ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Analysis of Various Attacks and Prevention of Dos Attack in P2PSIP Networks

Pooja Nandu[1] Narendra Shekoker[2]

Department Computer Enginerring, D.J. Sanghvi College of Engineering, Mumbai-400097, India[1]

Department Computer Enginerring, D.J. Sanghvi College of Engineering, Mumbai-400097, India[2]

Abstract: Recently, establishing a VoIP call using a P2P network instead of regular SIP-servers has been proposed; this novel approach to SIP-signaling is commonly referred to as P2PSIP. The main motivation for peer-to-peer (P2P) SIP is simple configuration, higher robustness and easy maintenance as compared to client-server SIP. However, these benefits come at the cost of security. Securing against adversary nodes which intentionally interrupt functionality of the network remains a major research problem. So evaluation of attacks is of utmost importance for enhancing security and standardization of P2PSIP network communication. In this survey we analyze the security challenges of using a P2P network as a substrate for SIP communication by analyzing the attacks that can be launched against them. The proposed system presents the evaluation of different attacks that can be launched against the services (access control, routing, bootstrap, storage, communication, and resource management) of P2PSIP architecture. Assessment of attacks using security parameters (integrity, confidentiality, non-repudiation, availability, authenticity) shows that out of all the attacks DOS attack is the most dangerous attack and multiple layer security mechanism is proposed to prevent the DOS attack. With these solutions, P2PSIP networks will be more robust against flooding DOS attacks.

Keywords: VOIP, SIP, P2PSIP, flooding DOS attack, multiple layer security

I INTRODUCTION

Voice-over-IP (VoIP) has gained importance in the last few years to a widely used application. During this process, the session initiation protocol (SIP) has evolved as a standard for signaling in multimedia connections [1]. The peer-to-peer session initialization protocol (P2PSIP) emerges as a complement to the session initialization (SIP) protocol where the SIP may fail due to technical, social, security problems that may arise. Some of the environments are small organizations without the technical resources to install their own server that do not want their internal communication to pass through external servers, limited or lack of connectivity ,ad-hoc groups, government censorship, or high scalability [2] .

P2PSIP relay on the P2P network where all the functions are handled in a decentralized way. The advocates of P2P-SIP state its quick setup, smooth, robustness against failure and smooth deployment as benefits compared to using servers used in SIP. To evaluate the worth or a probable business model for P2P-SIP is outside the scope. Instead, we focus on security in P2P-SIP networks.

The concept behind P2PSIP is that the location of a SIP User Agent (UA) (IP address and port number) is published not to a SIP Registrar, but in a Distributed Hash Table (DHT). This data is stored at other peers with peer identifiers (IDs) uncorrelated to the SIP UA. These peers, called replica nodes, reply to queries from any other peer looking for the UA. This makes the UA available for incoming VoIP phone calls and chat messages. However, the SIP UA has no control over knowing which peers have asked for its current location. Curious and malicious peers can perform a lookup for the SIP URI of the UA regularly. The IP addresses of the UA could then be mapped to geographic locations. Using this information, attackers could build location profiles of a user [8]. Even worse, attackers could crawl in the P2PSIP network and harvest location profiles of all participants.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Another privacy threat in P2PSIP is that replica peers can observe that communication is established between two SIP UAs and deduce knowledge about the social interaction of the two users. In this manner a number of attacks such as Man in the middle attack, fake routing attack, DOS attack, Id mapping attack, Sybil attack etc. can be launched against P2PSIP networks. Securing against attack is of prime importance for the P2PSIP network to function in required manner.

The proposed scheme tries to evaluate the different attacks on security requirements such as (integrity, confidentiality, non-repudiation, availability, authenticity) and verifies the most dangerous attack. Layered security mechanism is proposed to prevent the most dangerous DoS attack from hampering the working of P2PSIP network.

The remainder of this paper is organized as follows. We briefly review related work in Section II and then discuss the attacks that can be launched against P2PSIP architecture in section III. Section IV presents the overview of attacks and evaluation of different attacks. Section V describes DOS attack in P2PSIP network and an approach to prevent DOS attack. Section VI illustrates analysis of the proposed system and Section VII concludes this paper and points out future research directions.

II RELATED WORK

A significant amount of research has been done identifying security problems in structured peer-to-peer networksP2PSIP infrastructures are exposed to multiple security attack [7].We can typically consider (1) attacks targeting the P2P overlay network, such as Sybil attacks, routing attacks (2) attacks related to the signaling protocol, such as caller ID spoofing, call hijacking, and SPIT attacks, and (3) attacks targeting the media transport protocols, such as eavesdropping attacks.

H. Song, X. Jiang and M. Matuszewski proposed a

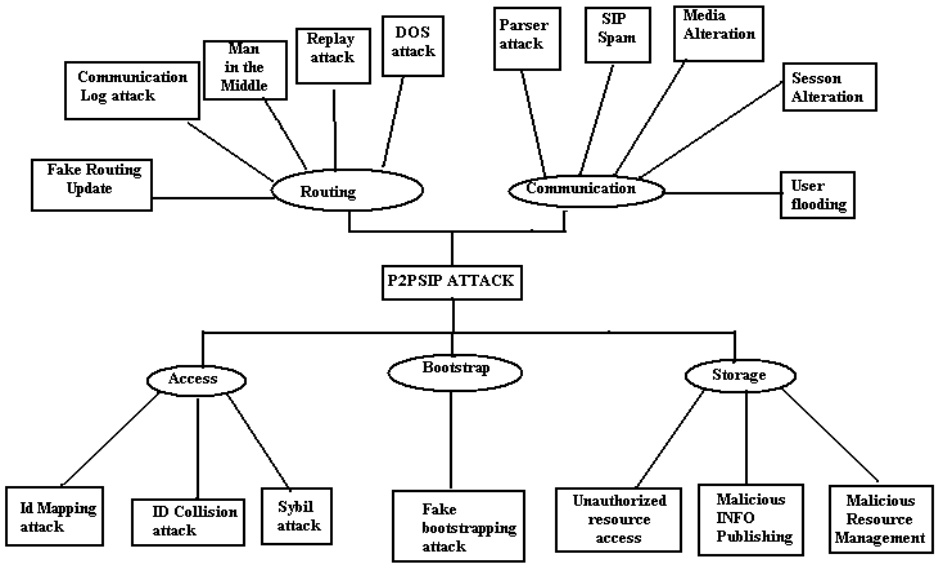

Fig. 1.1 Attacks against P2PSIP Networks

paper Security requirements in Peer-to-Peer Session Initiation Protocol (P2PSIP) in which they outlines the security requirements for a Peer-to-Peer Session Initiation Protocol (P2PSIP) overlay network [3].

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Roger Wattenhofer in his research Attacks on Peer-to-Peer Networks[4] has collected information about possible attacks on P2P network and tried to organize them as well as study the different various defense mechanisms. A defense mechanism based on pricing is proposed for DOS attack.

Pete Perlegos in his research Structured Peer-to-Peer Networks, Pete Perlegos proposes distributed approach to protect against DoS attack. This is done by collaboration of various other members of a structured peer-to-peer network [5].

Sven Ehlert, Dimitris Geneiatakis, Thomas Magedanz proposed a research Survey of network security systems to counter SIP-based denial-of-service attacks [6] .They explain three different types of DoS attacks on P2PSIP networks, called P2PSIP messag payload tampering, P2PSIP message flow tampering and P2PSIP message flooding.

To understand the attacks category wise, Jan Seedorf1, Frank Ruwolt, Martin Stiemerling and Saverio niccolini conducted a emulative study in their research Evaluating P2PSIP under Attack: An Emulative Study [7].

After the comparison done by Jiang and song, Jose M. sierra, andhenning schulzrinne presented a paper survey of attacks and defenses on P2PSIP communications in which they analyze the security of the system by studying attacks that can be launched attacks against them [8]. For each possible attack they review the defense mechanism that can be used to prevent the attack. They unlock the new challenges in world of P2PSIP network.

III ATTACKS LAUNCHED AGAINST P2PSIP ARCHITECTURE

This study conducts an analysis of the attack based on the architecture services, and identifying different categories of attacks as seen in Fig 1.

- **Bootstrap:** Bootstrapping is the process through which a node contacts other nodes (or servers) already connected to the network in order to initialize its status and be able to operate within the system. During this process, among other actions, the new node places itself in the location of the network indicated by its node ID, informs its neighbors about its presence in order to initialize its routing table and to store the resources it is responsible for [4].
  Attacks launched against Bootstrap service: Fake Bootstrapping attack

- **Routing:** The routing service is in charge of delivering all the messages exchanged between the nodes of a P2PSIP network. These messages range from users' contact information requests/answers to control and informational messages to maintain the overlay.
  Attacks launched against Routing service: Communication **L**og attack, Man in the Middle attack, Fake Routing Table attack, DOS attack, Replay attack.

- **Storage:** The storage service saves the contact information of the network's users in order to permit them to communicate with each other. Unlike client-server networks where this task is performed by a dedicated server, in P2P networks it is distributed among the nodes of the system. Also, it is responsible for storing private and public users' resources such as voicemail messages, public certificates, etc.
  Attacks launched against Storage service: Malicious Info Publishing, Unauthorized Resource attack, Malicious Resource Management.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Sr. No.	Attack name	Confidentiality	Integrity	Availability	Authenticity	Non-repudiation
1.	Sybil attack	No	Yes	Yes	No	No
2.	Id Collision attack	No	No	Yes	Yes	Yes
3.	Fake Boot strapping Attack	Yes	Yes	Yes	No	No
4.	Fake Routing Updates	No	No	Yes	No	Yes
5.	Man in the Middle	Yes	Yes	Yes	No	No
6.	Communication on Log Attack	Yes	No	No	Yes	No
7.	DOS attack	Yes	Yes	Yes	Yes	Yes
8.	Unauthorized Resource Access	No	No	Yes	Yes	Yes
9.	Malicious Contact Publishing	No	Yes	No	No	Yes
10.	SIP spam	No	No	Yes	No	No

Table 1: Evaluation of different P2PSIP network

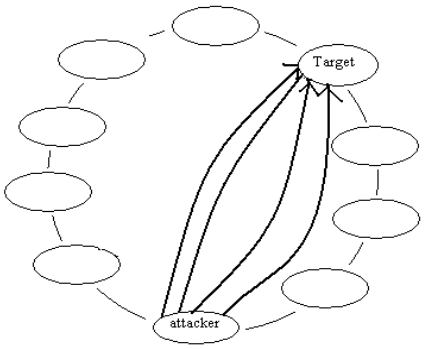

Fig. 2 DOS Flooding

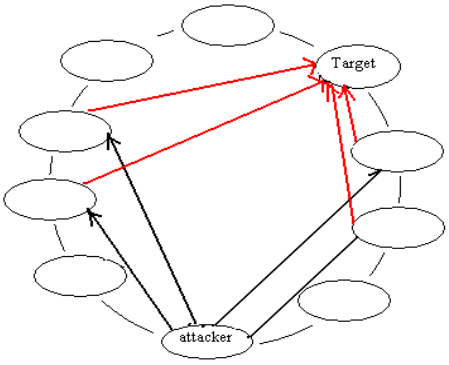

Fig. 3 DDOS Flooding Attack

- **Access Control:** Access control is the service in charge of deciding which users are allowed to join the system, and use its resources, and which ones are not. Once this decision has been taken, the service must assign a unique ID to each user that identifies it within the network. Also, it should link the user ID with its permissions on the system's resources. Without a robust access control system, the whole security of a P2PSIP network can be compromised.

Attacks launched against access control service:

ID Collision, Sybil attack, ID Mapping attack.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

IV EVALUATION of ATTACKS USING EVALUATION PARAMETERS

Evaluation of attack based on security parameters is carried out in Table 1 to show the most dangerous attack.

The various evaluation parameters are:

1. **Confidentiality:** It refers to averting the unveiling of information to unauthorized individuals or system

2. **Integrity:** In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle

3. **Availability:** For an information system to serve its objective, the information must be accessible when it is desired.

4. **Authenticity:** In E-business, information security and computing it is imperative to assure that the data transactions, documents and communications (electronic or physical) are etch.

5. **Non-repudiation:** It entails one's motive to fulfill their obligations to a contract. It also signifies that one party of a transaction cannot refuse that he has received a transaction nor can the other party deny that he has sent a transaction.

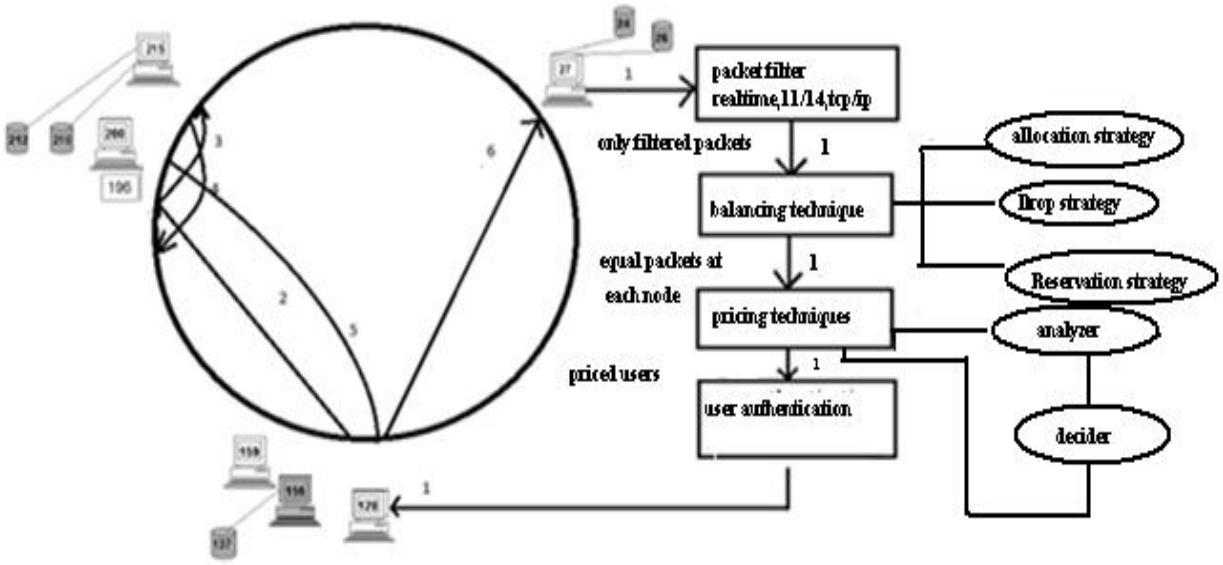

Fig.4: DOS Defense System Architecture

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Table 1 shows the possible attacks and the security parameters at risk; where yes indicates that parameter is affected and no indicated parameter is not affected. The attacks in P2PSIP network are analyzed on the basis of which security requirement such as confidentiality availability, integrity, authenticity and non-repudiation is affected by the possible attacks Thus we see that only in DoS attack all the five security parameters are hampered and hence we are in a position to analyze that the DOS attack is the most malicious attack that can be launched against P2PSIP networks. The strength of the attack and the damage it could cause is always known by the security requirements it affects. We analyze each and every possible attack in the P2PSIP network and have concluded that DOS and DDOS attack are the most dangerous attacks.

2. DOS and DDOS ATTACK in P2PSIP Network

One of the most famous and difficult to defend, attack that can be launched against an information system is the DoS (Denial of Service) attack or its large scale distributed DDoS (Distributed Denial of Service). The intention of a DoS attack is, as its name indicates, to prevent the victim or victims from accessing or providing services within the network. As shown in fig.2 in a DoS Flooding Attack, an attacker, or a coalition of them, saturates the victim's resources by flooding it with queries [4].

As shown in fig.2 the attack can be launched sending directly the queries to the victim or using other innocent users to amplify the attack by, for example, routing the queries to the victim through them using recursive routing or sending them queries with the victim node as source so that the replies from the innocent nodes flood the victim. Thus a new defense mechanism of multiple level securities is proposed which will protect the P2PSIP network against DOS and distributed DOS attack. With these solutions, ge neral SIP networks will be more robust against flooding DoS and Distributed DoS attack.

V PROPOSED SYSTEM

While to some degree the threat can be minimized by deploying a robust and hardened implementation (efficient parser, parallel processing, consequent authentication ...), this would not be able to cover the full scope of the DOS threat. Eventually, there is no other way than intelligent, external monitoring of the SIP traffic flow. In the end, this is how we want to target the DOS threat with our solution approach: we develop individual monitoring algorithms1, with each algorithm concentrating on a narrow scope of the DOS problem, and thus developing a strategy how this problem can be mitigated by monitoring network traffic flows. All algorithms analyze the network traffic to detect a certain DOS pattern.

1. FEATURES OF PROPOSED ARCHITECTURE

The architecture features of the diagram shown in Fig. 4 is discussed as below

1.1 Multi-layered architecture

The task of traffic monitoring has been split into individual and independent components. At the lowest layer, the filter- and scanner node ("Filter") intercepts all raw traffic and outputs re-assembled SIP messages. The actual analysis of the traffic for malicious requests is done in the analysis layer ("Analyzer"). It includes a SIP parser and performs local operations. Multiple Analyzers can operate in parallel, with the Filter forwarding only a subset of the traffic data to each Analyzer. To merge the input that come from multiple Analyzers, it is the responsibility of the decision node ("Decider") to take all the input from all local Analyzers and then decide on a global action, e.g. a user notification or a change in the firewall configuration. The firewall is part of the Filter.

1.2 Delayed reaction

For scalability reasons, the Filter does not take immediate actions whenever a packet is encountered. Running through the full stack of all nodes, i.e. Filter, Balancing, pricing and cryptography and firewall update would result in increased processing delays. Instead, whenever a packet is encountered, it is duplicated. One instance is forwarded to the Analyzer, while the other instance is passed on in the network.

2. DETAILS OF THE PROPOSED SYSTEM

2.1 Filter

The Filter is probably the most crucial component of the whole architecture for delivering real

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

time behavior. Its primary purpose is to fork incoming and outgoing traffic towards the Analyzers (scanning). Its second task is to apply filtering rules to all incoming traffic. For outgoing traffic from the protected proxy forking is also applied, with one copy as input for the Analyzers, and another copy send out to the internet, where it is routed normally. Filtering is not applied to outgoing traffic.

The Filter differentiates them according to the packets. Passing messages also undergo inspection by the firewall. The firewall is controlled by rules generated at the Decider. Rules consist of conditions and an action to be taken, if the conditions are met. A condition can be any IP, UDP, TCP or ICMP property. Additionally, a condition may be a regular expression, which is applied to a SIP message. Thus, it is possible to decide about a message by its SIP properties.

2.2 Balancing techniques:

Different balancing techniques are studied to prevent DOS attacks based on query floods:

- ***Incoming Allocation Strategies (IAS):***

IAS determines how many queries a node should accept from each peer (node/client) per time unit. Two options are studied: *Weighted IAS* (the number of queries accepted from a particular incoming link is proportional to the total number of queries arriving on that link) and *Fractional IAS* (each node is given an equal fraction of query bandwidth).

- ***Incoming Allocation Strategies (IAS):***

IAS determines how many queries a node should accept from each peer (node/client) per time unit. Two options are studied: *Weighted IAS* (the number of queries accepted from a particular incoming link is proportional to the total number of queries arriving on that link) and *Fractional IAS* (each node is given an equal fraction of query bandwidth).

- ***Drop Strategies (DS):***

If the amount of queries received from a remote peer is bigger than its allocation, DS determines which queries are accepted and which ones are discarded. Four strategies are presented: Proportional (the probability of acceptation of a query is proportional to the number of times it is received), Equal (all the queries have the same probability of being accepted), and PreferHighTTL (accept queries with the highest TTL), PreferLowTTL (accept queries with the lowest TTL).

2.3 Pricing

The pricing technique is used to limit the speed at which nodes send queries to other nodes of the network. When a node A sends a query to other node B in the network, B responds with a computational puzzle B will not process A's query until it receive a valid response to the puzzle.

- ***Analyzer :***

The Analyzer is the bottom half of the intelligence of the detection architecture. It analyses incoming traffic from the balancer. Analyzers are to decide about the start of an attack, its status and its end. If any attack parameters are encountered the message is transmitted to decider for further evaluation. Analyzers are running in parallel to allow easy scaling of the analysis load, which depends on the number and complexity of the deployed detection algorithms, as well as on the expected network load situation. Results of the analysis run are forwarded towards the Decider.

- ***Decider :***

The Decider is the top half of the intelligence of the security architecture. It gathers the output from all Analyzers and decides about the actual attack situation. It hosts an entity for each detection algorithm, which is capable of correlating the output of its specific Analyzer bottom half function. The Decider itself can also be scaled up, by deploying a dedicated Decider for each algorithm.

The Decider receives incoming reports from the Analyzers and delivers them to the corresponding algorithm-specific Decider modules. Modules decide whether an attack has been launched, and what can be done to counter it.. In an attack situation, all traffic is still delivered to the Analyzers. Thus it is possible to decide when the attack is over, and to remove the previously created rules.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

2.4 User Authentication

User authentication can be used to uniquely identify the sender of the query and discriminate malicious users, therefore helping to limit the number of messages coming on a particular node which will help prevent DOS attack.

VI ANALYSIS OF PROPOSED SYSTEM

In the research proposed by Dr. Roger wattenhofer to prevent the dos attack only the pricing technique is used that is only puzzle or captcha will be given to the node so that it incurs a high cost of processing and that makes it difficult to launch dos attack . In this proposed system pricing is implemented using the captcha and many more methods are implemented which will reduce the number of request coming at one node.

Pete perlegos in his work has suggested that only a limited number of nodes should be allowed in the network and The solution presented is a multilayered architecture which includes the filter, analyzer, decider, pricer, and authenticator. The filter first filters the packet according to the IP address or node id so a large amount of request will be suppressed .Then comes the balancer which balances the request on each node so that one particular node is not heavily loaded .thus when a node is not heavily loaded DOS attack will not take place .the analyzer check the packet an analyzes if there is a attack or not .here it uses the pricing technique which is the captcha or puzzle. If the analyzer finds any clue of attack it tells the decider, the decider checks the IP packet and further decides that whether the packet should be allowed or not .finally the authentication technique is used to prevent any unauthorized user from having an entry in system.

Thus packets are suppressed and finally only a few packets are allowed to enter the system. We see that a huge number of request never come to one node .Hence the DOS and DDOS attack are prevented.

VII CONCLUSION AND FUTURE WORK

Message flooding attack can be prevented using current proposed system. By using multiple layer security there is no chance that unlimited messages will be arriving at a node and launch the DOS attack or DDOS attack. Number of messages is limited at each stage thus, eliminating the chances of attacker to launch DDOS and DDOS attack.

The researchers can perform test bed analysis for various P2PSIP networks and Integrate the proposed mechanism with SIP-optimized firewalls, which both support use of standards-based security and provide the best possible protection where system-wide standards-based security is not possible.

REFERENCES

1. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630.
2. D. A. Bryan, B. B. Lowekamp, and C. Jennings, "SOSIMPLE Serverless, Standards-based, P2P SIP Communication System," in *Proc. First International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications*, (Washington, DC, USA), pp. 42–49, IEEE Computer Society, 2005.
3. H. Song, X. Jiang and M. Matuszewski , "Diagnose P2PSIP Overlay Network Failure," *Network Working Group,internet draft*,2008
4. Roger Wattenhofer, "Attacks on Peer-to-Peer Networks," *Distributed Computing Group,Thesis Computer Science* 2005.
5. Pete Perlegos,"DoS Defense in Structured Peer-to-Peer Networks,"*Computer Science Division,University of California* , Berkely.2004
6. Sven Ehlert a, Dimitris Geneiatakis b, Thomas Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks," *computers & security*, vol.29, pp.225-245, 2010.
7. Jan Seedorf1, Frank Ruwolt, Martin Stiemerling and Saverio niccolini, "Evaluating P2PSIP under Attack: An Emulative Study," *IEEE GLOBECOM*, 2008.
8. Diego Suarez Touceda, Jose M. Sierra, Antonio Izquierdo, and Henning Schulzrinne, "Survey of Attacks and Defenses of P2PSIP Communications,"IEEE *Communications Surveys & Tutorials*, vol. 14, NO. 3, 2012.
9. Sven Ehlert, Dimitris Geneiatakis, Thomas Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks," *Final thesis,electr and information technology*,technician university,berlin,2009.