JCSE International Journal of Computer Science and Engineering Open Access

Survey Paper Volume-2, Issue-5 E-ISSN: 2347-2693

DoS Flooding Attacks against SIP based VoIP Systems- a Survey

Mandeep Kaur[1*], Santosh Kumar[2] and Swati Sharma[3]

[1*,2,3] *Department of Computer Science, Graphic Era, India,*

www.ijcseonline.org

Received: 11/04/2014 Revised: 26 /04/2014 Accepted: 17/05/ 2014 Published: 31 /05/2014

Abstract— The success of the Internet has brought significant changes to the telecommunication industry. One of the remarkable outcomes of this evolution is Voice over IP (VoIP), which enables real time voice communications over packet switched networks for a lower cost than traditional public switched telephone networks (PSTN).VoIP networks are more vulnerable to security threats as compared to traditional PSTN due to their open environment such as the Internet and use of open standard like Session Initiation Protocol (SIP), launching an attack on a telephony server is much simpler. Availability is one of the major issues of computer security, along with confidentiality and integrity. Denial of service (DoS) is a threat that potentially violates the availability of a resource in a system. In this survey, we are discussing the DoS flooding attack on SIP server. Firstly, we present a brief overview about the SIP protocol. Then, we discuss security attacks related to SIP protocol. After that, we talk about the detection techniques of SIP flooding attack and various exploited resources due to attack.

Keywords/— *VoIP, SIP flooding, DoS, PSTN*

I. INTRODUCTION

Voice over Internet protocol (VoIP) is a mechanism that sends voice over the IP based network. VoIP usage is rapidly growing due to its cost effectiveness, greater ability to integrate new services and a significant increase in scalability over the traditional telephone network and its compatibility with PSTN. VoIP offers significant risks and vulnerabilities, in spite of offering lower cost and greater flexibility, DoS is one of them. VoIP utilizes the Internet Protocol (IP) to route packets containing small portions of audio from the conversations between the callers. Due to this, it also inherits the security issues associated with the IP protocol.

Apart from advantages like lower cost and more flexibility of VoIP it is also very important to analyze all the security related issues at different levels of VoIP. A denial of service (DoS) attack aims to deny access by legitimate users to shared services or resources. On the Internet, a DoS attack aims to disrupt the service provided by a network or server. The impact of a DoS attack depends on the target. If a particular client is a target then it can lead to denying the service to this user. But when a SIP server is the target, then it brings down the server. In this case, no user can get service [1].

Nowadays, VoIP technology mostly uses SIP as signaling protocol. It is simple and relatively easy to implement in nature and due these properties it became quite popular and many implementations of it exist in forms of free or paid SIP servers. Different SIP-server implementations have different weaknesses due to these weaknesses these are vulnerable SIP flooding attacks.

SIP servers are the most common targets of DoS attacks , VoIP technology becomes more widely deployed due to its economical advantages over traditional PSTN services so VoIP entities (server and clients) are likely to be attractive targets .H.323 [3] and SIP [4] are the two major protocols used to provide VoIP services. H.323 is the standard of International Telecommunication Union (ITU) while SIP is proposed by Internet Engineer Task Force (IETF) [8]. Generally, intrusion detection techniques are divided into two major approaches: signature based and behavior based. In the signature based approach, attack patterns are profiled as signatures and detection is based on pattern matching between ongoing traffic and the signatures. This approach is not viable in our case to detect the stealthy flooding attacks, as attackers can randomly manipulate their strategy which makes profiling every possible attack signature very difficult. In the behavior based approach, profiles of normal traffic are first established, and attacks are detected as long as significant deviations from the normal profiles are identified. Our detection scheme adopts the behavior based approach [4].

In this paper, we focus on DoS flooding attacks and detection techniques to detect attacks in wired networked systems. Here, our goal is to categorize the existing DoS flooding attacks and to provide a comprehensive survey of detection mechanisms categorized based on where and when they detect and respond to DoS flooding attacks. Such a study of DoS flooding attacks and the presented survey is important to understand the critical issues related to this important network security problem so as to build more comprehensive and effective defense mechanisms.

Paper Organization: Our survey of the research literature is given in Section II. Section III provides a brief overview of SIP, be like the most popular VoIP technology currently in use. Section IV summarizes the threat taxonomy of SIP flooding attacks, detection techniques and exploitable

Corresponding Author: *Mandeep Kaur*

resources in launching flooding attacks. We then discuss our findings in Section V.

II. Related Works

The detection and prevention of SIP flooding attack is addressed in several recent publications.
Chen proposes a method to detect SIP message flooding by altering the existing finite-state machines for transactions in SIP in such a way that transaction anomalies can be detected in a stateful manner [8].

Tang and Cheng [9] developed an online scheme by integrating a novel three-dimensional sketch design with the Hellinger distance (HD) detection technique to detect and subsequently prevent the flooding attacks,.

Rafique, M.Z.et al. [10]showed inadequacy of the robustness and reliability of generic SIP servers & on the basis of measurements a standard SIP server can be easily overloaded by sending simple call requests and can be crashed through 'INVITE of Death' - a malformed SIP packet maliciously crafted by our tool. To measure the effects of flooding attacks on real time services - VoIP in SIP environment we define the performance metrics and show the results on different SIP server Implementations. Their results also provide results on exploitable resources' by SIP servers during flooding attacks.

Abhishek Bansal et al. [11] 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.

Lou and Peng et al. [12] investigate the impact of DoS attacks on SIP infrastructure, using a popular open source SIP server as a test bed. We identify several security threats to SIP signaling infrastructure in terms of their vulnerability to DoS attacks and have also proposed several modifications of the SIP implementation that can greatly enhance the server's robustness against DoS attacks which also point out that strong authentication is not helpful in defending against DoS attacks.

Dongwon Seo et al.[15] 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 precompiles 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 our SIP-optimized approach, by contrast, indicate that it dramatically decreases overhead and can even be deployed in resource-constrained environments such as smartphones.

Abhishek Kumar et al.[17]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 DDoS attack detection. Experimental results show the effectiveness of the scheme.

Xianglin Deng et al. [18] 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, the performance of the system can be improved substantially.

Dahham Allawi et al.[19] 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.

III. SIP Overview

Session Initiation Protocol (SIP) is an application – layer signaling protocol developed by Internet Engineering Task Force (IETF). It is an ASCII-based peer to peer protocol that initiates, modifies, creates and terminates interactive multimedia communication session between two or more partners Because of the flexibility of SIP, it is used for audio, video and data packet transmission and communication. SIP is based on client server architecture similar to http and its message format is also similar to HTTP protocol, with message headers and corresponding values e.g. from: user@sip.org to denote the sender of a message. Several message types are defined (e.g. REGISTER, INVITE, ACK, BYE.) and encoded in the first line of each message (Request-URI).

A. SIP Components

SIP consists up of two types of entities: User agent (UA) and Network servers. User agent includes User agent client & User agent server [13].

User agent client: The UAC is an application that initiates calls or SIP requests to a UAS. The following are requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER.

User agent server: UAS is the Server that hosts the application responsible for receiving the SIP requests from a UAC, and on reception returns a response to the request back to the UAC. The UAS may issue multiple responses to the UAC, not necessarily a single response.

On the other hand Network servers includes Proxy Server, Redirect server, Registrar Server and location server

The Proxy server: The proxy server acts as a mediator it forwards services; It handles SIP requests for the source UA. A proxy server can perform as a server or a client to make a request in the name of clients.

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: Registrar server is a server which accept register request from a client, and update the location database, the location database is used to store contact information.

Location Server: Location server is used to store terminals location, and provide a terminals location to the proxy server or redirect server.

B. SIP Messages

The signaling messages in SIP support requests from clients to Registrars or proxies, and their corresponding replies.

For each request SIP server generates SIP response to indicate the status of the request. The different categories of request & response messages are shown in Table I.

REQUEST MESSAGES		RESPONSE MESSAGES		
Method	**Purpose**	**Status code**	**Description**	**Example**
INVITE	Initiate a session	1xx	Informational	100 trying
ACK	Acknowledge session initiation	2xx	Success	200 OK
OPTIONS	Query server capability	3xx	Redirection	300 Multiple choices
BYE	Terminate	4xx	Client Error	401 Unauthorized
CANCEL	Cancel pending request	5xx	Server Error	503 Service unavailable
REGISTER	Register user request	6xx	Global failure	600 Busy everywhere

Table I – SIP Messages

C. SIP Session setup and Teardown

The six steps for establishing communication in SIP protocol are shown in Figure 1:

- User registration, initiation and location.
- Media determination.
- Determining the willingness to accept or reject calls.
- Call setup.
- Call modification and handling.
- Terminating the call (end of call).

IV. CLASSIFICATION OF SIP FLOODING ATTACK

In spite of security mechanisms, SIP Services are vulnerable to certain security threats. The aim of any kind of attack is to disable the target machine and preventing user to use its services known as denial of service (DoS) or to gain some sort of unauthorized access in computation resources. One of the most well-known methods to create problems in the availability of the provided service is the consumption of existing resources by creating a large number of requests against the providing VoIP service. Another possible vulnerability is the exploitation of developing errors in SIP servers [5]. A flooding attack against an Internet application or service can be launched either from a single or multiple sources. Attack from single source is DoS and from multiple sources is DDoS. Below we describe how this type of attack can be launched towards the SIP infrastructure.

1. Registration Flooding Attack

One of the crucial network elements in SIP telephony service is the registrar. When an attacker manages to paralyze the registrar (e.g., by sending numerous bogus registration requests), it can easily cause a DoS. This situation can be avoided only if the SIP server blocks all messages coming from unknown origins as shown in Figure 2. In this, when the attacker ABC launches an attack against a REGISTRAR by employing a large number of registration requests, he/she aims to accomplish one of the following goals:

- To guess authorized users' passwords
- To cause a DoS in the SIP registrar

2. INVITE Flooding Attack

One of the most utilized messages that must be processed by SIP proxy servers is the INVITE message. The INVITE message is used to establish a connection among two or more participants in a SIP session. Until this connection is established, the SIP proxy must keep the connection state. This fact makes the proxy most vulnerable to flooding attacks. An attacker can possibly launch a flooding attack by utilizing INVITE messages not only against a proxy, but also against an end-user's terminal. For example, end-user devices have been designed mainly to respond under normal conditions. This means that they are able to process few incoming messages simultaneously. Considering the situation where an attacker impersonates himself as a legitimate user, he will possibly generate numerous INVITEs as illustrated in Figure 3. In this situation the attacker builds up INVITEs only, without waiting for any respond message trying to paralyze the victim. Additionally, in this scenario the SIP proxy is utilized by the attacker to amplify the generating INVITE messages.

3. *Authentication Flooding Attack.*

The SIP protocol uses HTTP Digest mechanism for authentication which requires maintenance of state by storing issued challenge at the server. This can be misused by unauthorized attacker to launch broken session attack if attackers ignore or falsely respond to authentication requests and start another session instead. SIP server needs to compute MD5 Digest response to match the received response in order to verify the valid password sent by client. The attacker machine needs not to calculate the MD5 Digest response using the realm, nonce, username and passwords values. An attacker can easily send the random Digest values stored. Using this mechanism an attacker can send more requests per second to target server to keep server busy [13].

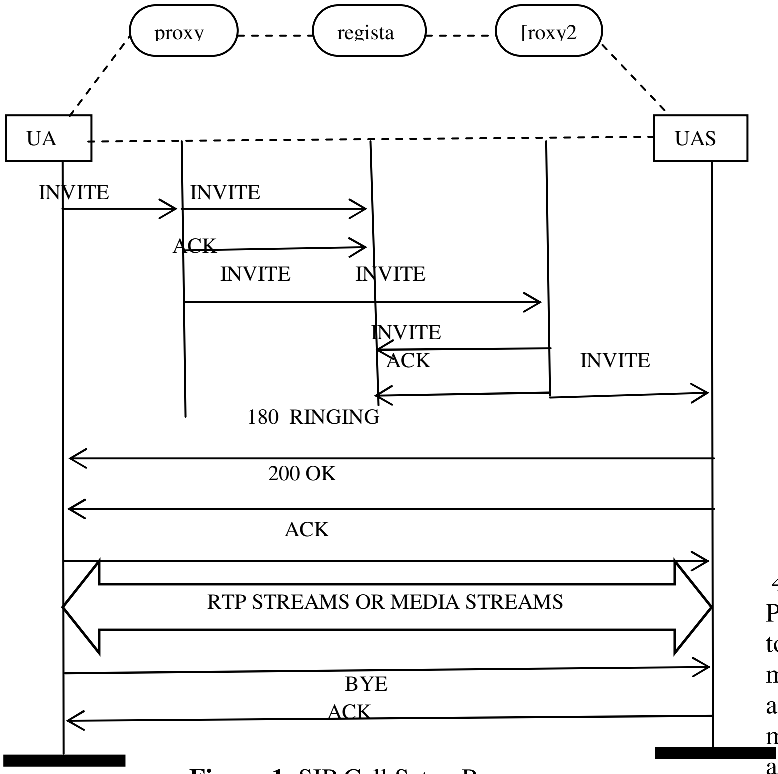

Figure 1. SIP Call Setup Process

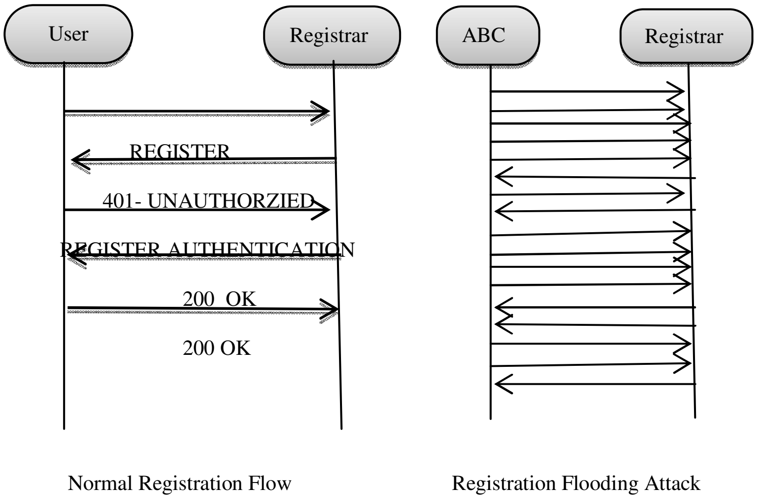

Figure 2. Normal Registration and Registration Flooding Attack[17]

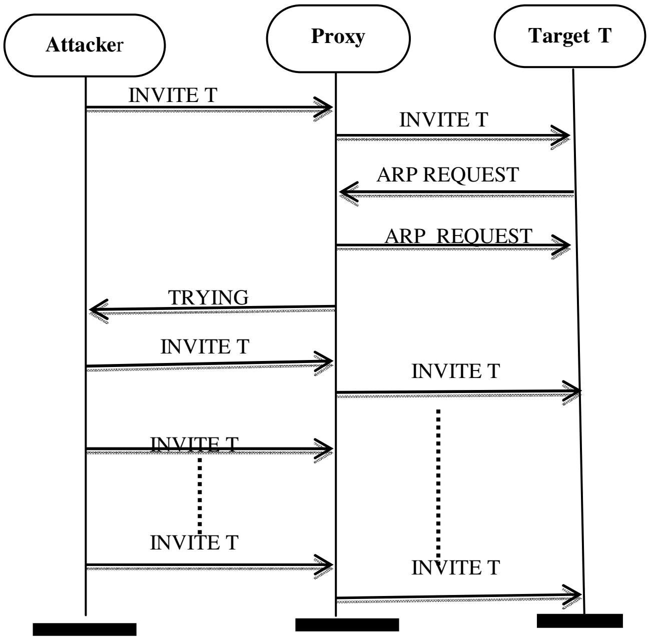

Figure 3. Flood with INVITE messages [6]

4. *PING Flooding Attack*

Ping message is used by SIP protocol in the application layer to check out the reachability of server, like SIP OPTIONs message. For security reason, a router or firewall do not allow (Internet Control Message Protocol) ICMP ping in many production network. However, ping message in application layer is allowed in VoIP systems for more reliable serviceability, but an attacker can misuse this message and can flood the SIP server with various ping messages. Beside of these major flooding attacks, an attacker can flood valid or invalid call control messages like SIP INFO, NOTIFY, Re-INVITE etc. after call set up [17].

A. Exploitable Resources by SIP flooding attack

The majority of DoS attacks is based on exhausting some of a server's resources and causing the server not to operate due to lack of resources. With SIP servers, there are three resources vulnerable to a Denial of Service attack: memory, CPU and bandwidth [7].

Memory: A SIP server needs to copy each received SIP request into its internal buffers to be able to process the message. The amount of buffered data and the time period the server is supposed to keep the buffered data varies depending on whether the server is working in a stateful or stateless mode which are described below:

– Stateless servers. Stateless servers need only to maintain a copy of the received message while processing it. As soon as the destination to which a message is to be sent to is determined and the message sent out, the server can delete the buffered data.

– Stateful servers. In general we can distinguish between two types of state in SIP:

* Transaction state. This is the state that a server maintains between the start of a transaction, i.e., receiving a request and the end of the transaction, i.e., receiving a final reply for the request. A transaction stateful server needs to keep a copy of the received request as well as the forwarded request.

* Session state. In some scenarios servers may need to maintain some information about the session throughout the lifetime of the session. This is especially the case for communication involving firewall or Network Address Translation (NAT) or for special accounting and security reasons as is the case for the 3GPP architecture.

CPU

After SIP message is stored in internal buffer of SIP server, the SIP server needs do some processing (e.g., authentication or destination address lookup etc.), perform transaction mapping and forward the message. Depending on the content and type of the message and server policies, the actual amount of CPU resources might vary. The CPU resource can become scarce if a huge amount of SIP requests are flooded at the SIP proxy server [18].

Bandwidth

This causes overloading the access links connecting a SIP server to the Internet to such a level as to cause congestion losses. By overloading the server's access links, one could cause the loss of SIP messages which causes longer session setup times or even the failure of session setups [7].

B. Detection Techniques for SIP flooding Attacks

Citation	Year	Technique	Advantages
[15]	2013	SIP–VoIP Anomaly Detection using a Stateful Rule Tree	• Provides higher detection accuracy, • Wider detection coverage • Faster detection than existing approaches
[19]	2013	Hybrid (anomaly and misuse) SIP flooding attack detection algorithm,	• High detection accuracy and high completeness • Ability to detect different types of SIP flooding attacks with lower false alarms rate. • It estimates the attack type that could help in prevention process.
[9],[16],[14]	2012,2009, 2008	Sketch-Based SIP Flooding Detection Using Hellinger Distance	• High detection accuracy even for low-rate flooding. • Robust performances under multi attribute flooding. • The ability to track the period of attack.
[5],[9],[16]	2011,2012,2 009	Wavelet analysis based detection using Sketch technique	• Quickly and accurately detect the attack. • The detection is independent of how many users exist in the network.
[17]	2011	Novel low rate detection scheme using area under curve of monitored dynamic SIP	• This technique achieves advantages of accuracy, fast, light weight, and Flexibility to deal with DDoS attack detection.
[8]	2006	Detection using Finite-state machine	• In this, system is implemented as an external program or network node, and therefore can work with most existing SIP applications. • Effective in detecting invalid message flooding and DRDoS attacks, as both types of attack cause errors in transaction and application layers in the target host.

V. CONCLUSION

In this paper, we have presented a deep analysis of the security concerns of the VoIP technology due SIP flooding attack. As SIP plays an integral part in current and future real time Communication networks, protection of SIP networks from different types of attacks is essential.

Firstly, we have presented a brief overview about the basics of the VoIP technology. Then, we have discussed the Background of SIP protocol and then we discussed various flooding attacks.

There are generally four different classes of DoS Flooding attacks against a SIP infrastructure: INVITE Flooding, Registration Flooding, Authentication Flooding and PING Flooding Attacks. These attacks exploit or deplete various resources of the system including memory, CPU & bandwidth and by enabling authentication on a SIP server means more processing resources are required to process each incoming request, which makes it easier to deplete CPU resources. At end we described various detection techniques year wise with their advantages in tabular format.

VI. REFERENCES

[1] D. Sisalem, J. Kuthan, T. Elhert," Denial of Service Attacks Targeting SIP VoIP Infrastructure: Attack Scenarios and prevention Mechanisms", IEEE Network, Page No (26-31), Oct 2006.

[2] Jan Stanek, Lukas Kencl, and Jiri Kuthan" Characteristics of Real Open SIP-Server Traffic",Springer , Page No (187-197) ,2013.

[3] ITU, Draft Revised Recommendation H.323 V5, Geneva, 20-30, May 2003.

[4] H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[5] Jin Tang and Yu Cheng, "Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks", IEEE ICC, Page No(1-5), 2011.

[6] D. Geneiatakis, A. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert, D. Sisalem," Survey of security vulnerabilities in Session Initiation Protocol", IEEE Communications Surveys and Tutorials, Volume-8,Issue-3,Page No(68-81), 2006.

[7] S. Ehlert, G. Zhang, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, and D. Sisalem, "Two layer Denial of Service prevention on SIP VoIP infrastructures", Elsevier, Computer Communications, Page No(2443-2456),2008.

[8] E. Y. Chen, "Detecting DoS attacks on SIP systems", 1st IEEE Workshop on VoIP Management and Security, Page No(53–58), April 2006.

[9] Jin Tang, Yu Cheng and Yong Hao," Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks",IEEE INFCOM,Page No(1161-1169),2012.

[10] Rafique, M.Z., Ali Akbar, M. Farooq., "Evaluating DoS Attacks against SIP-based VoIP Systems",IEEE GLOBECOM, Page No(1-6),2009.

[11] 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.

[12] Ming Luo Tao Peng & Christopher Leckie,"CPU-based DoS Attacks Against SIP Servers", IEEE,Page No(41-48),2008 .

[13] Harish C. Sharma Sanjay Sharma Sandeep Chopra Pradeep Semwal "The Protection Mechanism against DOS and SQL Injection Attack in SIP Based Infrastructure", IJARCSSE,Volume-3,Issue-1,Page No(252-256),Jan 2013.

[14] H. Sengar, H. Wang, D. Wijesekera and S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance", IEEE Transactions on Parallel and Distributed Systems, Volume-19, Issue- 6, Page No(794-805), June 2008.

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

[16] Jin Tang, Yu Cheng, and Chi Zhou" Sketch-Based SIP Flooding Detection Using Hellinger Distance",IEEE GLOBECOM, Page No(1-6), 2009 .

[17] 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

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

[19] 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.

[20] Gaston Ormazabal, Sarvesh Nagpal, Eilon Yardeni, and Henning Schulzrinne "Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems", Springer,Page No(107-132), 2008.

[21] Housam Al-Allouni1,Alaa Eldin Rohiem , Mohammed Hashem Abd El-Aziz Ahmed, Ali El-moghazy ," VoIP Denial of Service Attacks Classification and Implementation", 26th NATIONAL RADIO SCIENCE CONFERENCE ,Page No(1-12),17-19 March 2009.

[22] Mahak Chowdhary, Shrutika Suri and Mansi Bhutani, "Comparative Study of Intrusion Detection System," Proc. International Journal on Computer Science & Engineering, 2011, vol. 2, Issue 4, pp. 197-200.

MANDEEP KAUR, She has received her B.E Degree from RGPV unversity , Bhopal in 2012. Now, she is pursuing her M.tech from Graphic Era unversity ,Dehradun .

DR. SANTOSH KUMAR, Received Ph.D. from IIT, Roorkee(India) on dated October 12, 2012, M.Tech. (Computer Science and Engineering) From Aligarh Muslim University, Aligarh (India) in 2007 and B.E in Information Technology from C.C.S. University, Meerut (India) in 2003. He has membership of ACM, IAENG, ACEEE, ISOC (USA), and published 16 research papers in National and International Journals/conferences in the field of Wireless Communication Networks, Mobile Computing and Grid Computing. He has successfully completed a consultancy project titled "MANET Architecture Design for Tactical Radios" of DRDO, Dehradun. Project No: Consultancy Project DPT-1002/2009-10 Dated 15/12/2009, under-supervision of Dr. S. C. Sharma, Associate Professor, IIT Roorkee, (India).

SWATI SHARMA, She has received her B.E Degree from RGPV unversity ,Bhopal in 2012. Now, she is pursuing her M.tech from Graphic Era unversity ,Dehradun .