SFADS: A SIP Flooding Attack Detection Scheme with the Internal and External Detection Features in IMS Networks

Qibo SUN [a], Shangguang WANG [a,1] , Fangchun YANG [a]

[a] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China*

Abstract. IP Multimedia Subsystem (IMS) is a standardized Next Generation Networking (NGN) architecture. It takes Session Initiation Protocol (SIP) as the core signaling protocol of IMS and NGN. With IMS networks widespread deployment, SIP flooding attacks are becoming into a major threat to IMS network. However, the existing SIP flooding attack detection schemes are inefficient for detecting low-rate SIP flooding attacks and are lacking in poor recovery for detecting high-rate SIP flooding attacks. In this paper, we propose a novel SIP flooding attack detection scheme with the internal and external detection features in IMS networks, called SFADS (SIP flooding attack detection scheme). In SFADS, based on the analysis of SIP flooding attacks, we first extract the abrupt change of SIP session request as the external detection feature, and the abnormal abrupt change of difference between the sequence of legitimate SIP session establishment and the SIP session request messages as the internal detection feature. Then we use the improved cumulative sum control chart algorithm to analyze the two detection features. Finally, we take the analysis data as inputs and adopt Fuzzy Logic to detect SIP flooding attacks. To investigate the detection performance of the proposed SFADS, we conduct simulations with the prototype implement in an IMS network testbed. Simulation results show the performance of the proposed SFADS is better than that of other schemes.

Keywords. IMS network, SIP, Flooding attacks, Detection feature, Cumulative sum control chart, Fuzzy Logic

Introduction

IP Multimedia Subsystem (IMS)[1] is a standardized Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. IMS uses a Voice-over-IP (VoIP) implementation based on a 3GPP standardized implementation of Session Initiation Protocol (SIP)[2], and runs over the standard Internet Protocol (IP). SIP is defined by Internet Engineering Task Force (IETF). It is a kind of control protocol used for creating, modifying and terminating multimedia session.

At present, SIP is widely accepted by 3GPP (3rd Generation partnership Project), I-TU (International Telecommunication Union) and ETSI (European Telecommunications

[1] Corresponding Author: Shangguang Wang, Box 187, 10 No., Road Xitucheng, Beijing, China ; E-mail: sguang.wang@gmail.com

Standards Institute) as the core signaling protocol of IMS and NGN. This makes SIP to face many different kinds of security threats such as flooding attacks, SQL-injection attacks and SIP message flow attacks [3,4]. Because SIP flooding attack is easy to launch and capable of quickly draining the resources of both networks and nodes, it is among the most severe of all [5]. Hence, this paper focuses on SIP flooding attacks. Although the international standardization organization, including 3GPP and ITU-T, has developed several security technologies and protection mechanisms, such as encryption, authentication and secure transmission, for IMS network to withstand the registration hijacking, server masquerading, message tampering, session terminating, there is not an effective defense for SIP flooding attacks (even if there is an effective IMS authentication) [4,6,7].

The SIP flooding attack has a huge harmfulness [8]. Attackers send a large number of invalid SIP session establishment requests to the P-CSCF (proxy-session control function) server through the IMS terminals (such as smart phones, PDAs, etc.), which will exhaust signaling resources and lead the P-CSCF server to a denial of service (DoS), thus, preventing the legitimate users from receiving normal services [4-8] is critical to ensure an effective IMS network. The most severe SIP flooding attacks will cause the entire telecommunication signaling network paralyzed, and seriously impact on national security. B. Zhao, et.al [9] describes a new SIP DoS attack which aims at Presence Server and CSCF (Session Control Function) on IMS networks. They pointed that the attacker only needs 14 malicious clients to block the IMS network of a metropolitan area, such as Washington D.C. and New York City. With the IMS network widely development, attackers can launch attacks to any IMS networks by using a few access terminals. Hence, SIP flooding attacks will become a serious security threat for managers and telecom operators [10,11]. Although there are some good solutions [3,9,12-14], the biggest challenge is still how to detect the malicious attacks within shorter detection time and lower false alarm ratio. Moreover, the recovery time that is the time between the SIP flooding attacks over and the detection scheme reset, is also a challenge.

In this paper, we propose a novel scheme for detecting SIP flooding attacks in IMS networks by integrating the external and internal detection features with the improved cumulative sum control chart (CUSUM) algorithm and Fuzzy Logic for a more effective and efficient solution. The two detection features are the cornerstones of our design. The external detection feature that is capable of monitoring the abrupt change of SIP session request, is at a coarser-grained level. The internal detection feature which can be aware of the abnormal abrupt change of the difference between the sequence of legitimate SIP session establishment and the SIP session request messages, is at a fine-grained level. By the combination of two detection features, we can capture any slight abnormal changes quickly, while either the internal detection feature or the external detection feature can not find the anomalous traffic. In summary, Compared to previous work, we have made four main contributions:

1. To shorten detection time with low false alarm ratio, based on the analysis of SIP flooding attacks, we extract the abrupt change of SIP session request as the external detection feature, and the abnormal abrupt change of difference between the sequence of legitimate SIP session establishment and the SIP session request messages as the internal detection feature. To the best of our knowledge, no previous work has used two detection features for any anomaly traffic detection.
2. To improve the sensitivity of detection schemes, we propose an improved CUSUM algorithm by using the time-window concept. Since it only accumu-

lates the traffic in the time-window, it observably shortens the recovery time of SFADS.

3. We adopt Fuzzy Logic to make the detection decision. By using designed fuzzy rules, SFADS can make the detection decision quickly when the cumulative value is increasing (it is still less the detection threshold) according to the information from the external detection feature.
4. We conduct an IMS network testbed to investigate the performance of SFADS by implementing the prototype system [2].

The remainder of the paper is organized as follows: Section 1 analyzes SIP flooding attacks and explains how to extract detection features. Section 2 offers the SFADS detection scheme, including the improved CUSUM algorithm and the application of Fuzzy Logic. In Section 3, we evaluate the effectiveness of our proposed scheme. Section 4 discusses the related work. Section 5 concludes the paper.

1. SIP Flooding Attack Detection Feature

In this section, we fist describe the legitimate SIP session establishment process and then analyze the abnormal SIP session request in Section 1.2. Finally, based on Section 1.1 and Section 1.2, we extract the external detection feature and internal detection feature of the SIP flooding attack in Section 1.3 (our first main contribution).

In the SIP flooding attack detection, the extraction of detection feature that is an important work, directly impact on alarm rate and false positive rate of the detection system (algorithm). The SIP flooding attack mainly includes INVITE message flooding attack and REGISTER message flooding attack. Because the two message flooding attacks are similar to [3,4], we take the INVITE message flooding attack as an example to study the detection method of SIP flooding attacks in this paper. At first, we introduce the normal SIP session establishment process by the following section.

1.1. Legitimate SIP session establishment

Figure 1 shows the process of a legitimate SIP session establishment (more detailed process is in [2]). During the legitimate establishment process of SIP session, it will generate (INVITE, 200 OK, ACK) and (INVITE, 4xx/5xx/6xx, ACK) message sequence. The left side of Figure 1 shows the successful SIP session establishment process which generates (INVITE, 200 OK, ACK) sequence. The ”200 OK” shows that the session is established successfully or the request was processed successfully. The right side of Figure 1 shows the failing SIP session establishment process which generates (INVITE, 4xx/5xx/6xx, ACK) sequence. The ”4xx/5xx/6xx” indicates the failing establishment of SIP session. In this paper, we extract the message sequence of the legitimate establishment process with (INVITE, RES, ACK) where RES stands for ”4xx/5xx/6xx”. The header fields of all INVITE, ACK, RES messages have the same ”From tag” (identifying a initiator of session), ”To tag” (identifying a recipient of session) and ”Call-ID” (identifying a dialog), three of which can identify an established session.

[2] http://sguangwang.com/

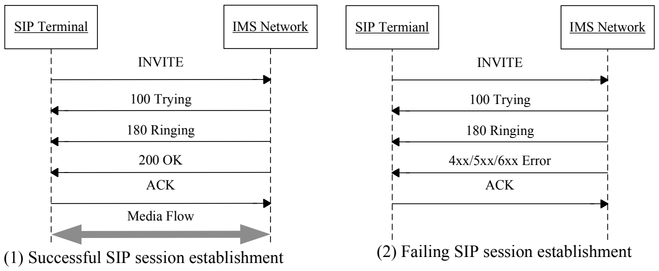

Figure 1. The process of a legitimate SIP session establishment

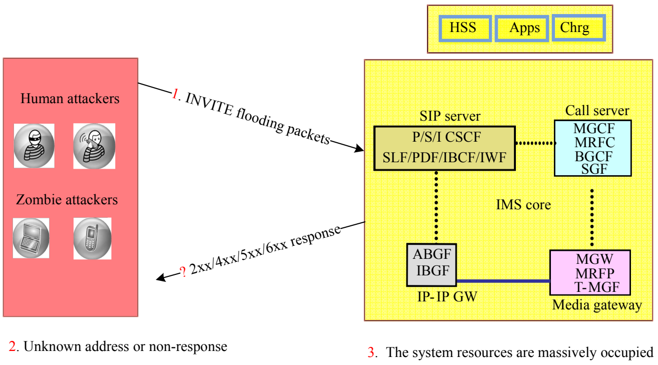

Figure 2. SIP INVITE flooding attacks

1.2. SIP flooding attacks

As shown in Figure 2, attackers usually use forged source addresses to send a large number of INVITE message to a specific SIP server, but not to reply the corresponding ACK response message in IMS networks. A large number of INVITE messages to the SIP server make the attacked SIP server busy to deal with these invalid INVITE messages and then run out of SIP server resources so that it cannot deal with the legitimate SIP messages. Although the legitimate SIP session establishment process also exist the abnormal situation of call-setup because of the network transmission or SIP terminal problem, the probability of the abnormal situation is very low since the communication network is relatively stable. Hence, this abnormal situation can be ignored.

The SIP flooding attack seems to be simple, but it is really hard to defense. On the one hand, this kind attack uses normal packages so that the IMS network does not prohibit them. On the other hand, attackers usually use forged source addresses, so the defense system cannot trace the attack source. Moreover, different from traditional Internet flooding attacks, the mobility and across-network of these attacks also increase the difficulty of the defense.

Based on the analysis of the legitimate SIP session process (Section 1.1) and SIP session attack process (Section 1.2), the following section will show how to extract the SIP flooding attack detection feature.

1.3. Extracting SIP flooding attack detection features

In this section, the extraction of the SIP flooding attack detection feature that contains the external detection feature extraction and the internal detection feature extraction, is our first main contribution.

1.3.1. Extracting the external detection feature

We assume $T_{invite}(n)$ denotes the amount of INVITE messages within the n-th sampling period. When an IMS network exists SIP flooding attacks within a detection time interval, $T_{invite}(n)$ will change abruptly. As shown in Figure 2, when SIP flooding attacks happen, the SIP session requests (i.e., INVITE messages) will increase sharply. Hence, we take the phenomenon as the external detection feature of SIP flooding attack, and take $\{\bar{X}_n\}(\bar{X}_n = T_{invite}(n), n = 1, 2, ...)$ as the external detection feature sequence which can be counted with the hash function [15,16] in this study.

Although the external detection feature can be used to determine whether SIP flooding attacks happen, it cannot find attacks accurately. For instance, on holidays, a large number of calls may make SIP traffic increase sharply. Because this abrupt change comes from the normal of SIP session requests, if we only use it as the SIP flooding attack detection feature, there will be false alarms. Hence, in order to detect the SIP flooding attack accurately, in this study, we also extract a concept, i.e., the internal detection feature of SIP flooding attack.

1.3.2. Extracting the internal detection feature

To make the description on the internal detection feature of the SIP flooding attack easy, based on the analysis of Section 1.1 and Section 1.2, we extract the message sequence of the legitimate SIP session establishment process as a triple (φ, ϕ, ψ) where $\varphi := \{INVITE\}$ is a set of INVITE request messages, $\phi := \{RES\}$ is a set of 2xx /4xx/5xx/6xx response messages, $\psi := \{ACK\}$ is a set of ACK messages, $\varphi.attribute = \phi.attribute = \psi.attribute$ and $attribute := \{From\,tag, To\,tag, Call-ID\}$.

We assume $S_{invite}(n)$ denotes the amount of all legitimate message sequence (φ, ϕ, ψ) within the n-th sampling period, and let $X_n (n = 1, 2, ...)$ be the number of $T_{invite}(n)$ minus that of the corresponding $S_{invite}(n)$ collected within one sampling period, i.e.,

$$X_n = T_{invite}(n) - S_{invite}(n)(n = 1, 2, ...). \tag{1}$$

In the normal IMS network environment, there is an obvious positive correlation between $T_{invite}(n)$ and $S_{invite}(n)$, i.e., X_n is close to zero. However, when INVITE flooding attacks happen, attackers send a large number of invalid INVITE messages which flood the legitimate message sequence, i.e., $T_{invite}(n) \gg S_{invite}(n)$. Then X_n increases sharply and is far more than zero within the n-th sampling period, i.e., $X_n \gg 0$ is seen as the internal detection feature of SIP flooding attack. It is similar to the external detection feature sequence, and we take $\{X_n\}$ $(X_n = T_{invite}(n) - S_{invite}(n) \quad (n = 1, 2, ...))$ as the internal detection feature sequence, which can be counted with the hash function [15,16] in this study.

In this paper, based on the internal detection feature and external detection feature of the SIP flooding attack, we propose a novel SIP flooding attack detection scheme, i.e., SFADS, in the following section.

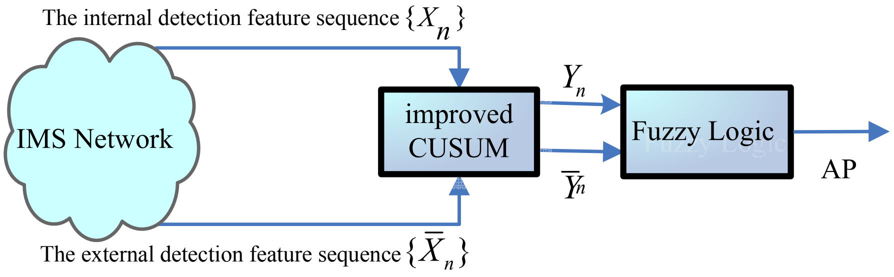
The internal detection feature sequence $\{X_n\}$
IMS Network
improved CUSUM
Y_n
$\bar{Y}_n$
Fuzzy Logic
AP
The external detection feature sequence $\{\bar{X}_n\}$

Figure 3. Procedure of SFADS

2. The Proposed Detection Scheme (SFADS)

In order to make SFADS easy to understand, we first introduce the application of the non-parametric CUSUM algorithm in SIP flooding attack detection in Section 2.1. Based on the application, we propose an improved non-parametric CUSUM algorithm in Section 2.2 and give its application in Section 2.3 (our second main contribution) to shorten the recovery time. Finally, we adopt fuzzy logic to determine whether anomalies happen in Section 2.4 (our third main contribution).

As shown in Figure 3, our proposed scheme first joints the internal detection feature and external detection feature of the SIP flooding attack from IMS environment, and then adopts the improved CUSUM algorithm as the basic detection algorithm to detect the external detection feature sequence $\{\bar{X}_n\}$ and the internal detection feature sequence $\{X_n\}$. Finally, we employ the fuzzy logic to analyze the detection results and determine whether attack happens.

To facilitate the presentation, If not otherwise specified, we substitute the CUSUM algorithm for the non-parametric CUSUM algorithm in this paper. In addition, there are some effective defense systems [5,25,26], the prevention is outside the scope of this study.

2.1. CUSUM algorithm

The CUSUM algorithm is based on the Sequential Change Point Detection [17] which is to determine whether the observed time series is statistically homogeneous, and if not, to find the point in time when the change happens. The CUSUM algorithm has been studied extensively by statisticians and it has been widely used for anomaly detection [18-20]. See [17] and [21] for a good survey. Because the IMS network is a dynamic and complex entity because of including Internet traffic and telecommunication traffic, we cannot find a random sequence parameter model to simulate it. The CUSUM algorithm can monitor random variables continuously to achieve the purpose of real-time detection, and it does not build a complex network traffic model. Hence, it is suitable to analyze the SIP traffic as the primary detection algorithm.

In this paper, the application of the CUSUM algorithm is similar to [18-20]. According to Eq.1, the internal detection feature sequence $\{X_n\}$ is a sequence which can react the change of difference values between $T_{invite}(n)$ and $S_{invite}(n)$. Generally, the mean of X_n is dependent on the size of SIP network. To make the CUSUM algorithm more general for different kinds of SIP network, we adopt the normalization on internal detection feature sequence $\{X_n\}$ with the average number $\tilde{F}(n)$ of $S_{invite}(n)$ during one sampling period. An example of recursive estimation and update of $\tilde{F}(n)$ is as the follows:

$$\tilde{F}(n) = \lambda \tilde{F}(n-) + (1-\lambda)S_{invite}(n), \bar{F}(0) = S_{invite}(1) \tag{2}$$

where $\tilde{F}(n)$ can be estimated in real time and updated periodically, n is the discrete time index, $\lambda(\lambda \in [0,1])$ represents the memory in the estimation.

By Eq.2, $\tilde{X}_n$ is no longer dependent on the network size or time-of -day. Hence, we can consider the internal detection sequence $\{\tilde{X}_n\}$ is a stable independent random process. The mean of $\tilde{X}_n$ denoted as c is much less than 1 and close to 0, i.e., $0 \simeq E(\tilde{X}_n) = c << 1$. We chose a parameter β as the upper bound of c, i.e., $\beta > c$, and convert $\{\tilde{X}_n\}$ into a negative mean during normal operation by the following:

$$Z_n = \tilde{X}_n - \beta. \tag{3}$$

For normal operation, the mean of $\{Z_n\}$ is negative, i.e., $a = c - \beta < 0$. However, when an attack takes place, $\{Z_n, n = 1,2,3...\}$ will suddenly become large positive, i.e., $Z_n = h + a > 0$. Suppose, during an attack, the increase in the mean of Z_n can be lower-bounded by h. Our change detection is based on the observation of $h \gg c$ where h is the mean leap of increasing mean values during attack, namely average attack strength.

Let Y_n represent the accumulating of $\{Z_n\}$ by the following:

$$Y_n = (Y_{n-1} + Zn)^+, Y_0 = 0, \tag{4}$$

with

$$Y = (X)^+ = \begin{cases} X, & X > 0 \\ 0, & X \leq 0 \end{cases}. \tag{5}$$

Because Y_n can clearly reflect the change of $\{Z_n\}$, a large Y_n is a strong indication of an attack. By setting a flooding threshold N, we use Y_n to make detection decisions. The following is the decision function of SIP flooding attack:

$$d_N(Y_n) = \begin{cases} 1, Y_n > N \\ 0, Y_n \leq N \end{cases}. \tag{6}$$

where $d_N(Y_n)$ represents the detection decision at time n. If Y_n is greater than N, the value of $d_N(Y_n)$ is 1 and it represents an attack occurs, otherwise, the value of $d_N(Y_n)$ is 0 and it represents that a normal operation. The larger Y_n is, the stronger the attack is.

2.2. *Improved CUSUM algorithm*

When an attack is going to end, the CUSUM algorithm has accumulated a high value of Y_n. After the attack, the drop of Y_n is very slow, which takes a long time to restore to normal state. As shown in Figure 4 (it is from experimental results in Section 3), the long recovery time reduces the sensitivity of the CUSUM algorithm in SIP flooding attack and increases false alarms. Therefore, the recovery time (RT) is a key indicator and has a great influence on the performance of the CUSUM algorithm. In this section, we propose an improved CUSUM algorithm by using the time-window concept as our second main contribution.

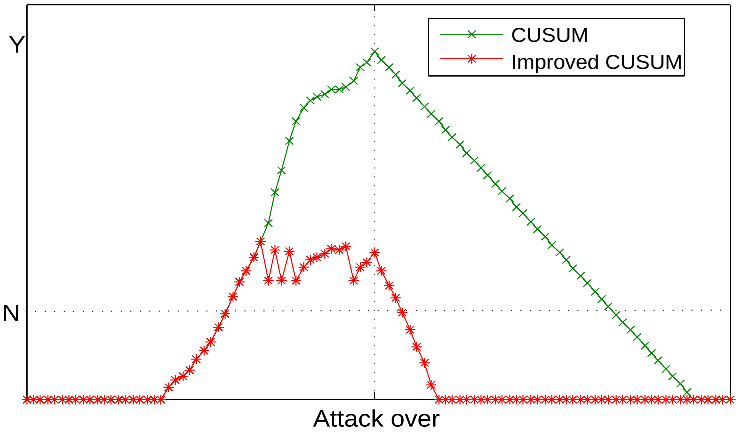

Figure 4. Comparison results on recovery time

The improvement of the CUSUM algorithm is to shorten the recovery time and improve the algorithm sensitivity. The key of the improved CUSUM algorithm is to convert Eqs.5 and 6 into Eqs.8 and 9 with the time-window concept.

Let $k(k = 1,2\ldots)$ be the size of time-window, and it also denotes the amount of the sampling period T in the time-window. In the improved CUSUM algorithm, we only accumulate $\{Z_n\}$ in the time-window by the following:

$$Y_n = \begin{cases} (Y_{n-1}+Z_n)^+ ,n \leq k \\ \left((Y_{n-1}+Z_n)^+ - Z_{n-k}^+\right)^+ ,n > k \end{cases} ,Y_0 = 0. \tag{7}$$

We choose a parameter N' that is the upper bound of N (N is the detection threshold of the CUSUM algorithm in Eq.7), i.e., $N' > N$. Then we use N' in dealing with Y_n to reduce the cumulative effect by the following:

$$Y_n = \begin{cases} Y_n, & Y_n \leq N' \\ N'', Y_n > N'' \end{cases} . \tag{8}$$

If Y_n is greater than N', the value of Y_n is N'' ($N \leq N'' \leq N'$), i.e., $Y_n = N''$. N'' and N' can be set according to the network environment. In improved algorithm, the detection decision is still Eq.7.

To evaluate the improved algorithm, Figure 4 shows the recovery time comparison results with the traditional CUSUM algorithm (the experimental environment is setup in Section 3) where the parameter N is 1. In Figure 3, the horizontal axis is the sampling period (5 seconds) and the vertical axis is the cumulative value, i.e., Y_n. From Figure 3, the improved CUSUM algorithm greatly eliminates the cumulative effects of the attack and the RT is much shorter than the traditional CUSUM algorithm. The RT reduces 47.4% ,on average, which improves the sensitivity of the algorithm in SIP flooding attack detection effectively. Moreover, we only accumulate $\{Z_n\}$ within a certain time-window, our proposed improved algorithm does not add extra load for SIP flooding attack detection.

2.3. *The application of the improved CUSUM algorithm*

According to the analysis in Section 1.3, if the CUSUM algorithm only detects the internal feature, the detection result has its limits in detection performance. Therefore, we use the improved CUSUM algorithm to analyze the internal detection feature and the external detection feature of the SIP flooding attack, which is also our second main contribution.

In this study, to improve the detection performance, we convert the single detection output of the CUSUM algorithm into two mixed detection outputs by the following five Steps:

Step 1 (Extraction): by using the hash function [15,16] on the sequence of both INVITE message and SIP session periodically, we can extract the internal detection feature sequence $\{X_n\}$ and the external detection feature sequence $\{\bar{X}_n\}$.

Step 2 (Normalization): by using Eq.2, we can normalize the internal detection feature sequence $\{X_n\}$ into $\{\tilde{X}_n\}$. Moreover, we also normalize the external detection feature sequence $\{\bar{X}_n\}$ into $\{\overset{\leftrightarrow}{X}_n\}$ by the following:

$$\overset{\leftrightarrow}{X}n = T_{invite}(n)/\bar{F}(n) \quad (n = 1, 2, ...) \tag{9}$$

with

$$\bar{F}(n) = \lambda \bar{F}(n-1) + (1-\lambda) T_{invite}(n), \bar{F}(0) = T_{invite}(1) \tag{10}$$

where the Eqs.10 and 11 is very similar to the Eqs.2 and 3 that give more illustration of these parameters.

Step 3 (Negativity): by using Eq.4, we convert $\{\overset{\leftrightarrow}{X}_n\}$ into the negative sequence $\{Z_n\}$ for sensing the attack. Moreover, we also convert $\{\overset{\leftrightarrow}{X}_n\}$ into the negative sequence $\{\bar{Z}_n\}$ by the following:

$$\bar{Z}_n = \overset{\leftrightarrow}{X}_n - \bar{\beta} \tag{11}$$

where the parameter $\bar{\beta}$ is similar to β that is the upper bound of the maximum of $\{\overset{\leftrightarrow}{X}_n\}$.

Step 4 (Accumulation): by using Eqs.7 and 8, we can obtain the accumulations of $\{Z_n\}$ and $\{\bar{Z}_n\}$, i.e., Y_n and $\bar{Y}_n$, respectively.

Step 5 (Detection): By the means of 4 Steps above, the improved CUSUM algorithm outputs two variable: Y_n and $\bar{Y}_n$. Because they keep more network state information, more accurate detection results can be obtained. Hence, we adopt Fuzzy Logic to detect SIP flooding attack where Y_n and $\bar{Y}_n$ are the two inputs of Fuzzy Logic and the network attacks probability (AP) as the detection decision is the output.

2.4. *Fuzzy logic for SIP flooding attacks detection*

In order to meet the requirement of high detection performance of SIP flooding attack for IMS network, we use fuzzy logic to infer the detection variables Y_n and $\bar{Y}_n$ from the improved CUSUM algorithm to shorten the detection time as our third main contribution as shown in Figure 5,

Due to the natural contradiction between detection time and false alarm, it is impossible to shorten the detection time while keeping false alarm constant in the practical

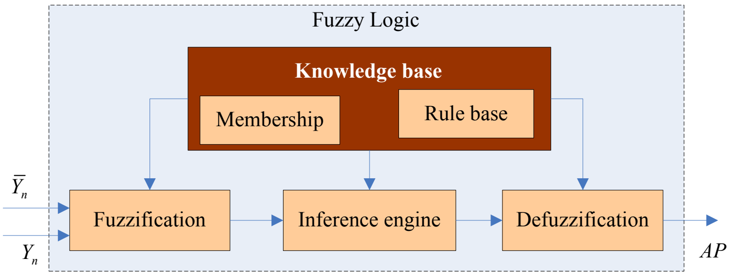

Figure 5. Procedure of Fuzzy Logic for SIP flooding attack detection

network environment. Hence, in terms of the practical application in IMS networks, the most important thing for our study is to shorten the detection time as much as possible while keeping the false alarm ratio low.

Different crisp systems, Fuzzy Logic uses possibility theory to handle uncertainty in their reasoning process [22]. It analyzes analog input values in terms of logical variables that take on continuous values between 0 and 1, in contrast to classical or digital logic which operates on discrete values of either 1 or 0 (true or false respectively). See [22] and [23] for a good survey. In this paper, Fuzzy logic for SIP flooding attack detection main contains four Steps as follows:

Step 1 (Memberships): Mathematically, a set is defined as a finite, infinite, or countable infinite collection of elements. In each case, each element is either a member of the set or not. However, in fuzzy systems, the element can be partially in or out of the set. Thus, the answer to the question: ”Is x a member of a set A” is not a matter of true or false anymore. Here, each fuzzy set (A) comprises several (countable or uncountable) pairs as (x, A(x)) where A(x) is called the membership function to show each member’s degree of truth or compatibility with the set. In this study, we adopt the triangular membership function as shown in Figure 6. This is formed by the combination of straight lines. The triangular graph is named as triangular membership function. We consider the above case, i.e., fuzzy set (A) to represent ”the number close to b”. So mathematically its membership function has the following form:

$$\mu A(x) = \begin{cases} \frac{x-a}{b-a}, & if\ a \leq x \leq b, \\ \frac{c-x}{c-b}, & if\ b \leq x \leq c, \\ 0, & \text{otherwise}. \end{cases} \tag{12}$$

Step 2 (Fuzzification): we set the detection variables Y_n and $\bar{Y}_n$ from the improved CUSUM algorithm as input, with the network attacks probability (AP) the detection decision $d_N(Y_n)$ as output. By using the defined membership functions, we translate the input values into a set of linguistic values and assign a membership degree for each linguistic value using triangular membership functions. As shown in Figure 7, the crisp values of the two variables Y_n and $\bar{Y}_n$ are mapped to Y_1 and Y_2 with linguistic terms using: L (little), ML (little middle), M (middle), MB (middle big), and B (big).

Step 3 (Inference): the inference engine makes decisions based on fuzzy rules. Each rule is an IF-THEN clause in nature, and it determines the linguistic value of AP according to the linguistic values of Y_1 and Y_2. To obtain the accurate detection results, as shown in Figure 8, we design 25 fuzzy rules to infer the inputs. For example, the first rule is ”If

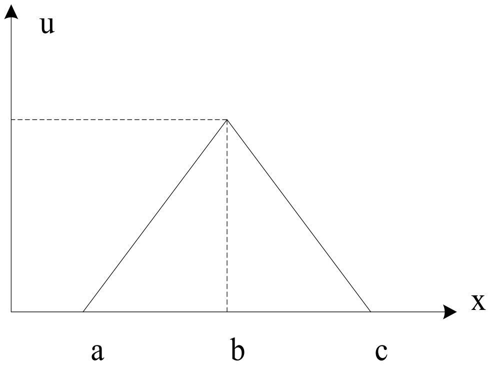

Figure 6. The triangular membership function

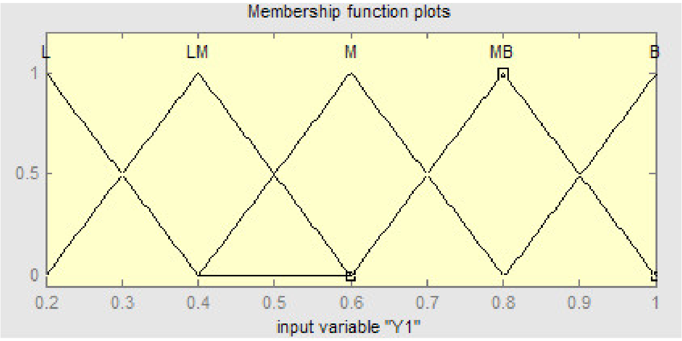

Figure 7. Membership functions for SIP flooding attack detection

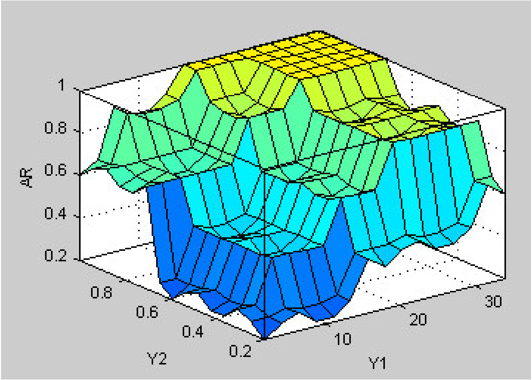

Figure 8. Fuzzy rules for SIP flooding attack detection

(Y1 is L) and (Y2 is L) then (AR is L)”; the 11th rule is ”If (Y1 is M) and (Y2 is L) then (AR is LM)”.

Step 4 (Defuzzification): Basically, defuzzification is a mapping from a space of fuzzy values defined over an output universe of discourse into a space of crisp values. A

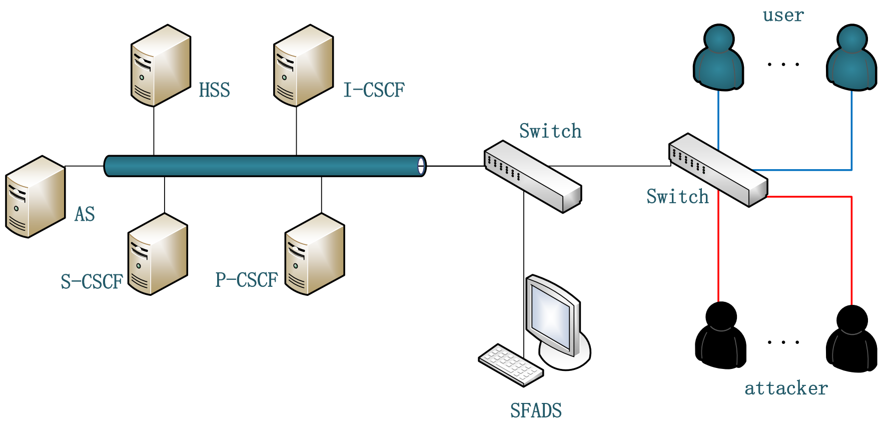

Figure 9. IMS network simulation environment

defuzzification strategy is aimed at producing a crisp value that best represents the possibility distribution of an inferred fuzzy value. There are many different methods of defuzzification as introduced in [24], such as First of Maximum, Last of Maximum, Center of Gravity, Weighted Fuzzy Mean and so on. Because the Weighted Fuzzy Mean is computationally faster and easier and gives fairly accurate result, we adopt it to defuzzify AP which is obtained by the weighted average of the each output of the set of rules stored in the knowledge base of the system) by the following:

$$AP = \frac{\sum_{i=1}^{n} (u_i \cdot w_i)}{\sum_{i=1}^{n} u_i} \tag{13}$$

where AP is the defuzzified output, n represents the number of fuzzy output sets, u_i is the membership of the output of each rule, and w_i is the weight associated with each rule. If the detection result AP is 1, it indicates that an attack occurs and alarm and then defense system [5,25,26] is activated. Otherwise, the network is normal.

3. Performance Evaluation

In this section, we construct an IMS network testbed to evaluate the performance of the proposed SIP flooding detection method as our forth contribution. We investigate the advantage of our scheme over the CUSUM algorithm that is used as the SIP flooding attack detection scheme in previous research [6,20]. The simulation is similar to [5], we also focuses on the INVITE flooding case first since other SIP attributes can be addressed in a similar way.

In Section 3.1, it introduces our established IMS network testbed based on OpenIMSCore[3]. Then to evaluate our scheme effectively, we give develop the prototype im-

[3] www.openimscore.org

plement in Section 3.2. Simulation results on normal traffic and attack traffic are given in Section 3.3 and Section 3.4, respectively. Finally, we discuss the advantage of our detection scheme.

3.1. Simulation Setup

As shown in Figure 9, in order to evaluate the performance of the proposed SFADS, we employ OpenIMScore and SIPp[4] to construct an IMS network testbed and SIP flooding attack scenarios, respectively.

The Open IMS Core is an open source implementation of IMS Call Session Control Functions (CSCFs including P-CSCF,S-CSCF,I-CSCF) and a lightweight Home Subscriber Server (HSS) which together form the core elements of all IMS/NGN architectures as specified today within 3GPP, 3GPP2, ETSI TISPAN and the PacketCable intiative. By using the OpenIMScore, we conduct an IMS network testbed on the PCs (Ubuntu 8.04, 521MB RAM and 3.0GHz).

SIPp is a free Open Source test tool/traffic generator for the SIP protocol. It includes a few basic SipStone user agent scenarios (UA and UAS) and establishes and releases multiple calls with the INVITE and BYE methods. SIPp can be used to test many real SIP equipments such as SIP proxies, SIP media servers, SIP PBX, and so on. By using SIPp, we simulate an INVITE flooding attack scenario. Moreover, we take OpenIC-Lite[5] (v1.0 for Windows) and SIPp as IMS terminal to simulate normal INVITE message requirements. SIPp is developed on the PCs (Ubuntu 8.04, 521MB RAM and 3.0GHz) and OpenIC-Lite is developed on the PCs (Windows XP sp2, 521MB RAM and 3.0GHz).

3.2. Prototype Implementation

To evaluate the performance of the proposed SFADS effectively, we develop the prototype system by using Snort[6] (snort-2.8.3.2.tar.gz) and Libosip[7] (libosip2-2.0.6). As shown in Figure 10, the prototype system consists of Collection Layer, Data Layer, Detection Layer and Responding Layer. The Collection Layer has a SIP packet Collection Module which is used to collect all SIP packets. The Data Layer contains a HASH Module which is responsible for preprocessing the SIP packets from Collection Layer and counting the total number of INVITE request and normal SIP session message sequence within each sampling period, respectively. The Detection Layer has a SFADS Module which is used to perform detection decision with our proposed SFADS scheme. The Responding Layer contains an Alarm Module, which is responsible for sending alarm signal when an attack occurs according to detection decision information.

In the simulation, we set the initial values of the parameters in the scheme according to previous research [6,18,20] and simulation environment, and empirically get their final values as: T=5 (second), $\lambda = 0.5, k = 30, \beta = 0.54, \bar{\beta} = 1, N = 1, N' = 4, N'' = 2$ to achieve desirable detection accuracy.

[4] http://sipp.sourceforge.net

[5] http://openic-lite.software.informer.com

[6] http://www.snort.org

[7] http://www.gnu.org/software/osip

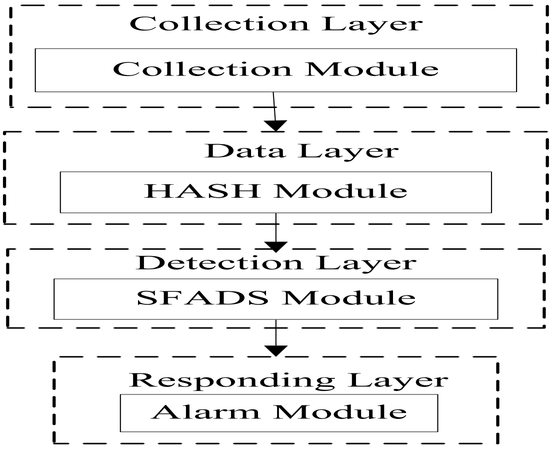

Figure 10. Procedure of the prototype implementation

3.3. Simulation results on normal traffic

In order to be close to the real IMS network status as much as possible, the SIP background traffic is simulated with the traffic model of Reference [27]. Reference [27] has observed China telecom IP network international links for eight months and came to a conclusion that the arrival of VOIP call in a sampling period (1 second) obeys the Weibull distribution as following:

$$f(x) = \frac{\upsilon}{\eta}(\frac{x}{\eta})^{\upsilon-1}e^{-(\frac{x}{\eta})^{\upsilon}} \tag{14}$$

where with the increasing sampling period, the call arrival distribution gradually tends to the normal distribution. As shown in Figure 7, we use several PCs with SIPp and OpenIC-Lite to simulate the normal users to send session request to the P-CSCF (SIP proxy server), whose purpose is to produce background traffic by using Eq.14.

Figure 11 shows the SIP background traffic and SIP flooding attack detection result. Figure 11 (a) gives the background traffic, including INVITE, 200 OK, ACK message which are from the normal session establishment. Figure 11(b) shows the detection result in normal background traffic. For different background traffic (between 20 and 600 calls per second), we do 20 times simulations. All the results show the proposed SFADS does not generate false alarm ratio while the SIP traffic is normal in IMS networks.

3.4. Simulation results on attack traffic

In SIP flooding detection, we also use several PCs with SIPp to simulate attacker to launch SIP flooding attacks. For ease of exposition, we take Figures 12 and 13 as examples to investigate the advantage of the proposed SFADS where the attack occurred in 60-th and 150-th sampling period and each attack lasted 30T. Moreover, as shown in Table 1, we also give the more simulation results in different attack scenarios.

In Figure 12, each horizontal axis is the sampling period (5 seconds), and from top to bottom, the vertical axises are the number of packets including legitimate INVITE

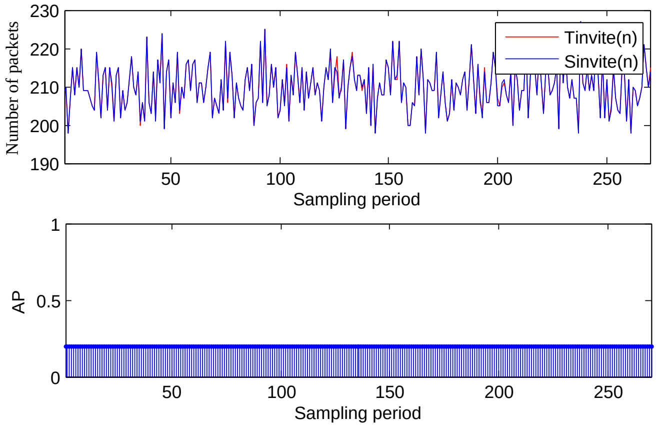

Figure 11. Simulation results on normal traffic

messages and attack messages, the detection decision $d_N(W_n)$ of the CUSUM algorithm, and the final detection result of SFADS (AP), respectively. From the results, when the attack is over, the attacks probability (AP) of the proposed SFADS can fall from 1 to 0.2 quickly. However, the CUSUM detection schemes take 30T to recover 0.2. Hence, by using the improved CUSUM algorithm, the recovery time of the proposed SFADS is shorter, which makes SFADS higher sensitivity for SIP traffic than other detection schemes [6,20].

In Figure 13, each horizontal axis is the sampling period (5 seconds) and from top to bottom, the vertical axises are the number of packets including legitimate INVITE messages and attack messages, the internal detection feature cumulative value $Y1$, the external detection feature cumulative value $Y2$, and the final detection result (AP), respectively. When attacks occur, different from other schemes, the proposed SFADS sharply increased from 0.2 to 1, which means that SFADS has a better detection performance. The main reason why our proposed SFADS can perform the SIP flooding attack detection efficiently and effectively is that SFADS can make the detection decision quickly when the cumulative value $Y1$ is increasing (it is still less the detection threshold) according to the information from the external detection feature.

As shown in Table 1, we give more simulation results where the simulations are run for 50 times and all results are reported, on average. From the results, our proposed SFADS (S) show its better advantage than the CUSUM schemes (Cs) on the alarm ration (AR), false alarm ration (FAR), detection time (DT) and recovery time (RT). Hence, the SFADS is inefficient for detecting low-rate flooding attacks (2.5 times as high as the background traffic) and has a short recovery for detecting high-rate flooding attacks (0.5 times as high as the background traffic)

3.5. Discussion

From the simulation results, it can be seen that SFADS has excellent detection performance in SIP flooding attack detection. Compared to the CUSUM detection schemes, SFADS has advantages in alarm ration and false alarm ratio, especially in detection time and recovery time as follows:

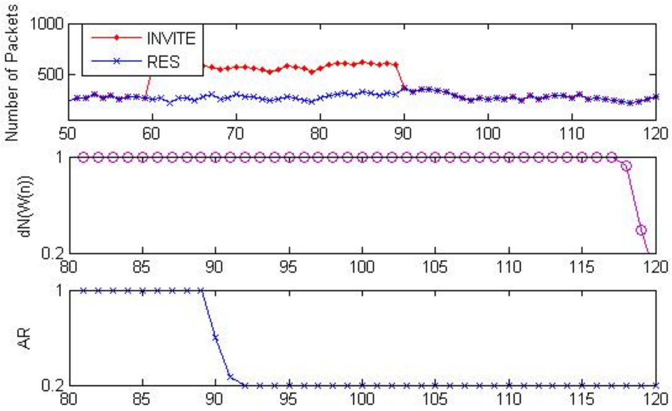

Figure 12. Simulation results on recovery time

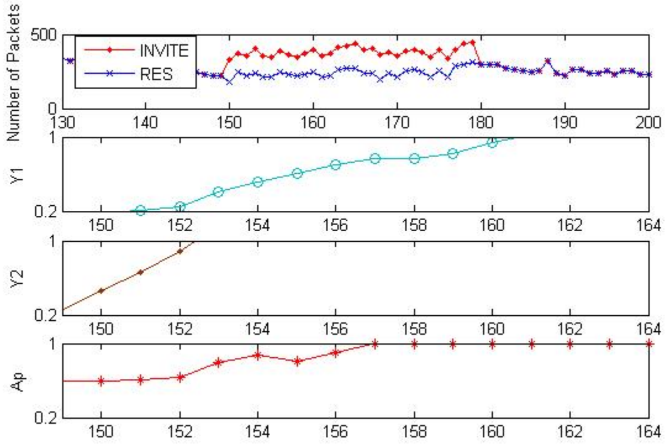

Figure 13. Simulation results detection time

Table 1. Comparison Results

ARe	AR		FAR		DT		RT	
	S	Cs	S	Cs	S	Cs	S	Cs
25	93.8%	-	2.8%	-	8.1	-	1.0	-
28	100%	88.9%	0.2%	0.9%	4.8	7.3	1.0	1.0
30	100%	94.6%	0%	0.5%	4.5	6.7	1.0	1.2
35	100%	100%	0%	0.2%	1.9	5.0	1.0	4.4
40	100%	100%	0%	0%	1.0	3.6	1.0	10.8
100	100%	100%	0%	0%	1.0	1.0	1.1	$\gg$50
900	100%	100%	0%	0%	1.0	1.0	1.1	$\gg$100

1. The CUSUM detection schemes cannot detect low-rate attacks where attackers send 25 INVITEs per second, on average. However, SFADS can detect these attacks with 8.1T detection time, on average. It also can be seen that SFADS has great detection performance for low-rate attacks, which is very beneficial for administrator to take corresponding measures to defense attacks as soon as possible at the beginning of massive attacks and make the loss to a minimum.
2. When the attacks rate is less than 100 INVITEs per second, The detection time (only 2.1T, on average) of SFADS is shorter than that of the CUSUM detection schemes.
3. The recovery time of SFADS is much shorter than the CUSUM detection schemes. In general, SFADS only need about 1T to recover the initiate status of the detection system. But the recovery time of the CUSUM detection schemes is very long, which leads to low sensitivity for attack detection and practical application.

4. Related Work

In the early stages, to detect and prevent SIP flooding attacks, several researchers have already made some research work [3,12-14]. E. Y.Chen [12] proposed a method to monitor the session ID of all SIP messages through modifying the finite state machine which is defined in RFC3261, and then judged whether the system has been attacked base on the statistics of the number of exception messages. However, it fails to detect the forged SIP messages which accord with its designed rules since it cannot give a valid identification. H.Sengar et al.[13] presented an online statistical detection mechanism which used Hellinger distance to compute the probability measure of SIP messages in normal flow and anomalous traffic caused by flooding attacks. S.Ehlert et al.[14] adopted the SIP state machine to detect SIP attacks. This scheme can block SIP flooding traffic and keep the network alive even under attack conditions by communication with a firewall component. However, the scheme cannot effectively recognize and detect the fake SIP messages, which lead to a low alarm rate. Y.Rebahi et al. [3] counted the number of INVITE messages collected within 10 seconds interval, and then used non-parametric CUSUM algorithm to detect SIP flooding attacks in IMS networks. Because the algorithm is solely based on the number of INVITE message to determine whether the attack occurs, it cannot distinguish between the transiently increasing normal traffic and the attack traffic.

Afterwards, with the increase of the SIP flooding attack threat to 3G network. More researchers engaged in the research and have already made some significant research work [5,9,11,17,28-30]. To stop DoS attack before the CSCF is congested. B.Zhao et al. [9] formulated online early detection as a change-point detection problem, which aims to detect when the system is under attack. This was achieved by monitoring the system resource usage. It can further identify the sources of this DoS attack by monitoring any abnormal behavior of a user, and finally block them. J.Tang et al. [5] proposed a versatile scheme for detecting and preventing the SIP flooding attacks in VoIP networks, by integrating the sketch technique with the HD-based detection, which significantly enhances the detection performance. Moreover, J.Tang et al. [28,29] also proposed other effective detection schemes for detecting SIP flooding attacks and have obtained good research results. The schemes presented in [11][17][30] work effectively to detect SIP flooding.

Difference from the existing schemes, our proposed detection scheme is efficient for detecting low-rate flooding and has a short recovery for detecting high-rate flooding by using the extracted two detection features.

5. Summary and future work

The IMS provides mobility and session management as well as message routing, security, and billing [31]. In order to detect SIP flooding attacks in IMS networks, in this paper, we first analyze SIP session establishment process and extract the two-feature detection features for SIP flooding attack detection. Based on the detection features, we proposed a novel SIP flooding attack detection scheme for IMS network. Its core is that we use the improved CUSMU algorithm to analyze the two-feature detection features that cover more detection information, and then take the analysis results as inputs and adopt Fuzzy Logic with 25 designed fuzzy rules to reason and output the detection result. With respect to the performance evaluation, we conduct an IMS network testbed and implement the prototype detection system. Simulation results shown the proposed scheme is effective and efficient.

In future work, we will focus on the self-adaptation of the proposed scheme for different SIP flooding attack environments. Moreover, Although there are several new solution for SIP flooding attacks such as packet-based analysis defense technique [32], Hellinger distance defense technique [33], and cross-analysis defense technique [34], it is still difficult to prevent SIP flooding attacks since illegitimate packets are indistinguishable from legitimate packets, making detection difficult. Hence, SIP flooding attack will continue to grow in scale and severity thanks to increasingly powerful (and readily available) attack tools, the multiple points of IMS vulnerability, and business' increasing dependence on SIP protocol. As the cost of these attacks rise, providers and enterprises must respond to protect their services and application.

Acknowledgements

The work presented in this study is supported by the NSFC(61202435); NSFC(61272521); Natural Science Foundation of Beijing under Grant No.4132048; Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20110005130001; Program for New Century Excellent Talents in University of China under Grant No.NCET-10-0263; and Innovative Research Groups of the National Natural Science Foundation under Grant No.61121061.

References

[1] L. Lin and A. Liotta, Presence in the IP multimedia subsystem, *Mobile Information Systems*, **3**, (2007), 187–202.

[2] J. Tang, Y. Cheng, and Y. Hao, Detection and prevention of SIP flooding attacks in voice over IP networks, *In Proceedigns of IEEE International Conference on Computer Communications (INFOCOM'12)*, (2012), 1161–1169.

[3] Y. Rebahi, M. Sher, and T. Magedanz, Detecting flooding attacks against IP Multimedia Subsystem (IM-S) networks, *In Proceedings of the 6th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA'08)*, (2008), 848–851.

[4] B. Zhao, C. Chi, W. Gao, S. Zhu, and G. Cao, A chain reaction DoS attack on 3G networks: Analysis and defenses, *In Proceedigns of IEEE International Conference on Computer Communications (INFO-COM'09)*, (2009), 2455–2463.

[5] F. Huici, S. Niccolini, and N. D'Heureuse, Protecting SIP against very large flooding DoS attacks, *In Proceedings fo the Global Communications Conference (GLOBECOM'09)*, (2009), 1–6.

[6] Z. Chen, W. Wen, and D. Yu, Detecting SIP flooding attacks on IP Multimedia Subsystem (IMS), *In Proceedings of the International Conference on Computing, Networking and Communications (ICNC'12)*, (2012), 154–158.

[7] S. Ehlert, D. Geneiatakis, and T. Magedanz, Survey of network security systems to counter SIP-based denial-of-service attacks, *Computers and Security*, **(29)**, 2010, 225–243.

[8] M. A. Akbar, Z. Tariq, and M. Farooq, A comparative study of anomaly detection algorithms for detection of sip flooding in IMS, *In Proceedings fo the 2nd International Conference on Internet Multimedia Services Architecture and Application (IMSAA'08)*, (2008), 1–6.

[9] B. Zhao, C. Chi, W. Gao, S. Zhu, and G. Cao, A chain reaction DoS attack on 3G networks: Analysis and defenses, *In Proceedigns of IEEE International Conference on Computer Communications (INFO-COM'09)*, (2009), 2455–2463.

[10] D. Sisalem, J. Kuthan and S. Ehlert, Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms, *IEEE Network*, **(5)**, 2006, 26–31.

[11] M. Z. Rafique, M. A. Akbar, and M. Farooq, Evaluating DoS attacks against SIP-based VoIP systems, *In Proceedings fo the Global Communications Conference (GLOBECOM'09)*, (2009), 1–6.

[12] E. Y. Chen, Detecting DoS attacks on SIP systems, *In Proceedigns of the 1St IEEE Workshop on Voip Management and Security VoIP (MaSe'06)*, (2006), 51–56.

[13] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, Fast detection of denial-of-service attacks on IP telephony, *In Proceedings of the 14th IEEE International Workshop on QoS (IWQoS'06)*, (2006), 199–208.

[14] S. Ehlert, C. Wang, T. Magedanz, and D. Sisalem, Specification-based denial-of-service detection for SIP voice-over-IP networks, *In Proceedings of the third International Conference on Internet Monitoring and Protection (ICIMP'08)*, (2008), 59–66.

[15] P. Mutaf and C. Castelluccia, Compact neighbor discovery: a bandwidth defense through bandwidth optimization, *In Proceedigns of IEEE International Conference on Computer Communications (INFO-COM'05)*, (2005), 2711–2719.

[16] S. Changhua, H. Chengchen, T. Yi, and L. Bin, More Accurate and Fast SYN Flood Detection, *In Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN'09)*, (2009), 1–6.

[17] F. Huici, S. Niccolini, and N. D'Heureuse, Protecting SIP against very large flooding DoS attacks, *In Proceedings fo the Global Communications Conference (GLOBECOM'09)*, (2009), 1–6.

[18] B. Zhao, C. Chi, W. Gao, S. Zhu, and G. Cao, A chain reaction DoS attack on 3G networks: Analysis and defenses, *In Proceedigns of IEEE International Conference on Computer Communications (INFO-COM'09)*, (2009), 2455–2463.

[19] M. Basseville and I. V. Nikiforov, Detection of Abrupt Changes : Theory and Application, *Prentice Hall*, New Jersey, USA, 1993.

[20] H. Wang, D. Zhang, and K. G. Shin, Detecting SYN flooding attacks, *In Proceedigns of IEEE International Conference on Computer Communications (INFOCOM'12*, (2012), 1530–1539.

[21] V. A. Siris and F. Papagalou, Application of anomaly detection algorithms for detecting SYN flooding attacks, *In Proceedings fo the Global Communications Conference (GLOBECOM'04)*, (2004), 2050–2054.

[22] P. P. C. Lee, T. Bu, and T. Woo, On the detection of signaling DoS attacks on 3G wireless networks, *In Proceedigns of IEEE International Conference on Computer Communications (INFOCOM'07*, (2007), 1289–1297.

[23] B. E. Brodsky and B. S. Darkhovsky, Non-parametric methods in Change-Point Problems: Kluwer Academic Publishers, 1993.

[24] Zadeh and L. A., Fuzzy sets, *Information and Control*, **(8)**, (1965), 338-353.

[25] G. Klir and B. Yuan, Fuzzy Sets and Fuzzy Logic Theory and Applications, *Prentice-Hall*, New Jersey, USA, 1995.

[26] W. V. Leekwijck and E. E. Kerre, Defuzzification: criteria and classification, *Fuzzy Sets and Systems*, **(108)**, (1999), 159–178.

[27] Y. Guoliang, Analysis of International VoIP Traffic Characterization, *Telecommunications Science*, **(6)**, 2007, 18–23.

[28] J. Tang and Y. Cheng, Quick detection of stealthy SIP flooding attacks in VoIP networks, *In Proceedings of the 2014 IEEE International Conference on Communications (ICC'11)*, (2011), 1–5.

[29] J. Tang, Y. Cheng, and C. Zhou, Sketch-based SIP flooding detection using Hellinger distance, *In Proceedings fo the Global Communications Conference (GLOBECOM'09)*, (2009), 1–6.

[30] D. Geneiatakis, N. Vrakas, and C. Lambrinoudakis, Utilizing bloom filters for detecting flooding attacks against SIP based services, *Computers and Security*, **(28)**, 2009, 578–591.

[31] G. Gehlen, F. Aijaz, Y. Zhu, and B. Walke, Mobile P2P Web Services using SIP, *Mobile Information Systems*, **(3)**, 2007, 65–185.

[32] Akbar M, Farooq M, Securing SIP-based VoIP infrastructure against flooding attacks and Spam Over IP Telephony, *Knowledge and Information Systems*, **(2)**, 2014, 491–510.

[33] Jin T, Yu C, Yong H, Wei S, SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design, *IEEE Transactions on Dependable and Secure Computing*, **(6)**, 2014, 582–595.

[34] Tsiatsikas Z, Geneiatakis D, Kambourakis G, Keromytis AD, An efficient and easily deployable method for dealing with DoS in SIP services, *Computer Communications*, **(1)**, 2015, 50–63.

Qibo Sun received his PhD degree in communication and electronic system from the Beijing University of Posts and Telecommunication in 2002. He is currently an associate professor at the Beijing University of Posts and Telecommunication in China. He is a member of the China computer federation. His current research interests include services computing, internet of things, and network security.

Shangguang Wang is an assistant professor at Beijing University of Posts and Telecommunications. He received his Ph.D. degree at Beijing University of

Posts and Telecommunications in 2011. His research interests include service computing and cloud computing. He has served as reviewers for numerous journals, including IEEE Transactions on Parallel and Distributed System, IEEE Transactions on Service Computing, The Computer Journal, IET Software, etc. He is an IEEE member, ACM member as well as a CCF senior member. Homepage: `http://www.sguangwang.com/`

Fangchun Yang received his PhD degree in communication and electronic system from the Beijing University of Posts and Telecommunication in 1990. He is currently a professor at the Beijing University of Posts and Telecommunication, China. His current research interests include network intelligence and services computing. He is a fellow of the IET.