Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

SIP Flooding Attack Detection Using Hybrid Detection Algorithm

Ranjini.R[1], Malathi.L[2]
[1,2]*Department of CSE, Vivekanandha College of Engineering for Women,*

Abstract—The session initiation protocol is the signalling protocol,for controlling voice and video communication over the internet protocol.SIP is however designed with open structure vulnerable to security attak.The SIP flooding attack is the most severe attack becouse it is easy to launch and capable of quickly draining the resources of both network and node. The existing flooding detection schemes are either anomaly based or misuse based.The anomaly based scheme can detect unknown attack it does not need the proir knowledge of the attack,but it generates some false alarm,suffers from accuracy problem and gives false positive.Similarly the misuse based schemes have high detection accuracy,no false positive but it cannot detect unknown attack.To overcome problems in both detection schemes a hybrid detection scheme is proposed.the proposed hybrid scheme consist features of both anomaly based scheme and misuse based scheme,and it gives fast response,increase accuracy of detection and no false alarm

Keywords- SIP, Anomaly based detection, Misuse based detection.

I. INTRODUCTION

The Session Initiation Protocol (SIP) is an application layer protocol, used for signaling protocols specified by the Internet Engineering Task Force (ITF) (Schulzrinne and Rosenberg, 2000). SIP has recently become the main signaling protocol for Internet applications, thus allowing the implementation of a number of features using SIP, such as video conferencing, online gaming, peer-to-peer application, instant messaging, presence services and voicemail. Hotline services for emergency calls and online flight booking also use SIP.

SIP also supports mobile applications, which are more flexible applications than others. The protocol was derived from the Hypertext Transfer Protocol (HTTP); several aspects of SIP protocol resemble HTTP. SIP is also implemented in web services and e-mail. A full SIP URI (Uniform Resource Identifier) is shown as: SIP URI = SIP username@ (IP or domain).

SIP is text-based, which makes it simpler to understand than most bit-oriented protocols, where knowledge of the significance of each bit position according to the rules and syntax of the defined protocol is required. The Transport of SIP messages can be carried by transport-layer over IP protocols, such as SIP over UDP or TCP. The SIP messages used to establish and terminate sessions are basically INVITE, 200 OK, ACK and BYE. They are also called the SIP methods or attributes.

A UAC initiates a SIP session by sending out an INVITE. Intermediate proxies look over the destination SIP address in the message and forward it to the destined UAS who will respond with a 200 OK. An ACK message then finishes the three-way handshake to establish the session and media will go directly between the UAC and the UAS. When the session is finished, it will be terminated by a BYE message from either of the calling parties.

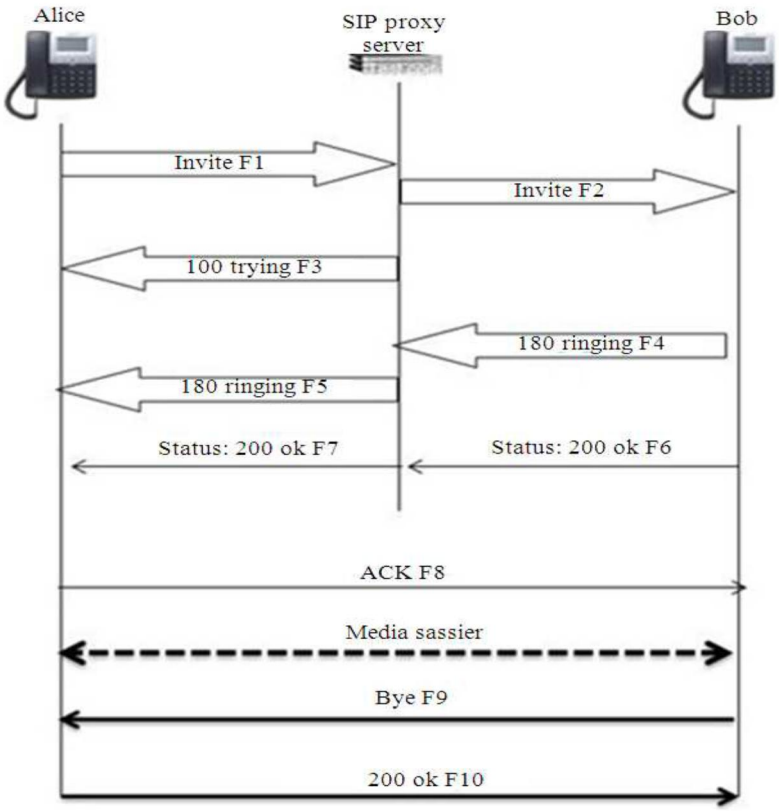

Figure 1. SIP process

II.RELATED WORKS

Generally, intrusion detection systems are classified into two major approaches, anomaly based and misuse based. The anomaly based approach builds models that represent normal behaviors on the network. Alarms are raised if the observed behaviors significantly deviate from the behaviors estimated by the model.

The main advantages of this approach are that a priori knowledge of attack strategy is not required and new anomalies unknown before can be detected.The Anomaly-based IDS might come up with several numbers of logs containing numerous network attacks which could possibly be a false positive.

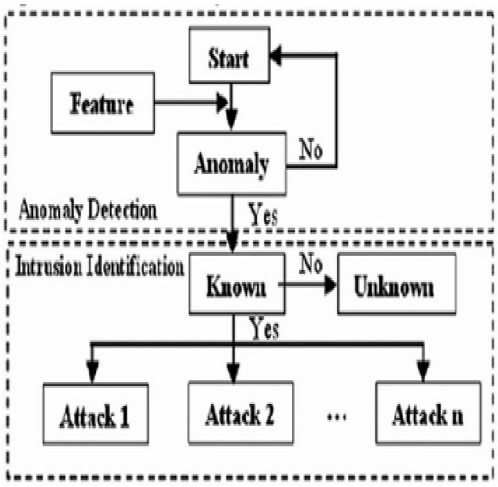

Figure2. Anomaly based detection technique.

Hellinger distance (HD) is used to find the deviation between two probability distribution. Let P and Q be two probability distribution on a finite sample space Ω where P and Q are N tuples (p1,p2, p3,....p_N) and (q1,q2 ,q3,....q_N) then the HD between P and Q is defined by

$$D^2{}_H(P,Q)=1/2\sum(\sqrt{p}+\sqrt{Q})2 \ (D^2{}_H=0 \text{ when } P=Q)$$

Cumulative sum algorithm (CUSUM) is a change point detection algorithm. Which belongs to the category of sequential test. CUSUM is a non parametric and stateless method. It can detect anomalies from the network based on inherent network protocol behaviors. Let $\Delta_n(n=0,1.....)$ be the number of request minus that of corresponding replays collected within one sampling period, Ŕ denotes the average number of replays, then $X_n=\Delta_n/Ŕ$ where X_n is a stationary random process under normal condition the mean of X_n denoted as c ,

$$X_n=X_n-a \quad \{\text{“a” is an upper bound of c}\}$$

The above expression have negative mean during normal operation. When DOS attack take place, Xn will suddenly increases and become a large positive number. The technique is very robust, generally applicable and deployment in much easier.

Adaptive Threshold algorithm is a straight forward and simple algorithm, which relies on testing whether the average of a given feature in a predefined time window exceeds a particular threshold. If X_n is the value of the feature in the nth time interval, and μ_n-1 is the estimated average of the feature from measurements prior to n, then the alarm condition is:

$$\text{If } X_n > (\alpha+1)\ \mu_n\text{-}1 \text{ then ALARM signaled at time n.}$$

$\alpha > 0$ is the amplitude factor, it indicates the percentage above the mean value that one considers to be an indication of anomalous behavior. The mean μ_n can be computed using an Exponentially Weighted Moving Average (EWMA) of previous measurements. Adaptive Threshold algorithm is used to detect the SIP flooding attack by checking the rate of SIP requests. Its performance varies significantly with the variation in attack metrics.

Most of these algorithms (Adaptive Threshold, CUSUM, and HD) are anomaly ones, they characterize the normal behavior and then seek for deviations. So these algorithms have no information about attacks types, they handle all attack types in the same way, making it impossible to have high detection accuracy for all attacks types. Make estimation about the next normal behavior depending on memorized quantity of previous samples. This memorized quantity brings up the attack masking and adaptation with attack problems

The misuse based approach profiles known attack patterns as signatures. Detection systems in this approach raise alert if the on-going traffic patterns match the profiled signatures. Misuse based Intrusion Detection System (IDS) helps in maintaining the integrity of data in a network controlled environment. Unfortunately, this type of IDS depends on predetermined intrusion patterns that are manually created. If the signature database of the Signature-based IDS is not updated, network attacks just pass through this type of IDS without being noticed.

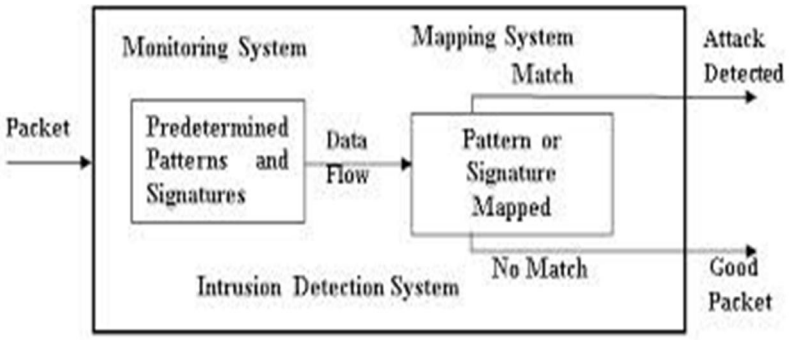

Figure3. Misuse based detection technique.

One big challenge of signature-based IDS is that every signature requires an entry in the database, and so a complete database might contain hundreds or even thousands of entries. Each packet is to be compared with all the entries in the database.

This can be very resource- consuming and doing so will slow down the throughput and making the IDS vulnerable to DOS attacks. Some of the IDS evasion tools use this vulnerability and flood the signature signature-based IDS systems with too many packets to the point that the IDS cannot keep up with the traffic, thus making the IDS time out and drop packets and as a result, possibly miss attack, this type of IDS is still vulnerable against unknown attacks as it relies on the signatures currently in the database to detect attacks.

Weighted Sum (WSUM) is misuse detection algorithm, it depends on a prior knowledge about attacks signature, it seeks for attacks signature in the incoming samples, this algorithm makes using attack effective time to detect the different types of SIP flooding attacks accurately.

The Honeycomb is a system that generate signatures for malicious network traffic automatically, pattern matching technique and protocol conformance checks are applied. The system is unique, it cannot read a database of signatures upon startup to match then against live traffic to spot matches. The system tries to spot pattern in the traffic previously seen on the honey pot. It uses longest common substring (LCS) algorithm to spot similarities in packet payloads, the LCS implementation is based on suffix tree. Each received packet causes honeycomb to initiate certain sequence of activities.

Pancake is a automated signature creator, solution for the manual signature creation. Through this system, signature will be created automatically. Before pancake can generate signature a module called log attribute selected module is implemented. Pancake will generate signature that is to be passed on and fed to the signature based IDS, The signature are generated based on non payload based detection rule.

Weighted Sum algorithm, Pancake, Honeycomb are existing misuse based detection method. The WSUM suffer from adaption with threshold setting. Pancake and Honeycomb have delay in their response.

III. PROPOSED ALGORITH

The proposed Hybrid detection algorithm have the features of both anomaly based and misuse based algorithm. The main idea of the proposed detection algorithm is full monitoring for SIP server behavior during operation. The monitoring is based on simultaneous observation of three parameters (attack rate, percentage of served requests, and average response time).

Depending on a previous knowledge about attacks signature, it seeks for attacks signature in the incoming requests, average of response delays, and percentage of served requests every second, and then it defines three dynamic thresholds to detect intrusions. No prediction about normal behavior is done, and inspection which is done on the current requests is not related to the previous ones. When SIP server is attacked, the algorithm will detects the different attack types of SIP flooding accurately.

We can summarize the steps of new method as following:

Calculate by counting the requests that arrive to the server, where is number of incoming requests (normal traffic is merged with attack traffic) to SIP server per second.

Distinguish source of that incoming requests depending on inspection operation in every request that arrives to server and determine source IP address of request sender.

Identify threshold for R_{incom} called TH_R depending on relationship between the attack effective time and attack effective rate.

Calculate P_{serv}, that indicates percentage of served requests per second, and it is given

$$P_{serv}=\text{Served Req/Total Incoming Req}$$

Identify threshold for P_{serv} called TH_P depending on behavior of SIP server when it is attacked by different types of flooding attacks.

Calculate T_{avg}, that indicates mean value of server request/response delays in seconds, and it is given by

$$T_{avg}=\sum_{i=1}^{N} SRD_i/N$$

Where SRD is the server response delay. N is the total number of outcoming from SIP server

Identify threshold for T_{avg} called TH_T depending on behavior of SIP server when it is attacked by different types of flooding attacks.

The system raises an alarm when all of the followings are true:

$$R_{incom} > TH_R$$

$$P_{serv} < TH_P$$

$$T_{avg} > TH_T$$

The new algorithm can detect all different flooding attack types. If the values of the compared three features with the three thresholds values are satisfied simultaneously, the algorithm will launch an alarm as indication of flooding attack.

IV. CONCLUSION

The proposed Hybrid detection algorithm has the ability to detect different types of SIP flooding attacks with lower false alarms rate, rapid response and high detection accuracy. The detection algorithm combine the features of both anomaly based and misuse based detection system, and perform full monitoring of the SIP server. It does not suffer from the attack masking, adaptation

with attack, negative change and adaption with threshold setting problems. Moreover, it estimates the attack type that could help in prevention process

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, IETF Network Working Group, 2002*

[2] H. Schulzrinne, S. Narayanan, J. Lennox, and M. Doyle, "SIPstone- benchmarking SIP server performance", Technical *Report, Department of Computer Science, Columbia University, New York, 2002*.

[3] H. Wang, D. Zhang, and K. Shin, "Change-Point Monitoring for the Detection of DoS Attacks", *IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 4, Oct.-Dec., 2004.*

[4] E. Chen, "Detecting DoS attacks on SIP systems," *in 1st IEEE Workshop on VoIP Management and Security, P 53–58, 2006.*

[5] Husam Al-Alouni, "An Intrusion Detection Approach to Computer Networks", *master of science thesis, military technical college, Cairo, 2003.*

[6] Vijay Katkar S. G. Bhirud," Novel DoS/DDoS Attack Detection and Signature Generation", *International Journal of Computer Applications (0975 – 888),Volume 47– No.10, June 2012*

[7] Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents" .*International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.*

[8] Lata, Kashyap Indu," Novel Algorithm for Intrusion Detection System", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013

[9] H. Sengar, D. Wijesekera, H. Wang and S. Jajodia, "VoIP Intrusion Detection Through Interacting Protocol State Machines," *Proc. IEEE International Conference on Dependable Systems and Networks,2006*

[10]E. Chen, "Detecting DoS Attacks on SIP Systems," *Proc. 1st IEEE Workshop on VoIP Management and Security, 2006.*

[11]D. Sisalem, J. Kuthan and S. Ehlert, "Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms," *IEEE Network*, vol. 20, no. 5, pp. 26-31, Sept.-Oct.2006.

[12]J. Tang, Y. Cheng and Y. Hao, "Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks," *Proc. IEEE INFOCOM, 2012*

[13]Husam Al-Alouni, "security of voice over internet protocol", *PhD of science thesis, military technical college, Cairo, 2010.*

[14]Xianglin Deng and Malcolm Shore, "Advanced Flooding Attack on a SIP Server", *In Proceedings of the The Forth International Conference on Availability, Reliability and Security, Fukuoka, Japan, March 2009.*

[15]B. Rozovskii, A. Tartakovsky, R. Bla˘zek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods*", IEEE Transactions on Signal Processing, 2006.*

