A Cost-Sensitive Automated Response System for SIP-based Applications

Mansoureh Ghasemi, Hassan Asgharian, Ahmad Akbari
Department of Computer Engineering
Iran University of Science and Technology
Tehran, Iran
ghasemi_m@cmps2.iust.ac.ir, asgharian@iust.ac.ir, akbari@iust.ac.ir

Abstract—**Network security technologies have different issues that is important in next generation networks because of the real-time nature of its applications (e.g. VoIP and IPTV). The main requirements of these types of applications is to handle the attack situations without quality degradation. There are many references for implementation of intrusion detection systems in VoIP infrastructures but there is little effort on intrusion response systems. We concentrate on response systems for SIP-based entities and present a cost sensitive response system which considers environmental dynamic conditions. We categorize the deployable responses into different groups based on their severity level by considering their side effects. We also propose a new quantitative metric for damage cost to compare it with response cost. Our proposed decision making process is done based on the comparison of these costs (response and damage costs), the environmental conditions (CPU, network and memory usages) and also the time of the detected attack. We verify our proposed framework by a real test-bed which is implemented by open-source tools such as OPENSIPS and SIPp. The implementation results show the effectiveness of our proposed SIP intrusion response system.**

Keywords-Intrusion Response System; Cost-Sensitive Response; VOIP; SIP Security.

I. INTRODUCTION

The Session Initiation Protocol (SIP) is an application-layer protocol standardized by the Internet Engineering Task Force (IETF), and is used for creating, modifying, and terminating sessions[1][2]. SIP is establishing itself as the de-facto standard for VoIP services in the Internet and next generation networks[3]. Unfortunately, SIP-based application services can suffer from various security threats such as denial of service (DoS) attacks[4]. The majority of DoS attacks are based on exhausting some of the server's resources and causing the server to operate improperly due to lack of resources. These attacks may target a VoIP entity, such as a SIP proxy, or supporting servers, such as a DNS, or DHCP server[5]. The basis for protecting a system against denial of service attacks is to understand these attacks and have the ability to identify and detect them. A prerequisite for Intrusion Detection Systems (IDS) is the ability to collect and analyze network traffic and classify it into normal and abnormal traffic behavior[6]. When an intrusive is detected, it is desirable to take actions to thwart attacks and ensure safety of the computing environment. Such countermeasures are referred to as *intrusion response*. Although intrusion response component is often integrated with the IDS, it receives considerably less attention than IDS[7].

In the given classification in[7] intrusion response systems can be classified according to the following characteristics:

- *Activity of triggered response (**Passive and Active**)*
- *Level of automation (**Notification systems, Manual response systems and Automatic response systems**)*

Also, because of the importance of automatic response systems, these systems are classified by characteristics as below:

- *Ability to adjust (**Static and Adaptive**)*
- *Time instance of the response (**Proactive /preemptive and Delayed**)*
- *Cooperation capabilities (**Autonomous and Cooperative**)*
- *Response selection mechanism (**Static mapping, Dynamic mapping and Cost-sensitive**)*

In this paper, we present an automated cost sensitive response system for SIP-based entities. Our aim in the paper is to classify applicable responses in SIP based systems, make the best decision to select them and then deploy appropriate responses based on our cost model.

The reminder of the paper is organized as follows. A brief overview of related work is given in Section II. Section III presents the details of the response system components. Experimental setup and analysis are given in Section IV. Section V concludes the paper with our future work.

II. RELATED WORKS

Most of previous works on SIP intrusion detection is summarized in[8]. Since our main contribution is on response systems, we only review the previous works with some idea on intrusion response. Authors in[9] introduced a new approach to detect CPU based DOS attacks that misuse the weaknesses of SIP authentication mechanism. This system is located in the entrance point of SIP network and automatically collects user profiles and acts as an independent anomaly

detection unit. An acceptance risk level is assigned to all users computed based on their recent history of activities. Then, if this risk level is greater than a pre-specified threshold, system generates appropriate response by raising corresponding alerts.

Authors in[10] implemented a SIP intrusion detection and response framework for classifying the incoming SIP traffic and limiting the access of the detected intruders to the SIP server. This framework has detection and reaction modules. The proposed reaction module writes notification alarms into a file, and also, blocks the suspicious access to the system.

In[11] the authors proposed a specification-based intrusion detection framework based on the SIP finite-state machine to distinguish deviation from its normal or expected behavior. Through communication with a firewall component, this scheme allows to block offending traffic and thus keep the service alive even under attack conditions.

These approaches have some pros and cons: some of them have just detection mechanisms without paying attention to response. Some of them trigger responses by using firewalls but none of them notice to calculate the damage and response cost and not to consider response side effects.

In Table I, we discuss recent SIP-based IDS or IRS and provide summery of their detailed characteristics.

TABLE I. COMPARISION OF SIP SECURITY SYSTEMS

System Name	System Type	Ability to adjust	Time of Response	Cooperation ability	Response selection method
Ref.[9]	Detection	static	delayed	autonomous	Dynamic
Ref.[10]	Detection and Response	static	proactive	autonomous	Dynamic
Ref.[11]	Detection and Prevention	static	proactive	autonomous	Dynamic
Proposed system	Response	adaptive	Delayed	autonomous	Cost-sensitive

III. PROPOSED SYSTEM

To generate an automatic cost sensitive response, it is necessary to determine the location of the proposed response system. After determining the appropriate placement of the response system, dynamic environmental conditions, response time and user's attack history should be considered to decide about the status of the detected attack. In addition to consider the state of detected intrusions, the corresponding costs of damage and response should be considered. In the following sections, our proposed solution is presented.

A. Placement of SIP Response System

A block diagram of the proposed system is shown in Figure 1. As is shown, the location of the intrusion detection system (IDS) is before the response system. In other words, the output of IDS is considered as an input to intrusion response system. Alerts generated by the IDS/IDSs besides network traffic are arrival traffic of response system. This system is placed before SIP proxy server to monitor the incoming traffic. Given that access to the VoIP network provided through a proxy server, the SIP-based systems all have at least one proxy server. The response system aims to provide both security and no changes to existing network architecture based on SIP, hence, it is proposed to locate this system before the main proxy of the system.

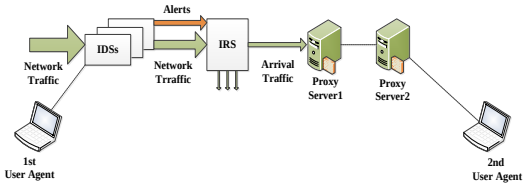

Figure 1. IRS Placement

B. Response System Components

Figure 2 shows the components of our proposed response system. Each of these components will be discussed in the following sections.

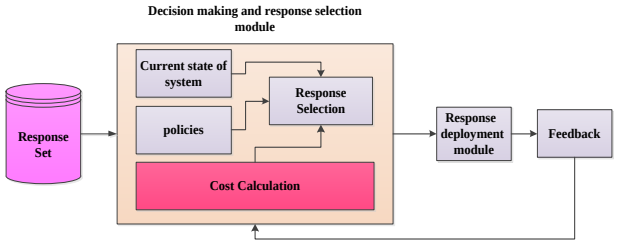

Figure 2. Proposed Response System Architecture

1) *Response Set:*

This set consists of a database which contains all possible responses in SIP-based systems. For each of the responses, number, type, priority and severity of response are stored. Response severity is defined based on system policies. It has divided into simple, conservative and strict. Response type has three categories include concurrent, delayed and intelligent responses. Response priority varies in range of 1 to 4 based on response intensity. Priority 1 is the highest and priority 4 is the lowest. We categorize and propose the SIP responses in Table II. It summarizes the responses which are applicable in SIP-based systems.

TABLE II. RESPONSE SET

Response Number	Response Intensity	Response Priority	Response Type	Responses
R1	Simple	2	Concurrent with detection	Terminate open and expired time transactions
R2	Strict	3		Terminate all of open transactions
R3	Strict	4		Terminate service
R4	Simple	1		No response
R5	Conservative	1		Prioritizing familiar calls
R6	Simple	3		Terminating transactions randomly
R7	Conservative	2	Delayed	Restrict user access By black and white lists

Response Number	Response Intensity	Response Priority	Response Type	Responses
R8	Strict	2		Disable user account
R9	Strict	1		Prevent user access
R10	Simple	4	Intelligent	Close calls intelligently by using Bye / Cancel messages

2) ***Decision Making and Response Selection Module****:*

This module consists of the following components:

a) Current State and working condition of the system:

The current state of the system is one of the inputs of response selection component. The current state of the system means the current dynamic condition of SIP- based system that is divided into three categories: environmental conditions, usage time and previous behavior of users. To select the appropriate response for SIP-based systems and provide an automated response system, environmental conditions (including the amount of system resources consumed), time (including time of response) and the users (for example, attackers or non-attackers) is required to be considered simultaneously.

b) Policies:

Policies considered in this section to determine the severity of the selected response in three levels: simple, conservative and strict. Simple responses have the lowest level of severity because they has no negative side effects. Conservative decisions taken in the circumstances where attacks does not have high usage of SIP-based systems resources but they may have potential to increase damage cost. In strict decisions we not only have high resource consumption but also serious damage costs. These decisions have both positive and negative impacts on the system. Table III shows a summary of these policies and their effects.

TABLE III. PLOLICIES IN PROPOSED RESPONSE SYSTEM

Decision Type	Positive Effect	Negative Effect
Strict	yes	yes
Conservative	yes	maybe
Simple	maybe	no

c) Cost Calculation:

In [12], Lee et al. propose cost sensitive model based on three factors: 1) operational cost, which refers to the cost of processing the events of IDS; 2) damage cost (D_{cost}), which refers to the amount of damage to a resource caused by an attacker when the IDS is ineffective; and 3) response cost (R_{cost}), which is the cost of applying a response when an attack detected. These factors present the foundation of intrusion cost model, i.e. total expected cost of intrusion detection, and consequently provides a basis for a selection of an appropriate response.

In a cost sensitive IRS, to determine whether response will be taken, D_{cost} and R_{cost} must be considered. If the damage done by the attack to resource r is less than R_{cost}, then ignoring the attack actually reduces the overall cost[13].

From SIP-based systems' point of view, we have three factors influenced by attacks: quality of service, resources and call setup time. Based on these three factors, we propose a three dimensional damage cost. IF we use Dcost1, Dcost2 and Dcost3 to symbolize them, total damage cost can be formulated as follow.

$$Dcost_{Total} = Dcost_1 + Dcost_2 + Dcost_3 \quad (1)$$

1. The quality of service dimension ($DCost_1$)

The quality of service in VOIP systems considered by the number of completed calls, rejected calls, or open calls. Thus, the ratio of these calls to total calls can be calculated as damage cost. In Equation (2), DCost1 is shown.

$$DCost_1 = A \times \frac{RC}{TC} + B \times \frac{OC}{TC} \quad (2)$$

In this formula, (RC / TC) shows the number of rejected calls regarding to the total calls at a specified time period, the proportion of (OC / TC) shows the number of open calls to the total calls during the specified time interval, and the coefficients A and B are determined based on SIP-based system policy, here are equally considered. The total cost of these products shows this damage cost.

2. The resource dimension ($Dcost_2$)

Since the vulnerable resources of VoIP systems are CPU, memory and bandwidth, in this dimension we considered these resource overheads. Therefore, we can compute $Dcost_2$ as follows:

$$Dcost_2 = CO + MO + BO \quad (3)$$

In this formula, CO, MO, BO represents CPU overload, memory overhead and bandwidth overhead respectively. These overheads calculate the difference between resource consumption in normal and attack state. The total cost of this damage by using these values is determined.

3. The call setup time dimension ($Dcost_3$)

In this dimension we considered the difference between call setup time in normal and attack state. The formula of Dcost3 is:

$$Dcost_3 = \frac{\Delta CST}{CST_{Attack}} = \frac{CST_{Attack} - CST_{Normal}}{CST_{Attack}} \quad (4)$$

In this formula we computed call setup time difference and then divided by attack call setup time to normalize this damage cost.

After calculating damage cost, we should determine response cost. In[14] response cost is performed in three

dimensions: **the operational cost (OC)** of a response in a given environment, **the response goodness (RG)** with respect to detected intrusion(s) and **the response impact on the system (RSI).**

The operational cost of a response measures various aspects of the response associated with its daily maintenance. The response goodness provides a measure of the ability of the corresponding response to mitigate damage caused by the intrusion to the system resources. Finally, the impact of a response on the system quantifies the negative effect of the response on the system resources and is estimated independently from the response success or failure in countering the intrusion(s). The combination of the **OC** and the **RSI** constitutes the penalty associated with the response, while the **RG** is the benefit of this response measure. One simple cost model describing the overall measure of response cost **RC** is:

$$RC = \frac{\text{OC+RSI}}{2} - RG \qquad (3)$$

Nevertheless, in VoIP systems, response cost is a function of the quality parameters. Therefore, these values cannot be calculated quantitatively. Hence, measuring the response with respect to the damage cost will replace with response conditions.

In our proposed approach total damage cost varies in a predefined window. We divide this window based on the policies into three different groups: acceptable, tolerable and critical (Figure 3).

Figure 3. Response Condition Intervals

d) Response Selection:

This component is one of the most important aspects of decision making that all important factors such as the current state of the system, policies and costs, are the entries of this module. The output of the decision making module is determined by this component. The desired conditions are as follows:

- Condition I: checking environmental conditions (whether the parameters α, β and λ is larger than the threshold or not)
- Condition II: checking time conditions (whether attack occurs in peak time or not)
- Condition III: checking user conditions (whether users have attack's history or not)

In addition to these conditions, we need to consider costs. So, we add checking total damage cost in respect to response condition to our flowchart. Response selection flow chart is shown in Figure 4.

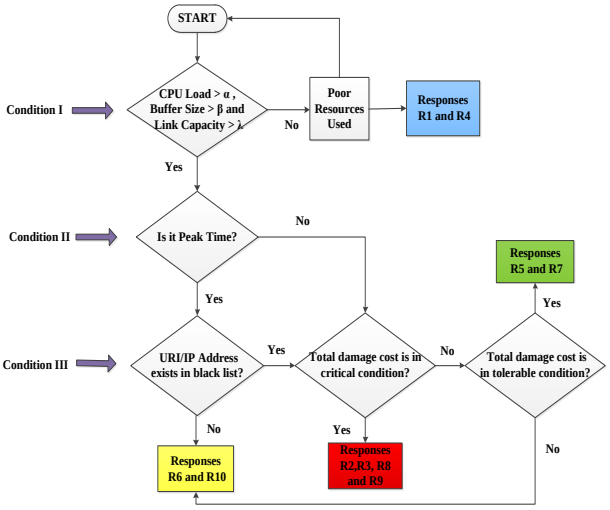

Figure 4. Response Selection Flowchart

After that we have six cases to select appropriate responses:

- **Case1)** this occurs when all of the above conditions are satisfied. In this case, the response system generate responses with more intensity. Also, total damage cost should be in critical condition. These responses can be R2, R3, R8 and R9 and the response type is strict.
- **Case 2)** this occurs when just condition I is satisfied but total damage cost is in critical condition. In this situation strict responses select again.
- **Case 3**) in this case, IRS chooses conservative responses because total damage cost is in tolerable condition whereas one or two of the conditions may not be satisfied.
- **Case 4, 5**) in these cases, condition I and II are satisfied. If condition III is satisfied and total damage cost states in acceptable condition, the IRS select simple responses such as R6 and R10. Otherwise, if condition III is not satisfied, IRS choose these responses again because the user have not any attack history.
- **Case 6)** this is the time that any of the above conditions are satisfied. Thus the system select simple responses such as R1 and R4.

Table IV summarizes these cases.

TABLE IV. RESPONSE SELECTION

Selection condition	Response type	Response intensity
Case 1,2	R2,R3,R8,R9	Strict
Case 3	R5,R7	Conservative
Case 4,5	R6, R10	Simple
Case 6	R1, R4	Simple

*3) **Response Deployment**:*

After finalizing the process of deciding about the response, calculating cost and selecting the desired response,

response should be applied on the SIP-based system. The answer can be applied in three ways:

- *Notification method:* Only an alert is generated.
- *Manual:* Responses can be applied manually to the system.
- *Automatic:* The answer is quite intelligently and automatically applied to the system. An example of this response can be terminating the session by sending BYE or CANCEL messages.

To do so, deployment conditions are as follows:

1. *If damage cost in terms of response condition states in acceptable interval, the system responds by notifying admin and only a warning generated.*
2. *If damage cost in terms of response condition states in tolerable interval, the system responds manually and appropriate responses apply by system administrator.*
3. *If damage cost in terms of response condition states in critical interval, the response system automatically generates a response.*

4) ***Feedback****:*

After deciding, selecting and applying a response, effectiveness of the applied response would be considered on SIP-based systems. For this purpose, the feedback has been used as a unit of IRS. The unit will maintain a history of previous responses. The lack of success of the previous response, the system responded (applied next response) more vigorously.

In the following section, our experiment setup environment of SIP based system is presented.

IV. Experiment Setup and Analysis

For evaluating the proposed system, architecture and details of the test bed configuration shown in Figure 5. In this architecture, we use an open source tools such as OPENSIPS proxy server next to SIPp for generating normal and attack traffics.

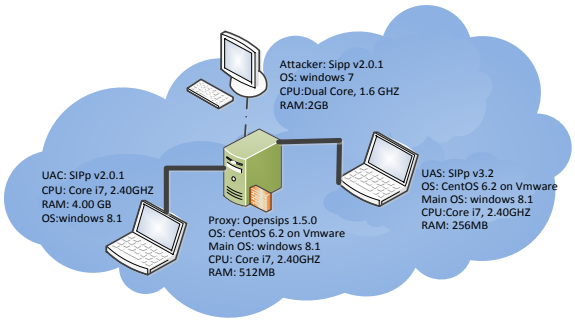

Figure 5. Our SIP test-bed

A. Normal Traffic

Since the capacity of the considered SIP proxy server is about 130 calls per second, we arrange the experiments based on this rate. For normal traffic we considered three different periods. In the first period, we generate the traffic with increasing rate up to its capacity to show the full load traffic. Then in the second period, we generate the traffic with constant rate which represents the steady state of system. Finally we generate the traffic with decreasing rate which exemplifies the offload periods of normal traffic. Total time slot of the experiments is about 6 minutes.

B. Attack Traffic

After 10 seconds, attack traffic generates and the increased rate of attack is carried to the proxy server. Attack rate starts from 10 calls per second, and this trend continued until the rate of 1000 calls per second. Every five seconds, the rate is increased by 20 calls per second.

C. Evaluation metrics

To evaluate the behavior of SIP proxy server in normal and abnormal traffic, we define the following metrics based on the normal behavior of SIP proxy server:

1. CPU consumption (CC)
2. Call setup time (CST)
3. Call completion rate (CCR)
4. Call rejection rate (CRR)

Open calls rate (OCR)

The value of these metrics has a significant difference in normal circumstances and attack periods. Shown Table V, the value of CC, CST, CRR and OCR in attack periods are increased but CCR is decreased. It means that our SIP server has limited processing capacity and reaching to its critical breaking point. For instance, in normal situations the value of CST varies from 1 to 3 milliseconds but in attack periods, CST even reaches to 6 seconds (e.g. in 355 to 375 interval). In higher rates, more calls are from attackers. Faced with this condition, calls of authorized users delayed and thus average CST has increased as expected. Also the significant drop in value of CCR's average from 99 percent to 37 percent in attack periods shows the effectiveness of this metric in highlighting the status of proxy server. Since all SIP entities are supposed to answer to the incoming INVITE messages, initial processing of incoming INVITE messages is mandatory and may effect on the normal behavior of system by increasing the open call rate and call rejection rate. The value of these metrics are summarized in the Table V.

D. Cost analysis

The evaluation metrics are parameters that used to calculate damage cost. Both damage cost and response condition need to be considered in this stage

TABLE V. METRICS COMPARISION BETWEEN NORMAL AND ATTACK STATE

	Normal					Invite Flooding Attack				
Time Interval	**Avg. CC (%)**	**Avg. CST(ms)**	**CCR**	**CRR**	**OCR**	**Avg. CC (%)**	**Avg. CST(ms)**	**CCR**	**CRR**	**OCR**
[15-35]	1.8	2.17	0.99417	0	0.00583	13.75	5.31	0.3752	0.0686	0.5562
[45-65]	4.5	3.4	0.99294	0	0.00706	14.2	17.93	0.34351	0.092	0.56449
[75-95]	6.1	2.71	0.98502	0	0.01499	9.15	110.88	0.30604	0.12357	0.57038
[105-135]	6.8	1.86	0.97622	0	0.0237	8.65	741.66	0.27944	0.17824	0.54233
[145-165]	8.3	1.82	0.98106	0	0.0189	7.6	163.34	0.27243	0.17824	0.54933
[175-195]	8.6	2.19	0.98364	0	0.0163	7.65	145.21	0.26013	0.18348	0.55639
[205-225]	8.15	2.01	0.98468	0	0.0153	7.1	165.74	0.24765	0.19381	0.55853
[235-315]	7.1	2.02	0.98569	0	0.0143	6.25	3029.48	0.25	0.19432	0.55567
[325-345]	6.95	2.06	0.98642	0	0.0135	8.8	4563.53	0.27991	0.1765	0.54359
[355-375]	6.7	2.12	0.98525	0	0.0147	8.3	6425.35	0.28941	0.17365	0.53694
[385-405]	4.1	1.94	0.98211	0	0.0178	8.6	1542.76	0.29297	0.17501	0.53202
[415-435]	2	2.31	0.98017	0	0.0198	6.45	1450.07	0.29448	0.17517	0.53036

E. Analysis the results

In Figure 7, the results of cost comparison between normal and the INVITE flooding attack state has been specified.

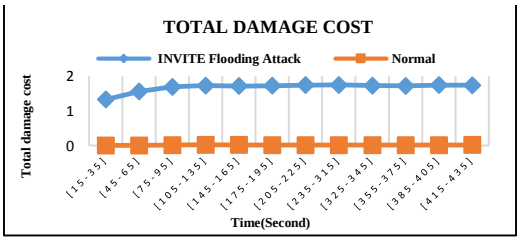

Figure 6. Cost comparision between normal and attack state

First, we specified the response condition intervals based on total damage cost measurement as shown in Figure 7:

Figure 7. Response condition intervals specification

In our proposed IRS, system administrator choose 0 to 1.4, 1.4 to 1.6 and 1.6 to 2 intervals for acceptable, tolerable and critical conditions respectively. Then, according to Figure 6, at 15 to 35 seconds our proposed IRS selects simple responses. At 45 to 75 seconds selects conservative responses and at 75 to 435 (i.e. 360 seconds) selects strict responses. Also, response deployment can be based on admin's point of view to apply notification, manual or automatic responses. As a result our proposed IRS prefer to select either simple or conservative responses unless our SIP based system's damages states in critical conditions and our IRS force to use strict responses.

V. CONCLUSION

In this paper we present an automated cost sensitive response system for SIP-based entities. We classify applicable responses in SIP based systems and introduce a new approach to calculate costs. This method can help to make right decision in respect to response severity and increase system availability. To evaluate the proposed response system, a SIP-based test bed was implemented. We intend to explore response cost parameters in SIP-based systems and investigate the effectiveness of our IRS responses by adding feedback to the response system.

REFERENCES

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

[2] H. Asgharian, A. Akbari, and B. Raahemi, "Feature engineering for detection of Denial of Service attacks in session initiation protocol, " Security and Communication Networks, 2014.

[3] D. Sisalem, J. Kuthan, and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," Network, IEEE, vol. 20, no. 5, pp. 26-31, 2006.

[4] D. Allawi, A.A, Rohiem, A. El-moghazy, and A.Z. Ghalwash, "New misuse detection algorithm for SIP faked response attacks," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol.2, NO.2, pp. 201-209, 2013.

[5] G. Ormazabal, S. Nagpal, E. Yardeni, and H. Schulzrinne, "Secure sip: A scalable prevention mechanism for DoS attacks on SIP based voip systems," Principles, systems and applications of IP telecommunications. Services and security for next generation networks, Springer, pp. 107-132, 2008.

[6] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, H. Schulzrinne, "SIP Security", John Wiley and Sons, 2009.

[7] N. Stakhanova, S. Basu, and J. Wong, "A taxonomy of intrusion response systems," International Journal of Information and Computer Security, vol.1, no.1, pp. 169-184, 2007.

[8] 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.

[9] S. Pourmohseni, H. Asgharian, and A. Akbari, "Detecting authentication misuse attacks against SIP entities," 10th International ISC Conference on Information Security and Cryptology (ISCISC), pp. 1-5, IEEE, 2013.

[10] 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.

[11] S. Ehlert, C. Wang, T. Magedanz, D. Sisalem, "Specification-based denial-of-service detection for SIP Voice-over-IP networks," Third international conference on internet monitoring and protection, 2008.

[12] W. Lee, W. Fan, M. Miller, S.J. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," Journal of Computer Security, vol.10, no.1, pp. 5-22, 2002.

[13] Y. Sun and R. Zhang, "Automatic Intrusion Response System Based on Aggregation and Cost," International Conference on Information and Automation, pp. 1783 – 1786, 2008.

[14] C.R. Strasburg, N. Stakhanova, S. Basu, and J.S. Wong, "The methodology for evaluating response cost for intrusion response systems, " Computer Science Technical Reports, 2008.