International Journal of Research in Advent Technology, Vol.7, No.6S, June 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Survey on Detection Techniques for Denial-of-Service Attacks in SIP-based Voice over IP networks

Namratha N, Dr R Ashok Kumar

Abstract—VoIP provides real-time voice communications over packet-switched networks. VoIP is widely used as it offers more flexibility when compared to the traditional Public Switched Telephone Network (PSTN). Session Initiation Protocol (SIP) is a protocol used for initiating a session between the caller and the callee in the VoIP system. SIP is a text-oriented protocol and is implemented in a susceptible environment. These features make SIP protocol vulnerable to various security risks such as Denial of Service, Registration hijacking and Eavesdropping. Detection of these attacks plays a vital role. The Survey focuses on different techniques used for detection of DoS attacks and differentiating between the proposed mechanisms for identifying abnormalities and then notifying the end-users about the possible intrusions.

IndexTerms— Attacks, Denial of Service, SIP, Reliability, VoIP.

I. INTRODUCTION

Voice over IP (VoIP) is a technology which provides higher flexibility and portability when compared to the circuit-switched network. VoIP has a complex infrastructure as it connects the conventional telephone network with Voice over IP endpoints [1]. VoIP network comprises of various components namely, gateway, server and end-user equipment. Gateway is used for voice compression or decompression, packetization and routing calls. The server is used for performing network management functions. The end-user equipment acts as a terminal for providing connection to a network. VoIP uses two main protocols namely, signaling protocol and media protocol. The Signaling protocols are used to monitor call setup and teardown. Examples of signaling protocols include SIP and H.323. The Media protocols are used to monitor the communication between different voice over IP networks. It can be used for Real-time Transport Protocols (RTP).

VoIP has several disadvantages such as power outages, issues in interoperability, complexity of service architecture and security issues. The serious security problem faced by VoIP networks is DoS attacks, which disrupts the availability of service to the customers. The call quality can be degraded when VoIP services are made inaccessible or unusable [2]. SIP is a protocol used for initiating a session between the caller and the callee in the VoIP network. It follows the request/response model for call setup and call management. SIP provides request and response messages which are used to perform ordinary SIP operations. The SIP messages illustrate the identity of the participants in a call and how the participants communicate over an IP network..

Manuscript revised May 13, 2019 and published on June 5, 2019
***Namratha N**, MTech CNE, Dept. of ISE, BMS College of Engineering, Bangalore, India*
***Dr R Ashok Kumar**, Associate Professor, Dept. of ISE, BMS College of Engineering, Bangalore, India*

II. LITERATURE REVIEW

Many kinds of research were made to deal with the attacks against SIP-based Voice over IP networks. The techniques were considered based on the nature of attack namely DoS and VoIP flooding, which mainly targeted the vulnerable communications. Senger et al. [3] used an online statistical detection technique to deal with DoS attacks known as VoIP Flooding Detection System(vFDS). vFDS is a framework which employs Hellinger's distance technique to estimate the abnormal variations in collections of packet streams as probability distributions. The scheme identifies the DoS attacks quickly and precisely, but it is inefficacious against low-level attacks as they exhibit the same probability distributions as the regular traffic.

Ehlert et al. [4] proposed a double-layered architecture to preclude and reduce Denial of Service attacks in SIP-based Voice over IP networks. This technique uses a bastion host along with traffic scanning module. The proposed technique is effective when a minimal amount of processing overhead is introduced. It becomes inefficient when flooded packets use IP addresses which are spoofed randomly.

Huici et al. [5] used a SIP Defender, a distributed filtering mechanism, which uses the existing mechanisms repeatedly. This mechanism has a complex architecture, which can lead to difficult deployment issues. It can handle large amounts of traffic when compared to other techniques.

Bansal and A R Pais [6] proposed a mitigation mechanism to secure a Voice over IP server from a Denial of Service attack. This technique includes an algorithm to analyze SIP messages and calls and a teardown tool to separate all SIP messages which are being occupied before repelling the attack.

Zargar and Moghaddam. [7] proposed an entropy mechanism to identify and avoid DoS attacks on SIP-based Voice over IP networks. This system is used for examining the VoIP network traffic behavior. It can be controlled by increasing the size and the computation time. The system can detect thechanges which occur in attacks by compressing the datapresent in the SIP packet on a table.

doi: 10.32622/ijrat.76S201919

Akbar and Farooq. [8] proposed a Packet-based SIP IntrusionProtector (pbSIP) technique to detect Denial of Service attackon SIP-based Voice over IP systems. pbSIP is a techniqueused to identify malicious messages by analyzing theincoming packets. This technique fails to detect attacks in theevent of a malformed packet and good tracking of the INVITEpackets in which entropy is not disturbed.

Cadet and Fokum. [9] proposed a mechanism to detect andobstruct DoS attacks on a SIP server. This system employsSnort, which is an Intrusion Prevention system used to managenetwork traffic in real-time. Snort uses Rules to protect theSIP server from the furtive activities.

III. SIP-BASED VOICE OVER IP NETWORKS OVERVIEW

Voice over IP protocol is used for transmission of voicecommunication over the Internet. VoIP can be implementedusing different transport and signaling protocols such as SIPand H.323. Signaling protocols are employed to allow callmanagement and to create connections between endpoints.Session Initiation Protocol is a text-based protocol which isused for Signaling, Call Setup and Call Management. SIPresponse is generated for each request message sent to specifythe status of the request [10]. The SIP specificationrecommends the reusability of security techniques such asHTTP digest, SIPS, Transport Layer Security (TLS), as theprotocol is hard to secure.

The SIP protocol is susceptible to Denial-of-Service attacksand Distributed Denial-of-Service attacks, in which theattacker can overload a SIP server with many malformedmessages. These vulnerabilities are due to the inadequacy ofaccess to control policies.The SIP protocol consists of four main entities:

• **User-Agent**: It includes IP, mobile phones andcomputers that run on SIP-based software to initiateand terminate a SIP request.

• **Registrar Server**: Database which maintainsinformation about locations and user preferences asspecified by user agents.

• **Proxy Server**: It is responsible for forwarding therequests received by the caller to the callee.

• **Redirect Server**: It is a User Agent Server (UAS)which allows the client to directly contact the server.

Request messages include INVITE, ACK, CANCEL, BYE,REGISTER and OPTIONS. Fig 1 represents a SIP call setupestablished between the caller and the callee. An INVITErequest will be sent by the caller to the callee, which containsinformation about the session he wants to begin. 100 Trying issent from the User Agent Server indicating that the request hasbeen received by the UAS and is in progress. Ringing statuscan be indicated using 180 Ringing response messages. TheCaller receives 200 OK response messages if the call isaccepted by the Callee. A call can be terminated by Caller orCallee using the BYE message. This process constitutes a 3-way handshake between Caller and Callee [1].

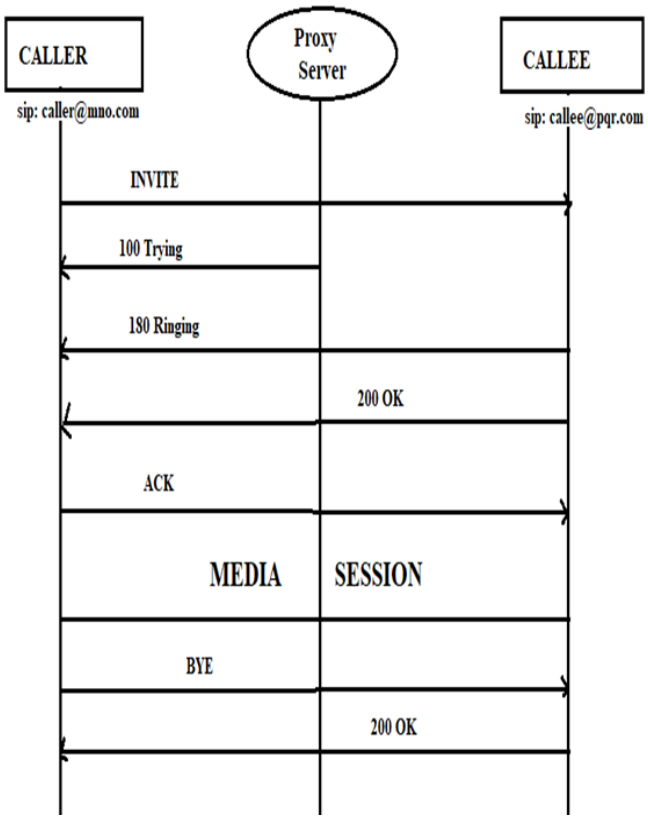

Figure 1 SIP Call Setup

Attacks encountered in SIP-based Voice over IP Networks

VoIP networks are exposed to security threats, as they use the public network as a way of communication [11]. The attacks encountered in SIP-based Voice over IP networks include [1]:

- **Registration Hijacking**: The attacker may spoof an Authentic User Agent to a registration server and register it using a fake IP address. It contains several steps such as traffic snipping, removing the message and forwarding the manipulated message to the server. Due to these steps of Registration Hijacking, the attacker can reroute, answer or terminate the call. Private information and calls can be lost when the attacker uses Registration Hijacking.
- **Denial of Service attack:** DoS attack is a type of cyber-attack where the attackers tries to intercept legitimate users from accessing the service. The attacker sends an enormous number of INVITE messages to worsen the SIP entities. The Flooding attack mainly targets the proxy server, registrar server and end users. It can be created by single or multiple sources.
- **Spam over IP Telephony**: SPIT produces a large number of unwanted calls and messages using the IP network to target a group of individuals and users. It employs Zombies and Bots to attack a specific user.
- **Eavesdropping:** It is an illegal interception of personal communication between the Caller and the

doi: 10.32622/ijrat.76S201919

Callee. The network packets can be analyzed by the attacker using Wireshark and Nmap

IV. COMPARISON OF DETECTIVE TECHNIQUES

Abhishek Bansal, Alwyn R. Pais [6] proposed a Mitigation scheme based on SIP messages and call analysis. A Legitimate user must send one or more INVITE messages to establish a call. It is impossible for the user to make another call without disconnecting the previous call. Attacker forwards multiple INVITE messages without sending a BYE message. An Attacker can be identified by counting the number of INVITE and BYE messages received. Every SIP message consists of "From" and "To" fields, which holds details about the source and destination extensions, port number and IP address. It is possible for the attacker to manipulate the IP address of the phone. The mitigation scheme consists of various analysis tools to detect the DoS attacks.

- **Asterisk:** The Asterisk tool is used as a SIP server to combine any number of telephony hardware and software with any telephonic application.
- **SIPp tool:** This tool is used to impersonate concurrent calls. It is mainly used to forward multiple SIP messages to the Asterisk Server.
- **EKIGA Soft-phone**: This tool is employed to test whether a call can be made during a Denial-of-Service attack. It is used as a video conferencing application.

The Proposed Mitigation system fails to encode the SIP messages. It is vulnerable to Phishing attack as it allows the attackers to capture data from SIP messages.

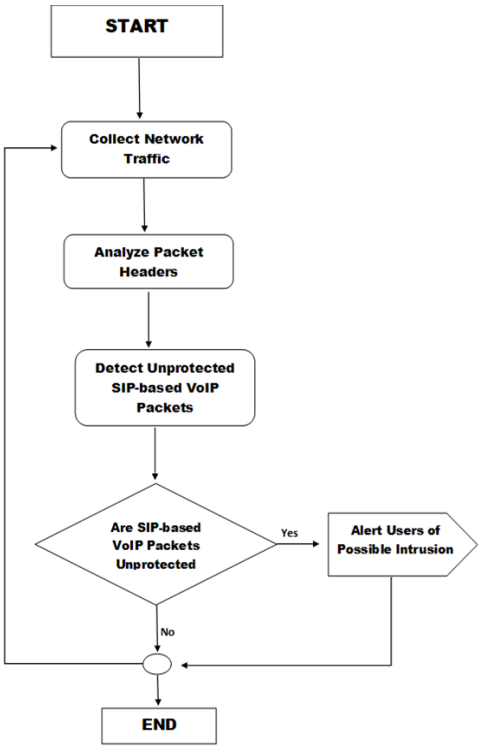

Figure 2 System Flowchart

Carvajal et al. [12] proposed a system to identify unprotected SIP-oriented Voice over IP traffic to warn the end-users about the viable intrusions. The method consists of three main processes namely, a collection of network traffic, evaluating the packet headers and detecting whether the SIP-oriented VoIP packets are protected or unprotected. The Collection phase is used for encapsulating the traffic in the network. The process used a Sniffer tool for capturing all the traffic present in the network. The Analysis process is responsible for examining the headers of the IP packet. It checks the Protocol field of the IP header. If it contains the value 17, the User Datagram Protocol will be deployed to transmit messages. The SIP-based VoIP packets will be dealt within the UDP packets. The UDP packet consists of data-payload, which represents the actual data that must be transmitted.The Detection process is responsible for analyzing the payload of the UDP packets which holds the port number 5060 to initiate a call. An alert will be sent to the users if the conditions outlined in the detection process are found. Fig 2 depicts the working of the program. This technique is less effective as it considers only the 5061 port for detection.

Golait and Hubbali [13] proposed an anomaly detection system known as Voice over IP Flooding Detection (VoIPFD). It consists of two states of operations namely, the training state and the testing state. The Training state is responsible for collecting and building normal behavior profile of the VoIP SIP messages. Poisson distribution is used for creating a profile of normal behavior for the VoIP system. Poisson distribution describes the chances of occurrence of several events in a given time interval, only when the value of the average number of occurrences of the event is known in advance [13].

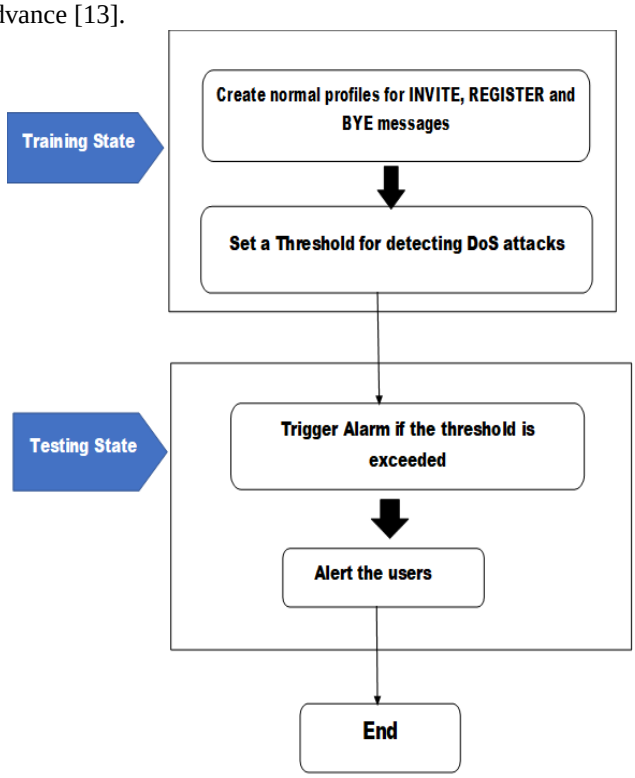

Figure 3 VoIPFD Flowchart

doi: 10.32622/ijrat.76S201919

VoIPFD system specifies a threshold for identifying the flooding attacks using the Poisson distribution. The Testing phase is responsible for comparing the current SIP operation profile with the previously built profile to detect DoS attacks. The VoIPFD system employs Asterisk, VoIP Bots and JavaScript for the detection process. It uses the default port of 5060 of Session Initiation Protocol for transferring the network traffic using UDP. Fig 3 depicts the working of VoIPFD system. The algorithm deployed by the system is very complex and requires more than two parameters to be modified every time to improve the reliability of the system.

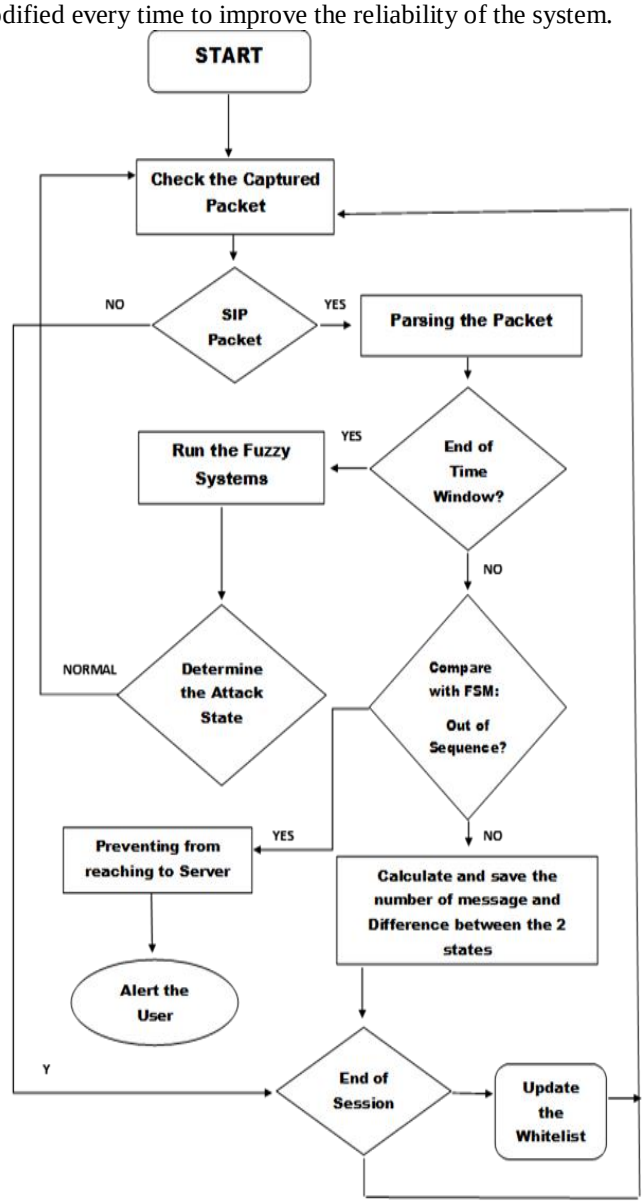

Figure 4 Attack Detection Technique using Fuzzy Systems

Mahsa Hosseinpour [14] proposed a technique for detecting DoS attacks by using the SIP traffic modeling mechanism. It constitutes 2 phases namely, the training phase and the testing phase. The Training phase is used for creating Finite State Machine (FSM) and deriving the required specifications from the regular SIP messages. The Testing phase employs fuzzy systems to detect the flooding attacks and alert users about the intrusions. Parser module is used to extract main parameters such as FROM, TO, CALL-ID from each message of the existing sessions. The calls will be contrasted with those observed in the created Finite State Machine. The calls are made in different intervals of time, due to which the extracted values in each time interval will be compared with those collected from the training phase at the same time interval. The system uses whitelisting mechanism which provides special privilege to its users. The phone numbers present in the whitelists will be accepted and approved. The acquired values are sent to the fuzzy system to diagnose the attack states (NORMAL, ALARM or ATTACK) [14]. Fig 4 depicts the Attack Detection system using Fuzzy systems. If the Fuzzy system is in the Attack State, the users present in the whitelist can progress with their calls and the other calls will not be allowed to reach the server. If the Fuzzy system is in Alarm State, the users are requested to answer a captcha, which can be completed by the genuine user only. If the Fuzzy system is in Normal State, the end-users can proceed with their calls without any disruptions. The Fuzzy system is based on rules. Rules need to be accurate for better detection of flooding attacks. A change in the value of the Finite State Machine will affect the other parameters present in the rules.

Rababe Safoine, Soufyane Mounir [1] proposed a method to enhance the authenticity of the detecting algorithm. The security methods are applied to both the ports namely, 5060 (used for non-encrypted traffic) and 5061 (used for encrypted traffic with Transport Layer Security). The headers of the IP packets are examined, and the system checks whether the User Datagram Protocol is used for transmission of SIP messages between the VoIP endpoints.

doi: 10.32622/ijrat.76S201919

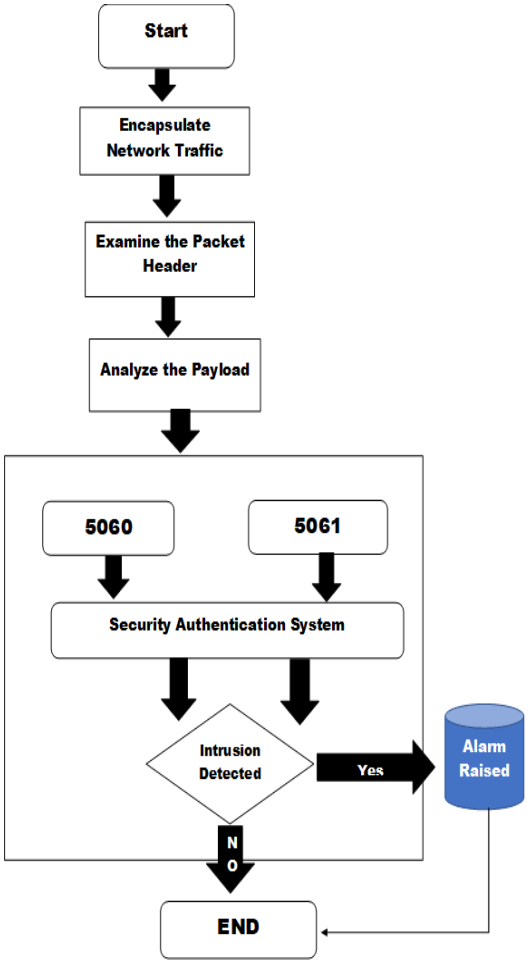

Figure 5 System flowchart for Attack Detection

Different security methods will be applied based on the characteristics of each port. The system uses two different security methods to provide enough security in both the transmission ports. The port number 5061 is used to protect the packets that pass through it based on the Transport Layer Security protocol. Fig 5 represents the working of the detection algorithm. Transport Layer Security (TLS) protocol is a type of Cryptographic protocol that provides end-to-end security over networks. It consists of two layers namely, the TLS Record Protocol and the TLS Handshake protocol [15]. The TLS Record protocol is used for providing connection security and the Handshake protocol is used for enabling the client and server to authenticate each other and to confirm the security keys before any data is transmitted. In the port 5060, the system will generate a reference profile for an existing SIP traffic. A threshold will be determined for every SIP event based on the reference profile created. The behavior of incoming packets will be compared with that of the reference profile. If the packets are considered unprotected (or attacks), an alarm will be triggered to alert the users about the possible intrusions.

V. CONCLUSION

SIP-based VoIP networks have become more popular due to its reliability. This communication has led to various security threats such as flooding attacks, eavesdropping and Denial of Service attacks. There are several detection techniques proposed by several researchers to detect and prevent DoS attacks. This survey presents a literature review of SIP-based VoIP security techniques. Different algorithms have been proposed for recognizing SIP-based Voice over IP network DoS attacks. The Detection techniques used in the survey focuses on detection of Denial-of Service attacks in SIP-based Voice over IP networks and to alert the users about the possible intrusions. The survey includes a comparative study on different detection techniques used for detecting the intrusions in SIP- oriented VoIP network.

REFERENCES

[1]. RababeSafoine and Abdelmajid Farchi, “Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks”, IEEE Transactions on, pp. 978-982, 2018.
[2]. A. Ghafarian and M. Dehghani, “An Empirical study of Security of VoIP System” in SAI Computing Conference, pp. 1031-1036, IEEE, 2016.
[3]. H. Sengar and D. Wijesekera, “Detecting VoIP Floods using the Hellinger’s distance”, IEEE transactions on Parallel and distributed systems, pp. 794-805, 2008.
[4]. S. Ehlert et al, “Two-layer Denial-of Service prevention on SIP VoIP infrastructure”, Computer Communications, vol 31, pp. 2442-2456,2008.
[5]. F. Huici et al, “Protecting SIP against Very Large Flooding DoS Attacks” in Global Telecommunications Conference, IEEE, pp. 1-6,2009.
[6]. A. Bansal and A R Pais, “Mitigation of Flooding-Based Denial of Service Attack against Session Initiation Protocol based VoIP System”, in International Conference for Computational Intelligence Technology (CICT), IEEE, 2015, pp. 391-396.
[7]. R H M Zargar and M H Y Moghaddam, “An Entropy-based VoIP Flooding Attacks Detection and prevention System”, in 4th International Conf. on Computer and Knowledge Engineering (ICCKE), pp. 691-696, IEEE,2014.
[8]. M A Akbar and M Farooq, “Securing SIP-based VoIP infrastructure against flooding attacks and Spam over IP Telephony”, pp. 491-510, 2014.
[9]. F Cadet and D T Fokum, “Coping with DoS Attack on the IP Telephony System”, in Southeast Conference, IEEE,2016.
[10]. R Preeti and R Baniwal, “Security issues in Voice over IP: A Review”, in International Journal of Engineering and Computer Science, vol. 3 Issue 2, pp. 3879-3883,2014.
[11]. V Srihari and R Anitha, “Security aspects of SIP-Based VoIP networks: A Survey”, in Current Trends in Engineering and Technology (ICCTET), pp. 143-150, 2014.
[12]. L Carvajal, L Chen and D Rawat, “Detecting Unprotected SIP-based Voice over IP Traffic”, in 4th International Symposium on Digital forensics and Security (ISDFS’16), pp. 44-48, IEEE, 2016.
[13]. D Golait and N Hubballi, “VoIPFD: Voice over IP Flooding Detection” in 22nd National Conf. on Communication (NCC), pp. 1-6, IEEE,2016.
[14]. MahsaHosseinpour, YaghmaeeMoghaddam and Seved Amin Hosseini Seno, “Modeling SIP Normal Traffic to Detect and Prevent SIP-VoIP Flooding attacks using Fuzzy Logic”, in 6th Int. Conf. on Computer and Knowledge Engineering (ICCKE’17), 2017.
[15]. D Ozden, “Analysis of Recent Attacks on SSL/TLS Protocols”,2016

doi: 10.32622/ijrat.76S201919