International Journal of Computer Applications Technology and Research
Volume 5–Issue 12, 775-781, 2016, ISSN:-2319–8656

Review of SIP based DoS attacks

Abdirisaq M. Jama
Department of Telecommunication, Faculty of Engineering
Open University Malaysia(OUM)
Kuala lumpur, Malaysia

Othman O. Khalifa
Department of Electrical and Computer Engineering
International Islamic University,
Malaysia

Abstract: The Voice over Internet Protocol (VoIP). The VoIP is relatively new and is gaining more and more popularity as it offers a wide range of features and is much more cost effective as compared to the traditional PSTN. But the VoIP brings with it certain security threats which need to be resolved in order to make it a more reliable source of communication. Session Initiation Protocol (SIP) today is considered the standard protocol for multimedia signaling, and the result is a very generic protocol. SIP is specified by the IETF in RFC 3261. From a structural and functional perspective, SIP is application layer signaling text-based protocol used for creating, modifying, and terminating multimedia communications sessions among Internet endpoints. Unfortunately, SIP-based application services can suffer from various security threats as Denial of Service (DoS). attacks on a SIP based VoIP infrastructure that can severely compromise its reliability. In contrast, little work is done to analyze the robustness and reliability of SIP severs under DoS attacks. In this survey, we are discussing the DoS flooding attack on SIP server. Firstly, we present a brief overview about the SIP protocol. Then, security attacks related to SIP protocol. After that, detection techniques of SIP flooding attack and various exploited resources due to attack were discussed and finally the paper reviews previous work done on SIP based DoS attacks.

Keywords: Voice over IP; Session Initiation Protocol; attack; security; Denial of Service

1. INTRODUCTION

VoIP is a technology which allows users to use telephone services using Internet connection in IP based network.
These telephone services are provided by the Public Switched Telephone Network(PSTN)

The fundamental process of VoIP includes conversion of voice into digital signals with the segmentation of voice signals into a stream of packets and then sending those voice packets across the network using Real Time Transport Protocol (RTP) [1].

All we need to make a VoIP call is a microphone, speakers and an internet connection. The main advantages of using Internet to make calls is that (i) it is very cheap as compared to the traditional PSTN system of making calls (ii) offers a rich feature set and (iii) is highly flexible.

Session Initiation Protocol (SIP) is the IETF standard for IP telephony and it is defined in RFC 3261 as an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants [2].

SIP is structured as a layered protocol, which means that its behavior is described in terms of a set of quite independent processing stages with only a loose coupling between each stage.

The lowest layer of SIP is its syntax and encoding and the second layer is the transport layer. It defines how a client sends requests and receives responses, and also, how a server receives requests and sends responses over the network. The third layer is the transaction layer. Transactions are the fundamental component of SIP. A transaction is a request sent by the client transaction layer to the server transaction layer, along with all responses to that request which are sent from the server transaction layer back to the client transaction layer. The transaction layer handles application-layer re-transmissions, matching of responses to requests, and application-layer timeouts. The layer above the transaction layer is called the transaction user (TU). When a TU wants to send a request, it creates a client transaction instance and passes the request along with the destination IP address, its port, and its transport layer information as shown in figure 1.

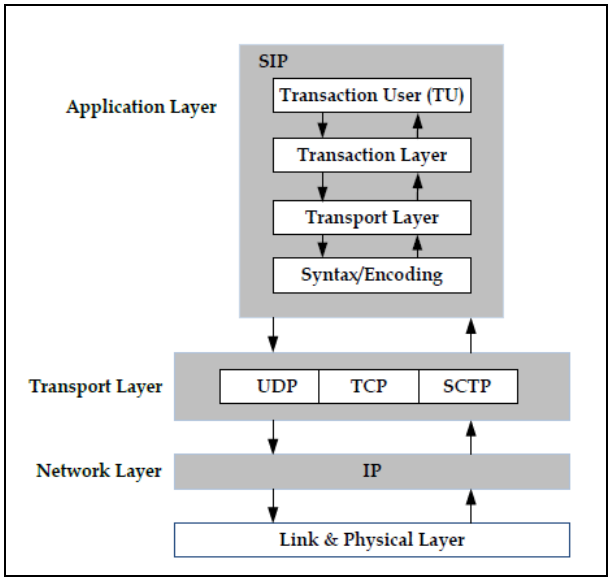

Figure. 1 SIP Protocol layers

SIP is a lightweight application layer protocol designed to manage and establish multimedia sessions such as video conferencing, voice calls, and data sharing through requests and responses. It is increasingly gaining favor over H.323 in the VoIP environment. Three advantages of SIP are as follows [2] :-

- It uses Uniform Resource Locators (URL): addressing scheme, which is physical location independent. Addressing can be a phone number, an IP address, or an e-mail address.
- It allows multiple media sessions during one call. This means that users can share a game, Instant Message (IM), and talk at the same time.
- It is a "light" protocol and is easily scalable.

VoIP has gained tremendous acceptance and is widely deployed today mainly due to the reduced costs, demand for multimedia communications, and demand for convergence of voice and data networks.

Securing VoIP is not an easy task, as it needs efforts in several stages. One of the essential issues in VoIP security is protecting the signalling messages being exchanged between VoIP infrastructures. As it is built on standard IP networks, it is vulnerable to the wide range of network attacks associated with the Internet, such as Denial of Service (DoS).

Much attention is paid to enhance the features and interoperability of SIP protocol with less focus on security. A SIP based VOIP network is potentially vulnerable to general IP and VOIP attacks as well as attacks which are unique to SIP. To secure a SIP based VOIP system, it is necessary to understand the nature of different kinds of attacks and how they can affect to degrade the performance of a SIP system. Many solutions and strategies have been proposed to solve SIP based VoIP security issues.

This paper attempts to explore the SIP based DoS security issues. The following section presents the general components of the SIP architecture. Section 3 addresses the security requirements and the possible threats and attacks in SIP based VoIP, while it briefly describes SIP's security mechanisms. Section 4 emphasizes DoS attacks and section 5 illustrates related work on SIP DoS attackes and section 6 concludes the paper providing some pointers to future research work.

2. SIP OPERATION

The Session Initiation Protocol is a text-based signaling communications protocol, which is used to creation, management and terminations of each session. It is responsible for smooth transmission of data packets over the network. It considers the request made by the user to make a call and then establishes connection between two or multiple users. When the call is complete, it destroys the session.

SIP can be used for two party (unicast) or multi party (multicast) sessions. It works in along with other application layer protocols that identify and carry the session media.

2.1 SIP Components

SIP is a text based client-server protocol similar to Hyper Text Transfer Protocol (HTTP). A SIP-based VoIP system is composed of the following types of entities [2] as shown in figure 2 each having specific functions to perform:-

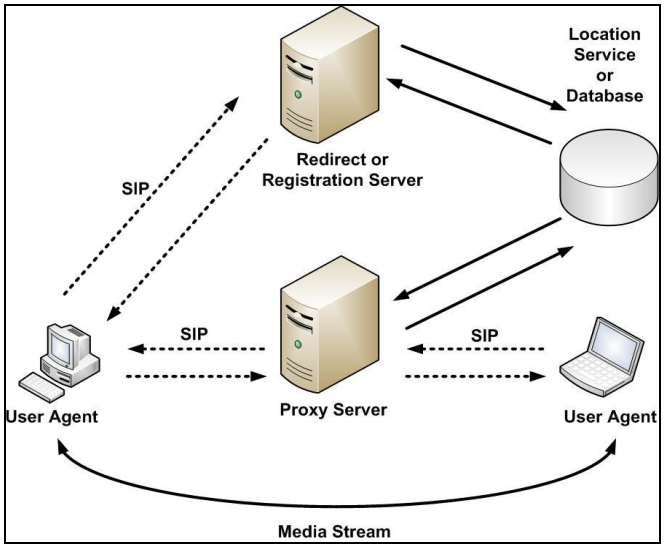

Figure. 2 Basic logical components of a SIP based system

User Agent (UA): is the component interacting with the end user to complete a SIP request. A SIP client can act as both a SIP User Agent Client (UAC) and a SIP User Agent Server (UAS), where the UAC generates outgoing SIP requests which mean that it is the entity that initiates the call, and UAS handles incoming SIP call requests.

SIP proxy server: the SIP proxy server receives SIP requests from various user agents and forwards them to the appropriate hosts. It may also contain an authentication function. It is used as mediators in VoIP and forwards requests to UAS, UAC or other proxies. A proxy server is often responsible for a domain that a client is registered to. A Proxy may enforce a policy and for example, verify that a user is allowed to initiate a call. A proxy can also interpret and if necessary, rewrites specific parts of a SIP request before forwarding it.

Location Server: A location server is used to store the locations of registered users. It is used by a proxy to find the destination client's possible location.

Redirect server: Redirect server accepts SIP request from a client, maps the SIP address of the called party and returns the address to the client. Redirect Server doesn't forward request to other servers.

Registrar server: It processes REGISTER messages, and it maps the users URI to their current location. It is a server that accepts register requests from a UA and stores the information into a location service in the domain it handles. When an UAC wants to initiate a session with a UAS, UAC must discover the current host (IP address) where the UAS is reachable. This discovery process is often done by SIP proxy servers and redirect servers which are responsible for receiving a request, determining where to send it based on knowledge of the location of the user, and then sending it there. To do this, SIP network elements asks the location service, that responds with a UA address within a particular domain.. In some systems, the registrar server is located on the SIP proxy server.

2.2 SIP Messages

In [2] defines the various types of messages that the SIP can support. The SIP messages fall widely under two categories, Requests and Responses. Some of the SIP supported Requests and Responses are listed in Table 1 and 2 respectively.

Table 1. SIP requests

SIP Request	Purpose
INVITE	To initiate a session
BYE	To terminate an existing session
OPTIONS	To determine the SIP messages and codecs that the UA or server understands
REGISTER	To register a location from a SIP user
ACK	To acknowledge a response from an INVITE request
CANCEL	To cancel a pending INVITE request (it is important to note that this operation does not affect a completed request
SUBSCRIBE	To indicate the desire for future NOTIFY requests
NOTIFY	To provide information about a state change that is not related to a specific Session
REFER	To transfer calls and contact external resources

Table 2. SIP responses

SIP Response	Purpose
100 Trying	To indicate a proxy has received an INVITE request, and is processing it.
180 Ringing	The INVITE has been forwarded to the destination
200 OK	A session has been set up
401	A response to a REGISTER request, if the user did Unauthorized not provide correct authentication information
407	Proxy Authentication Required A response to an INVITE request, if authentication is enabled on the proxy, and the user did not provide correct authentication information
408	Request timeout To indicate there is no response to a request within a certain time
503	Service unavailable. To indicate the current request cannot be processed

2.3 SIP Process

The SIP operation is introduced as a specific example. Communication between Alice and Bob is used to explain SIP operation. Besides, their end to end controls. An initial request starts from SIP server. It may be used as a user agent server. Otherwise, it will act as proxy server. The SIP proxy server was considered as the example here, for SIP signaling it should pass through SIP proxy server. When Alice log on to her SIP soft phone or hard-phone first step will be to register to the server sending invite messages, the server will response to Alice by informational trying, then proxy server will forward a second trying which will be received by Bob's telephony device. Bob will ring his phone. The assumption is that Bob will pick up his incoming call, the message will be send for both SIP proxy server and Alice. When the SIP messages request succeeds, Final response to the INVITE "ACK" will be sent from Alice to Bob as illustrated in Figure 3.

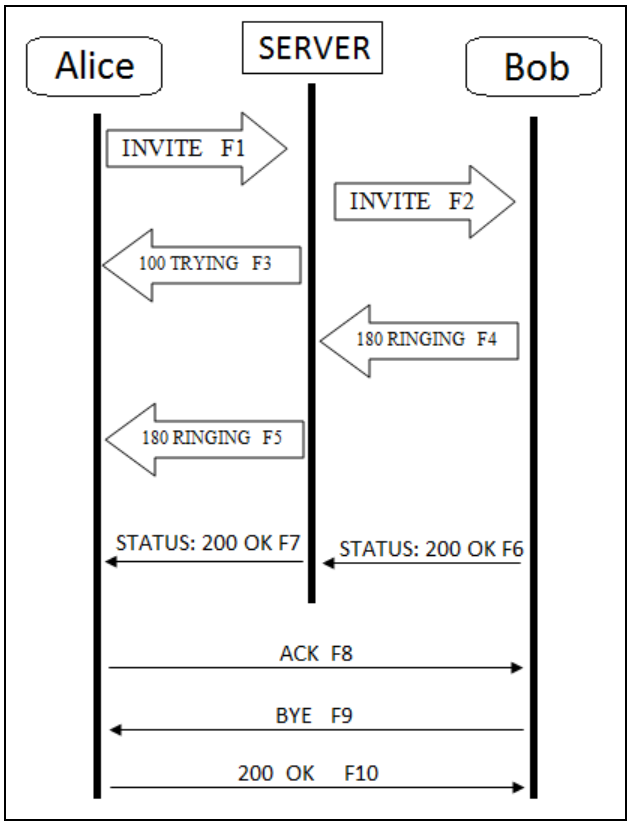

Figure. 3 SIP Process

So, the media will start unless Bob ends the call. Thus, message from Bob will inform the server BYE and server will forward his request to Alice. After that, final agree message will be exchanged. RTP works point to point even if there are SIP proxy servers. SIP normally uses Real Time Protocol (RTP). The purpose is to establish a media session.

3. SIP BASED VOIP SECURITY

Security and privacy requirements in a VoIP environment are expected to be equivalent to those in PSTN, even though the provision of secure Internet services is much more complicated. SIP messages may contain information that a user or a server wishes to keep private.

The flexibility and rich feature-set of SIP based IP telephony compared to traditional PSTN based phone comes with the additional security risks. SIP based IP telephony system is vulnerable to general Internet attacks, as well as attacks which are specific to SIP. As most of SIP development so far has focused on features and interoperability, there exists ample opportunity to work on SIP security. Various security attacks

and threats applicable to SIP are discussed in the following subsections.

3.1 SIP Vulnerability issues

As with any other network protocol, SIP is exposed to a wide range of security attacks. When deployed in a private network where network equipment and users are trustworthy and physical security is agreeably sufficient, SIP security may not be needed. However, since SIP can be deployed in an unreliable and untrustworthy environment like Internet, it is susceptible to various security attacks that include the common TCP/IP attacks.

The following Table 3 illustrates what people need to secure their network and how it may be vulnerable.

Table 3. Vulnerability issues

What You Must Do	What Hackers Can Do
Protect every point of entry Attack the weakest point of entry	Attack the weakest point of entry
Be constantly vigilant 24 / 7 / 365	Attack at a time of their choosing
Close every vulnerability	Exploit all vulnerabilities
Close every known vulnerability	Search for new vulnerabilities

For instance, VoIP suffers from all known attacks associated with any Internet application or subsystem. Table 4 illustrates some of the identified threats - attacks, their impact on the overall SIP security.

Table 4. Network and application security issues

Issues	Impact
Eavesdropping: Unauthorized interception decoding of signaling messages	Loss of privacy and confidentiality
Viruses and Software bugs	DoS / Unauthorized access
Replay: Retransmission of genuine messages for reprocessing	DoS
Spoofing: Impersonation of a legitimate user	Unauthorized access
Message tampering/Integrity: The message received is the message that was send	Loss of integrity, DoS
Prevention of access to network services e.g. by flooding SIP proxy servers / registrars	DoS
SIP-enabled IP phones: Trivial File Transfer Protocol (TFTP) Eavesdropping, Dynamic Host Configuration Protocol (DHCP) Spoofing, Telnet	Loss of confidentiality, Unauthorized access, DoS

4. SIP DOS ATTACKS

SIP system is deployed in the Internet that can be Considered hostile environment, in which SIP messages may be exposed to a range of security threats and attacks. Following are some classified attacks on the SIP protocol.

Denial-of-Service (DoS) attacks are a class of network attacks performed to interrupt or terminate applications, servers, or even whole networks, with the aim of disrupting legitimate users' communication. Disruption targets are web browsing, listening to online radio, or even interrupting essential communication, e.g. power plant network control traffic. DoS attacks are commonly performed intentionally and in most cases difficult to counter.

Several components in a VoIP system, including media gateways, IP phones, IP PBX, VoIP firewalls and so on process signaling, causing DoS against the signaling interfaces to be a major issue [3].

DoS attacks can have different forms, and they can also be differently motivated. Generally, users might like the feeling of having power to force their will onto others by disrupting some sort of their communication.

The goal of a DoS attack is to render the service or system in-operable. Hence an attack can be directed toward different entities in the network, depending on the attacker's intent. If the aim is to render the service as a whole inoperable, the main target will be the core servers in the SIP infrastructure.

Three different types of SIP DoS attacks were classified. They are SIP Message Payload Tampering, SIP Message Flow Tampering and SIP Message Flooding. A classification, to be illustrated below and as depicted in Figure 4 below.

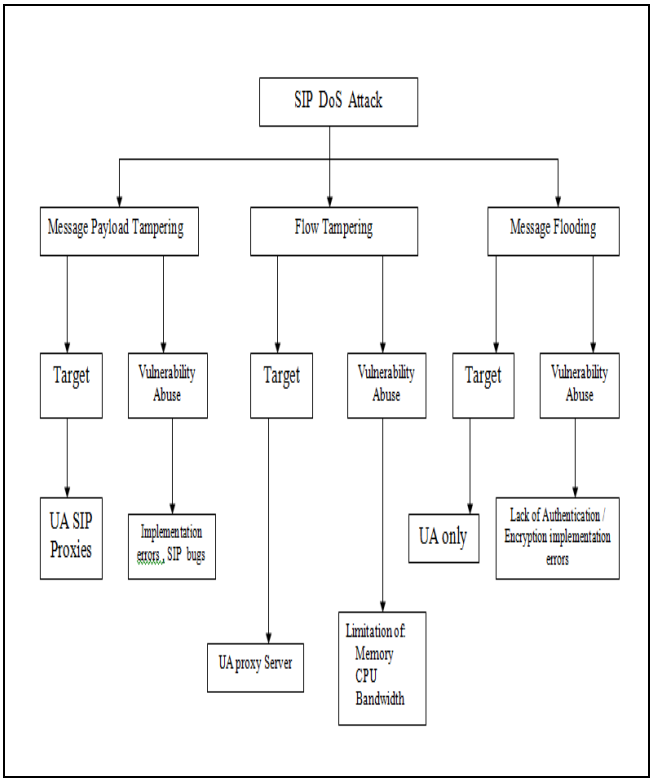

Figure. 4 Classification of SIP DoS attacks.

4.1 DoS by Message Payload Tampering

The first class of attacks is based on tampering with the actual SIP message or more specifically, the SIP payload. SIP is a text-based protocol and messages are transported usually with clear text.

On the other hand, it makes the implementations of the protocol vulnerable to malformed message attacks. SIP message parsers that process incoming messages have to be efficient to handle the degree of protocol flexibility and also be robust against malformed message attacks.

Attackers can try to inject harmful content into a message, e.g. by entering meaningless or wrong information with the goal of creating a buffer overflow at the target. Also, such messages can be used to probe for vulnerabilities in the target. Harmful code that will be executed in an unforeseen context can be introduced into the payload.

This kind of vulnerability exploitation, an attacker sends messages crafted in a specific way that takes advantage of that given vulnerability. By launching a Nuke attack on e.g. the TCP/IP stack, the whole system might crash eventually. Such vulnerabilities are easy exploited by an attacker, but also easily eliminated. As soon as the vulnerability is detected, it can be fixed by modifying the source code. Usually, vendors provide patches for their software soon after a new exploit has become known. The local system administrator then has to install the patch to prevent further attacks.

4.2 DoS by FlowTampering

One common way to achieve a DoS attack is to exploit vulnerabilities in a software component on the target machine. This includes vulnerabilities in application servers, network stacks, or general operating system vulnerabilities.

Flow based DoS attacks aim at causing a disruption to an ongoing call by impersonating one of the call participants. The SIP protocol defines a specific sequence of message exchanges for call setup and termination [2].

The attacker needs to know the session parameters in order for these attacks to function correctly. The parameters can be sniffed from the network. By sending a message out of its expected sequence, an attacker can disrupt the regular call flow. Such attacks are mostly targeted at SIP User Agents.

There are two common strategies to launch a DoS attack, by either exploiting software vulnerability or by depleting resources at the target host. This type of attacking a Resource is to overwhelm a resource at the target. The attack tries to overwhelm resources at the target by generating more requests than the target can handle.

There are three common resources an attacker can exploit:
1. Memory
2. CPU power
3. Link Bandwidth

4.3 DoS by Message Flooding

The most common incarnation of a DoS attack is where an attacker sends a huge amount of SIP related messages to a target with the goal to overwhelm the target's processing capabilities, and hence rendering the target inoperable.

Message flooding DoS attacks are the most common attacks on the SIP architecture. REGISTER floods are aimed at the SIP registrar, INVITE floods target the SIP proxy/redirect server and authentication DoS affects either or both. DoS attacks are easy to launch requiring an attacker to simply craft a SIP message and send it.

Such attacks are generally hard to detect, as the utilized attack messages are usually valid messages and thus not easily distinguishable from regular messages.

5. RELATED WORK

There are different studies which focus on security issues and countermeasures of SIP based DoS.

In [5] focuses on SIP DoS attacks, The study examine how SIP flooding attacks affect the performance of a SIP-based system, and propose an Improved Security-Enhanced SIP System (ISESS) to counter such attacks. Experimental results are provided to demonstrate the effectiveness of ISESS. The Experimental results show that with ISESS, during a flood-based denial of service attack.

In [6] describes DoS attack are realized by people for key security issues and also it is implemented to increases the security threat, protecting systems against DoS attack. The fast growing concern are improved by DoS attack which are noticed with more researchers where the attacker design a flow or system bug to report as a resource of a victim system,

and also users can prevent from accessing the service or to degrade the quality of service which they get. For example, the operating systems with DoS were early work with type of resource exhaustion attack. The services are to be exhausted when supposed to be not available. The computer or network resource exists by DoS attack to avoid damage, e.g. a user account or network connection. The resource availability, and the affected will users are collate by attack. The DoS attack is not only necessary at the unique one but also materialized to resource exhaustion.

In [7] aims to provide scheme to detect low rate SIP flooding attacks using area under curve of monitored dynamic SIP traffic with classification of SIP flooding attacks and its influence on SIP server under low rate DoS attack. Compared to the other detection technique our technique is better, due to its advantages of accuracy, fast, light weight, and flexibility to deal with DoS attack detection. Experimental results show the effectiveness of the scheme. the only drawback of this study is that it detects of low rate attacks and prevention methods are missing.

In [8] proposes a new hybrid (anomaly and misuse) SIP flooding attack detection algorithm, which overcomes the existing problems in many of other detection algorithms & is better than existing algorithms. The proposed algorithm is tested using simulated traffic datasets, and compared with three well known anomaly algorithms and one misuse detection algorithm. The test results show that the new algorithm has high detection accuracy and high completeness.

Another study in [9] , The authors built and configured a real test-bed for SIP based services to generate normal and assumed attack traffics. the test-bed was validated and evaluated our intrusion detection system with the dump traffic of this real test-bed and we also used another specific available dataset to have a more comprehensive evaluation. The experimental results show that the approach was effective in classifying normal and anomaly traffic in different situations. The Receiver Operating Characteristic (ROC) analysis is applied on final extracted results to select the working point of our system. the only drawback of this study was that the authors only focused for detection which lacks prevention mechanisms.
In [10] authors proposed a VoIP-aware attack-detection scheme. The proposed scheme is able to detect VoIP network attacks including VoIP DoS and SPAM. It can detect VoIP DoS attacks with low false negatives using a statistics-based detection algorithm and can recognize SPAM with low false positives using a caller behavior-based detection algorithm. Authors have included experimental
results to confirm the proposed scheme. this study focused detection mechanisms only.

In [11] proposed a two layer DoS prevention architecture that handles both SIP flooding and malformed packet attacks on a standard VoIP network hence real network topology simulation test is missing.

In [12], proposed a stateful SIP inspection mechanism, called SIP VoIP Anomaly Detection (SIPAD), that exploits a SIP-optimized data structure to detect malformed SIP messages and SIP flooding attacks. SIPAD pre-compiles a stateful rule tree that rearranges the SIP rule set by hierarchical correlation. On the basis of current state and the message type, SIPAD computes the corresponding branches from the stateful rule tree, and examines a SIP message's structure by comparing it to the branches. The SIPAD provides higher detection accuracy, wider detection coverage and faster detection than existing approaches. Conventional SIP detection schemes tend to have high overhead costs due to the complexity of their rule matching schemes. Experimental results of their SIP-optimized approach, by contrast, indicate that it dramatically decreases overhead and can even be deployed in resource-constrained environments such as smartphones. However, this study lacks prevention techniques.

In [13], has given more priority to DoS attack by flooding of different SIP-messages. A small work is done to analyze the performance of SIP server and quality of ongoing VoIP calls under DoS attacks. We show the utilization of CPU and memory during the multiple simultaneous calls. On the basis of measurements we show that a standard SIP server can be easily overloaded by simple call requests. It also shows that simple call request can degrade quality of ongoing calls.

The study proposed in [14] detects DoS attacks using an entropy-based IDS. In such a system, however, an attacker can sniff the network and obtain an entropy value.
In other words, entropy-based DoS solutions are vulnerable to spoofing attack because an attacker can keep the entropy value within an expected range and, therefore, provide realistic conditions to DoS attacks to occur. First, the attacker monitors the entropy before launching the attack and then calculates the mean, standard deviation and variance values. Subsequently, it spoofs the entropy during the attack. The authors show that this detection system can be deceived because the spoofed packets not only penetrate into the network but also help DoS attacks to occur.

6. CONCLUSION

IP is not an easy signaling protocol to secure. A discussion of some present solutions for SIP security malfunctions consisting of implementations and simulations is presented in this study. The SIP security solutions identified suggest that security mechanisms cannot provide 100% protection against SIP attacker, but threats can be mitigated significantly. A number of studies were reviewed and some common problems and their solutions were presented. Several SIP security solutions were found to be ultimately related to device security. The solutions presented here are not achieved by securing a single protocol but should involve the whole system.

7. REFERENCES

[1] Anchal Sehgal, Dervish Ghosh and Dr.Charu Gandhi. 2015. Literature Survey of VoIP Security International Journal of Emerging Technology and Advanced Engineering , Volume 5, Special issue 1, April 2015

[2] IETF Network Working Group. (2016) . SIP: Session Initiation Protocol. Retrieved September 21, 2016. http://www. ietf.org/rfc/rfc3261.txt.

[3] Liu, Z.H., J.C. Chen and T.C. Chen. 2009. Design and analysis of SIP-based mobile VPN for real-time applications. IEEE Trans. Wireless Commun., 8: 5650-5661. DOI: 10.1109/TWC.2009.090076

[4] Tarendra G. Rahangdale1, Pritish A. Tijare and Swapnil N.Sawalkar. 2014. An Overview on Security Analysis of Session Initiation Protocol in VoIP network, International Journal of Research in Advent Technology, Vol.2, No.4, April 2014 E-ISSN: 2321-9637

[5] Xianglin Deng, Malcolm Shore. 2009. Advanced Flooding Attack on a SIP Server. IEEE Computer Society,Page No(647- 652), 2009.

[6] Lin Fan, 2010. "A Group Tracing and Filtering Tree for REST DDoS in Cloud Computing", International Journal of Digital Content Technology and its Applications, 4(9).

[7] Abhishek Kumar, Dr. P. Santhi Tilagam," A Novel Approach for Evaluating and Detecting Low Rate SIP Flooding Attack" International Journal of Computer Applications,Volume 26– No.1,Page No (0975 – 8887),July 2011.

[8] Dahham Allawi, Alaa Aldin Rohiem, Ali El-moghazy and Ateff Ghalwash,"New Algorithm for SIP Flooding Attack Detection",IJCST , Volume- 4, Issue- 3, Page No(10-19), March 2013.

[9] Zoha Asgharian; Hassan Asgharian; Ahmad Akbari and Bijan Raahemi Detecting Denial of Service Message Flooding Attacks in SIP based Services Electrical & Electronics Engineering Journal / Vol . 44 / No.1 / Spring 2012

[10] Jonghan Lee & Kyumin Cho & ChangYong Lee & Seungjoo Kim , VoIP-aware network attack detection based on statistics and behavior of SIP traffic, Peer-to-Peer Netw. Appl. (2015) 8:872–880

[11] S. Ehlert, G. Zhang, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, and D. Sisalem. (2012). Two layer Denial of Service prevention on SIP VoIP infrastructures. Computer Communications. Page No(2443-2456).

[12] Dongwon Seo ,Heejo Lee , Ejovi Nuwere "SIPAD: SIP–VoIP Anomaly Detection using a Stateful Rule Tree",Elsevier,Computer communication,Page No(562-574),2013.

[13] Abhishek Bansal, Prashant Kulkarni, Alwyn R. Pais" Effectiveness of SIP Messages on SIP Server", Proceedings of 2013 IEEE International Conference on Information and Communication Technologies,Page No(251-256),2013.

[14] Ozcelik I, Brooks RR. Deceiving entropy based DoS detection. Computers and Security 2015; 48: 234–245.