IJICTR International Journal of Information & Communication Technology Research

ITRC

Volume 8- Number 1- Winter 2016 (33-41)

Detecting Flood-based Attacks against SIP Proxy Servers and Clients using Engineered Feature Sets[1]

Hassan Asgharian
Department of Computer Engineering,
Iran University of Science and Technology,
Tehran, Iran
Asgharian@iust.ac.ir

Ahmad Akbari
Department of Computer Engineering,
Iran University of Science and Technology,
Tehran, Iran
{Asgharian, Akbari}@iust.ac.ir

Bijan Raahemi
Knowledge Discovery
and Data Mining Lab,
University of Ottawa,
Ottawa, Canada
raahemi@uottawa.ca

Received: October 21, 2015- Accepted: April 8, 2016

Abstract— **Session Initiation Protocol (SIP) is the main signaling protocol of the next generation networks. The security issues of SIP-based entities (i.e. proxy servers and clients) have a direct impact on the perceived quality of experience of end users in multimedia sessions. In this paper, our focus is on the SIP flooding attacks including denial of service and distributed denial of service attacks. After classifying various types of SIP attacks based on their sources, we extract four feature sets based on the specification of its attack group, as well as the normal behavior of the SIP state machine specified in RFC 3261. We then minimize the number of derived features in each set to reduce the computational complexity of our proposed approach. This facilitates employing the engineered feature sets in embedded SIP-based devices such as cell phones and smart TVs. We evaluate the performance of the proposed feature sets in detecting SIP attack sequence. For this, we design and implement a real test-bed for SIP-based services to generate normal and attack traffics. The experimental results confirm that the engineered feature sets perform well in terms of detection accuracy and false alarm rates in classifying benign and anomaly traffic in various attack scenarios.**

Keywords- ***SIP Security, SIP Feature Set, SIP intrusion detection system, Application Layer DoS Attack (DDoS), SIP state machine, VoIP IDS, NGN and IMS Security***

I. INTRODUCTION

The session initiation protocol (SIP) is an IETF protocol for controlling VOIP and other multimedia communication sessions like IPTV and instant messaging. SIP is designed with an open architecture vulnerable to security attacks. Therefore, effective detection of flooding attack to the SIP proxy server is critical to ensure robust multimedia communications over IP networks. Due to the increasing popularity of the SIP-based services (such as VoIP, IPTV, IMS infrastructure), the security concerns of the end users and service providers should seriously be taken into consideration. The existing security mechanisms

[1] This work was supported partly by the CyberSpace Research Institute (CSRI) of IRAN under contract NO 17164/500.

against SIP flooding attacks work less than expected. These mechanisms may fail when flooding is launched by simultaneously manipulating different types of SIP messages [1]. Furthermore, SIP is a transactional protocol and possesses multiple controlling message attributes [2] [3] and its behavior is defined as a set of relatively independent steps with not a fixed coupling between them [4].

SIP entities (i.e. proxy servers and clients) encounter various types of Denial of Service (DoS) attacks because of both implementation and protocol weaknesses [5]. Since SIP works in application layer of TCP/IP without any consideration about lower layers (IP), the definition of distributed DoS on SIP entities is a little different with other protocols. In other words, SIP DDoS attack is a special flooding attack that uses the inefficiencies of SIP implementations.

Generally VoIP attacks classify to six different groups: social threats, eavesdropping, interception and modification, service abuse, intentional and non-intentional interruption of service [4] [6]. VoIP systems have predominantly software-based implementations which are vulnerable to application layer flooding attacks [5]. The SIP flooding attacks exhaust the resources of both networks and entities and can be launched easily [7].

We categorize the flooding attacks into four groups based on their generation complexity: basic flooding (DoS), advanced flooding (DDoS), authentication and memory based attacks (incomplete transactions). This categorization is based on the production process and also the target of attacks. The basic flooding attacks are generated by sending a large amount of SIP messages to server containing random generated fields. These messages deplete memory, processor and bandwidth of the victim. Since the attacker doesn't care about the random generated fields, this class can be considered as SIP DoS. The advanced flooding attacks are generated by smart use of special SIP messages. SIP brute force attack [8] is an example of this class. As it is defined by RFC 3261, SIP has four layers: syntax and encoding; transport; transaction; and transaction user (TU). Handling the current state of transactions in transaction and transaction user layers needs a considerable memory which will be exhausted if the number of concurrent calls is larger than the predicted amount of memory. Therefore, the intruder generates messages belonging to different transactions to occupy more memory. We call them advanced SIP flooding attack which depletes the memory with lower number of SIP messages. These attacks are categorized as SIP DDoS. The third class of SIP flooding attacks called authentication attack misuses the simple authentication process of the SIP entities and tries to deplete CPU as shown in Figure 1. Much of the processing power of a typical SIP component is consumed for security checks and also message parsing. SIP uses a challenge based authentication mechanism that is based on HTTP authentication [9]. In this authentication mechanism when client wants to communicate to a SIP proxy, receives a "407 Proxy authentication required" response with an authentication header contains a random string (challenge) generated by server called nonce. Client program generates an authentication header by applying MD5 algorithm on received nonce and embed its URI and password and send the request message back to the server. Server similarly calculates the response value and compares it with the desired value. This procedure requires significant processing resources from server in generating random numbers and also comparing the extracted nonce from input messages. Accordingly, attacker can occupy server processing resources (CPU) by organizing the following attack scenarios [10]:

- Static nonce-based flooding attack: intruder uses spoofed nonce to create authentication enabled requests. In other words, the attacker uses valid nonce to generate new calls.
- Adaptive nonce-based flooding attack: the intruder continuously refreshes nonce, to create valid requests that not filtered before processing.
- Adaptive nonce-based flooding attacks with spoofed IP addresses: the intruder sends requests with valid nonce and by using spoofed IP addresses tries to harden the detection process.

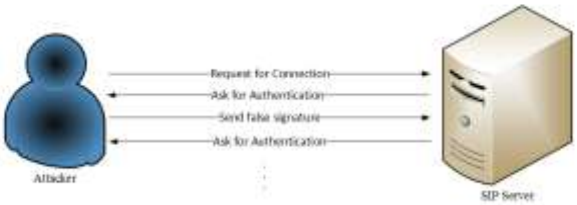

Fig. 1- A sample authentication based attack

We call the fourth SIP flooding attack scenario as memory-based attack or incomplete transaction. The attacker prolongs the call control sessions by misusing the SIP state machine. These attacks usually are generated by cooperation of one valid host in the VoIP network as shown in Figure 2. In this scenario, an INVITE request is sent by an attacker. He repeats sending 1xx responses and do not send the final response (2xx) to exhaust the memory of the SIP server.

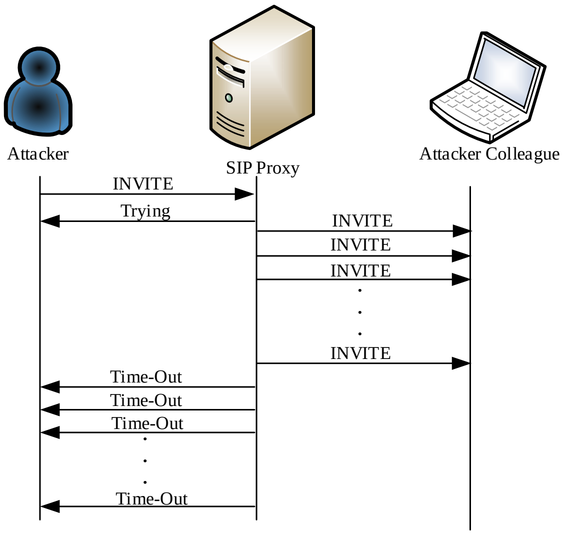

Fig.2 - Prolong the SIP sessions for memory depletion attack

The real-time nature of VoIP systems requires the security mechanisms to work with minimal delay, and also, minimal false alarm. In this paper, we propose four different feature sets for detecting the abovementioned attack groups. The proposed features in all groups use only the explicit extracted information of incoming packets. As such, they are calculated with minimum overhead and delay. We also reduce the number of features in each group to minimize the runtime computation complexity. We show the effectiveness of the proposed feature set by comparing its performance with all features and also random selected features. The main contributions of this paper are as follows:

- We concurrently employ of the SIP state machine (normal behavior) and SIP attack scenarios to engineer features
- We propose a specification-based intrusion detection system by combining the SIP finite state machine and machine learning-based approaches
- We deploy the proposed minimal feature set in a specification-based SIP anomaly detection systems
- Our proposed technique detects all SIP flooding based attack scenarios including DoS and DDoS

The rest of the paper is organized as follows. The related works are summarized in the following section. The proposed feature sets are introduced in the section III, followed by the experiment setup and database preparation described in details in Section IV. The results analysis and conclusion are given in Sections V and VI, respectively.

II. RELATED WORK

Intrusion detection in SIP based systems classifies into statistical approaches and machine learning techniques [11]. We proposed a method based on the SIP state machine in [12] to detect SIP flooding attacks. We followed the original SIP state machine in [12] with different thresholds in such a way that the transaction anomalies are revealed. The main drawback of [12] is its parameter setting which is time consuming and traffic specific. Moreover, it has lower detection rate in comparison to machine learning techniques. A cross layer detection scheme is proposed in [13]. It simultaneously utilizes the RTP and SIP protocol stacks and their relationships. Since concurrent accessibility to the signaling and media protocols (in a detection system) is a very preventive assumption on VoIP systems, their proposed solution seems not to be appropriate in real world applications. A basic security architecture for monitoring, detecting, analyzing and countering SIP attacks is presented in [14] as VoIP defender. It offers the essential facilities for analyzing the SIP layer down to the transport, network and MAC layers. The real-time applicability and the transparency to SIP entities are main advantages of VoIP defender. A protected robust SIP state machine is proposed in [15] to resist against SIP flooding attacks but their proposed architecture cannot detect some advanced attacks like brute force or CPU based attacks which have more complicated construction process. Another specification based intrusion detection framework is presented in [3]. It extracts some explicit features directly from SIP state machine and utilizes threshold values to make decision about abnormality of designated traffic in real-time which makes it susceptible to low rate SIP attacks. Using bloom filters is another statistical approach that used in some SIP IDS systems [6]. The main problem of bloom filters is their high false alarm rates. Some classic statistical approaches like Hellinger distance is also used in SIP anomaly detection systems [16]. The authors of [1] use a multidimensional system based on Hellinger distance to detect SIP DoS attacks.

Using machine learning techniques alongside with appropriate feature definition makes another class of SIP intrusion detection systems. Real-time operation of SIP related applications makes it necessary to use online and incremental learning approaches. An online SIP monitoring system is presented in [17]. A set of 38 statistical features (in five groups) is defined to highlight the abnormal SIP activities. These features are fed to the support vector machine (SVM) for classification in [18]. Another comprehensive engineered feature set for detection of flooding attacks is presented in [11]. The feature definition of [11] is done by the normal behavior of SIP state machine and also by considering the attack scenarios. The main weakness of [11] and also [17] is their maximal approach in feature definition which makes the detection of attack types unachievable, and therefore, limits their usages in intrusion response systems.

We propose four sets of specialized features by focusing on the SIP vulnerabilities and SIP state machine for each class of SIP flooding attacks based on the attack types. The proposed feature sets are engineered by carefully investigating the VoIP reported vulnerabilities in many previous research papers such as [19] [20] [21] [22]. We also propose a specification-based intrusion detection system by combining the SIP finite state machine and machine learning-based approaches. The engineered feature sets are described in the following section and their applicability is shown in different conditions.

III. SIP FEATURE SET ENGINEERING

We propose four different subsets of features based on the characteristics of SIP attacks that enable us to predict the attack types. Prediction of attack class helps the intrusion response systems to make appropriate reaction. We consider the SIP state machine and SIP normal traffic in our feature set engineering process. The proposed feature sets detect the SIP anomalies in real-time and are grouped into four different subsets based on their underlying attack group. Table-1 summarizes the proposed feature sets. In addition to detection of anomalies in SIP traffic, the determination of attack type will be possible by using these proposed small feature sets. The following sub-sections describe the engineered features in details.

Table 1. Engineered features for each flooding attack

Title	# of Features	Engineered Features
Basic Flooding	3	$(\frac{\text{SIP Messages}}{\text{Time Window}})$, $(\frac{\text{Number of SIP Requests}}{\text{Total Number of SIP Messages}})$, $(INVITE - ACK)$
Advanced Flooding	5	$\left(\frac{\text{SIP Messages}}{\text{Time Window}}\right), \left(\frac{\text{Number of SIP Requests}}{\text{Total Number of SIP Messa}}\right.$ $(\frac{\text{Number of Transactions}}{\text{Number of SIP Messages in Window}})$, $(\frac{\text{Number of 1xx}}{\text{Number of Messages in Current Window}})$, $\left(\frac{\text{Number of 2xx}}{\text{Number of Messages in Current Window}}\right)$,
Authentication Based Flooding	5	$(\frac{\text{Number of 4xx}}{\text{Number of Messages}})$, $(\frac{\text{Number of 5xx}}{\text{Number of Messages}})$, $(\frac{\text{Number of REGISTER Messages}}{\text{Number of 2xx Messages}})$, $(\frac{\text{Number of Senders}}{\text{Number of Transactions}})$, $(\frac{\text{Number of Request Messages}}{\text{Number of Response Messages}})$
Memory Based Flooding	5	$(\frac{\text{Number of 1xx}}{\text{Number of Messages in Current Window}})$, $(\frac{\text{SIP Messages}}{\text{Time Window}})$, $(\frac{\text{Number of 4xx}}{\text{Number of Messages}})$, $(\frac{\text{Number of Senders}}{\text{Number of Transactions}})$, $(\frac{\text{Number of Transactions}}{\text{Number of SIP Messages in Window}})$
ALL	14	All above features

A. *Engineered Features for Basic Flood Detection*

Since the SIP entities designed for a specific maximum workload, the number of input requests should not exceed this threshold. Thus, we define a feature for monitoring the online SIP message rate in a designated time period. This feature is computed as the ratio of all input messages (regardless of its request or response nature) within the specified time interval $(\frac{\textbf{SIP Messages}}{\textbf{Time Window}})$. We expect a considerable increase in this ratio during the basic flooding attack periods. In this class of flooding attacks, the intruder can use INVITE, OPTION, CANCEL, BYE, 1xx or any other SIP messages. However, using INVITE method is more convenient because according to the RFC 3261, all SIP components have to support the INVITE method. Moreover, all SIP entities (including user agents and proxies) design to accept incoming SIP requests without preceding session setup. Accordingly, the intruder can expose an attack vector based on this method to deplete the bandwidth, memory or CPU of the designated SIP entity. It is also clearly expressed in SIP state machine that each SIP request requires at least one response. All SIP INVITE messages should be accompanied by an appropriate temporal (i.e. 1xx) and final (i.e. 2xx) response messages. Consequently we expect that the number of SIP request messages in any selected time window become less than the total number of SIP messages. Accordingly we define the second feature for detecting SIP basic floods as $\left(\frac{\textbf{Number of SIP Requests}}{\textbf{Total Number of SIP Messages}}\right)$.

The previous two features are helpful for detecting simple attacks where the intruder forwards a high volume of SIP messages with random value fields towards victim. Since SIP is a stateful protocol, two types of sessions are defined in SIP: transaction and dialog. Almost all SIP entities works in transaction level and initiates, maintains and terminates calls appropriately. Each SIP call is initiated with INVITE packet and its transaction is terminated by 200 OK message accompanied by ACK and its dialog is terminated finally by BYE message. Since all valid INVITE requests should have a final ACK, we define the third feature of this group as the difference between the INVITE and ACK messages $(\boldsymbol{INVITE - ACK})$ which indicates the number of incomplete or in-progress calls.

Despite of its simplicity, this group of attacks can be very harmful because when the proxy or user agent faces with more input requests than its capacity, a breakdown in performance is occurred. Moreover, based on the RFC 3261, all SIP components have to support the INVITE method and all SIP user agents and proxies are by design ready to accept incoming invitations without prior session setup. Consequently the intruder can expose an attack vector based on this method to deplete the bandwidth, memory or CPU of the designated SIP entity.

B. *Engineered Features for Advance Flood Detection*

Since the stateful SIP proxy servers reserve a specific amount of memory for each transaction uptoits completion, it may fail to respond to new incoming requests, if the number of concurrent calls reach a specified threshold. The intruder abuses this issue and arranges a brute force attack (large number of SIP packets with different transaction identifiers). In other words, brute force flooding attacks are made by altering the transaction and dialogue related parameters of SIP messages (i.e. VIA Branch, CSeq Method, CALL-id, TO Tag and From Tag) which is equivalent to application layer distributed DoS.

We expect that monitoring the statistics of transactions and dialogs in SIP reveals advanced flooding attacks. In normal circumstances, each SIP transaction involves of one request message (i.e. INVITE); one or more provisional response message (i.e. 1xx) and finally it will finish with one successful response message (i.e. 2xx) followed by an optional ACK message. Accordingly we expect that the distribution of number of transactions in each time window has a noticeable variation in attack periods. Therefore we define the ratio of transactions to total number of SIP messages in each selected window to detect this kind of attacks $(\frac{\textbf{Number of Transactions}}{\textbf{Number of SIP Messages in Window}})$.

Since this group of attacks is made by generating high volume of packets, we monitor the ratio of SIP packets in time windows too. This feature can be used in detection of basic flooding attacks. Another useful information for SIP flood detection is the ratio of provisional and successful SIP response messages. We expect that the distribution of SIP response messages in attack situation differs from normal states because of stateful nature of SIP components. Therefore we monitor the number of SIP provisional responses and SIP final responses within the current window $(\frac{\textbf{Number of 1xx}}{\textbf{Number of Messages in Current Window}})$ and $(\frac{\textbf{Number of 2xx}}{\textbf{Number of Messages in Current Window}})$.

C. Engineered Features for Authentication Flood Detection

We categorize the flood attack scenarios against authentication mechanism into three separate groups. These attacks attempt to deplete the processing resource of victim by sending smart set of SIP requests. Based on these attack vectors, and also, by considering the SIP state machine, we propose five features to detect this attack group as follows.

In static nonce and valid URI flooding attack, it is assumed that attacker has collected some valid URIs from the corresponding SIP domain. Attacker sends INVITE and REGISTER requests to server by using these valid URIs. Depending on request type, server replies by 401 or 407 message containing authentication header with a valid nonce. Attacker resends request including a fake authentication header, containing valid nonce and a wrong response. When server receives this request it is compelled to check its validity by calculating the correct response using appropriate hash algorithm. By performing this procedure consistently with different URIs, attacker wastes processing resources of server. In mentioned scenario, attacker uses valid nonce and valid URIs in each request to lead his behavior appears normal and make detection of attack harder.

In the next scenario, attacker uses invalid URIs in static nonce-based flood to make server perform authentication signaling, and also, access database of URIs. Facing with valid nonce string, server has to access database and consume processing power; and then reply to the sender by a 401 or 407 messages; meaning invalid URI or invalid password in the authentication header of received SIP message. We can also detect this class by monitoring the rate of 4xx and 5xx messages.

Attacker can alternatively send authentication request message to the server and use received valid nonce to make several SIP messages with URI of first message or invalid URIs to perform dynamic nonce flooding attack. Receiving messages with valid nonce; if URI in the received message doesn't differ from the URI of the first message, server replies by a 401 or 407 message; otherwise server has to respond by a 403 not here message; meaning that the profile of transaction couldn't be retrieved.

In comparison with normal situations based on the SIP state machine, we expect to see more client error messages (i.e. 4xx) and server error message (i.e. 5xx) in authentication attack intervals. Consequently we define the two separate features for monitoring the client and server error messages $\left(\frac{Number\ of\ 4xx}{Number\ of\ Messages}\right)$ and $\left(\frac{Number\ of\ 5xx}{Number\ of\ Messages}\right)$. We also monitor the ratio of successful REGISTER messages, and we expect that the distribution of successful registration might change in authentication attack intervals because we witness high rate of unsuccessful registration attempts $\left(\frac{Number\ of\ REGISTER\ Messages}{Number\ of\ 2xx\ Messages}\right)$. Another authentication related attack to SIP entities can be launched by misusing the NAT technology because we cannot restrict the input requests by their IP addresses. The SIP users may not have concurrent calls (or have a very limited number of simultaneous calls), then we also used this information in our features by considering the number of senders. Therefore, if we monitor the normalized ratio of senders to transactions, we can detect this kind of attacks $\left(\frac{Number\ of\ Senders}{Number\ of\ Transactions}\right)$. This feature can detect the simple SPIT (SIP SPAM) too. The final engineered feature of this group is the ratio of request to response messages. This ratio reveals the unusual situations in which the intruder tries to forward invalid request or response messages $\left(\frac{Number\ of\ Request\ Messages}{Number\ of\ Response\ Messages}\right)$.

D. Engineered Features for Memory Flood Detection

By prolonging the transaction time, the memory of SIP entity may deplete. The intruder generates as much as different transactions by randomly selected initiators for his SIP messages (i.e. "VIA Branch", "To TAG" and "From TAG"). Accordingly, the number of concurrent unique transactions may be an operational feature for detecting the memory based attacks $\left(\frac{Number\ of\ Transactions}{Number\ of\ Messages}\right)$. In addition to number of different transactions, we observe that in normal situations the total number of senders is less than the total number of transactions. Consequently, we consider this ratio as a new feature $\left(\frac{Number\ of\ Senders}{Number\ of\ Transactions}\right)$. Another sample attack of this class is incomplete transactions with host cooperation or ringing based attacks in which the attacker sends INVITE requests to his colleague and he prolongs the lifetime of a transaction by sending provisional responses (e.g. 1xx). According to RFC3261, the transaction time can be prolong to several minutes which misused by attacker. For further extending the transaction lifetime, the target destinations may collaborate in attack and reply just with provisional responses [23]. Therefore, we expect that monitoring the number of provisional responses in different time intervals can reveal the memory based attacks $\left(\frac{Number\ of\ 1xx\ Messages}{Number\ of\ All\ Messages}\right)$. As it is mentioned in the previous sections, if the attacker generate requests with different transactions and dialog identifiers, his requests require more memory than simple flooding attacks. As such, we consider the number of client error message especially the 403 Not Here message to detect the memory based flooding attacks $\left(\frac{Number\ of\ 4xx\ Messages}{Number\ of\ All\ Messages}\right)$.

IV. Evaluation of the Engineered Feature Sets

The evaluation of the proposed feature sets and our experimental setup is presented in this section. Three different datasets are exploited for studying the efficiency of the proposed feature sets. Because of diversity of SIP attack types, we may not access to the attack traffic before their occurrence and for this reason we have to use the one class classifiers. One-class classification systems are categorized to two groups: OCSVM and non-OCSVM. We employ a sample one class support vector machine in this paper to study its accuracy in detecting the SIP anomalies with our proposed feature sets. Since the available datasets did not include all SIP attack types, we also prepare a SIP test bed in our experiments to generate the authentication and memory based attacks.

A. Experimental Setup

The architecture and main components of our test-bed is shown in Figure 3. We use the OPENSIPS [24] as a SIP proxy server and SIPp [25] as user agents (server and client). All additional attacks (authentication and memory based attacks) are implemented by these tools. We also used three different datasets in our experiments. The NRG-IUST [4] is generated and collected in our test-bed. Traffic generation is described in our previous published works [4], [8] and [26]. We extend this testbed to generate new types of attacks. The second dataset is based on OPENSIPS and the last one is collected with ASTERISK in INRIA [18].

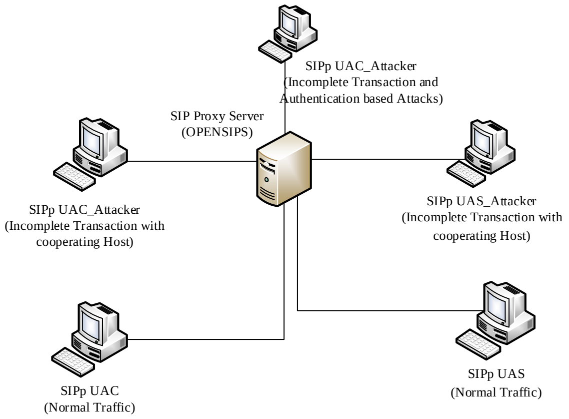

Fig.3 - The SIP Test-bed (extended version of [4])

The performance of designated features in normal and attack periods is shown initially. It is revealed by comparing the value of the selected feature in normal and attack periods in all datasets. Finally we used the engineered features as an input of sample classifier to show its performance in terms of accuracy, detection and false alarm rates.

B. *Quantitative Evaluation of the Engineered Individual Features*

To show the efficiency of each nominated feature in attack periods, we take one sample feature in each four suggested groups and quantitatively compare the variation of its value in normal and attack periods. The "Normalized Number of Requests per Window" feature highlights the basic flooding attacks in OPENSIPS INRIA [18] traffic. Figure 4 shows the behavior of this feature over a window of 1000 ms. As shown in Figure 4, the value of the feature fluctuates (increased and decreased) significantly during attack intervals in comparison to the normal traffic interval. According to RFC 3261, there must be at least one response to each request in normal circumstances. Alongside other features of this group, the ratio of request messages to all messages can be used to detect the basic flooding attacks.

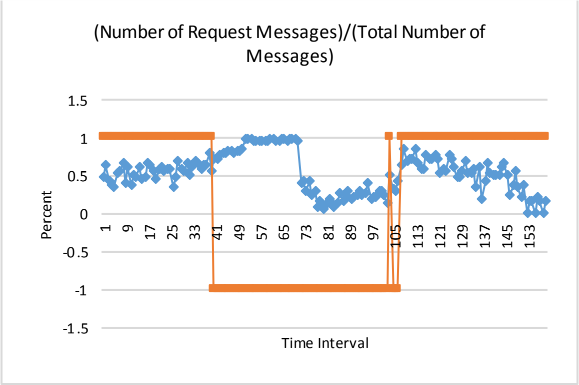

Fig. 4- The value of "*Normalized Number of Requests per Window*" feature (window size = 1000 ms and attack periods are highlighted by "-1" value in red line)

The derived feature "*Number of Transactions per Message per Window*" is studied for advanced flooding attacks. Figure 5 shows the behavior of this feature in IUST-NRG advanced flooding attack during normal and attack intervals. In normal circumstances, the value of this feature should be around 0.25 because we have at least one provisional (usually more than one) and one final response to each request in all successful transactions. Since the SIP proxy reserves a specific amount of memory and processing power for each call, if the number of concurrent calls become more than the specific threshold value, the throughput of the proxy server drops significantly. The attack periods are tagged with "-1" in this figure that indicate their perceptible change of this feature encountering attacks.

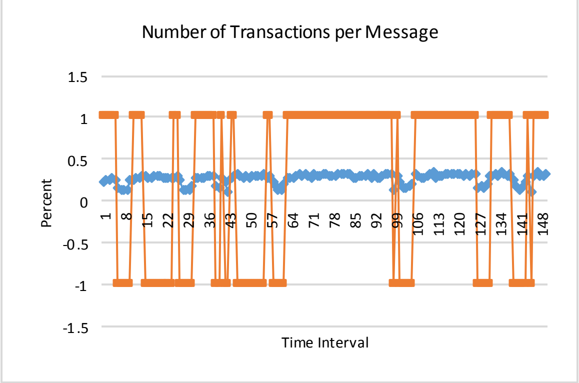

Fig.5 - "Number of Transactions per Message per Window" is shown in the IUST-NRG dataset as a sample feature of second group (advanced flooding attacks). This feature reveals the periods that the attacker tries to deplete the memory of victim proxy by producing new calls with different transaction information. The attack intervals are labelled with "-1" in red line.

Next, we study authentication-based attacks. The proposed feature "*Number of REGISTER messages per 2xx Messages*" reveals the status of the system facing with authentication attacks. In **Error! Reference source not found.** this feature is shown in one sample traffic of IUST-NRG for REGISTER flooding.

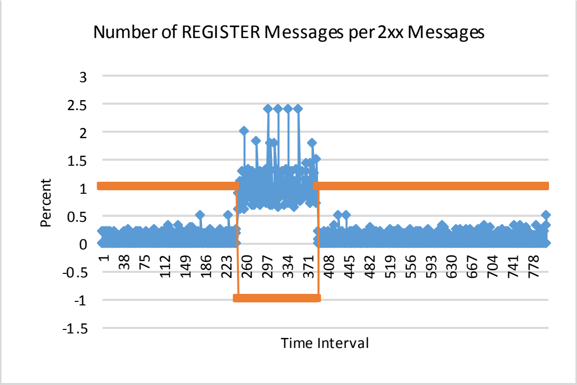

Fig. 6- "*Number of REGISTER messages per 2xx Messages*" is shown in IUST-NRG dataset as a sample feature of third proposed group (authentication based attacks). Variation of the successful SIP registration messages reveals the authentication-based attacks. The attack intervals are labelled with "-1" in red line.

As shown in Figure 7, the number of provisional responses in attack intervals grow significantly. Consequently, the ratio of provisional response per messages in each window is employed as a feature to highlight the memory based attacks. The behavior of this ratio is shown in one sample of RINGING based attacks of IUST-NRG traffics in Figure 7.

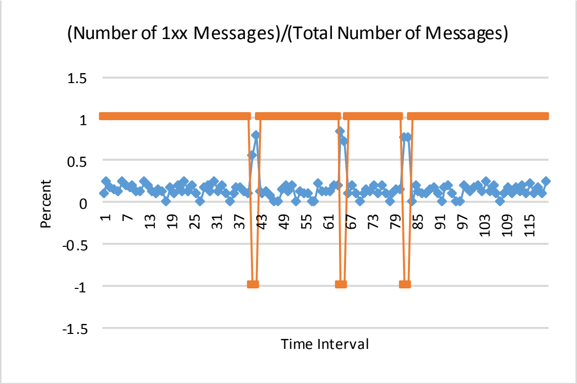

Fig. 8- "*Number of provisional responses per messages per window*" is shown in IUST-NRG dataset as a sample feature of forth proposed group (memory based attacks). The ratio of provisional responses to total number of messages reveals the periods that the attacker tries to deplete memory by prolonging the sessions. The attack intervals are labelled with "-1" in red line

In the following section we evaluate the performance of the proposed feature sets (including accuracy and false alarm) when employed in a sample classification system.

C. Performance Analysis of the Engineered Feature Sets in a Classification System

In order to investigate the effectiveness of the proposed derived features, we test them on a sample one class classifier designed to detect given SIP flooding attacks. Figure 8 shows the block diagram of the training and testing phases of the classifier.

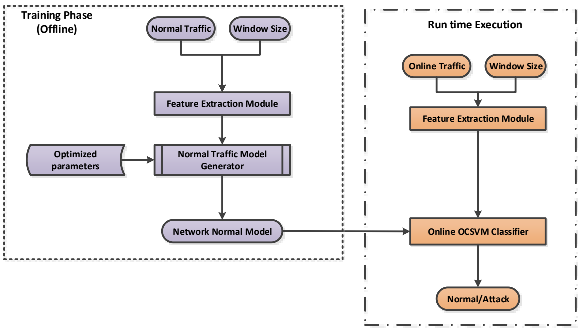

Fig. 7 - OCSVM based classification used for performance evaluation of engineered feature sets

The efficiency of the engineered feature set in terms of accuracy, detection rate and false alarm rate are measured in four different conditions: (a) using the suggested set of features, (b) using randomly selected features, (c) using all features and finally (d) using not appropriate set of proposed features. Since we used OCSVM based classifier in our evaluations, only normal traffic is used in the training phase. The parameters of the classifier is tuned by considering the ROC curve for maximizing the classification accuracy. The selected input traffics for this evaluation are summarized in the Table-2. As shown in this table, the evaluation is done on seven different datasets from INRIA and IUST-NRG.

Table 2. Datasets used for evaluation of the engineered feature sets

Title	Attack Type
NRG-Basic Flood	Basic SIP Message Flooding by using different SIP request and response messages
INRIA-OPENSIPS	Simple advanced INVITE flooding attack
INRIA-ASTERISK	Simple advanced INVITE flooding attack
NRG-Advanced Flood	Advanced SIP Flooding by generating traffic with different transaction and dialog identifiers
NRG-Authentication Attack	Authentication attack by generating request messages with random nonce
NRG-Ringing Attack	Simple memory based attacks by prolonging the sessions with appropriate misuse of provisional SIP responses
NRG-Memory Attack	Advanced memory based attacks by generating incomplete transactions which can be categorized in advanced flooding

The attacks include INVITE flooding attack in INRIA OPENSIPS dataset (normal=100 cps, attack=100 cps), Register flooding attack in NRG dataset (normal=10 cps, attack=10 cps), Ringing based SIP attack in NRG dataset (normal=18 cps, attack=10 cps), Simple request message flooding in NRG (normal=18 cps, attack=80 cps), Mixture of all flooding attacks in NRG dataset (normal=18 cps), Authentication attack based on static random nonce values (normal=20 cps, attack=20 cps) and Invite flooding attack in INRIA ASTERISK dataset (normal=10 cps, attack=100 cps).

Figure 9 and Figure 10 show the comparison between the performances of the classifier with proposed feature set versus the performances of the classifier with other feature sets.

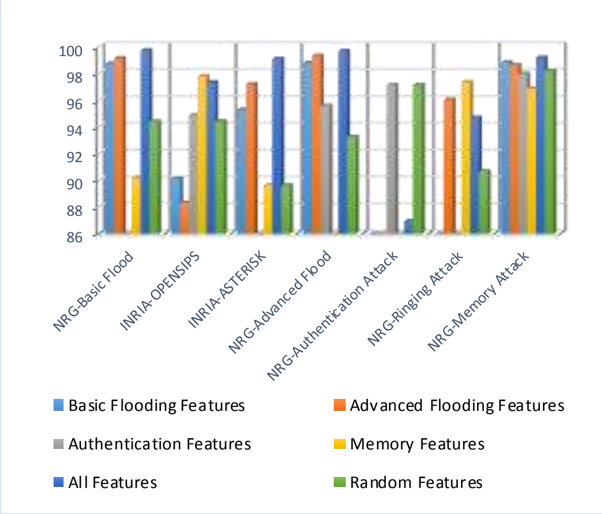

Fig.9- Detection rate of the OCSVM based classifier on various datasets using the engineered feature sets. The detection rates are selected based on the ROC considering maximum accuracy and an acceptable false alarm rate

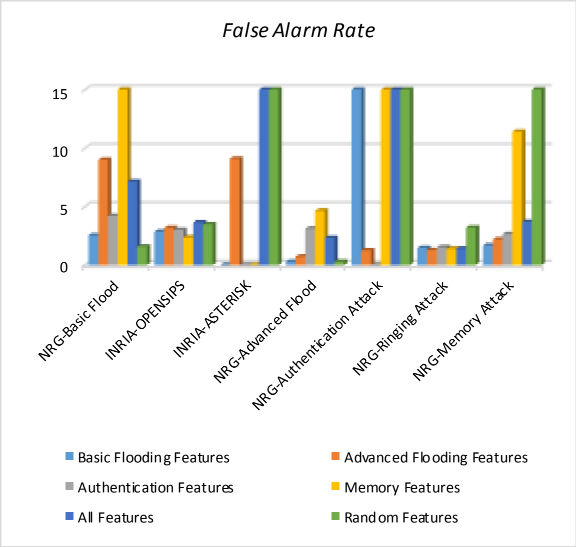

Fig. 10- Comparison of False Alarm Rates of the OCSVM based classifier on different datasets using the engineered feature sets. The reported false alarm rates are selected based on the ROC while maximum accuracy is considered

The following table summarizes the results of employing the engineered feature sets in different scenarios. As it can be seen, in some circumstances, the performance of all features in terms of detection rate is better than the proposed feature set but the relationship between detection rate and false alarm rate should not be ignored.

Table 3. Performance of classifier with attack specific feature sets

#	Title (input traffic)	Feature Set	Detection Rate	False Alarm Rate
1	NRG-Basic Flood	Basic flood features	98.69	2.54
2	INRIA-OPENSIPS	Memory Features	97.76	2.37
3	INRIA-ASTERISK	Basic flood features	95.28	0
4	NRG-Advanced Flood	Advanced Flooding Features	99.28	0.72
5	NRG-Authentication	Authentication Based Features	97.1	0
6	NRG-Ringing	Memory Features	97.33	1.4
7	NRG-Memory	Advanced Flooding Features	98.58	2.2

Shown in Table 3, the classifier exhibits good performance by using the proposed feature sets. The results of this experiment highlight that the proposed engineered feature sets can be employed to effectively detect attacks and the performance of the reduced size attack-specific engineered feature set is completely comparable with all features. Extracting the reduced size engineered feature sets has a reasonable low computational complexity. As such, they can be implemented in SIP-enabled devices to shield them against specific type of attacks.

D. Conclusions and Future Works

The security issues of SIP-based entities (e.g. proxy servers and clients) have a direct impact on the perceived quality of experience of end users in multimedia sessions. In this research, we focused on SIP flooding attacks including denial of service and distributed denial of service attacks. After classifying various types of SIP attacks based on their sources, we extracted four specific feature sets to detect these attacks. Each derived feature set is extracted from the specification of its attack group, and also, the normal behavior of the SIP state machine. This feature categorization helps to minimize the computation complexity of intrusion detection systems encountering different classes of attacks. Consequently, it will be feasible to embed the detection mechanisms into end user devices (e.g. mobile, smart TV, etc.). We studied these feature sets in different scenarios of SIP attacks to show its performance in attack sequence detection. The experimental results confirm that the engineered feature sets perform well in terms of detection accuracy and false alarm rates. We plan to expand our research by defining appropriate features for detecting SIP malformed messages and SIP spam (SPIT) detection in our future works.

REFERENCES

[1] J. Tang, Y. Cheng, Y. Hao and W. Song, "SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design," IEEE Transactions on Dependable and Secure Computing, pp. 1-14, 2014.

[2] RFC3261, SIP: Session Initiation Protocol, 2002.

[3] S. Ehlert, C. Wang, T. Magedanz and D. Sisalem, "Specification-based Denial-of-Service Detection for SIP Voice-over-IP Networks," in 3rd International Conference on Internet Monitoring and Protection, 2008.

[4] Z. Asgharian, H. Asgharian, A. Akbari and B. Raahemi, "Detecting Denial of Service Attacks on SIP Based Services and Proposing Solutions," in Privacy, Intrusion Detection and Response: Technologies for Protecting Networks, P. Kabiri, Ed., IGI Global, 2012, pp. 145-167.

[5] J. Tang, Y. Cheng and Y. Hao, "Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks," in INFOCOM, 2012.

[6] D. Geneiatakis, N. Vrakas and C. Lambrinoudakis, "Utilizing bloom filters for detecting flooding attacks against SIP based services," Elsevier Computers and Security, vol. 28, pp. 578-591, 2009.

[7] S. A. Baset, V. K. Gurbani, A. B. Johnston, H. Kaplan, B. Rosen and J. D. Rosenberg, "The Session Initiation Protocol (SIP): An Evolutionary Study," JOURNAL OF COMMUNICATIONS, vol. 7, pp. 89-105, 2012.

[8] Z. Asgharian, H. Asgharian, A. Akbari and B. Raahemi, "Detecting Denial of Service Message Flooding Attacks in SIP based Services," Amirkabir Journal of Technology, vol. 44, no. 1, pp. 74-81, 2012.

[9] M. Luo, T. Peng and C. Leckie, "CPU-based DoS attacks against SIP servers," in IEEE Symposium on Network Operations and Management, 2008.

[10] S. Pourmohseni, H. Asgharian and A. A., "Detecting authentication misuse attacks against SIP entities," in 10th International ISC Conference on Information Security and Cryptology (ISCISC), 2013.

[11] H. Asgharian, A. Akbari and B. Raahemi, "Feature engineering for detection of Denial of Service attacks in session initiation protocol," SECURITY AND COMMUNICATION NETWORKS, Wiley , no. DOI: 10.1002/sec.1106, 2014.

[12] Z. Asgharian, H. Asgharian, A. Akbari and B. Raahemi, "A framework for SIP intrusion detection and response systems," in International Symposium on Computer Networks and Distributed Systems (CNDS), 100-105, 2011.

[13] W. YS, S. Bagchi, S. Garg, N. Singh and T. Tsai, "SCIDIVE: a stateful andcross protocol intrusion detection architecture for Voice-over-IP environments," in International conference on dependable systems and networks, 2004.

[14] J. Fiedler, T. Kupka, S. Ehlert, T. Magedanz and D. Sisalem, "VoIP defender: highly scalable SIP-based security architecture," in Principles, Systems and Applications of IP Telecommunications (IPTComm), 2007.

[15] H. Sengar, D. Wijesekera, H. Wang and S. Jajodia, "VoIP intrusion detection through interacting protocol state machines," in International Conference on Dependable Systems and Networks, 2006.

[16] H. Sengar, H. Wang, D. Wijesekera and S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 19, no. 6, pp. 794-805, 2008.

[17] M. Nassar, R. State and F. Olivier, "Monitoring SIP Traffic Using Support Vector Machines," in 11th international symposium on Recent Advances in Intrusion Detection, 2008.

[18] M. Nassar, R. State and O. Festor, "Labeled VoIP Data-Set for Intrusion Detection Evaluation," Lecture Notes in Computer Science Networked Services and Applications - Engineering, Control and Management , vol. 6164, pp. 97-106, 2010.

[19] M. Y. Arafat, M. M. Alam and F. Ahmed, "Study on Security Issue in Open Source SIP Server," Modern Applied Science, vol. 8, no. 2, pp. 124-141, 2014.

[20] A. D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," IEEE Communications Surveys and Tutorials , vol. 14, no. 2, pp. 514-537, 2012.

[21] R. Sadiwala and M. Sharma, "SECURITY THREATS OF VOIP," Journal of Innovative trends in Science, Pharmacy & Technology , vol. 1, no. 1, pp. 7-18, 2014.

[22] A. D. Keromytis, Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research, Springer, 2011.

[23] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend and H. Schulzrinne, SIP Security, Wiley, 2009.

[24] "The New Breed of Communication Engine," OPENSIPS, [Online]. Available: http://www.opensips.org/. [Accessed 4 10 2014].

[25] HP, "SIPp," HP, [Online]. Available: http://sipp.sourceforge.net/. [Accessed 20 01 2014].

[26] M. Alidoosti, H. Asgharian and A. Akbari, "Security framework for designing SIP scanner," in 21st Iranian Conference on Electrical Engineering (ICEE), 2013.

[27] M. Patel, "Analysis of Security Threats in Voice Over Internet Protocol," International Journal of Control Theory and Informatics, vol. 3, no. 5, pp. 30-37, 2013.

[28] E. Y. Chen, "Detecting DoS attacks on SIP systems," in 1st IEEE Workshop on VoIP Management and Security, 2006.

[29] D. Carney, "Evaluation Of Methods For Improving Network Security Against SIP Based DoS Attacks On VoIP Network Infrastructures," in Selected Computing Research Papers, University of Sunderland, 2013, pp. 21-27.

Hassan Asgharian received his Ph.D. in Computer Engineering from Iran University of Science and Technology (IUST) in 2016. He also received his M.Sc. in Computer Engineering from Amirkabir University of Technology (AUT) in 2009 and He also has got his B.Sc. from Computer Engineering Department of Iran University of Science and Technology (IUST) in 2006. Currently he works as a research assistant in the Network Research Group (NRG) of the Research Center of Information Technology (RCIT) of Computer Engineering Department in Iran University of Science and Technology. He works on next generation networks focusing on its security aspects.

Ahmad Akbari received his Ph.D. in Electrical Engineering from the University of Rennes 1, Rennes, France, in 1995. Dr. Akbari is currently an associate professor at Iran University of Science and Technology, Iran. Dr. Akbari works on Speech Processing related research topics (especially speech enhancement) for more than 20 years. His current research interests include Intrusion Detection and Response Systems, VoIP Communications, Next Generation Networks, VoIP and SIP Security and also Data Communications Networks. Dr. Akbari's work has appeared in several peer-reviewed journals and conference proceedings.

Bijan Raahemi received his Ph.D. in Electrical and Computer Engineering from the University of Waterloo, Canada, in 1997. He then held several research positions in telecommunications industry, including Nortel Networks and Alcatel-Lucent, focusing on Computer Networks Architectures and Services, Dynamics of Internet Traffic, and Performance Analysis of Data Networks. Dr. Raahemi is currently an associate professor at University of Ottawa, Canada. His current research interests include Data Mining, Information Systems, and Data Communications Networks. Dr. Raahemi's work has appeared in several peer-reviewed journals and conference proceedings. He is a senior Member of IEEE, and a member of ACM.