International Journal of Hybrid Information Technology
Vol.7, No.5 (2014), pp.257-272
http://dx.doi.org/10.14257/ijhit.2014.7.5.24

SIP Flooding Attacks Detection and Prevention Using Shannon, Renyi and Tsallis Entropy

Reihaneh Haji Mahdizdeh Zargar* and Mohammad Hossein Yaghmaee Moghaddam

Department of Computer Engineering, Ferdowsi University of Mashhad (FUM)
Mashhad, Iran
re.mahdizadeh@stu.um.ac.ir, yaghmaee@ieee.org

Abstract

Voice over IP (VOIP) network, also known as Internet telephony, is growing increasingly having occupied a large part of the communications market. With the growth of each technology, the related security issues become of particular importance. Taking advantage of this technology in different environments with numerous features put at our disposal, there arises an increasing need to address the security threats. Being IP-based and playing a signaling role in VOIP networks, Session Initiation Protocol (SIP) lets the invaders use weaknesses of the protocol to disable VOIP service. One of the most important threats is denial of service attack, a branch of which in this article we have discussed as flooding attacks. These attacks make server resources wasted and deprive it from delivering service to authorized users. Distributed denial of service attacks and attacks with a low rate can mislead many attack detection mechanisms. In this paper, we introduce a mechanism which not only detects distributed denial of service attacks and low rate attacks, but can also identify the attackers accurately. We detect and prevent flooding attacks in SIP protocol using Shannon (FDP-S), Renyi (FDP-R) and Tsallis (FDP-T) entropy. We conducted an experiment to compare the percentage of detection and rate of false alarm messages using any of the Shannon, Renyi and Tsallis entropy as a measure of disorder. Implementation results show that, according to the parametric nature of the Renyi and Tsallis entropy, by changing the parameters, different detection percentages and false alarm rates will be gained with the possibility to adjust the sensitivity of the detection mechanism.

Keywords: *VOIP networks, Flooding attacks, Entropy*

1. Introduction

DoS attacks aim to disable a service or application by sending offensive messages or a high volume of useless traffic. In 2005, the National Institute of Standards and Technology of America introduced DoS attacks as a threat to VOIP network infrastructure [1]. SIP protocol is commonly used as a basis protocol for signaling in VOIP networks. Unlike closed architecture of PSTN networks, SIP networks have been developed on open IP stack being vulnerable to a lot of security attacks such as DoS attacks. There are proposed different types of DoS attacks on SIP networks, the most basic of which are transport layer DoS attacks and IP network. These attacks have already been known and studied for many years. In addition to these attacks, there are presented new attacks that are targeted directly at SIP in the application layer. The design of IP protocol architecture has a direct impact on the security features of SIP protocol. IP protocol and Internet have been designed to aim at open source being extensible. This, along with its many benefits, provides a suitable ground for attackers

ISSN: 1738-9968 IJHIT

to get right into the network [1]. DoS attacks on SIP networks can be divided into the following three categories:

1. Manipulating the SIP packet payload.

The attacker can put harmful content to a message (entering wrong or pointless data) aiming to overflow a buffer in the destination. These messages can also be used to find the target vulnerabilities.

2. Manipulating the flow of SIP messages

In SIP real time communication networks, a communication is created between two users in a conversation by which the content is transmitted continuously between the two sides of the conversation. An attacker can fake up this relationship by signaling targeted messages.

3. Flooding Attack in SIP messages

When DoS attack is talked about, its main branch is flooding attacks which overflow the victim's resources. The main sources of the SIP flooding attacks include: bandwidth, CPU, or memory [1].

a) Bandwidth: A goal with many messages that the network is able to manage can be attacked. This kind of attacks does not waste victims` resources, but through the occupancy of capacity of the channel through which the server is connected to the network, it actually makes the server fail to work.

b) CPU: Since SIP is a text-based protocol, each received message has to be analyzed first. A special case is when the CPU is waiting for a message from the database or DNS server. Another method by which an attacker can restrict the server for processing the authorized requests is to forward the high volume of messages or the messages requiring a lot of processing to the server for CPU occupancy. Forwarding the Register messages in the wrong form, even if the number of messages is not great, can have a devastating impact on the server.

c) Memory: The great number of requests makes a session be created at the destination. When a server accepts a SIP message, it should store some information about it. Preserving time depends on the type of server (whether the server is Stateful or Stateless). When a transaction begins, its related information will be kept in memory until the transaction is completed or the time is out. These messages occupy the server resources and make them wasted and the server will not deliver service to the authorized users [2].

There are definitive solutions for the first two attack categories, *i.e.*, manipulating data and the flow of SIP messages, but there are few comprehensive approaches on flooding attacks. There are seen a lot of articles and researches carried out on this type of attack (*i.e.*, Flooding) in the SIP networks, but with existence of several methods of detection and prevention in this area, it is still considered as an open research topic.

Flooding attacks on SIP protocol can be divided into the following four categories:

1. SIP Registration Flooding Attacks

An attacker can forward a large number of Register messages with a fake ID and incorrect password and address to the SIP server. In response, the attacker will receive 401 UNAUTHORIZE message. And ignoring it, the attacker will send more messages. Processing address, ID and password will waste server resources and server will fail to response the authorized users.

2. INVITE Flooding Attacks

After registration as an authorized user, the attacker will send INVITE messages to the server. Since the server sends the message to the destination and must wait a period of time for each INVITE request and during this time it keeps information related to the request, this high volume of unanswered messages takes server resources and therefore server will be unable to respond to the authorized users.

3. BYE Flooding Attacks

In this type of attacks, an attacker attempts to send messages of session termination to the server. These messages can terminate the authorized sessions without requesting for session termination by authorized users and suddenly a large volume of sessions will be disconnected unwontedly.

4. Combinational Attacks

A smart attacker can generate attack traffic including a combination of SIP packets to bypass some attack detection mechanisms. These attacks can be classified into the category of combinational attacks while they can take place by an attacker or multiple attackers (distributed DoS attacks) [3].

Flooding attacks can have several causes. First, it can be a planned attack aimed at damaging the designed network, or these attacks occur without any intention and the reason is defective device or wrong SIP implementation. For example, consider a REGISTER Flooding after power failure; all devices try to send REGISTER message at the same time. Also, faulty design of re-REGISTER time scales may result in such a case. However, due to the same consequences for the two states, detecting and fixing the problem in both cases are mandatory. Clearly, it would be easier to detect unintentional attacks since real attackers will consider measures to evade detection.

The remainder of this paper is structured as follows: In section 2 we discuss briefly the related works done in this field, section 3 will describe the attack detection and prevention system and will discuss about threshold computing, sketch structure and entropy formula, in section 4 the implementation method and results will be discussed, in section 5 we discuss about future work and section 6 concludes the paper.

2. Related Works

In a general classification, attack detection techniques can be divided into two categories: signature-based techniques and behavior- or anomaly-based techniques. In signature-based techniques, attack patterns are recorded as a signature while the recognition is based on pattern matching between the current traffic and signature. But this technique is not suitable to detect flooding attacks at a low rate, because the attacker can choose different strategies to generate attack traffic and thus makes it difficult to produce a signature.

But in the anomaly-based approaches, by monitoring traffic and anomaly investigation, we detect the attack. Among the anomaly-based methods, we refer to method that presented in the paper [4] as a lightweight method to detect flooding attacks on SIP protocol. In the approach presented in this paper, based on each host, the rate of incoming traffic is limited. Subsequent messages sent from the host will not be processed for a limited time. In the same year, the authors of [5], offered a mechanism for flooding attacks by detection of active SIP sessions. In this attack detection mechanism, attacks will be recognized based on message rates relation of connection setup (INVITE) and positive responses (200 OK). So, when the rate suddenly changes, the change will be considered as an indication of Flooding attack.

Sengar *et al.*, in 2006, presented a statistical method to detect flooding attacks named vFDS based on Hellinger Distance, which is actually the developed method of Reynolds [5]. Authors of the paper in the same year (2006) presented another attack detection system called vIDS. The system is based on the protocol state machine that can detect the SIP messages of tampering attacks and flooding attacks. Flooding attack of message INVITE can be detected by counting the number of messages compared with a threshold. In 2007, Rebahi et al. presented a method to detect DDoS Flooding Attacks on VOIP networks and IMS systems based on change-point detection using CUSUM algorithm. In this method [7], an attack detection system based on data mining has been proposed in order to detect multiple attacks. This method is based on the signature and on anomaly detection.

One of the weaknesses of most of the approaches taken is the attack with low rate. In the low rate flooding attacks, an attacker begins his attack with very low rates and over every stage, the packet transmission rate increases while the increase is negligible and can be done over time. Although the attack rate is very small in the beginning, over time it will bring a waste of network resources and reduce productivity. In paper [8], it has been pointed out that entropy-based methods are suitable method for detection of DDoS attacks with low rates. In another approach, the authors of [9] presented, in 2011, a method based on a signal processing technique called wavelet being able to rapidly detect changes from the attack onset. In the same year, in [10] a method for protecting UAs against Flooding attacks in SIP was presented. This method can be implemented for both proxies of Stateful and Stateless. Each user, regarding the resources at disposal, responds to a certain number of requests per time interval. In 2011, Lima et al. did a research on the selection of appropriate features for detecting attacks. The authors believed that the first step to detect attacks of unauthorized entry into network was to select an optimal set of features of network traffic among all features. Optimal feature selection was done using a decision tree algorithm and the entropy of Shannon, Renyi and Tsallis as a criterion in rate calculation in a decision tree [11]. In [12], the authors used techniques of Least Mean Square and Pearson Chi-square divergence on the data collected to detect the attack. In paper [13], the generalized entropy measure was used to detect DDoS attacks with a low rate. This mechanism is presented due to the cooperation of routers while having complete control over them in networks. In another paper [14], two criteria of Hellinger distance and the Chi-square divergence were compared in Flooding attacks detection. Factor of comparison is the rate of attack detection and rate of false alarm messages. The results show, despite a higher rate of false alarm messages, HD can detect Flooding attacks faster while the Chi-square can show these attacks more clearly (with greater changes in values before and after the attack). In 2012, the authors of [15] presented an entropy-based method to detect the attacks of unauthorized entry in to network and analyze an IDS alarm message. The authors of this paper achieved their goal by Shannon entropy which is calculated based on five features. In the same year, in [16], an anomaly-based detection mechanism of flooding attacks in high speed networks was presented. This mechanism has been implemented based on Jensen-Shannon method. Paper [17] has proposed a method similar to that of the previous article except that it has the Power Divergence criterion. In another method, authors of [18] used Chi-square criterion to detect network anomalies. This criterion is applied on incoming packets at a specified interval. In [19], a method is presented which uses the Hellinger Distance technique to detect the attacks and the packets sent by the attacker while preventing damage and denial of service. It is noteworthy that this approach is the extended version of the proposed method in the paper [20] by the same author. In another mechanism, authors of [24] used a fixed threshold to prevent flooding attacks on mobile UAs. They proposed a stateful rule tree, and checked for flooding attacks during parsing packets by rule tree.

3. Attack Detection and Prevention System

We used entropy criteria for traffic analysis related to SIP protocol signaling packets in the network. In order to take advantage of the entropy criteria; we would need a proper infrastructure. Compressed summarized table of packet data (Sketch) provides a suitable infrastructure for us. With the help of Sketch table, we can provide the information needed to detect the attack at a constant volume. Figure 1 shows location of our proposed mechanism.

3.1. Entropy

Entropy is a criterion to measure uncertainty (uncertainty) of a random variable. Entropy of a random variable (X) with a discrete probability distribution $p_i = p_1, p_2, \ldots, p_n$ is defined as follows:

$$H(X) = -\sum_{i=1}^{n} p_i \log p_i \tag{1}$$

This entropy known as Shannon entropy has been the basis to define other entropies. The value of S set entropy is maximum when the probability of all its members becomes equal ($p_i = 1 / n$). In other words, the entropy is considered to be maximum when the uncertainty is maximum and redundancy in the set S is minimum [22]. Another type of entropy is Renyi that introduced by Alfred Renyi, which is a generalization of Shannon entropy expressed in parametric form. Renyi entropy of order α is defined as follows:

$$\mathrm{R}_\alpha(\mathrm{X}) = \frac{1}{1-\alpha} \log \sum_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{p}_\mathrm{i}^\alpha \ , \alpha \geq 0, \alpha \neq 1 \tag{2}$$

where,

$$\sum_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{p}_\mathrm{i}^\alpha = 1 \, , \lim_{\alpha \to 1} R_\alpha (\mathrm{X}) = \mathrm{H}(\mathrm{X}) \tag{3}$$

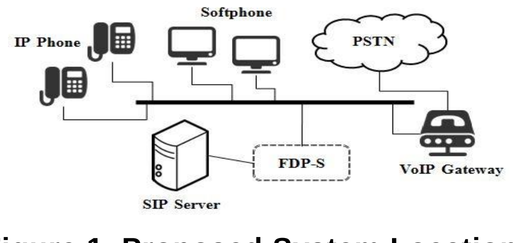


Figure 1. Proposed System Location

As is clear, when α approaches 1, the value of Shannon and Renyi entropy will be equal. When α approaches ∞, if $\mathrm{R}_\alpha(\mathrm{X}) = 0$, the probability density is located in the maximum concentration. Indeed, the role of α is to increase the deviation between different probability distributions. Tsallis entropy is another generalization of Shannon entropy which is defined as follows:

$$S_{\alpha}(\mathrm{X}) = \frac{1}{\alpha-1}\left(1-\sum_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{p}_{\mathrm{i}}^{\alpha}\right) \quad (4)$$

where,

$$\alpha \geq 0, \lim_{\alpha \to 1} S_{\alpha}(X) = H(X) \quad (5)$$

3.2. Three-dimensional Compressed Summarized Table of Packet Data

We used Sketch in order to create the conditions required to apply entropy criterion. The table is presented in [23] as a suitable structure for gathering networks data needed to perform analysis on network traffic. In order to cover different types of the SIP protocol signaling packets (including: INVITE, 200 OK, ACK and BYE) and avoid being misled by the combinational attacks, we have used a three-dimensional Sketch.

The first dimension of Sketch table is considered to separate the analysis of different types of SIP protocol signaling packet, and for any of these packet types we will have a two-dimensional structure (Fig. 2), which is produced with the help of hash functions. To create the three-dimensional Sketch, after the packet is received, the type of packet will be extracted; then, by applying the hash function on the SIP address of the sender (SID), the packet is placed in one of the cells of Sketch.

The two-dimensional Sketch formation for each packet types, in addition to improving the efficiency of detection mechanism of combinational attacks, increases extensibility of the proposed strategy. Fixed volume of these tables makes optimal use of resources available in detection mechanism. It is noteworthy that only in attack prevention phase, we need to maintain addresses of incoming packets over the same period and there is no need to maintain a high volume of addresses while the address will be kept only until the start of the new period.

For detection, we just need to restore the number of packets in every cell of Sketch. In other words, in every cell of Sketch we will store value of $\sum_{n=1}^{m} \mathrm{V}_{\mathrm{n}}$, where V_{n} is the output of hash function for SID_{n} and m is the number of received packets in this interval. We have considered the value of V_{n} to be 1 for the cell that packet is placed in it and 0 for all other cells. In the choice of hash functions, we have to consider two factors of low computational overhead and least overlapping of functions relative to each other.

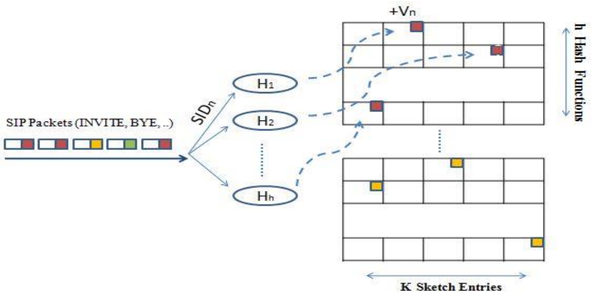


Figure 2. Sketch Structure

3.3. Detecting Attacks

The first step of our proposed mechanism is attack detection. We consider this assumption that at the beginning of this process, the network traffic is free from attack. An interval (length d × n seconds) is considered to be the first interval of training. After the data collection of SIP protocol signaling packets in this interval is done, the Sketch structure can be formed on these data. The Sketch is formed based on SIP address of packet sender by applying a hash function on it. After the Sketch table in the first interval of training is completed, the value of entropy on the structure will be calculated. In the next step, considering the next interval of length d seconds as the test interval, we will constitute re-structuring Sketch. Calculating the value of entropy in the new interval (the test interval) and comparing it with the entropy of the previous interval (interval of training), we will achieve a difference amount. The difference will be compared to a dynamic threshold. If the difference is not greater than the threshold, the mechanism continues propelling its training period (adding test interval to training interval and deleting the first d seconds of training interval) which will continue to work and repeat the same process.

Otherwise if calculated difference is not tolerated with the threshold, a warning of flooding attacks will be announced. When the attack is detected, two processes of keeping the training interval and the threshold fixed and attack prevention will be executed. In the process of fixing training interval and threshold, proceeding training interval will be refused to avoid attack traffic entering this interval and the threshold value will not be updated. This process is continued until the attack continues or in other words, the entropy difference between training and testing intervals is greater than the threshold value.

After the attack termination, the mechanism returns to its normal state and intervals of training are updated with the attack-free testing intervals. Also we update threshold at the end of each periods.

3.4. Preventing Attacks

An important step that must be implemented is to prevent the attack. In this part, we get help of the different hash functions that we used in Sketch tables for the test intervals. According to different hash functions and by intersecting between SIP addresses of Sketch cells from which the largest amount of change of entropy is obtained, we will identify SIP address of attacker and the packets related to these addresses are discarded; also, having informed the server of these addresses, we prevent their being serviced or limit the transmission rate for them. The attackers` list is dynamic and each member, in the absence of anomalous behavior after a specified time interval, can be removed from the list. Through this mechanism, even if the addresses are fake or related to the victims of attacker, our aim at protecting the SIP server and servicing to authorized users can be achieved.

3.5. Length of Training and Testing Intervals

One of the most important parameters of the proposed mechanism is taken to be the length of both training and testing intervals. Selecting the appropriate length for these intervals influences the time of attack detection from its onset and identification of network behavior. One of the most important factors for selecting length of these intervals is network traffic volume and the dynamics of network traffic. Selecting a short time for testing interval in a network with low traffic volume will lead to an increase in false alarm messages. However, increasing the length of the test period will increase the time required to detect the attacks. In contrast, a short training interval is adapted to the network traffic rapidly, but a longer training interval will provide a more appropriate view of the network status in the long-term. Thus, according to network traffic conditions, we must create a proper balance between these factors.

3.6. Detection Threshold

Because the network traffic is dynamically changing, the threshold needs to be updated corresponding to the changes. Failure to update the detection threshold can lead to the increase of incorrect alarm messages in addition to reducing attack detection rate. At each period, we update threshold regarding to three factors of the previous period threshold, the mean and standard deviation.

The new threshold is a combination of its previous value and the current situation if we do not detect the attack. In order to calculate the mean and standard deviation of the new phase, the technique of exponential weighted moving average (EWMA) was used.

Suppose μ_k and σ_k^2, respectively, are the mean and squared standard deviation in period k. To calculate them, the average of those obtained from the previous period (μ_{k-1}) and the calculated entropy difference between the two intervals of training and testing in previous period (D_{k-1}) was used:

$$\mu_k = \beta\mu_{k-1} + (1-\beta)D_{k-1} \qquad (6)$$

In order to calculate the standard deviation we will have:

$$\sigma_k^2 = \beta\sigma_{k-1}^2 + (1-\beta)(D_k - \mu_k)^2 \qquad (7)$$

Eventually the new threshold would be a combination of the average and standard deviation which is calculated from the equation below:

$$Thresh_k = \mu_{k-1} + \lambda\sigma_{k-1} \qquad (8)$$

We performed several experiments to obtain the suitable value of β as 0.75 and the value of λ as 2. In fact, raising the value of β increases the effect of the previous threshold values to generate new threshold and λ is responsible in the regulation of the sensitivity of threshold to changes. Selecting the appropriate value for λ will have a significant impact on reducing the false alert messages.

4. Implementation Results

4.1. Experiments Test Bed

The test bed consists of four main sections: Call generator, SIP server, attack generator and attack detection and prevention mechanisms of Flooding attack. We conducted various experiments with different users and scenarios to investigate the performance of the proposed mechanism.Given the importance of training and testing interval lengths in the attack detection rate and speed, we set d = 10 and n = 10 for each period. Actually, given the training interval length to be n*d seconds and that of test interval to bed seconds, for these two intervals, 100 seconds and 10 seconds, respectively are obtained.

4.1.1. Call Generator: In the first section, call generator, we use the Spirent server as the producer of VOIP network normal traffic. Spirent server with the ability to produce calls with different distributions with the help of SIP server can provide us a local VOIP network with thousands of users. This server provides a wide setting which can produce the calls with different distribution and scheduling. Defining VOIP network users in Spirent server in the source and target groups; the server makes calls between the two groups with the desired duration.

4.1.2. SIP Server: We used Asterisk server as the SIP server in the experiments .Asterisk server is one of well-known open source servers in VOIP networks in the world, and now most of the existing IPPBXs have been produced based on these servers. Asterisk server is based on the C programming language installed on various platforms such as Linux NetBSD, OpenBSD, FreeBSD, Mac OSX, Solaris, and UNIX. In addition, there are some versions of this server which are able to install on Windows OS.

4.1.3. Attack Generator: To generate attacks, Sipp software that provides the possibility of producing different attack rates, was used. By defining various attack scenarios for this software, we can generate the required attacks using a SIP signaling packet, or a combination of these packets. Attack scenarios have been designed and implemented by a separate team.

4.1.4. Flooding Attacks Detection and Prevention Mechanisms: This mechanism consists of three main modules including collecting information of packets module, module of attack detection and announcement and attack prevention module.

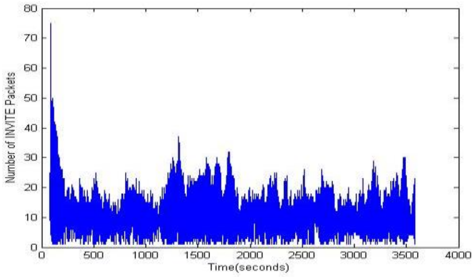


Figure 3. INVITE Packets Rate

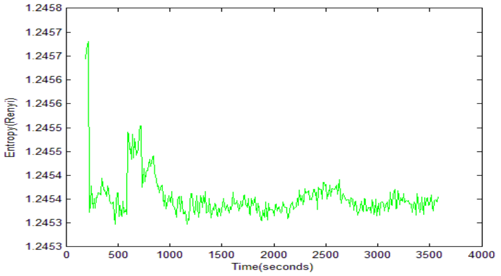


Figure 4. Renyi Under Normal Traffic (α=0.8)

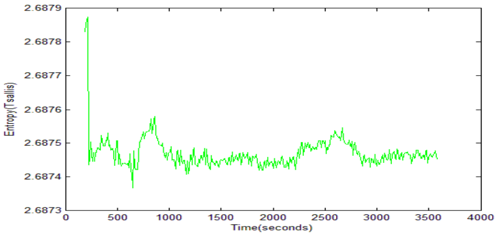


Figure 5. Tsallis Under Normal Traffic (α=0.1)

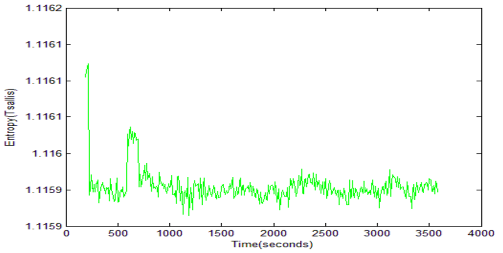


Figure 6. Tsallis Under Normal Traffic (α=0.9)

Simultaneous with the start of network, data collection module provides the required information of packet that contains the time of receiving packet and sender's address and restores it in the file. Packet collection module, depending on the type of SIP signaling packets, filters the incoming traffic and stores packets of each type in a separate file.

In order to control the volume of stored files and facilitate to manage them, the useless files are transferred to file server of packet information archive. Keeping these files provides the possibility to perform more statistical analysis for giving more and better services by the SIP server. In order to maintain the privacy of users` information obfuscation algorithms are used.

Attack detection module sets out to analyze the data collected from the packets, with the help of entropy criterion, and if an attack is detected, in addition to forwarding the warning message, the module will also activate the attack prevention module. To compare different types of entropy in the attack detection, every experiment was repeated with three types of entropy, Shannon, Renyi and Tsallis.

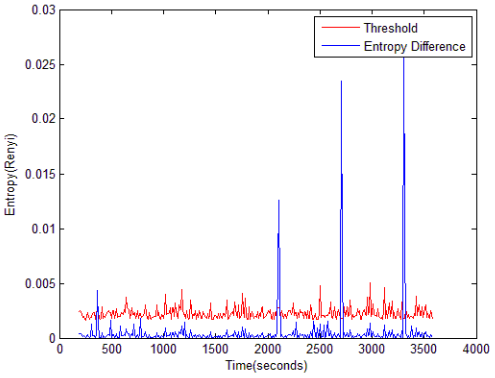


Figure 7. Renyi under attack (α=0.1, λ=2 and β=0.75)

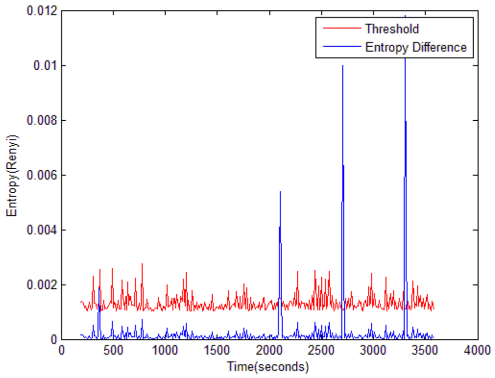
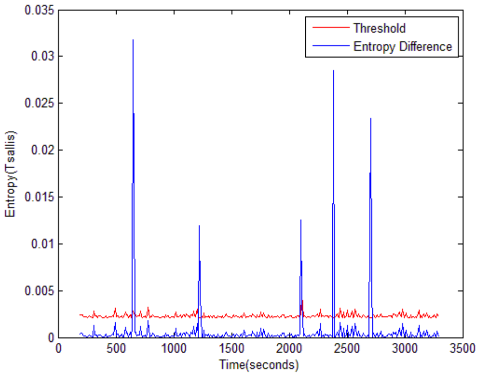


Figure 8. Renyi under attack (α=0.9, λ=2 and β=0.75)



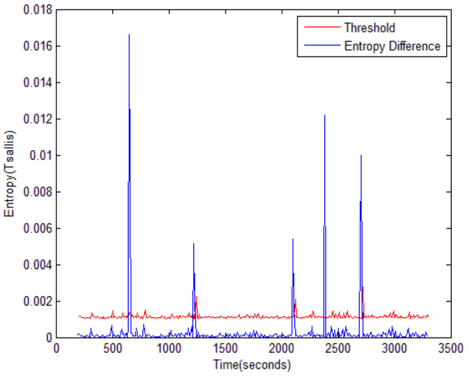


Figure 9. Tsallis under attack (α=0.1, λ=2 and β=0.75)

Figure 10. Tsallis under attack (α=0.9, λ=2 and β=0.75)

4.2. Scenarios of Attacks

In order to cover different types of Flooding attacks which we mentioned, the design team of attack scenarios, depending on the type of SIP signaling packet, designed the single and combinational attacks with different rates. Attack Scenario 1 consists of a single type attack using INVITE packets with rates of 15, 20 and 30 packets per second. In Scenario 2, the team used combinational attacks with rates of 50, 30 and 20 in seconds and in scenario 3, the single type attacks were generated in a distributed form. In Scenario 3, multiple attackers simultaneously start sending attack traffic to the server. This scenario evaluates the efficacy of the proposed mechanism against DDoS attacks.

4.3. Experiment Results

Spirent server, which is responsible for the call generation, divides the members into two groups and generates actual calls between them depending on the selected distribution. Figure 3 shows INVITE packets rate of SIP protocol in a 200-user experiment.

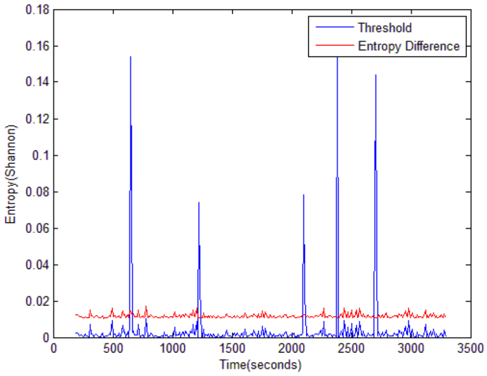


Figure 11. Shannon under attack (λ=2, β=0.75)

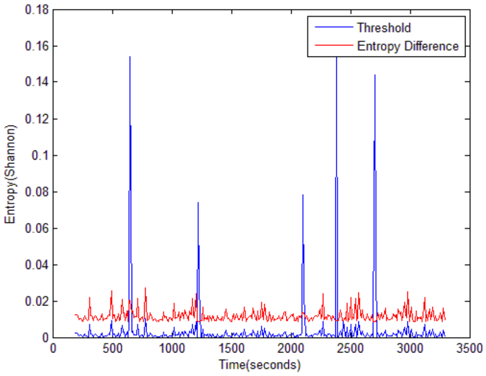


Figure 12. Shannon under attack (λ=10, β=0.8)

As shown in Figure 3, the incoming INVITE packet rate was changed between 1 to 40 packets per second. In the attack-free intervals of VOIP network traffic, the calculated entropy was varied in a certain specified interval. Figure 4 shows the rate of Renyi entropy with α = 0.8 for INVITE packet in attack-free VOIP network. As can be seen in Figure 4, the value calculated for the Renyi entropy (α = 0.8) of a training interval is at least 1.2453 and at most 1.2455 approximately, which indicates very little change in the calculated entropy during normal activity of VOIP network.

Figures 5 and 6 show, respectively, the value of Tsallis entropy related to the INVITE packets with α = 0.1 and α = 0.9 during 3300 seconds in attack-free network. By increasing the value of α towards 1 in Tsallis entropy formula, the intensity of changes is reduced. Variances of data sets in Figures 5 and 6 are 2.24889E-09 and 5.1622E-10 respectively. In other words, data scattering is reduced when we close up α to 1.

Figures 7 and 8 show, respectively, the Renyi entropy difference calculated for α = 0.1 and α = 0.9 between the test and training intervals compared with the threshold in dealing with a single attack with rates of 20 and 15 packets per second with duration of 5 seconds. A significant change in the entropy, during performing an attack, provides the attack detection possibility simply. As shown in Figures 7 and 8, by increasing the value of α toward 1, data scattering will be reduced and also we received fewer false alarms. In other words, the sensitivity of detection mechanism (the mechanism reacts to changes in traffic) and the probability of false alarms for α = 0.9 in comparison to the values obtained for the Renyi entropy at α = 0.1 will be decreased. Implementation results show that we have up to 600 percent reduction in false alarms in α = 0.9 in comparison to α = 0.1. So we can set α according to our needs of detection mechanism sensitivity. Figures 9 and 10 show, respectively, the Tsallis entropy difference calculated for α = 0.1 and α = 0.9 between the test and training intervals compared with the threshold in dealing with 5 single attack sets with rates of 20 and 15 packets per second with duration of 3-5 seconds. As shown in figure 10, by increasing α, Tsallis values will be increased more significantly with the intensity of attacks.

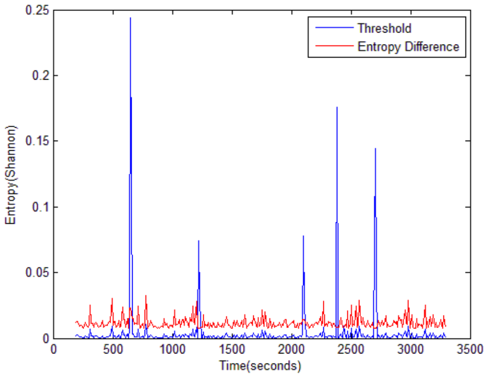


Figure 13. Shannon under attack (λ=2, β=0.75)

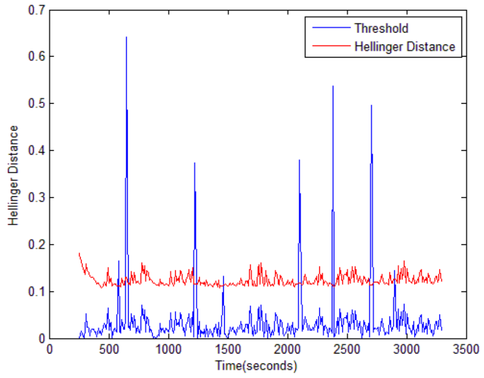


Figure 14. HD under attack (λ=2, β=0.75)

Of course, along with an accurate criterion such as entropy, we require an appropriate threshold to reduce the number of false alerts. As noted above, we update the threshold at each period to respond this need. For calculating threshold in each period, we should set three constants (β and λ). By increasing the value of β the effect of the previous threshold to generate new threshold will increase. Also λ is responsible in the regulation of the sensitivity of threshold to changes. Figures 11 and 12 show the effect of these constants on threshold values. As shown in Figure 12, setting λ=10 makes threshold to react more aggressively by traffic changes. When we are faced with an ever changing network, λ helps us to reduce false alarms.

With the increase in the value of α to 1 in Renyi and Tsallis entropy, the results will be very close to the results of similar experiments with the Shannon entropy. The following table (Table 1) shows the percentage of detecting flooding attacks for different attack rates. Based on these results, we see that entropy criteria can detect attacks with low rates by a significant detection percentage.

We also implement our proposed mechanism based on Hellinger Distance (HD) which is used to detect flooding attacks in [19] and [21]. Implementation results help us to compare our proposed mechanism more accurately with previous approaches. As shown in Figure 14, HD is more impressionable than Shannon entropy (Figure 13) in dealing with network traffic changes. Implementation results show that Hellinger Distance achieves a good detection but with higher false alarm ratio. Furthermore, FDP-S makes a better view of network traffic and its value increases more significantly with the intensity of attacks (Figure 13). We run both approaches (HD and FDP-S) on the same data sets with different flooding attacks rates. Attack team used single type flooding attacks with 15, 20 and 50 packets per second rate and three different data sets. We used Spirent server and Asterisk SIP server to generate these data sets. Figures 13 and 14 show one of our experiment results. As shown in figure 14, although attack team generates 5 sets of attack during this experiment, but HD approach generates 8 attack alarms. It means we received 5 true alarms and 3 false alarms. But FDP-S generates exactly 5 attack alarms without any false alarms.

Table 1. Detection Result

Scenario Number	Attack Rate (Per Sec.)	Detection Threshold	Number of Experiments	Detection Probability (FDP-S)	Detection Probability (FDP-R (α = 0.1-0.9))	Detection Probability (FDP-T (α = 0.1-0.9))
Scenario 1	15	Dynamic (λ=2,β=0.75)	30	95.8 %	(99.1-95.8)%	(99.1-95.8)%
	20	Dynamic (λ=2,β=0.75)	30	98.3%	(99.4-98.3)%	(99.4-98.3)%
	30	Dynamic (λ=2,β=0.75)	20	100%	(100-100)%	(100-100)%
Scenario 2	20	Dynamic (λ=2,β=0.75)	30	93.4%	(98.6-93.4)%	(98.6-93.4)%
	30	Dynamic (λ=2,β=0.75)	30	95.2%	(99-95.2)%	(99-95.2)%
	50	Dynamic (λ=2,β=0.75)	20	97.9%	(99.5-97.9)%	(99.5-97.9)%
Scenario 3	15	Dynamic (λ=2,β=0.75)	30	95.8%	(99.1-95.8)%	(99.1-95.8)%
	20	Dynamic (λ=2,β=0.75)	30	98.3%	(99.4-98.3)%	(99.4-98.3)%
	30	Dynamic (λ=2,β=0.75)	20	100%	(100-100)%	(100-100)%

Table 2 shows false alarms rate for HD and FDP-S. Experiment results show that FDP-S can detect attacks with high accuracy and lower false alarms.

4.4. The Memory, Computation and Delay Overhead

Given that the our proposed mechanism acts online and Sketch tables keep only data for the same interval at constant volume in each period, the memory consumption of the proposed mechanism will be fixed and minimal for the SIP server, but it is noteworthy that we can implement this mechanism individually on another hardware, in which case no overhead in terms of memory and computation will be imposed on the SIP server and only the delay discussion will be considered.

Since the delay in making the call cannot be accepted by any service provider, due to the provision of secpurity in phone networks, minimizing delays will be an important factor for the proposed mechanism, since the proposed mechanism acts in parallel with the server, it doesn't create significant delays in server services.

4.5. Required Time for Detecting Attacks

Another important factor for flooding attack detection mechanisms is the time required to detect the attack from its onset. The maximum time required to detect the attack by our proposed mechanism is one and a half times the testing interval. It is noteworthy that the attack length would not be effective on detecting time and the attack detection percentage.

Table 2. False Alarms Rate

Data set No.	Number of Experiments	False alarms rate	
		Hellinger Distance (%)	FDP-S (%)
Data set 1	20	14.2	3.5
Data set 2	20	12.8	2.1
Data set 3	20	17.8	4.2

5. Future Work

Our proposed mechanism uses three constants (α, β and λ) which are responsible for determining its sensitivity in flooding attacks detection. Choosing suitable values for these constants helps us to achieve higher detection rate and fewer false alarms. We set them according to experiment results for achieving these goals. In the future work, we plan to propose a module which is setting these constants dynamically according to network traffic and server needs of sensitivity. This module will control constants to achieve even more flooding attacks detection rate and fewer false alarms by changing constants in suitable situations.

6. Conclusion

In this paper, we proposed a method based on Shannon, Renyi and Tsallis entropy to detect and prevent of flooding attacks on SIP protocol. Entropy criterion provides possibility to detect changes in network traffic accurately. Therefore, compared with other distance metrics, it can perform better in detecting attacks. We used the sketch table of the packet data to collect the required packet data at constant volume. In order to increase attack detection percentage and false alarm message reduction, at each period, the attack detection threshold has been updated due to network traffic in the previous interval and calculated threshold in all passed periods. Since each type of SIP signaling packets is individually assessed, in addition to increasing the extensibility of the proposed mechanism, the probability of being misled by combinational attacks is greatly reduced. Parameters included in the calculation of entropy in FDP-R and FDP-T provides adjustable sensitivity for detection mechanism. With the decreasing value of the parameter α on the FDP-R and FDP-T to 0, mechanism sensitivity is increased and consequently the rate of false alarm messages will increase. Whatever α value is closer to zero, the network traffic changes will have a greater impact on entropy value in that interval. By increasing α value towards 1, the sensitivity of detection mechanism will be reduced and the experiment results will approach to the results of FDP-S. Due to the dynamic nature of the attack detection threshold and training interval information, the proposed mechanism is compatible with network behavior and can be used in networks with different distributions. In comparison to HD-based approaches, we achieve a good detection, but with lower false alarm ratio. Furthermore, FDP-S makes a better view of network traffic and its value increases more significantly with the intensity of attacks.

References

[1] S. Ehlert, D. Geneiatakis and T. Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks", Elsevier computers & security, **(2010)**.

[2] M. Voznak and J. Safarik, "DoS Attacks Targeting SIP Server and Improvements of Robustness", International Journal of Mathematics and Computers in Simulation, **(2012)**.

[3] A. Kumar and S. Tilagam, "A Novel Approach for Evaluating and Detecting Low Rate SIP Flooding Attack", International Journal of Computer Applications, **(2011)**.

[4] B. Iancu, "SER PIKE excessive traffic monitoring module", **(2003)**: http://www.iptel.org/ser/doc/modules/pike.

[5] B. Reynolds and D. Ghosal. "Secure IP telephony using multi-layered protection", 10th annual network and distributed system security symposium. San Diego, USA, **(2003)** February.

[6] Y. Rebahi, M. Sher and T. Magedanz, "Detecting flooding attacks against IP multimedia subsystem (IMS) networks", The sixth ACS/ IEEE international conference on computer systems and applications (AICCSA-08). Doha, Qatar, **(2008)** March.

[7] Y. Bouzida and C. Mangin, "A framework for detecting anomalies in VoIP networks", Third international conference on availability, reliability and security (ARES 08), Barcelona, Spain, **(2008)** March.

[8] J. Zhang, Z. Qin, L. Ou, P. Jiang and J. Liu, "An Advanced Entropy-Based DDOS Detection Scheme", International Conference on Information, Networking and Automation (ICINA), **(2010)**.

[9] J. Tang and Y. Cheng, "Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks", IEEE International Communications Conference (ICC), **(2011)**.

[10] I. Hussain and F. Nait-Abdesselam, "Strategy based proxy to Secure User Agent from Flooding Attack in SIP", 7th International Wireless Communications and Mobile Computing Conference (IWCMC), **(2011)**.

[11] C. Lima, F. M. Assis and C. Souza, "A comparative study of use of Shannon, Rényi and Tsallis Entropy for Attribute Selecting in Network Intrusion Detection", Measurements and Networking IEEE International Workshop (M&N), **(2011)**.

[12] O. Salem, A. Makke, J. Tajer and A. Mehaoua, "Flooding Attacks Detection in Traffic of Backbone Networks", 36th Annual IEEE Conference on Local Computer Networks, **(2011)**.

[13] Y. Xiang, K. Li and W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics", IEEE Transaction on Information Forensics and Security, vol. 6, no. 2, **(2011)** June.

[14] J. Tajer, A. Makke, O. Salem and A. Mehaoua, "A Comparison Between Divergence Measures for Network Anomaly Detection", 7th International Conference on Network and Service Management (CNSM), **(2011)**.

[15] Q. Qia and Z. Wang, "A New Attack Detection in Large Scale Network based on Entropy", Journal of networks, vol. 7, no. 5, **(2012)** May.

[16] O. Salem, F. Nait-Abdesselam and A. Mehaoua, "Anomaly Detection in Network Traffic using Jensen-Shannon Divergence", IEEE ICC - wireless networks symposium, **(2012)**.

[17] A. Makke, O. Salem and M. Assaad, "Flooding Attacks Detection in Backbone Traffic Using Power Divergence", The 7th ACM International Workshop on Performance Monitoring, Measurement and Evaluation of Heterogeneous Wireless and Wired Networks, **(2012)**.

[18] C. Hui and H. Chao, "Monitoring SIP Traffic Using Statistical Approaches," 2nd International Conference on Electronic & Mechanical Engineering and Information Technology, **(2012)**.

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

[20] J. Tang, Y. Cheng and C. Zhou, "Sketch-based SIP flooding detection using Hellinger distance", Global Telecommunications Conference,GLOBECOM, **(2009)**.

[21] H. Sengar, H. Wang, D. Wijesekera and S. Jajodia. Detecting VoIP floods using the Hellinger distance, IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 6, **(2008)** June, pp. 794-805.

[22] M. Cover and A. Thomas, Elements of Information Theory, 2nd Edition, ISBN: 0-471-24195-4, Hardcover, **(2006)** July, pp. 776.

[23] A. Gilbert, S. Guha, P. Indyk, S. Muthukrishnan and M. Strauss, "Quicksand: quick summary and analysis of network data", DIMACS, Tech. Rep. 2001-43, **(2001)**.

[24] D. Seo, H. Lee and E. Nuwere, "SIPAD: SIP–VoIP Anomaly Detection using a Stateful Rule Tree", Computer Communications, vol. 36, no. 5, **(2013)** March 1, pp. 562-574.

Authors

Reihaneh Haji Mahdizdeh Zargar, she received the B.S. degree in software engineering from Ferdowsi University of Mashhad, Mashhad, Iran, in 2010. She is M.S. student of software engineering in Ferdowsi University of Mashhad, Mashhad, Iran since 2011. Her research interest includes VOIP networks and SIP Security.

Mohammad Hossein Yaghmaee Moghaddam, he is an associate professor at Department of Computer Engineering of Ferdowsi University of Mashhad. He received the Ph.D. and M.S. degrees from Department of Electrical Engineering, Amir Kabir University of Technology and B.Eng. degree from Department of Electrical Engineering from Sharif University of Technology. His research interests are in the general area of computer networking, including TCP/IP networking, IP/MPLS networks, wireless sensor networks, Quality of Service (QoS), transport protocols, resource management, network routing, and smart grid networks. He is an IEEE Senior member and head of IP-PBX type approval lab. He is member of several university committees. He was the director of the Department of Computer Engineering of Ferdowsi University of Mashhad for two 2 years period, in 1977.