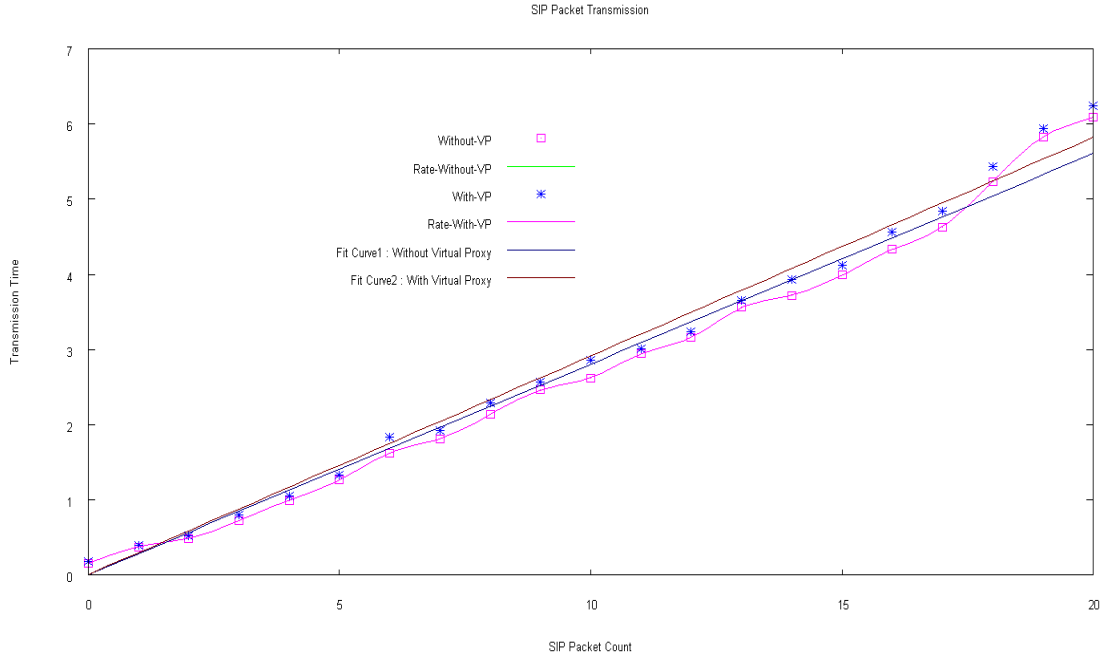

Fig. 11. SIP Proxy Packet Transmission Latency Time

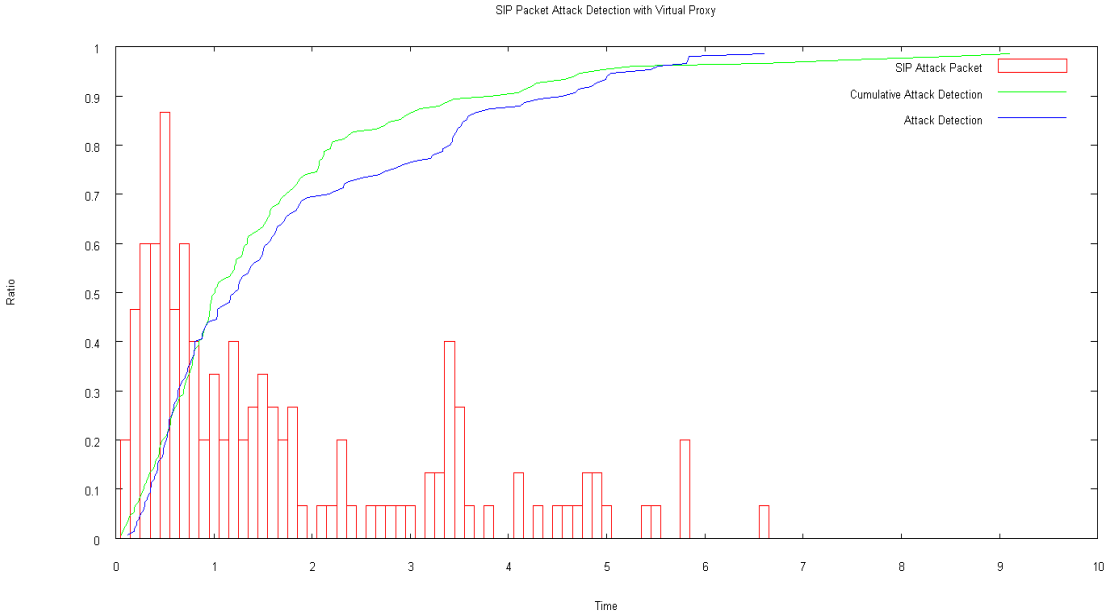

Fig. 12. SIP Attack Detection on the Virtual Proxy

Additionally, this study considered various SIP open system to compare functional differences. It is possible to compare the existing vIDS (existing intrusion detection system on SIP system) [16][17][18] with the VP (virtual proxy) proposed in this study. Existing vIDS consider various states, but do not consider some highly possible states, such as Busy here and Request Terminated. Most message flooding attacks mainly target the call set-up procedure

and its termination in the overall SIP session. The technique proposed in this study provides a SIP packet analysis function and a SIP session classification function, as in existing vIDS systems. However, it additionally provides the function to detect abnormal wired/wireless SIP traffic, and enhances the performance of the SIP proxy server. Moreover, the technique proposed in this study can detect states not considered in vIDS and detect more attacks.

6. Conclusions

We proposed a SIP protocol state diagram and designed methods to detect SIP attacks using a virtual proxy. The technique proposed in this study was designed to build a virtual proxy to execute filtering and IP/MAC authentication for SIP packets. When using the proposed virtual proxy, the SIP message is transmitted to the actual SIP proxy server to monitor actual SIP sessions through analyzing the sessions to detect abnormal events in SIP packets based on the SIP Formal Model. With the proposed virtual proxy, we could detect and block abnormal attacks, such as SIP malformed message attacks, efficiently.

Evaluation of its performance confirmed that the proposed technique solves the problems in existing security techniques, minimizes load and traffic delay caused by the packet monitoring process, and detects SIP attacks efficiently. Based on the method proposed in this study, further research will be made to detect and block SIP attacks actively in wireless network environments. We will develop secure SIP and formal description based SIP attack prevention.

References

[1] P. C. Mehta, S. Udani, "Overview of Voice over IP," Technical report MS-CIS-01-31, University of Pennsylvania, Feb. 2001.
[2] ITU-T, Recommendation H.323, "Packet based Multimedia Communication Systems," version 4, June 2006.
[3] J. Rosenberg, et al., "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.
[4] J. Franks. et al., "HTTP Authentication: Basic and Digest Access Authentication," IETF RFC 2617, June 1999.
[5] T. Dierks, et al., "The Transport Layer Security (TLS) Protocol Version 1.2," IETF RFC 5246, August 2008.
[6] S. Dusse, et al., "S/MIME Version 3 Message Specification," IETF RFC 2633, June 1999.
[7] H. Schulzrinne, et al., "RTP: A Transport Protocol for Real-Time Applications," IETF RFC 3550, July 2003,
[8] S. Niccolini, "VoIP Security Threats," Internet-Draft, *NEC SPEERMINT Working Group*, 2007.
[9] S. Salsano, et al., "SIP Security Issues: The SIP authentication procedure and its processing load," *IEEE Network*, November/December, 2002.
[10] D. Sisalem, J. Kuthan, S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: Attack scenarios and prevention mechanisms," *IEEE Networks Magazine*, Vol 20, No. 5, 2006.
[11] C. Chang. et al., "Design and Implementation of SIP Security," in *Proc. Of ICOIN 2005*, LNCS 3391, pp.669-678, 2005.
[12] D. Endler, M. Collier, "Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions," McGraw-Hill, Osborne, 2007.
[13] S. Vuong, Y. Bai, "A survey of VoIP intrusions and intrusion detection systems," in *Proc. of 6th International Conference on Advanced Communication Technology*, 2004.
[14] D. Seo, H. Lee, E. Nuwere, "Detecting More SIP Attacks on VoIP Services by Combining Rule Matching and State Transition Models," in *Prof. of the IFIP TC 11 23rd Int. Information Security Conference*, pp.397-411. 2008.

[15] H. Sengar, et. al., "VoIP Intrusion Detection Through Interacting Protocol State Machines," in *Proc. of 2006 International Conference on Dependable Systems and Networks*, pp.393~402, 2006.
[16] E. Fernandez, A. Kumar, "A Security Pattern for Rule-based Intrusion Detection," in *Proc. of the Nordic Pattern Languages of Programs Conference*, 2005.
[17] G. Ormazabal, et. al., "Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems," In *Proc. of International Conference on Principles, Systems and Applications of IP Telecommunications 2008*, LNCS 5310, pp.107-132, 2008.

Ha-Na Yun received the B.S. degree in Computer Science and Engineering from Hanshin University in 2008. He is currently a Masters student. His research interests include the security of wireless networks, home networks, VoIP, and Internet and computers.

Sung-Chan Hong is a professor in the Division of Information & Telecommunication from Hanshin University, Korea. He received M.E. and Ph.D. degrees in Administration Engineering from Keio University, Yokohama, Japan in 1990 and 1994. In 1994, he was with LG-CNS CO., Ltd., in the consulting team developing Information Systems. From 1995, he worked in the Dept. of Information Systems at Sangmyoung University, as an assistant professor. He joined Hanshin University in March 1997. He is the vice president of the Korea Internet and Information Society. His research areas include internet Commerce Technology, Information Systems Architecture and Ubiquitous computing. He is a member of KSII, KIPS and KICS.

Hyung-Woo Lee received the B.S., M.S. and Ph.D. degrees in Computer Science from Korea University in 1994, 1996 and 1999, respectively. From 1999 to 2002, he was an assistant professor in the Division of Information and Communication Engineering, Cheonan University. He is currently an associate professor in the School of Computer Engineering, Hanshin University, Korea. His research activities are mainly in the areas of information security, network security, and wired/wireless IDS/IPS.