Sketch-Based SIP Flooding Detection Using Hellinger Distance

Jin Tang, Yu Cheng, and Chi Zhou
Department of Electrical and Computer Engineering
Illinois Institute of Technology, Chicago, IL, USA 60616
Email: {jtang9, cheng, zhou}@iit.edu

***Abstract*—The Voice over IP (VoIP) application utilizes the Internet to provide voice service; thus it is susceptible to various security issues common on the IP networks, such as the flooding attack. Moreover, VoIP uses the Session Initiation Protocol (SIP) for session control and management. The transactional nature of SIP makes flooding attack an even severer threat, which can consequentially lead to denial of service (DoS). In this paper, we develop an efficient online SIP flooding detection scheme by integrating the sketch technique with Hellinger distance (HD) based detection. The sketch data structure can summarize the SIP call generating process into a fixed set of data for developing a probability model. The HD technique, combined with on-line traffic estimation, can efficiently identify attacks by monitoring the distance between current traffic distribution and the estimated distribution based on history information. Compared to the original HD detection system, our technique achieves the advantages of higher accuracy, flexibility to deal with multi-attribute attacks and DDoS attacks, and the ability to track the period of attack. Computer simulation results are presented to demonstrate the performance of the proposed technique.**

I. Introduction

The Voice over IP (VoIP) is becoming prevailing, not just a supplement of the traditional public switched telephone network (PSTN), due to various benefits such as cost-efficient deployment, plenty of features, and convenience for service integration. However, since the Internet Protocol (IP) network is an open transport infrastructure, the security issues (for example the flooding attack) become a major concern, although such network anomalies are considered minimal in PSTN. Moreover, VoIP services depend on the Session Initiation Protocol (SIP) [1] to establish, manage and terminate sessions. The open and transactional nature of SIP makes VoIP suffer more from flooding attacks since resources will be exhausted easily [9]. This paper addresses the important issue on how to timely and accurately detect the SIP flooding attack.

Generally, there are two major approaches for anomaly detection, namely, *signature based* and *behavior based*. The signature based approach profiles known network anomalies as signatures. Detection systems in this approach raise alert if the on-going traffic patterns match the profiled signatures. It can accurately identify known attacks but is not able to detect new anomalies. Rather than profiling known attacks, the behavior 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 advantage of the behavior based approach is that new anomalies can be detected. Our SIP flooding detection developed in this paper adopts the behavior based approach.

A natural idea for flooding detection is to identify changes in traffic volume or rate [6], [17]. In such schemes, alarms are raised if the traffic volume during a time interval is larger than a threshold predicted according to past normal conditions. A main issue of volume/rate monitoring is that the detection accuracy can be severely degraded if the normal rate is dynamic in the observation window due to the random nature and the flooding attack rate is not very high. The Hellinger distance (HD) [2], which describes the deviation between two probability distributions, has been proposed as a detection method. The HD scheme has shown its strong capability to detect flooding attack [3], because the low-rate flooding is likely to have different probability distributions from the normal traffic. Nevertheless, the detection scheme in [3] will be ineffective, if attackers simultaneously flood the four SIP attributes that are used to build the probability model; such an attack is referred to as *multi-attribute attack* in this paper. Moreover, the paper [3] does not address how to maintain an accurate threshold reflecting the normal condition under attacks, which is critically important to the HD based detection system.

In this paper, we integrate the sketch technique [5], [6] with the HD scheme to achieve a more efficient and flexible flooding detection scheme. The fundamental reason for the ineffectiveness of the HD scheme [3] regarding multi-attribute attack is that the probability model is directly based on the physical SIP attributes. The *sketch* is a technique for random data aggregation, which can summarize the traffic associated with one or more physical attributes into a pre-determined number of states by the hash operation. In our scheme, the probability model is established based on the sketch data, rather than directly on the physical attributes. Thus, our scheme is fully effective to the multi-attribute attacks. Moreover, we develop an *estimation freeze scheme* that can protect the HD threshold estimation from being impacted by the attacks. A side benefit of the estimation freeze scheme is that the duration of attacks can be traced.

In summary, the paper has contributions in four aspects. 1) We adopt sketch to establish a behavior probability model, which enables our detection scheme to efficiently deal with the SIP flooding attack. 2) The sketch is further augmented with a

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

voting scheme for higher detection accuracy. 3) An estimation freeze scheme is developed to maintain the information about normal behavior under attack. 4) The flexibility of our scheme in dealing with distributed denial of service (DDoS) attack and multi-attribute attack has been discussed.

The remainder of this paper is organized as follows. Section II describes the system model. Section III presents the proposed flooding detection scheme. Section IV presents some computer simulation results to demonstrate the performance. Section V reviews more related work. Section VI gives the conclusion remarks.

II. System Model

A. VoIP with SIP

SIP is an text-based application layer signaling protocol to establish, manage and terminate VoIP calls. User Agent Client (UAC), User Agent Server (UAS) and SIP proxy/server are three basic components in a SIP environment. To establish a VoIP call, UAC sends a SIP INVITE message to UAS through a SIP proxy. The SIP address of the calling UAC is encoded at the first line of the INVITE. After UAS answers the call, two additional messages, 200 OK and ACK are then exchanged to accomplish the procedure of call establishment. The termination of a SIP call is indicated by a BYE message sent from either UAC or UAS after hanging up.

B. Threat Model

SIP is vulnerable to network anomalies such as the INVITE flooding attack. Such attacks can be easily mounted by utilizing various SIP traffic generators openly available on the Internet, for example, SIPp [4]. SIP proxies or servers will be overwhelmed by thousands of INVITE messages just within a short period of time. Moreover, being a transactional protocol, SIP may require the proxies to maintain a state for each INVITE message for some time when it is expecting the associated 200 OK. The resources of SIP proxies will be exhausted in nearly real time if the attack rate is high enough. Thus the SIP INVITE flooding attack is deteriorating to the VoIP network. We focus our discussion on the INVITE flooding case first. Attacks utilizing other SIP attributes can be addressed in a similar way and will be further discussed in Section IV.

C. Sketch

The sketch data structure is a probabilistic data summary technique. It randomly aggregates high dimensional data streams into smaller dimensions.

In the data model used by sketch, each data item $a_i = (k_i, v_i)$ consists of a key k_i and its associated value v_i. When a new data item arrives, its value will be added to an entry with the same key in the model. In our scheme, we use SIP address as the key and the number of INVITE from the address as the related value.

A sketch is basically an $H \times K$ table, each row of which is associated with a hash function [7] and all the hash functions are independent from each other. Thus sketch can also be interpreted as an array of H hash tables of size K. Suppose the original data set has a high dimension of X, applying a hash function to the data can reduce its dimension to a much smaller fixed number K. This is also how the random aggregation is applied. Data items whose keys are hashed to the same value will be put in the same entry in a hash table and their values will be added up to obtain the value of that entry. The resultant K "sketched" data entries in each of the rows are used to define a probability distribution and then serve as the input to the HD change detection. Since random aggregation brings information loss, identifying attack from just one row can affect the detection accuracy. Thus, we will apply a voting procedure among all the H rows to find an agreement among them. Figure 1 gives an example of a sketch table. It is shown that when a new data item (k_i, v_i) arrives, it will be added to the entry with index $h_j(k_i)$ in each of the H rows.

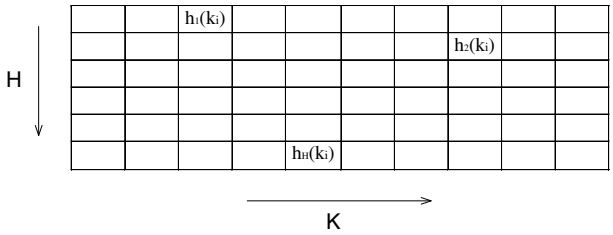

Fig. 1. Illustration of a sketch table.

Using sketch makes our scheme flexible. No matter how many normal users exist in the VoIP network, sketch can derive a fixed-size traffic summary.

D. Hellinger Distance

The Hellinger distance (HD) is used to measure the distance between two probability distributions [2]. To compute HD, suppose we have two distributions on a same sample space, namely, P: $(p_1, p_2, \cdots, p_n)$ and Q: $(q_1, q_2, \cdots, q_n)$. The HD between the two distributions is defined as follow

$$H^2(P, Q) = \frac{1}{2} \sum_{i=1}^{n} (\sqrt{p_i} - \sqrt{q_i})^2 \quad (1)$$

HD will be up to 1 if the two probability distributions are totally different and down to 0 if they are identical. This property provides a good approach to quantify the similarity of two data sets in either attack or normal situations. Recall that we aim to build a behavior based anomaly detection system which needs a statistical model to represent normal conditions and raises alarm when significant deviations from normal are observed. The property of HD makes it well suited to this role. A low HD value implies that there is no significant deviation between two probability distributions along an evolving process and a sudden high HD is a strong indication that anomalies have happened and altered the distribution.

III. Detection Scheme Design

Our detection scheme is based on integrating the two techniques introduced in Section II, sketch and Hellinger distance.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

The details of the scheme are presented in this section.

A. Training and Estimation

Let SIP messages in a VoIP network be the input stream to the detection system. Time is divided into discrete intervals and each interval is of a fixed length Δt. In each detection cycle, we organize the data being analyzed into a training set and a test set. The training period consists of n consecutive time intervals and the test period is the interval right after.

Assumably there is no attack in the initial training set. We then build an $H \times K$ sketch from the set for the INVITE messages. As described in Section II, we use the SIP addresses of the senders of the INVITEs as the hash keys. For messages hashed to the same position in a sketch table, the total number of them will be the value of that entry. Similarly, a $H \times K$ sketch is built for the messages in the test set as well. The resultant two sketches will be the input to calculate the Hellinger distance.

For the $H \times K$ table of the training set, we obtain a probability distribution P_1 from the first row of it. In order to achieve this, suppose the values of the K entries are $n_1, n_2, \cdots, n_K$, we add them up and get a number N. Then we define the distribution P_1

$$P_1 = (\frac{n_1}{N}, \frac{n_2}{N}, \cdots, \frac{n_K}{N}) \tag{2}$$

Similarly, for the $H \times K$ table of the test set, we also obtain a distribution Q_1 from its first row. Suppose the values of the K entries are $m_1, m_2, \cdots, m_K$, we add them up and get another number M. Thus we have

$$Q_1 = (\frac{m_1}{M}, \frac{m_2}{M}, \cdots, \frac{m_K}{M}) \tag{3}$$

The Hellinger distance of the above two probability distributions is then calculated as

$$H^2(P_1, Q_1) = \frac{1}{2} \sum_{i=1}^{K} (\sqrt{\frac{n_i}{N}} - \sqrt{\frac{m_i}{M}})^2 \tag{4}$$

We mark this HD as HD_1 since it is calculated from the first row. Similar to this, we calculate the Hellinger distances between all the following rows in the two $H \times K$ sketches and consequently obtain $HD_2, HD_3, \cdots, HD_H$. We identify attacks by monitoring these distances and applying a voting procedure to find an agreement among them.

In normal condition, no significant deviation happens in the call generating process, thus the value of HD_1 is smaller than a threshold. The first row of the training set sketch will then include the first row of the current test set sketch and move forward for one time interval. Correspondingly, the first row of the test set sketch will proceed to the next interval as well. All the other related rows in the two sketches will have similar operation when traffic condition keeps normal.

Such a sliding window approach better estimates the pattern of the input stream than directly analyzing two consecutive individual time intervals. It well reflects the dynamic of the evolving traffic and sudden fluctuation in normal situation can be smoothed out too.

B. Threshold Estimation and Attack Detection

1) Detection Threshold: As we want to utilize HD to model an evolving process along time, a detection threshold is needed to be the actual indicator of anomalies. We know that usually even the normal behavior is changing and will cause fluctuation in HDs over time, thus a constant threshold is neither practical nor sensitive in the case. In order to properly model the process, we adapt the Exponential Weighted Moving Average (EWMA) method [8] in our scheme to calculate a dynamic threshold.

$$H_{n+1} = (1 - \alpha) \cdot H_n + \alpha \cdot h_n \tag{5}$$

$$\sigma_n = |H_n - h_n| \tag{6}$$

$$S_{n+1} = (1 - \beta) \cdot S_n + \beta \cdot \sigma_n \tag{7}$$

$$H_{n+1}^{Thre} = \lambda \cdot H_{n+1} + \mu \cdot S_{n+1} \tag{8}$$

h_n is the current value of the Hellinger distance. H_n and H_{n+1} are estimation averages of the current and next HDs. σ_n measures how much H_{n+1} deviates from h_n. S_n and S_{n+1} represent the current and next mean deviations. The principle of using EWMA here is to forecast future values based on current values. Given H_{n+1} and S_{n+1}, we compute the estimated threshold H_{n+1}^{Thre}. In order to avoid false alarms, the threshold should be greater than HD in normal situation. Two parameters λ and μ then come into play to set a safe margin for the threshold. The parameters α, β, λ and μ are all tunable parameters in the model. We can set proper values for them in the experiments to achieve desirable detection accuracy.

2) Estimation Freeze Scheme and Attack Detection: When flooding attack comes, it will disturb the probability distribution obtained from the current test set sketch. Thus the Hellinger distance between the first rows of the two sketches, HD_1 will become larger than the threshold and an anomaly detection is registered. Note that no attack alarm is raised yet at this point.

We then perform an "estimation freeze scheme" that consists of two actions. First, we freeze the current training set and only proceed the test set to the next time interval. As a result, in the next cycle the Hellinger distance will be between the frozen normal training set and the proceeded current test set. This "one freezing one proceeding" action will keep on until HD_1 goes below the threshold. The purpose for doing this is to keep HD_1 high during attack. Second, we freeze the threshold and will not update it according to equations (5), (6), (7) and (8) until HD_1 drops below it. This can protect the threshold from being impacted by the flooding attacks and make it stable during attack. As a side effect, these two actions together determine the duration of a registered anomaly because HD_1 is above the threshold all through the attack and goes down right afterwards.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

When the detected anomaly is over, we will include the next normal test set into the training set, move forward the training set for one time interval accordingly and update the threshold. The traffic during attacking intervals will never be included in the training set.

Similar actions are taken between every two related rows in the two sketches if they also detect significant changes in traffic and each of them will register anomaly independently. Note that every two related rows maintain their own independent evolving threshold as well.

Random aggregation in sketch brings information loss in each row. Thus in one time interval certain rows may detect changes whereas others may not. As mentioned above, to increase detection confidence and assure high accuracy, we apply a voting procedure: if at least z rows out of H register anomalies, an attack alarm is finally raised.

IV. Performance Evaluation

In this section, we evaluate the performance of the proposed SIP flooding detection scheme. The trace data used in our study is obtained by simulating VoIP signaling flows which consist of the four SIP attributes, namely INVITE, 200 OK, ACK and BYE. We analyze the data through Matlab and focus the analysis on the INVITE flooding case first. DDoS attack and multi-attribute attack are then discussed as well.

A. Normal Traffic Behavior

We parse INVITE messages from the trace data. In the normal condition, the INVITE generating rate is uniformly distributed from 25 per second to 75 per second with a mean of 50 per second. The senders of the messages are randomly chosen from 100,000 simulated users in a VoIP network. As in [3], to achieve higher detection accuracy and lower computational cost, we set the length of a time interval Δt to 10 seconds. Also, as longer training set better captures the pattern of the traffic whereas shorter training set responses quicker to change, in order to find a good balance between them, the number of time intervals in a training set n is set to 10.

We build two sketches for both the training set and the test set and calculate the Hellinger distance between their related rows along time as described in Section III. Figure 2 shows HD_1 in the normal condition when we choose $K = 32$ and $H = 5$. We can see that the distances are distributed around 0.01. Similar values can be seen from other related rows of the two sketches as well. We do not plot them all in the figure for the purpose of a more clear presentation. These low HD values show the similarity of the training set and the test set when the traffic behaviors are normal.

B. Ineffectiveness of Rate Based Approach

In the flooding attack experiment, we use the normal traffic described above as background and mix it with the flooding traffic from an attacking source. The flooding rates vary from 35 per second to 500 per second. The durations of the attacks are all 30 seconds. 35 per second is lower than the mean normal rate whereas 500 INVITE messages per second can easily overwhelm a SIP proxy or server. The purpose of choosing such a range is to see that despite effectively detecting high rate flooding, our scheme is even capable of identifying low rate attacks which can hide in the normal traffic and still preserves high accuracy. Comparatively, as in Figure 3, we show the dynamic of traffic rate when there are five attacks of 50 INVITEs per second mixed with normal traffic. We see that there is no sign of abnormal behaviors in the figure since the normal traffic itself has fluctuation as well.

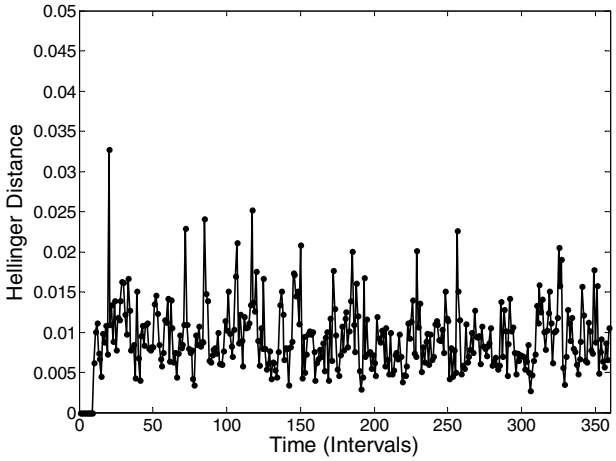

Fig. 2. Hellinger distance under normal condition.

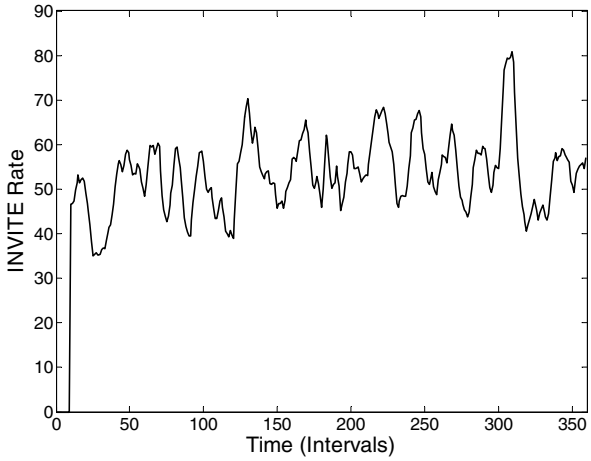

Fig. 3. Dynamic traffic rate.

C. Flooding Attack Detection

We set the parameters in our scheme as $\alpha = 0.125$, $\beta = 0.25$, $\lambda = 5$, $\mu = 1$, $z = 0.8$ and apply the scheme to detect the same five attacks of 50 INVITEs per second as described above. We empirically get the values of the parameters as shown to achieve desirable detection accuracy. Figure 4 shows the dynamic of HD_1 and the associated threshold. The five spikes clearly identify the five flooding

978-1-4244-4148-8/09/$25.00 ©2009

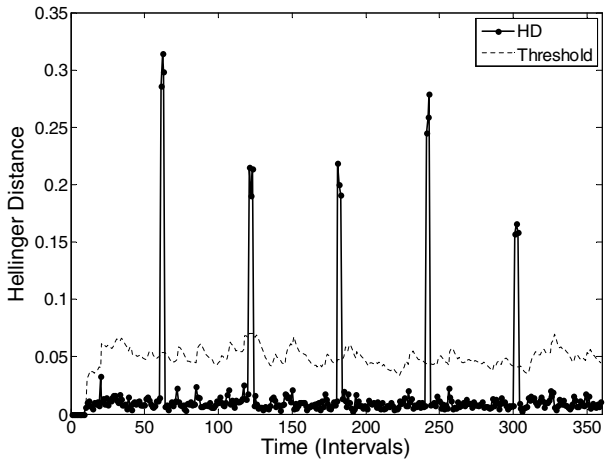

Fig. 4. Detection of flooding attacks.

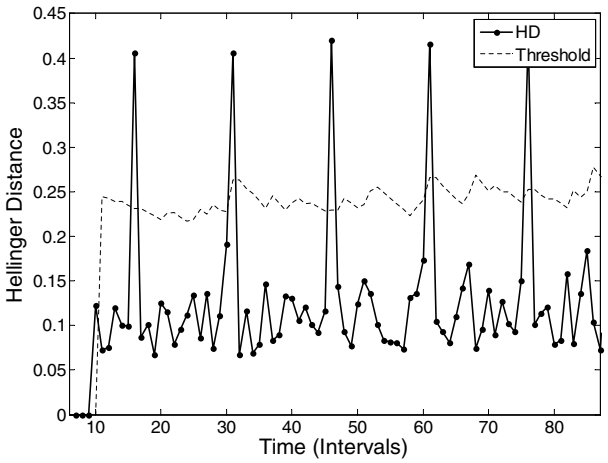

Fig. 5. Performance under DDoS attack.

attacks. Other rows may not have the same detection accuracy due to different aggregations of INVITE messages, but the voting procedure finds an agreement among the 5 rows and raises attack alarm accurately. Also in Figure 4, due to the "estimation freeze scheme" used, we can see that HD_1 remains high and threshold keeps constant during attack. They together precisely determine the duration of an attack, which lasts for 3 time intervals. Both the HD and threshold evolve with the dynamic of the traffic and thus preserve the ability to detect attack online. Whereas in [3], the threshold does not react accordingly under attack and remain low as if it is always predicted from normal condition. We think this approach does not accurately reflect the online traffic situation.

We repeat the experiment for several times and change the attack rates accordingly. The detection results are shown in Table I. We can see that even the attack rate is as low as 35 per second, our scheme can still identify it with the accuracy of 100 percent.

TABLE I
DETECTION RESULT

Flooding Rate	Number of Experiments	Detection Probability
35	30	100%
50	30	100%
75	30	100%
100	30	100%
500	30	100%

D. DDoS Attack and Discussion

In the case of the Distributed Denial of Service (DDoS) attack, numerous attackers in a VoIP network initiate flooding to a SIP proxy or server simultaneously. Our scheme can identify such kind of attacks effectively if the parameter K is greater than the number of attackers. Figure 5 shows five DDoS attacks from 300 attackers causing deviation in HD_1 along time with a K of 1024. A longer Δt of 40 seconds is used to obtain a relatively stable distribution under normal condition. The five spikes of HD in the figure clearly identify the attacks. The benefit of a large K is that the attackers can not be evenly distributed by the hash functions to every entry of a sketch and consequently the probability distribution obtained from the sketch will be disturbed by the attack. The condition of a K greater than the number of attackers may bring a scalability problem to our scheme. However, since the computation involved in the scheme is not extensive, the major cost incurred from a large K will be memory. We think this cost is acceptable because memory is not expensive in modern hardware. Nevertheless, if the memory cost becomes too large when we monitor a whole VoIP network, one possible approach to address it is to have the detection system located in every stub of the whole network and assume that there are a few attackers in each of the stubs as described similarly in [11], [12]. Due to our scheme's ability to accurately identify low rate attacks, the flooding can be detected right after it is initiated in its own stub and the attackers is possibly to be located as well.

Another form of DDoS, named Distributed Reflection DoS happens in the VoIP network [9]. In this attack, attackers send fake SIP requests with a forged source address to some reflector proxies or servers. In reply to these fake requests, the reflectors will send numerous responses to the forged source address and overwhelm the host. The forged source can be any SIP nodes in a VoIP network, such as SIP phones, proxies and servers. Our scheme can well address this issue because the sender address of the flooding SIP requests will be concentrated on the forged source, which will clearly increase the value of certain entry in sketch and thus disrupt the probability distribution and HD.

E. Multi-Attribute Attack

Attackers can simultaneously flood the four SIP attributes, namely INVITE, 200 OK, ACK and BYE together. We re-

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

ferred to this attack as the multi-attribute attack. This attack does not disturb the probability model directly based on the physical SIP attributes much. In our scheme, we establish the distribution model from sketch data summarized from single SIP attributes. To deal with the multi-attribute attack, four sets of sketches are built for each of the SIP attributes and HDs are computed with operations similar to the INVITE case. When the four attributes flood together, the distributions will all be altered and the attack can be effectively detected by the suddenly increasing HDs.

V. Related Work

Several studies for anomaly detection are based on the classic time series forecasting analysis [13]. The standard techniques include the EWMA method used in our scheme. Sketch [5] is a technique to summarize high dimensional data and provide scalable input to the time series forecasting model. Krishnamurthy et al. [6] utilize sketch in change detection. However, their approach is based on the traffic volume.

Using the destination addresses to profile traffic is a common approach to address the DoS problem [14], [10], since even though the attackers can be dispersed, their target is concentrated on the victim addresses. This causes the distribution of destination addresses significantly deviating from the normal traffic condition and thus effectively detect the attack. However, such an approach is not practical in the SIP case if the flooding target is a proxy or server. This is because SIP messages can be sent to one proxy or server no matter what address is in the SIP destination header field. Hence destination SIP address here does not make sense.

Schemes presented in [15], [16] work effectively to detect the SIP flooding DoS attacks. SIP transactional models are built to detect deviations from normal behaviors. However, these schemes are customized specifically to the SIP protocol and can not be easily generalized to be applied in other flooding detection case. In our scheme, we can use attributes in protocols other than SIP as key to profile traffic and thus have a generic method to detect other flooding attacks.

VI. Conclusion

Flooding attack is a severe threat in a VoIP network. In this paper, we propose an online VoIP flooding detection scheme by integrating two techniques, sketch and Hellinger distance. We first utilize sketch to build fixed-size compact summaries of the SIP signaling message flows. The random aggregation property of sketch provides flexibility to summarize high dimensional user data into much lower dimensions. Hellinger distance is used to profile normal traffic behaviors and detect attacks based on probability distributions defined from the sketch tables. The "estimation freeze scheme" presented shows its ability to both protect the threshold estimation from being impacted by the attacks and determine the durations of the attacks. Finally, a voting procedure is applied to assure the detection accuracy. Since we define distributions based on single SIP attributes, our scheme is fully effective to the multi-attribute attack. Performance evaluation shows that the scheme preserves high detection accuracy even when the attack rate is very low. In our future work, we will work on to develop our scheme in detecting the DDoS attack.

Acknowledgment

The first author would like to thank Wei Tang for his generous help.

References

[1] J. Rosenberg, H. Schulzrinne and G. Camarillo, "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002

[2] G. Yang and L. Le Cam, *Asymptotics in Statistics: Some Basic Concepts*, second edition, Wiley, March 2006.

[3] H. Sengar, H. Wang, D. Wijesekera and S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 6, pp. 794-805, June 2008.

[4] SIPp, [Online:]http://sipp.sourceforge.net/.

[5] A. Gilbert, S. Guha, P. Indyk, S. Muthukrishnan and M. Strauss, "Quicksand: Quick Summary and Analysis of Network Data," DIMACS Technical Report 2001-43, 2001.

[6] B. Krishnamurthy, S. Sen, Y. Zhang and Y. Chen, "Sketch-based Change Detection: Methods, Evaluation, and Applications," in *Proc. ACM SIGCOMM IMS*, 2003.

[7] M. Thorup and Y. Zhang, "Tabulation Based 4-Universal Hashing with Applications to Second Moment Estimation," in *Proc. the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, 2004.

[8] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*, fourth edition, Addison Wiley, April 2007.

[9] 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, 2006.

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

[11] H. Wang, D. Zhang and K. Shin, "Detecting SYN Flooding Attacks," in *Proc. IEEE INFOCOM*, 2002.

[12] S. Jin and D. Yeung, "A Covariance Analysis Model for DDoS Attack Detection," in *Proc. IEEE International Conference on Communications*, 2004.

[13] C. Chen and L. Liu, "Forecasting Time Series with Outliers," *Journal of Forecasting*, 1993.

[14] A. Lakhina, M. Crovella and C. Diot, "Mining Anomalies Using Traffic Feature Distributions," in *Proc. ACM SIGCOMM*, August 2005.

[15] S. Ehlert, C. Wang, T. Magedanz and D. Sisalem, "Specification-based Denial-of-Service Detection for SIP Voice-over-IP Networks," in *Proc. the Third International Conference on Internet Monitoring and Protection*, 2008.

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

[17] 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" in *Proc. IEEE INFOCOM*, 2006.

978-1-4244-4148-8/09/$25.00 ©2009