Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 12, December -2016

Denial of Service Flooding Attack Protection Mechanism in Session Initiation protocol By Hybrid Detection Algorithm

Sinju N S, [2]Ranjini Ramachandran, [3]Amrutha H Hingmire

[1,3]Asst.professor Computer Department, RSCOE,Pune

[2]PG Scholar, RSCOE,Pune

ABSTRACT- *The session initiation protocol (SIP) is widely used for controlling multimedia communication session over the internet protocol. Denial of service attacks are the main concern causing loss of multimedia availability. Its impact ranges from decreasing of service level to complete loss of service. Effectively detecting a flooding attack to the SIP proxy server is critical to ensure robust multimedia communication session over the internet. The existing SIP flooding detection schemes are either anomaly based or misuse based. The anomaly based detection scheme uses Hellinger Distance algorithm (HD), Cumulative Sum algorithm (CUSUM), Adaptive Threshold algorithm, etc to detect anomaly. The anomaly based scheme can detect unknown attack it does not need the prior knowledge of the attack, but it generates some false alarm, suffers from accuracy problem and gives false positive. Similarly the misuse based scheme uses Weighted Sum algorithm (WSUM), Expression matching method for the detection. These algorithms have high detection accuracy, no false positive but it cannot detect unknown attack. To overcome problems in both SIP flooding 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- *Session initiation protocol, Network security, Anomaly based detection, Misuse based detection.*

I. INTRODUCTION

The Session Initiation Protocol (SIP) is an application layer protocol, used for multimedia communication [7]. The Transport of SIP messages can be carried by transport layer over IP protocols, such as SIP over UDP (User Datagram Protocol) or TCP (Transmission Control Protocol). 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 SIP messages used to establish and terminate sessions are basically INVITE, 200 OK, ACK and BYE [8] as shown in Figure 1.1. They are also called the SIP methods or attributes. A UAC (User Agent Client) 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 (User Agent Server) 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.

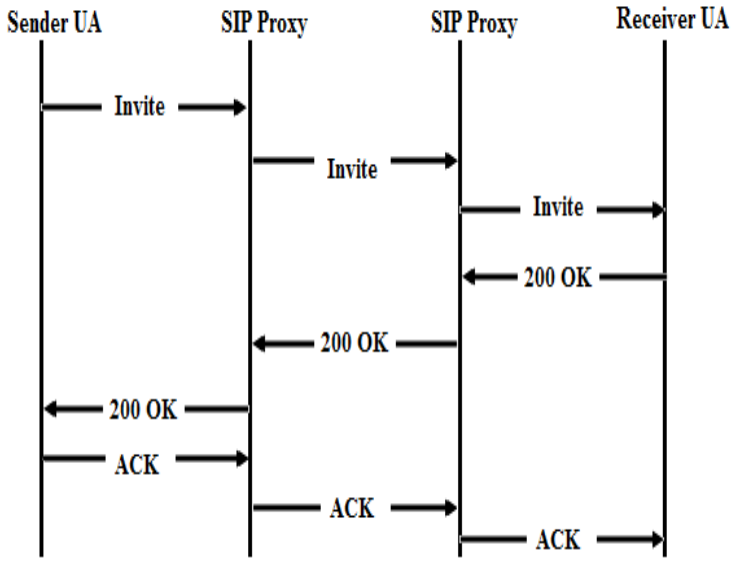

Figure 1. SIP Session Establishment

SIP also supports mobile applications [5], which are more flexible applications than others. The protocol was derived from the Hypertext Transfer Protocol (HTTP), several features 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).

II. RELATED WORKS

SIP is designed with open structure due to its openness vulnerable to security attack. The SIP flooding attack is the most severe attack because it is easy to launch and capable of quickly draining the resources of both network and node. The attack disrupts perceived quality of service (QoS) and subsequently leads to denial of service (DoS). The existing SIP flooding detection schemes are either anomaly based or misuse based.

The anomaly based approach builds models that characterize normal behaviors on the network. Alarms are raised if the observed behaviors significantly deviate from the behaviors estimated by the model. The anomaly based scheme can detect unknown attack it does not need the prior knowledge of the attack, but it generates some false alarm, suffers from accuracy problem and bounces false positive.

Likewise the misuse based schemes raise alert if the ongoing traffic patterns match the profiled signatures. It has high detection accuracy, no false positive but it cannot detect unknown attack, throughput of the system will decreases.

2.1 SIP Flooding Detection Schemes

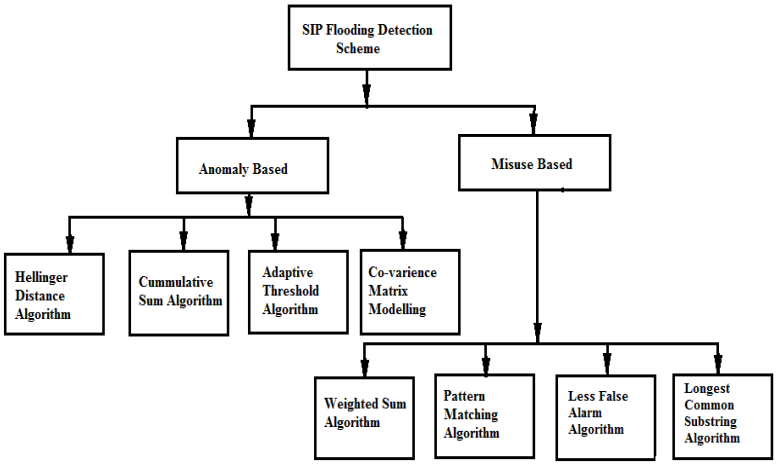

Figure 2.1 SIP Flooding Detection Schemes

2.1.1 Hellinger Distance Algorithm

Hellinger distance is used to find the deviation between two probability distribution [9]. 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,

$$D_H^2(P,Q) = \frac{1}{2}\sum\left(\sqrt{P} + \sqrt{Q}\right)^2$$

HD algorithm consists of training and testing phases. In the training phase, the normalized frequencies are $p_{INVITE,}$ $p_{200OK,}$ $P_{REGISTER}$ for INVITE, 200OK and REGISTER respectively. They are calculated over the training normal dataset. Similarly, the normalized frequencies are $q_{INVITE,}$ $q_{200OK,}$ $q_{REGISTER}$ are calculated in the testing phase for each time-window n or interval. The HD between these frequency distributions of two phases is,

$$= \left(\sqrt{p_{INVITE}} - \sqrt{q_{INVITE}}\right)2 + \left(\sqrt{p_{2000K}} - \sqrt{q_{2000K}}\right)2 + \left(\sqrt{p_{REGISTER}} - \sqrt{q_{REGISTER}}\right)2$$

HD

To keep track of the normal attribute behaviors more accurately, use a dynamic threshold for detection. The threshold value is a function of the average of observed HDs and their mean deviation. Such a dynamic setting of threshold makes an attack harder to evade. They employ the stochastic gradient algorithm to compute the dynamic threshold based on the HD observed during the previous training period. Fast estimators for average ν and mean deviation ε given measurement HD, are computed as follow,

Err= $HD_n - V_{n-1}$

V_n= $V_{n-1} + g \times Err$

n= $n - 1 + h \times (|Err| - n - 1)$

where HD_n is the current sample of the HD, V_{n-1} and V_n are the previous and current means of HD, respectively, $n-1$ and n represent the previous and current deviations.

During the testing periods, the Threshold (TH) is computed using the mean of HD and the mean deviation as following. $TH_n = X * V_n + y * n$

The purpose of the multiplication factors x and y is to get a safe margin for the setting of the threshold value, so that HD avoids false alarms without degrading its detection sensitivity. These two factors are adjustable parameters, and can be properly tuned during the training period.

2.1.2Weighted Sum Algorithm

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 AET (attack effective time) to detect the different types of SIP flooding attacks accurately. The algorithm defines a new attack parameter called Attack Effective Factor (AEF), and it equals to the inverse of AET.

This parameter introduces a quantized evaluation for the harm done by flooding attack into the server each second, as the AEF increases the danger of attack increases. Since the AEF for the different flooding attacks is already known, the algorithm can calculate the attack effect during Δt seconds, it is Δt*AEF. In other meaning, during Δt seconds, the attacked server is pushed by Δt*AEF value toward compromised state. For example, if AET value equals to 100 second, then during Δt = 5 second, the server will be loss 5 * 0.01 = 0.05 of its resources, this percentage of resources will be unavailable.

To keep trace of the attack effect, the Weighted Sum algorithm samples the incoming requests each Δt seconds. For each sample (i) it calculates the average request rate (λi), and then allocates the corresponding AETi and AEFi, finally it computes the sample effect (Δt*AEFi). At the sample (n), the attack effect can be computed by cumulating the previous samples effects, calculating Cumulative Attack Effect (CAE), given by,

$$CAE_n = \sum_{i=1}^{n} \Delta t * AEF_i$$

CAE_n reflects the server state at the time nΔt seconds, it expresses how much the server is pushed toward compromised state. When the server is in the normal state the CAE equals to zero. As the server is pushed towards the compromised state, the CAE increases, finally when the server is fully compromised the CAE will be equal to one.

PROBLEM STATEMENT

The open architecture of the Internet and the use of open standards like Session Initiation Protocol (SIP) constitute the provisioning of services (e.g., Internet telephony, instant messaging, presence, etc.) vulnerable to known Internet attacks. The security problems in the SIP protocol that may lead to denial of service. Such security problems include flooding attacks, security vulnerabilities in parser implementations, and attacks exploiting vulnerabilities at the signaling application level.

SIP flooding attack detection algorithms (anomaly and misuse) have several problems, these problems create an opportunity for an attacker to make undetectable harm. Generally SIP flooding detection schemes are either misuse based or anomaly based. Misuse detection approaches cannot detect unknown attack, it systematically scan the system for

occurrences of the patterns or signatures.So throughput of the system will decreases. While anomaly detection approaches attempt to detect intrusions by noting significant deviations from a normal behavior, but they generate false alarm.

III. PROPOSED WORK

The Hybrid detection algorithm calculate incoming request rate every second. It counts the received INVITE messages for the same destination within a certain amount of time. If there is a sudden surge of INVITE requests that exceed a predefined threshold, it is considered as a strong indication of flooding attack.

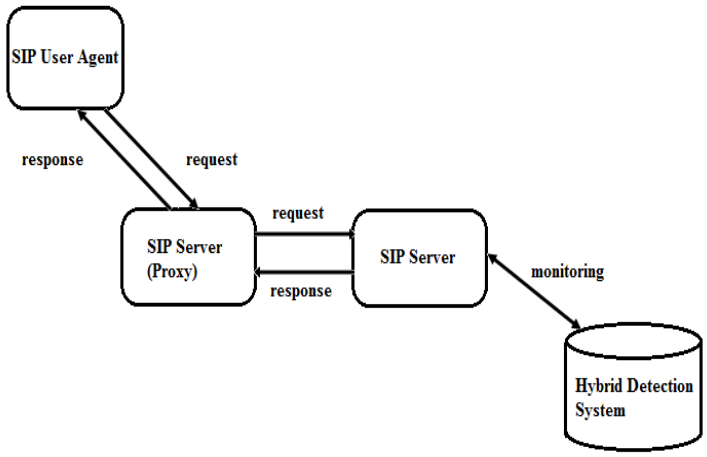

Figure 4.1 SIP system

The main idea of the proposed algorithm is full monitoring for SIP server behavior during operation,as shown in Figure 4.1. The monitoring is based on simultaneous observation of three parameters (attack rate,percentage of served requests and average response time.

No prediction about normal behavior is done, and inspection which is done on the current requests is not related to the previous ones. These features eliminate the chance for attack masking or adaptation with attack problems.

The proposed algorithm is given by,

- Calculate R_{incom} by counting the requests that arrive to the server, where R_{incom} is number of incoming requests (normal traffic is merged with attack traffic) to SIP server per second.
- 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 $P_{serv=}$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 $T_{avg}=\sum^{N}_{i=1} SRD_i/N$ 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.

$$R_{incom} > TH_R$$

$$P_{serv} < TH_P$$

$$T_{avg} > TH_T$$

IV. IMPLEMENTATION AND RESULT

The monitoring system will analyze the network traffic and capture the incoming request to the server and outgoing service from the SIP server. When the clients begin to request their services, at the same time the monitoring system begins to capture the traffic.

When SIP server is attacked, the algorithm will detect SIP flooding accurately. The Hybrid detection algorithms have the feature of Hellinger Distance algorithm and Weighted Sum algorithm. HD can used to model normal behavior, ie to check traffic statistically deviant as shown in figure 4.2. The Weighted Sum algorithm depends on a prior knowledge about attacks signatures, it seeks for attack signature in the incoming sample, it is used for rule matching.

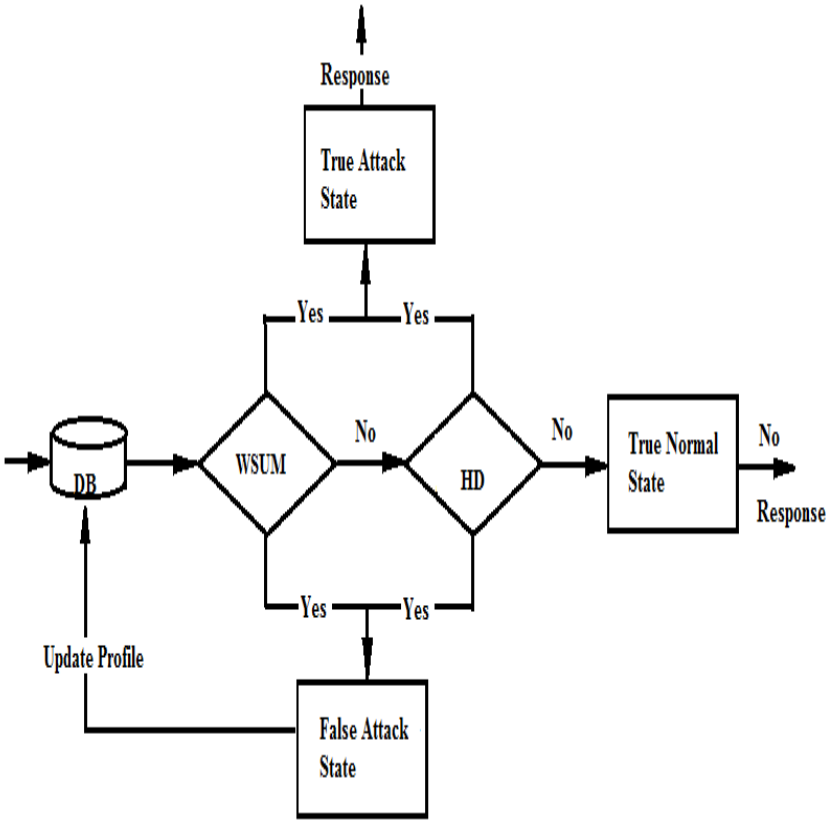

Figure 5.1 Hybrid System

The algorithm calculates incoming requests rate, average of response delay, and percentage of served requests, after that, it calculates the three threshold. 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.

The evaluation process is done using several simulated datasets. Each dataset represents the SIP requests. For each dataset, the detection completeness, false alarms rates, and the corresponding detection accuracy, and response rapidity are measured for the proposed algorithm, HD algorithm and the WSUM algorithm. The results are shown in Table (1).

Proposed algorithm has very high detection accuracy, and very high completeness, so it has minimum false alarms rate.

Table 1. Evaluation parameter for detection algorithm

parameter		**Proposed algorithm**	**HD**	**WSUM**
Accuracy	Dataset1	1	0.76	1
	Dataset2	1	0.83	0.98
	Dataset3	1	0.91	0.99
	Dataset 4	1	0.93	0.97
	Average	1	0.86	0.99
Completeness	Dataset1	1	0.99	1
	Dataset2	1	0.99	0.99
	Dataset3	1	0.99	1
	Dataset 4	1	1	0.98
	Average	1	0.99	0.99
Response Rapidity	Dataset1	0.16	0.04	0.50
	Dataset2	0.10	0.05	0.50
	Dataset3	0.11	0.05	0.50
	Dataset 4	0.07	0.09	0.50
	Average	0.11	0.06	0.50

V. CONCLUSION

The Hybrid detection algorithm for SIP flooding attack has the ability to detect different type of SIP flooding attack with lower false alarm rate. It is a hybrid (misuse and anomaly) detection algorithm which utilizes features of Hellinger Distance algorithm and Weighted Sum algorithm to detect SIP flooding attack. These features reflect effectiveness of the flooding attacks on the server performance as a signature which is used in the detecting process. It does not suffer from the attack masking, adaptation with attack, negative change and adaption with threshold setting problems. It can detect unknown attack with higher accuracy.

REFERENCE

[1] B. Rozovskii, A. Tartakovsky, R. Blaˇzek, 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.

[2] C. Kreibich, and J. Crowcrowft, "Honeycomb: Creating Intrusion Detection Signatures Using Honeypots," ACM SIGCOMM Computer Communication Review, vol. 34, no. 1, pp. 51-56, Jan. 2004

[3] De ocambo,Frances Bernadette ,Del castillo,ThrishamariL Gomez,miguel Alberto N "Automated Signature Creator For a Signature Based Intrusion Detection System With network Attack Detection Capability(Pancake) "The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012).

[4] Dimitrics geneitakis,nikosvrakas costos Lambrinoudais" Utilizing bloom filters for detecting flooding attacks against sip based service" computers & s e c u r xxx(2009)1-14

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

[6] 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.

[7] 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

[8] Jea-Tek Ryu, Byeong-Hee Roh and K i-Yeol Ryu," Detection of SIP Flooding Attacks based on the Upper Bound of the Possible Number of SIP Messages" KSII Transactions On Internet And Information Systems Vol. 3, No. 5, October 2009

[9] Jin Tang,Yu Cheng,Yong Hao and Wei Song "SIP Flooding attack detection with a multi dimensional sketch design"IEEE Transaction on dependable and secure computing.2014

[10] Ki yeol rayu,jv wan kim and byeong-hoe-roh "White- list based sip flooding attack detection using a Bloom filter"

[11] 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

[12] 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

[13] R. Schweller, Z. Li, Y. Chen, Y. Gao, A. Gupta, Y. Zhang, P. Dinda, M. Kao and G. Memik, "Reverse Hashing for High-Speed Network Monitoring: Algorithms, Evaluation, and Applications," Proc. IEEE INFOCOM, 2006

[14] Rahul, S.K.Prashanth, B.Suresh kumar,G.Arun" Detection of Intruders and Flooding In Voip Using IDS, Jacobson Fast And Hellinger Distance Algorithms*"* IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278 0661 Volume 2, Issue 2 (July-Aug. 2012).

[15] 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

