This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks

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

***Abstract*—Denial of Service (DoS) attacks such as the SIP flooding pose great threats to normal operations of VoIP networks, and can bear various forms to elude detection. In this paper, we address the stealthy SIP flooding attack, where intelligent attackers deliberately increase the flooding rates in a slow pace. As the attack only gradually influences the traffic, it can effectively be disguised from previous SIP flooding detection methods. In order to identify the stealthy attack in its early stage for timely response, we propose a detection scheme based on the signal processing technique *wavelet*, which is able to quickly expose the changes induced by the attack. In particular, we monitor the percentage of energy corresponding to the detail signal obtained from the wavelet analysis as an indication of the attack. Also, considering the scalability of the proposed scheme, we resort to the *sketch* technique, which can summarize the traffic observations to a fixed-size hash table to provide raw traffic signals for the wavelet analysis regardless of how many users exist in the VoIP network. We validate the performance of the proposed scheme through computer simulation and demonstrate its ability to quickly and accurately detect the attacks.**

I. Introduction

The immense popularity of Voice over IP (VoIP) brings increasingly rising security concerns. VoIP widely adopts the Session Initiation Protocol (SIP) [1] to control and manage calls. Thus exploiting the openness of SIP and the underlying IP infrastructures, attackers can easily launch Denial of Service (DoS) attacks such as the SIP flooding to exhaust the resources of their targets. Such attacks pose great threats to the VoIP services and can totally put normal network operations in jeopardy. One special form of the attacks is called the stealthy SIP flooding attack, where intelligent attackers deliberately increase the flooding rates in a slow pace. Although slow and seemingly unnoticeable, the attack is still able to gradually degrade the processing capability of the targets and bring serious damages to the network. In this paper, we address the important issue on how to quickly and accurately detect the stealthy SIP flooding attack.

Generally, intrusion detection techniques are classified into two major approaches: signature based and behavior based. In the signature based approach, attack patterns are profiled as signatures and detection is based on pattern matching between ongoing traffic and the signatures. This approach is not viable in our case to detect the stealthy flooding attacks, as attackers can randomly manipulate their strategy which makes profiling every possible attack signature very difficult. In the behavior based approach, profiles of normal traffic are first established, and attacks are detected as long as significant deviations from the normal profiles are identified. Our detection scheme adopts the behavior based approach.

The SIP flooding attacks normally cause sudden changes in the network traffic, and previous schemes [2], [3] utilize this fact to detect the attacks. However, as the stealthy flooding attack does not induce immediately noticeable changes to the traffic, it is able to elude detection from these schemes. Particularly, as the attacking rate only increases slightly or even keeps the same in consecutive sampling periods, existing detectors such as the Hellinger distance are not able to effectively identify changes in traffic.

In this paper, we propose a scheme based on the *wavelet* analysis to address quick detection of the stealthy SIP flooding attack. The fundamental reason for the ineffectiveness of the detection schemes in [2], [3] is that they fail to identify the deviation from normal traffic brought by the attack. Wavelet is a signal processing technique which can extract information from the raw traffic signal by decomposing the signal to enable observations on different levels, i.e., approximation signal and detail signal. This is also known as multi-resolution analysis (MRA). In the proposed scheme, we monitor the percentage of energy corresponding to the detail signal obtained from the wavelet analysis, which keeps low under the normal traffic condition but will increase sharply after the attack starts. This enables the scheme to expose the deviation brought by the stealthy attack in real time and achieve quick detection even though the attack only slowly influences the network traffic. Moreover, considering the scalability of the proposed scheme, we resort to the *sketch* technique, which can summarize the traffic observations to a fixed-size hash table regardless of how many users exist in the VoIP network. Sketch provides raw traffic signals for the wavelet analysis and has crucial impact on attack detection.

In summary, the paper has contributions in three aspects. 1) We propose a scheme to quickly detect the stealthy SIP flooding attack based on the wavelet analysis, by realizing the fact that the attack will cause immediate and sharp changes in the percentage of energy corresponding to the detail signal. 2) We adopt the sketch technique to establish fixed-size summaries of the traffic and provide raw signals for the wavelet analysis, regardless of the number of users in the network. 3) Computer simulation is conducted to validate the performance of the proposed detection scheme.

978-1-61284-233-2/11/$26.00 ©2011 IEEE

The rest of the paper is organized as follows. Section II reviews more related work. Section III describes the stealthy SIP flooding attack. The proposed detection scheme is presented in Section IV. Section V presents the performance evaluation through computer simulation. And Section VI concludes the paper.

II. Related Work

VoIP security surveys can be found in [4], [5]. SIP is one fundamental component of VoIP, and the SIP flooding attack is among the most severe threats to VoIP due to its simplicity to launch and abundance of available tools online. A natural idea for detecting flooding attacks is directly monitoring the traffic volume/rate [6], [7], where alarms are raised if the traffic volume during a time interval is larger than an adaptive threshold estimated based on historical traffic conditions. Unfortunately, such schemes can not detect the stealthy attack as the adaptive threshold is always prompted by the attack. If static thresholds are used, volume/rate based schemes are able to detect the stealthy attack, but may result in long detection latency and high false alarm rates. However, using the proposed scheme, we can quickly and accurately detect the attack right after the attack starts.

Wavelet analysis has been used in [8], [9], [10] for network anomaly or DoS attack detection, which utilize the coefficients transformed from the original traffic signal to identify changes induced by the attack. However, none of them explore wavelet's power to detect the stealthy flooding attack.

The malformed message attack is another major category of DoS attacks on VoIP networks [11]. SIP defines many open-ended control message implementations to allow including additional capabilities over time. However, this also provides attackers easy chances to send malformed signaling messages by simply modifying values of some SIP header fields. Such attacks can easily consume a considerable amount of processing capacity of their targets, downgrading the targets' performance to process normal messages and manage calls. Evaluation and detection of these attacks can be found in [12], [13].

III. Stealthy SIP Flooding Attacks in VoIP Networks

A. VoIP with SIP

SIP is a signaling protocol widely used in VoIP to control and manage calls. A typical SIP environment consists of three basic components, User Agent Client (UAC), User Agent Server (UAS) and SIP proxy server. To establish a VoIP call, UAC sends an INVITE message to UAS through intermediate proxy servers, each of which also keeps a state for the call upon receiving the INVITE. If the UAS is willing to answer the call, it will respond with a 200 OK message. And the UAC will then send an ACK message to finish the three-way handshake for call establishment. The established media is transmitted directly between the two UAs and is carried by the Real-time Transport Protocol (RTP) [14]. Finally, when either of the UA wants to end the call, it sends a SIP BYE message again through the intermediate proxy servers to the other UA. The proxy servers then release the state kept for the call to make their resources available for future calls.

B. Stealthy SIP Flooding Attacks

Attackers can flood malicious INVITE messages to SIP proxy servers only aiming to overwhelm the servers. The traditional flooding attacks with sudden high rates bring quicker damages to the VoIP networks, but also cause obvious changes in traffic, i.e., the number of INVITE messages received at a certain proxy server suddenly becomes very high. This makes the attack easily noticeable and may soon be detected. If adequate prevention measures are also in place, the overall damage of the attack can quickly be mitigated.

The stealthy SIP flooding attack is launched by intelligent and patient attackers who start their attacks with no rush using a low initial rate r_0. And then they will periodically increase the current attack rate r_n in a slow pace following

$$r_n = r_{n-1} + \Delta r \tag{1}$$

where Δr is the increment of the attack rate at each burst period T. The stealthy attack does not cause sudden directly observable changes in traffic. Also, attackers can manipulate a smaller Δr and a longer T to further hide the attack behavior. The attack can bring damages to the network in a long time scale even though initially it may seem harmless. Even worse, attackers can take advantage of the open-ended implementation of SIP to cause more harms. In particular, they can specify desired call durations to the proxy servers through the "Session-Expires" extension header [15] in each INVITE message of the stealthy attack and reserve resources for these INVITEs on the servers as long as they want. Thus no matter how slow the attack rate initially is, the attackers can gradually eat up all the resources on the proxy servers and paralyze the VoIP services. To effectively prevent the stealthy SIP flooding attack from severely damaging the VoIP networks, we need to quickly detect it in the early stage.

IV. Detection Scheme Design

Our detection scheme mainly consists of two steps, namely, the sketch traffic summarization and the wavelet based attack detection. Sketch provides fixed-size manageable raw traffic signals no matter how many users exist in the VoIP network. And wavelet analysis extracts information from the raw signals to quickly expose changes brought by the stealthy SIP flooding attack. The two steps are performed after every sampling period Δt to identify whether there is attack existing in the period.

A. Sketch Traffic Summarization

The sketch data structure is a probabilistic data summarization technique. It randomly aggregates high dimensional data streams into a fixed-size summary with smaller dimensions through the use of hash operations.

Each input data item $a_i = (k_i, v_i)$ to sketch consists of a key k_i and its associated value v_i. When a new data item a_i

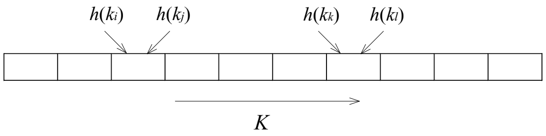

Fig. 1. Illustration of a sketch table.

arrives, its key is first hashed through $h(k_i)$, which becomes the index of a_i in the sketch table. The associated value v_i will then be added to the entry with the index $h(k_i)$ of the table. In our scheme, we use SIP address as the key and the number of INVITE messages from the address as the associated value.

Fig. 1 illustrates a sketch table of size K. As shown in the figure, the hash function $h(x)$ randomly aggregates INVITE messages from multiple SIP addresses into one entry. Therefore, suppose that the original message stream has a high dimension of X, applying the hash function can reduce its dimension to a smaller fixed number K. We use one sketch table to summarize the traffic stream from one sampling period Δt and the resultant "sketched" data will be used in the following wavelet analysis.

The random aggregation of sketch comes with a cost of information loss due to the use of hash operations. A remedy for this can be using multiple sketch tables each of which is associated with an independent hash function [3]. Wavelet analysis could then be applied separately to every sketch table and the final detection result would be based on the consensus among them. However, as we will see, just one hash table is already able to achieve high detection accuracy. Thus it is not necessary to use the multiple table approach.

The sketch traffic summarization is crucial for our detection. Even though the number of users in a VoIP network is dynamic, sketch can ensure that raw traffic signals from all sampling periods are of the same length, which provides great convenience for the wavelet based detection. We will also see the impact of sketch on detection in our experimental results.

B. Wavelet Based Detection

Suppose that the raw traffic signal obtained from sketch of a sampling period is S, which has K elements. We use wavelet analysis to decompose S into an approximation signal A and a detail signal D, and monitor the percentage of energy corresponding to D for attack detection.

As S has limited number of elements, we perform wavelet analysis through the Discrete Wavelet Transform (DWT). In particular, we choose one of the most commonly used DWT, the Daub4 [16] transform due to its simplicity and also its effectiveness in identifying the stealthy flooding attacks. The Daub4 transform has two sets of coefficients, the scaling coefficients $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and the wavelets coefficients $\{\beta_1, \beta_2, \beta_3, \beta_4\}$. The coefficients are pre-defined constants [16] and satisfy the relationship $\beta_k = (-1)^{k-1}\alpha_{4-(k-1)}$. Using the scaling coefficients, the Daub4 scaling signals V can be expressed as a $\frac{K}{2} \times K$ matrix

$$V = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_3 & \alpha_4 & 0 & 0 & 0 & 0 & \dots & \alpha_1 & \alpha_2 \end{pmatrix}.$$

Similarly, using the wavelets coefficients $\{\beta_1, \beta_2, \beta_3, \beta_4\}$, we can express the Daub4 wavelets also as a $\frac{K}{2} \times K$ matrix W.

Applying V and W to transform S, we obtain the trend signal and the fluctuation signal

$$a_i = \sum_{j=1}^{K} S_j V_{ij} \qquad \text{for} \quad i \in \{1, 2, \dots, \frac{K}{2}\} \tag{2}$$

$$d_i = \sum_{j=1}^{K} S_j W_{ij} \qquad \text{for} \quad i \in \{1, 2, \dots, \frac{K}{2}\}. \tag{3}$$

Next, using the trend signal and the fluctuation signal as coefficients, we calculate the approximation signal A and the detail signal D through

$$A_j = \sum_{i=1}^{\frac{K}{2}} a_i V_{ij} \qquad \text{for} \quad j \in \{1, 2, \dots, K\} \tag{4}$$

$$D_j = \sum_{i=1}^{\frac{K}{2}} d_i W_{ij} \qquad \text{for} \quad j \in \{1, 2, \dots, K\}. \tag{5}$$

Then our detector, the percentage of energy corresponding to the detail signal D is

$$P^d = \frac{\sum_{j=1}^{K}(D_j)^2}{\sum_{j=1}^{K}(A_j)^2 + \sum_{j=1}^{K}(D_j)^2}. \tag{6}$$

P^d keeps low under the normal traffic condition. However, when the stealthy flooding attack starts, P^d will immediately have a sharp increase even though there has not been directly observable changes in traffic. Thus monitoring P^d enables us to quickly identify whether there is attack existing in the network.

A threshold is needed to define the detection rule for each sampling period. To accurately keep track of the normal traffic condition, we use a dynamic threshold h based on the Exponential Weighted Moving Average (EWMA) method. Suppose that p^d_{n-1} is the smoothened P^d and v_{n-1} is the mean deviation of the previous sampling period computed through EWMA [3]. We have the threshold h_n of the current sampling period as

$$h_n = \lambda \cdot p^d_{n-1} + \mu \cdot v_{n-1} \tag{7}$$

where λ and μ are multiplication factors used to set a safe margin for the threshold and thus avoid false alarms. Also, to maintain the information about normal traffic behavior under attacks, we freeze h as a constant once it is exceeded by P^d and only restart to update h again after P^d comes below [3]. As a side benefit, this "threshold freezing scheme" also helps us trace the durations of attacks, because only during attacks can h be lower than P^d.

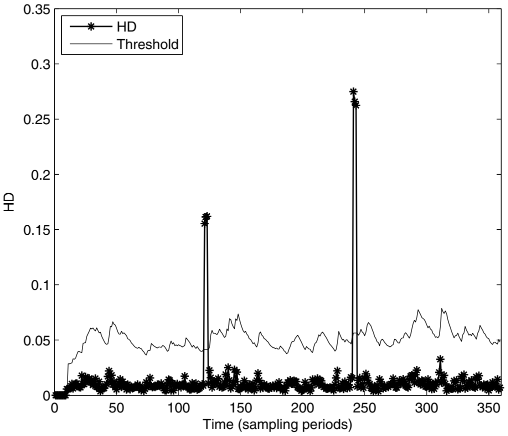

Fig. 2. Detection of traditional flooding using HD.

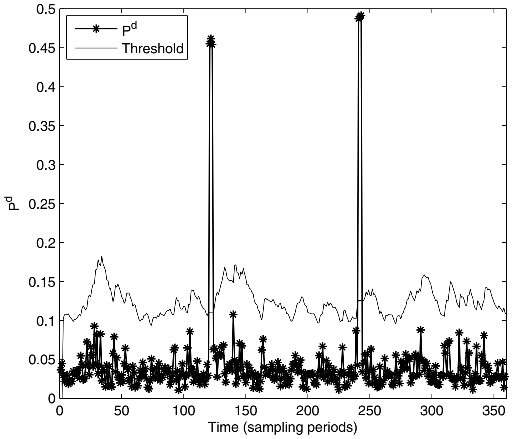

Fig. 3. Detection of traditional flooding using P^d.

Finally, suppose that P_n^d is the value of P^d of sampling period n, the detection rule is given by

$$\delta_n = \begin{cases} 1 & if \quad P_n^d \geq h_n \\ 0 & if \quad P_n^d < h_n \end{cases} \tag{8}$$

where δ_n is also an indicator function of whether there is attack existing in the VoIP network during the sampling period.

V. Performance Evaluation

A. Simulation Setup

We set up a VoIP network through computer simulation. In the normal traffic condition, the SIP INVITE generating rate is uniformly distributed from 25 per second to 75 per second with a mean of 50. The senders of these messages are randomly chosen from 100 normal users. Using the normal traffic as background, we inject malicious traffic from an attacker who is able to manipulate its INVITE generating rate. For the sketch traffic summarization, we set the sampling period $\Delta t = 10s$ and the table size $K = 32$ to achieve high detection resolution and low computational cost. For the threshold estimation parameters, we set $\lambda = 2.5$ and $\mu = 1$ as they are sufficient to capture the deviations brought by attacks without generating false alarms.

B. Detection of Traditional SIP Flooding Attacks

We first check the capability of the proposed scheme to detect the traditional flooding attacks, where the attack rate is suddenly brought up to a certain degree. We inject two attacks with the constant rate of 50 INVITEs per second, both of which last for 30 seconds. Fig. 3 shows the dynamic of P^d and the associated threshold. The two spikes clearly identify the two instances of attacks. Also due to the "threshold freezing scheme", the durations of the attacks, which are 3 sampling periods each, are precisely determined. Compared to Fig. 2, we see that the proposed scheme has comparable performance with the Hellinger distance (HD) based detection scheme [3] when dealing with traditional flooding attacks.

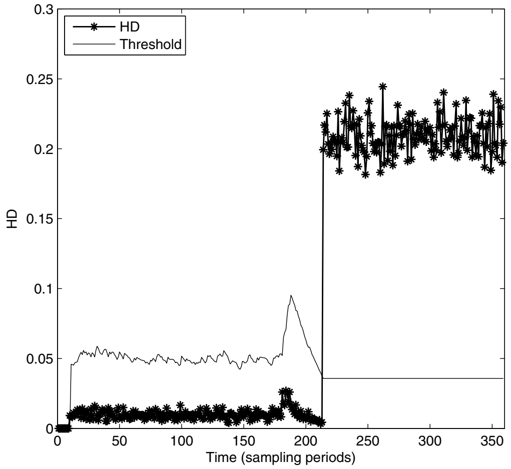

Fig. 4. Ineffectiveness of HD on stealthy flooding.

C. Detection of Stealthy SIP Flooding Attacks

We inject one instance of the stealthy flooding attack where the attacker gradually increases its INVITE generating rate by 5 every 30 seconds, i.e., $\Delta r = 5$ and $T = 30$, from the initial rate $r_0 = 0$. The attack starts from the 180th sampling period and lasts for 300 seconds.

Fig. 4 shows the result when we apply the HD based detection scheme against the attack. We can see that the attack totally tricks the scheme. First, as it does not bring great changes to HD, the attack is able to prompt the threshold higher rather than driving HD to exceed the threshold. Second, when the attack ends, it causes sudden decrease of the overall traffic rate in the network and consequently results in great changes to the traffic distribution. Therefore HD becomes suddenly high and the threshold ironically keeps freezed after traffic becomes normal [3], leading to persistent false alarms. Thus the HD based scheme is ineffective against the stealthy attack.

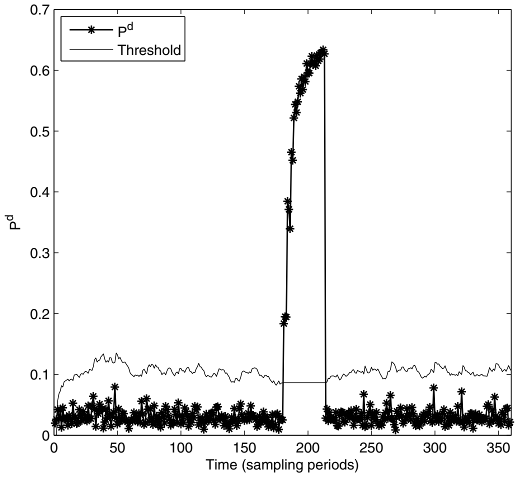

Fig. 5. Detection of stealthy flooding using P^d.

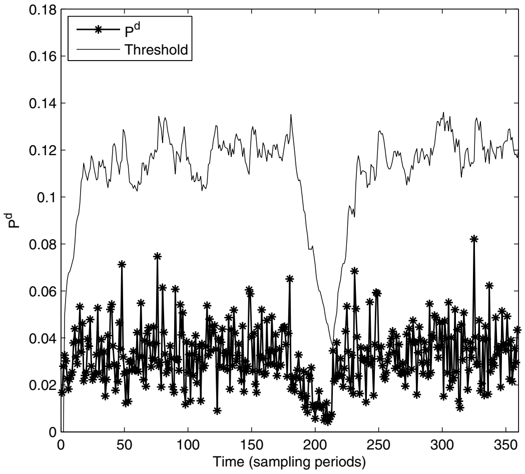

Fig. 6. Ineffectiveness of P^d on stealthy flooding without sketch.

Fig. 5 shows how the proposed detection scheme responds to the stealthy attack. As illustrated in the figure, P^d is very sensitive to the attack and has a sudden sharp increase almost right after the attack starts. Also, P^d is able to come down immediately to normal values after the attack ends as energy corresponding to the detail signal can not be affected by the attack any more. Due to the "threshold freezing scheme", we can again precisely determine the attack duration of 30 sampling periods, i.e., 300 seconds. Overall, the proposed scheme preserves the ability to quickly and accurately detect the stealthy flooding attack.

D. Impact of Sketch on Detection

Sketch provides fixed-size manageable raw traffic signals to the wavelet based attack detection regardless of the number of users in the network. Despite addressing the scalability issue, sketch also has crucial impact on detecting the attack. Fig. 6 shows the dynamics of the detector P^d in responding to the same stealthy attack as described above without taking the raw signals from sketch. Apparently P^d loses its sharpness in detecting attacks when sketch is not in place.

VI. Conclusion

In this paper, we propose a wavelet based detection scheme to address the stealthy SIP flooding attack in VoIP networks. Wavelet allows us to extract information from the raw traffic signal by decomposing the signal into different levels. Thus the detector identified by us, namely the percentage of energy corresponding to the detail signal, is able to quickly expose the changes brought by the stealthy attack even though the attack only slowly influences the traffic. Also, we utilize the sketch technique to provide fixed-size manageable raw traffic signals as the input to the wavelet based detection regardless of how many users exist in the network. Through computer simulation, we demonstrate the ability of the proposed scheme to quickly and accurately detect the attack. In our future work, we will work on to address the distributed stealthy flooding attacks and study the detection performance using different wavelet transforms.

References

[1] J. Rosenberg, H. Schulzrinne and G. Camarillo, "SIP: session initiation protocol," IETF RFC 3261, Jun. 2002.

[2] 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, pp. 794-805, Jun. 2008.

[3] J. Tang, Y. Cheng and C. Zhou, "Sketch-based SIP flooding detection using Hellinger distance," in *Proc. IEEE GLOBECOM*, 2009.

[4] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," *IEEE Network*, vol. 20, no. 5, pp. 26-31, Sept.-Oct. 2006.

[5] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert and D. Sisalem and S. Ehlert, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communication Surveys & Tutorials*, vol. 8, no. 3, pp. 68-81, 3rd. Qtr. 2006.

[6] B. Krishnamurthy, S. Sen, Y. Zhang and Y. Chen, "Sketch-based change detection: methods, evaluation, and applications," in *Proc. ACM SIGCOMM Conference on Internet Measurement*, 2003.

[7] 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.

[8] C. Huang, S. Thareja and Y. Shin, "Wavelet-based real time detection of network traffic anomalies," in *Proc. Securecomm and Workshops*, 2006.

[9] W. Lu, M. Tavallaee and A. Ghorbani, "Detecting network anomalies using different wavelet basis functions," in *Proc. Communication Networks and Services Research Conference*, 2008.

[10] G. Carl, R. Brooks and S. Rai, "Wavelet based denial-of-service detection," *Computers & Security*, vol. 25, no. 8, pp. 600-615, Nov. 2006.

[11] VoIPSA, "VoIP Security and Privacy Threat Taxonomy," Public Release 1.0, 2005.

[12] M. Rafique, M. Akbar and M. Farooq, "Evaluating DoS attacks against SIP-based VoIP systems," in *Proc. IEEE GLOBECOM*, 2009.

[13] J. Tang, Y. Hao, Y. Cheng and C. Zhou, "Detection of resource-drained attacks on SIP-based wireless VoIP networks," in *Proc. IEEE GLOBECOM*, 2010.

[14] H. Schulzrinne, S. Casner, R. Frederick and V. Jackson, "RTP: a transport protocol for real-time applications," IETF RFC 3550, Jul. 2003.

[15] S. Donovan and J. Rosenberg, "Session timers in the session initiation protocol (SIP)," IETF RFC 4028, Apr. 2005.

[16] I. Daubechies, *Ten Lectures on Wavelets*, Philadelphia, PA: SIAM, 1992.