Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 6705347, 9 pages
https://doi.org/10.1155/2019/6705347

Research Article

CCID: Cross-Correlation Identity Distinction Method for Detecting Shrew DDoS

Cheng Huang,[1] Ping Yi,[1] Futai Zou,[1] Yao Yao,[2] Wei Wang,[2] and Ting Zhu[2]

[1] *Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, School of Cyber Security, Shanghai Jiao Tong University, Shanghai, 200240, China*
[2] *Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, MD, 21250, USA*

Correspondence should be addressed to Ping Yi; yiping@sjtu.edu.cn

Received 28 June 2018; Revised 6 January 2019; Accepted 28 January 2019; Published 20 February 2019

Academic Editor: Pierre-Martin Tardif

This study presents a new method for detecting Shrew DDoS (Distributed Denial of Service) attacks and analyzes the characteristics of the Shrew DDoS attack. Shrew DDoS is periodic to be suitable for the server's TCP (Transmission Control Protocol) timer. It has lower maximum to bypass peak detection. This periodicity makes it distinguishable from normal data packets. By proposing the CCID (Cross-Correlation Identity Distinction) method to distinguish the flow properties, it quantifies the difference between a normal flow and an attack flow. Simultaneously, we calculated the cross-correlation between the attack flow and the normal flow in three different situations. The server can use its own TCP flow timer to construct a periodic attack flow. The cross-correlation between Gaussian white noise and simulated attack flow is less than 0.3. The cross-correlation between single-door function and simulated attack flow is 0.28. The cross-correlation between actual attack flow and simulated attack flow is more than 0.8. This shows that we can quantitatively distinguish the attack effects of different signals. By testing 4 million data, we can prove that it has a certain effect in practice.

1. Introduction

DDoS (Distributed Denial of Service) needs to send a large amount of data packets to the server in a short time, so that the server rejects the normal user's request. The attacker controls some of the hosts in the network and forges the network service request, so as to achieve the purpose of sending a large number of data packets to the server [1].

DDoS is no longer a traditional point-to-point attack mode. Attackers use different hosts to attack the server, so it is difficult for the server to detect the attacker through the port or IP header. When an attacker uses a random port attack, a large number of packets are sent to the target for different ports. When an attacker uses a fixed port attack, a large number of packets are sent to the target for the same port. At the beginning of the attack, the attacker will send a unified attack command to the hosts. Then the hosts send a large number of packets to the server at the same time, causing the server to be paralyzed.

Targeted traditional IDS (intrusion detection system) determines whether the server is attacked or not, according to the number of packets in the unit time [2]. When a flow of the server exceeds the system preset limit, the system will have a defensive response, thereby reducing the effect of DDoS [3].

According to the detection time classification, IDS is divided into real-time intrusion detection and delay intrusion detection. Real-time intrusion detection is based on the user's operation. When the invasion is found, the server immediately disconnects the attacker from the server [4]. Delay intrusion detection is mainly responsible for sorting the server's history. Analysis of the contents is handed over to the specialized management staff.

The TCP flow control mechanism typically uses a sliding form mechanism. When the sender's sending rate is too fast, it will trigger the TCP flow control mechanism. This mechanism can effectively solve the congestion problem and avoid deadlock.

Shrew DDoS is a variant of DDoS. Shrew DDoS is also known as ROQ (Reduction of Quality) attack. Because of low flow cyclical attacks, the server is forced to provide low quality services. An attacker needs to send a request to the server at a certain frequency to obtain the execution of the server TCP (Transmission Control Protocol) timer. Accordingly, the attacker sends the corresponding periodic pulse data flow and makes the route of the server congested. It will trigger a common speed limit mechanism for TCP flows, causing the server to reduce the packet rate to handle congestion problems.

Shrew DDoS attack flow limit is lower than ordinary DDoS. Shrew DDoS is often hidden in the normal TCP data flow, making IDS lost the effect [5]. The attack will cause the server to be in an inefficient operation, in some cases, more damaging than an ordinary DDoS attack.

In this study, we will focus on distinguishing between attackers and users.

(i) We characterize the simulated attack flow time domain curve, according to the reasonable cycle characteristics and flow characteristics, through the implementation of the server TCP timer.

(ii) We propose a CCID (Cross-Correlation Identity Distinction) flow differentiation method. By comparing the flow history with the correlation coefficient, the quantitative comparison results between the different flow histories are obtained. Different flow histories represent different flow users, and then we can distinguish between attackers and normal users.

The paper is organized as follows. Related works are discussed in Section 2. The distinction between normal user hosts and attacker hosts is discussed in Section 3. The validity of the correlation function is tested and evaluated in Section 4. The conclusion is drawn in Section 5.

2. Related Works

Researchers have conducted lot of work in security [6–8], including secure routing [9], intrusion detection [10–15], intrusion prevention [16, 17], smart grids security [18], and wireless network security [19, 20].

Since the signal has different characteristics in the frequency domain and in the time domain, we need to put the signal in the frequency domain for a considerable amount of processing. We use the Fourier transform to process the signal [21].

There are a lot of researches for DDoS detection and defense. Hao Chen and Yu Chen proposed an optimized design of reconfigurable PSD accelerator [22]. Then they also proposed a novel embedded accelerator for online detection [23]. Software flexibility that includes machine stability has proposed an embedded accelerator that uses FPGA for PSD analysis.

Jiahui Jiao et al. proposed a method to detect TCP-based DDoS attacks [24]. They identify two attack modes: fixed source IP attacks (FSIA) and random source IP attacks (RSIA).

In order to solve the DDoS attack, there are very many studies on IPS and IDS. Yali Yuan et al. have proposed two layers multiclass detection method for network intrusion detection system [25]. They compared the proposed TLMD method with the performance of existing algorithms using the detection rate, accuracy, and false alarm rate. The experimental results show that the proposed TLMD method has a low false alarm rate and a good detection rate based on the unbalanced data set.

With the development of machine learning, Valli Kumari V and Ravi Kiran Varma P have proposed a semisupervised intrusion detection system using active learning SVM and fuzzy c-means clustering [26]. This work demonstrates a hybrid semisupervised machine learning technique that uses active learning support vector machine (ASVM) and fuzzy C-means (FCM) clustering in an efficient IDS design. The algorithm was tested and found promising.

The group of E.M.Kakihata also proposed an intrusion detection system based on flows using machine learning algorithms [27]. They proved that this system could detect three different types of attacks and showed how it was used in machine learning algorithms.

Since DDoS attacks are no longer valid on the network, some variants of DDoS are generated. Among them, Shrew DDoS is a DDoS that can bypass IDS [28]. Shrew DDoS's maximum flow and total flow are similar to normal users, so it is difficult for IDS to distinguish between attackers and normal users.

TCP flow control flow mechanism can handle TCP high flow situation. But it may also be used by Shrew DDoS [29].

The system needs to detect Shrew DDoS attacks before the identity distinction. Yu Chen, Kai Hwang, and Yu-Kwong Kwok have done the relevant work [30].They identify and detect attacks by proposing new signal processing methods to address this challenge by checking the frequency domain characteristics of the server's inbound flow. The main advantage of the technology they propose is that their detection time is less than a few seconds.

A group of ZengGuang Liu has proposed a way in cloud computing to defend Shrew DDoS [31]. The simulation results show that the method proposed in this paper distinguishes the detection rate of abnormal network flow and the faster response time and prevents the impact of abnormal network flow group.

3. Distinguish between Normal User Hosts and Attacker Hosts

3.1. Converting Different Historical Data Flows into the Appropriate Time Domain Signal. When the system detects DDoS attacks, the system gets the server side data flow history. The server arranges the flow data according to the time, thus arranging the historical flow into a limited time domain signal. For different users, the historical flows are different. Attack flow must reach certain conditions before it can achieve the purpose of attack.

For a TCP timer, it checks congestion every fixed duration T. This is a system setting that is visible to the server. Considering the worst case, we assume that an attacker can use a simple heuristic to get the value of this T. We achieve the purpose of simulating the attack signal by constructing a T-cycle gate function in the time domain.

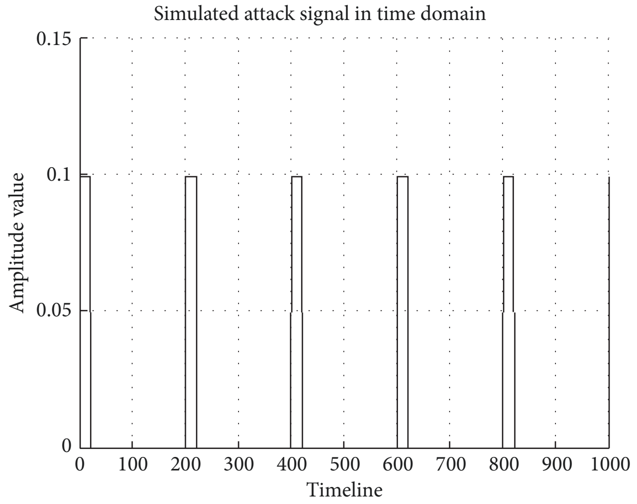


Figure 1: Simulated attack signal in time domain.

Figure 1 shows, according to the characteristics of simulated attack flow, that we constructed the simulated attack flow according to the preset period. The cycle of this flow is the same as the detection period, the width is the same as the detection duration, and the signal energy is normalized to the unit energy.

The signal is constructed from the system according to its own parameters as the basis for system testing.

The simulated attack flow characteristics are as follows:

(1) Periodic: Shrew DDoS attack flow constantly adjusts the attack cycle and the number of packets during the attack, until the system detection cycle is suitable. When a Shrew DDoS attack cannot be suitable for the server's TCP timer, it will reduce the attack effect or even failure.

(2) Lower Maximum: Shrew DDoS attack flow maximum is low. It is generally similar to the normal user's maximum or even lower. Ordinary DDoS can be detected by the IDS system because the maximum value is higher than the normal user. Shrew DDoS is more subtle than ordinary DDoS.

(3) Normal Fragment Flow: The single-cycle signal shape of the attack flow is similar to the short-term use of the normal user. The historical flow of an attack cycle is not enough to distinguish between attackers and normal users. The server needs to detect attack flow with historical flow for multiple attack cycles.

After Fourier transform, we can get the amplitude value in its frequency domain.

Figure 2 shows that this function has a higher amplitude in the low frequency domain.

3.2. Distinguishing between Different Time Domain Signals with Cross-Correlation Coefficients. We will treat different historical flow as a time domain signal, so that we can calculate the cross-correlation of various time domain signals. Since the total amount of different flow signals may be different, it needs to be normalized before or after calculation. For any two flow signals, the formula for calculating the inner product is as follows:

$$\left\langle u_i(t), u_j(t) \right\rangle = \int_{-\infty}^{+\infty} u_i(t)\, u_j(t)\, dt \tag{1}$$

The inner product is the cross-correlation coefficient of any two unit energy functions. It can reflect the similarity of any two unit energy functions. In this study, since the simulated attack signal has an arbitrary start in the time domain, the phase may not match the actual attack signal. When we calculate the inner product of the simulated attack signal and other signals, we need to shift simulated attack signal in the X axis and take the largest inner product for the cross-correlation coefficient. The formula is as follows:

$$R_{u_i,u_j} = \max_{\tau} \left\langle u_i(t), u_j(t+\tau) \right\rangle \tag{2}$$

At this time, we have $R_{u_i,u_j} = \rho_{u_i,u_j}$. Through this calculation, we can obtain the cross correlation coefficient of any two unit energy functions. As the situation of each user is not the same, the energy of the flow signal is different. The signal is not a unit energy function necessarily, so the signal needs to be normalized. One way to deal with, we will calculate the energy of each signal. The formula is as follows:

$$\epsilon_i = \int_{-\infty}^{+\infty} u_i^2(t)\, dt \tag{3}$$

Then we normalize the signals. The formula is as follows:

$$v_i = \frac{u_i(t)}{\left\| u_i(t) \right\|} = \frac{u_i(t)}{\sqrt{\epsilon_i}} \tag{4}$$

Each signal is processed into a unit energy function, and then the formula (x) is applied. Another way to deal with is that we directly calculate the correlation coefficient of two arbitrary functions. The formula is as follows:

$$\rho_{u_i,u_j} = \frac{\max_{\tau} \left\langle u_i(t), u_j(t+\tau) \right\rangle}{\sqrt{\epsilon_i \cdot \epsilon_j}} \tag{5}$$

By removing the energy factor while calculating the inner product, the cross-correlation coefficient between the two arbitrary functions is obtained.

3.3. Calculating the Correlation Coefficient in the Frequency Domain. We carry the Fourier transform of the signal. The formula is as follows:

$$F(\omega) = \mathscr{F}\left[f(t)\right] = \int_{-\infty}^{+\infty} f(t)\, e^{-i\omega t}\, dt \tag{6}$$

Since any function is translated in the time domain, after the Fourier transform, the performance in the frequency domain is the same. We can use the signal shape in the frequency domain to determine the similarity between the signals. The energy of the signal in the frequency domain is calculated in the same manner as in the time domain, and the normalized formula is the same. The inner product formula in the frequency domain has a little change. The formula is as follows:

$$\left\langle U_i(\omega), U_j(\omega) \right\rangle = \int_{-\infty}^{+\infty} U_i(\omega)\, U_j(\omega)\, d\omega \tag{7}$$

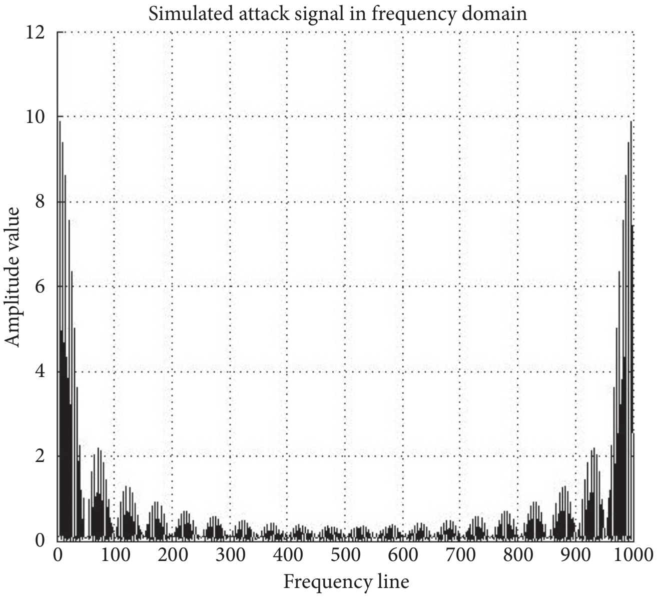


Figure 2: Simulated attack signal in frequency domain.

The inner product of frequency domain and time domain is similar, one for integration on the time axis and the other for integration on the frequency axis. We can also directly calculate the cross-correlation of two arbitrary functions on the frequency domain. The formula is as follows:

$$\rho_{U_\omega,U_\omega} = \frac{\left\| \left\langle U_i(\omega), U_j(\omega) \right\rangle \right\|}{\sqrt{\epsilon_i \cdot \epsilon_j}} \tag{8}$$

These two approaches are consistent and the conclusions are the same. By comparing the correlation coefficients, we can get the degree of similarity between the two signals. The server can calculate the similarity between the users and the simulated attack signal, in order to judge the rationality of user's data flow. By separating the attackers from the legitimate users, the server can only serve the legitimate users and ignore the attackers, so as to achieve the purpose of protecting the server.

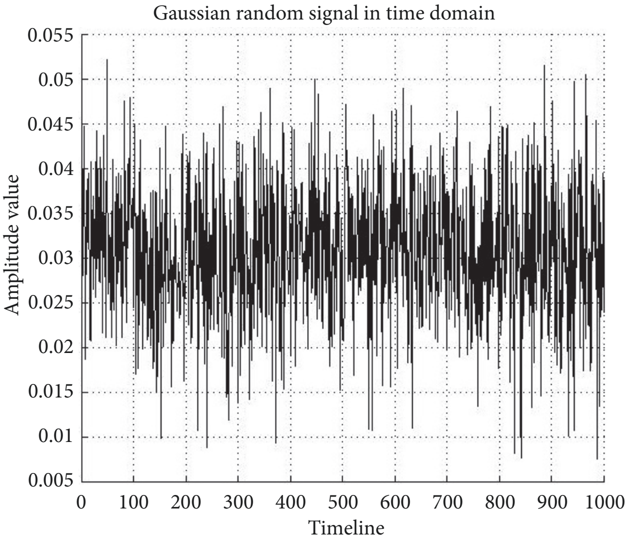


Figure 3: Gaussian random signal in time domain.

4. Test and Analysis

4.1. Test the Difference between Gaussian White Noise and Simulated Attack Flow. We have generated a set of random flow in the time domain to simulate the normal user who has been requesting the service. Figure 3 shows that we use Gaussian white noise to make the flow have certain randomness.

At the same time, we turn it into a signal representation on the frequency domain. In the time domain and the frequency domain, the distribution of Gaussian white noise is generally averaged and the details are not averaged. The characteristics of Gaussian signal and noise are closest. Gaussian signal is more convincing than other signals.

Figure 4 shows that the Gaussian white noise in the frequency domain is more average. At the same time, this flow can be seen as a result of a linear addition to a signal with a small cycle and a random signal.

According to the formula for calculating the cross-correlation in Section 3, we can calculate the cross-correlation between Gaussian white noise and simulated attack flow. As shown in Figure 5, we compare their cross-correlation to their autocorrelation.

Figure 5 shows the three columns are time domain correlation coefficient, frequency domain cross-correlation coefficient, and autocorrelation coefficient. We can see that the correlation between Gaussian white noise and attack flow is low. Since the signal has values in the finite time domain, it can reflect their correlation. But it is sufficient to see that they are less interrelated and the degree of similarity is not high.

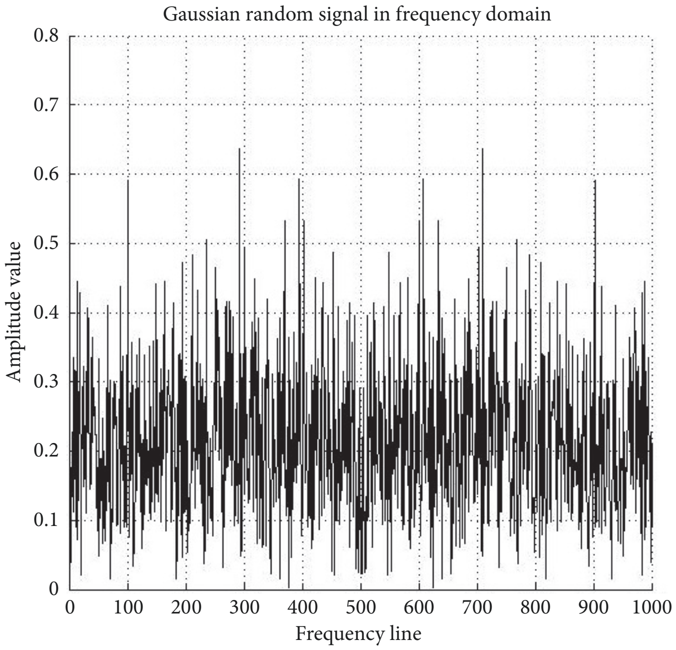


Figure 4: Gaussian random signal in frequency domain.

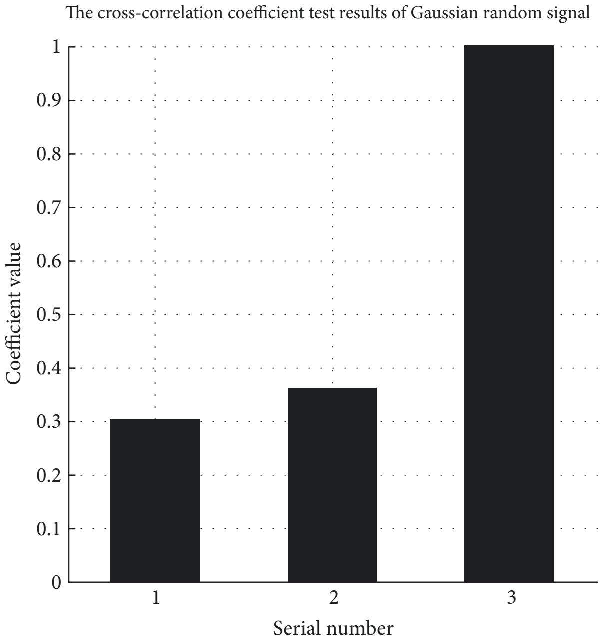


Figure 5: The cross-correlation coefficient test results of Gaussian random signal.

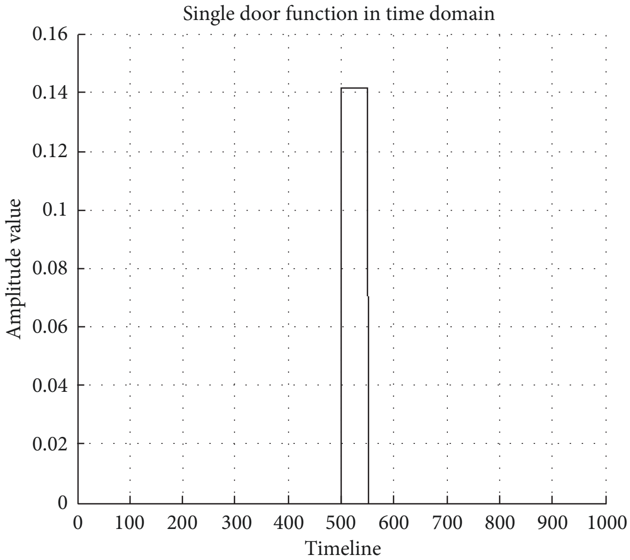


Figure 6: Single-door function in time domain.

It is shown that the correlation between the attack flow and the flow with different cycles is low and the correlation between the attack flow and the random message flow is low.

4.2. Test the Difference between a Single-Door Function and a Simulated Attack Flow. Figure 6 shows that we have generated a set of single-gate signals in the time domain to simulate bursts of users who use a large number of requests for services.

It has the same proportion but does not have the periodicity. In the frequency domain, the shape of the gate signal is similar to the sinc function.

Figure 7 shows that a single-gate signal in a narrower time can also be regarded as a pulse signal. In practice, the users may suddenly generate a large number of request service packets to the server which belong to the normal range. The results are shown as Figure 7.

Figure 8 shows that the three columns are time domain correlation coefficient, frequency domain cross-correlation coefficient, and autocorrelation coefficient. We can see that the correlation between the single-gate signal and the attack

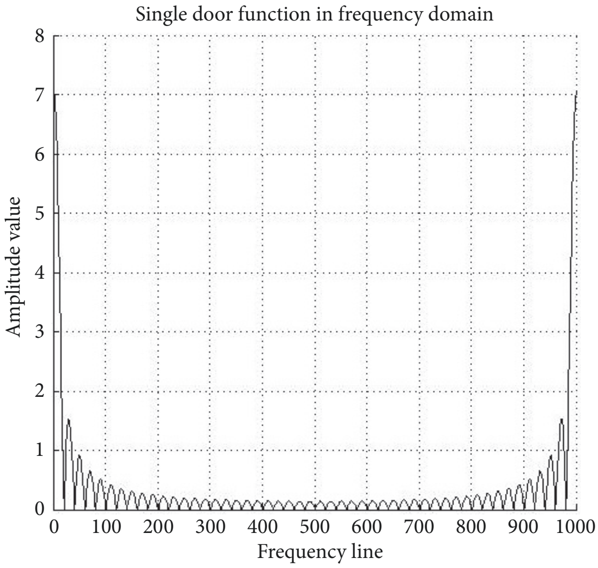


Figure 7: Single-door function in frequency domain.

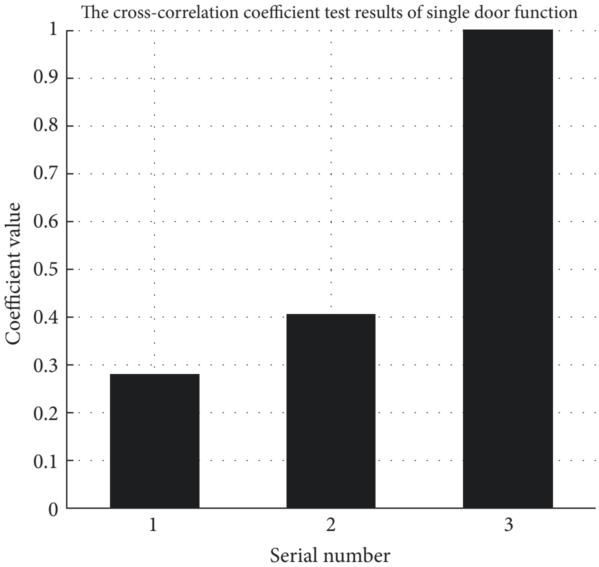


Figure 8: The cross-correlation coefficient test results of single-door function.

flow is low. Single-door functions do not have periodic characteristics, so they are not similar and the correlation coefficient is low.

It is shown that the correlation between attack flow and nonperiodic flow is low.

4.3. Test the Difference between Actual Attack Flow and Simulated Attack Flow. We use the user host to Shrew DDoS attacks and record the packet history flow on the server side to get the actual attack flow.

In practice, the initial gate function is adjusted according to the server's speed limit strategy and attack signal will quickly change to the appropriate periodic function, as the picture shows.

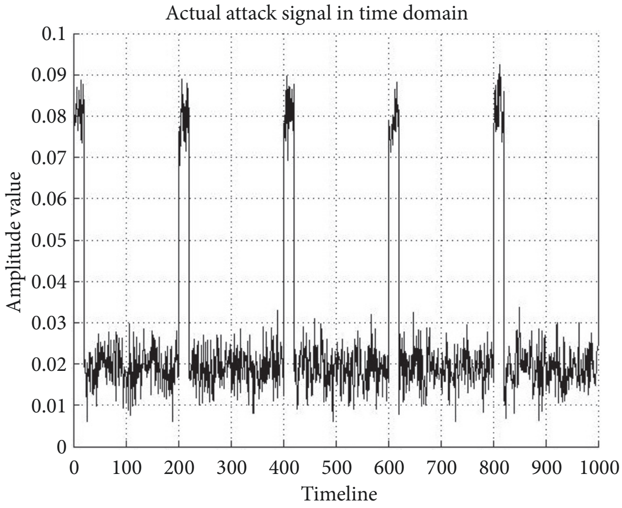


Figure 9: Actual attack signal in time domain.

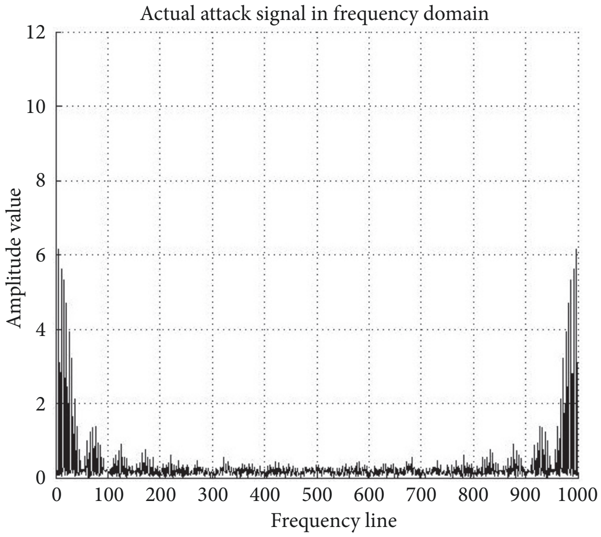


Figure 10: Actual attack signal in frequency domain.

Figure 9 shows that the actual attack flow has a certain channel disturbance. Its shape will be some Gaussian white noise characteristics, as the picture shows.

Figure 10 shows that the difference between the actual attack flow and the simulated attack flow is mainly reflected in the difference between the initial value and the translation in the time domain. According to the formula in Section 3, we calculate and compare.

In practice, when the attack flow changes based on the feedback of the server, it tends to approach the simulated attack flow. Even if the attacker found our detection strategy, it cannot modify the attack cycle. If the attack flow cycle keeps away from the TCP timer cycle, it will lead to a sharp decline in the attack effect. The results are as Figure 11.

Figure 11 shows that the three columns are time domain correlation coefficient, frequency domain cross-correlation coefficient, and autocorrelation coefficient. We can see that

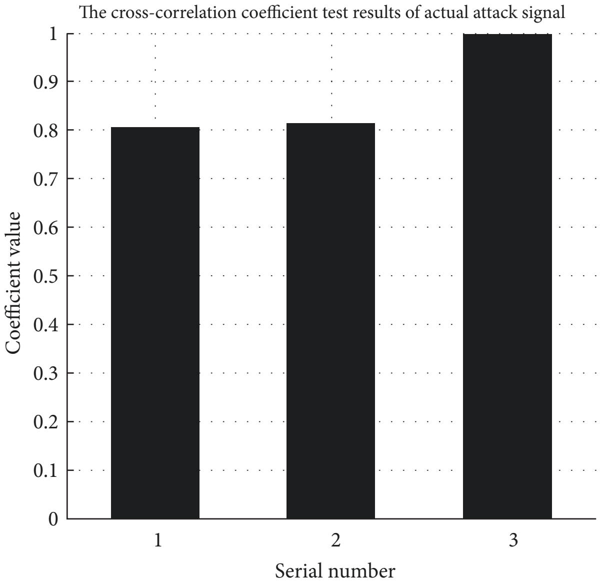


Figure 11: The cross-correlation coefficient test results of actual attack signal.

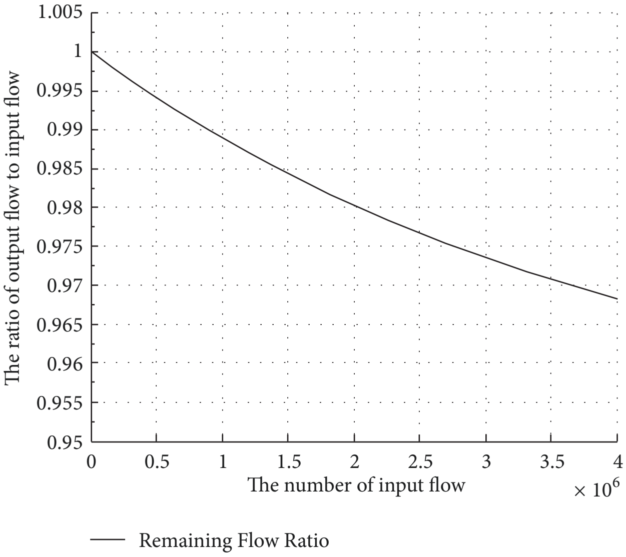


Figure 12: Ratio of input flow to output flow.

similar degree between the actual attack flow and the simulated attack flow is very high.

While the period of the attack flow is close to the period of the TCP timer, the cross-correlation between the actual attack flow and the simulated attack flow rises sharply.

4.4. Real Environment Test. In this study, we experiment on more than 4 million DNS messages of BAIDU from regular sources. Figure 12 shows that data cleaning was performed. The curve dropped fast and stabilize at a value. It shows that some packets in the data flow are filtered. By monitoring the cross-correlation between them, the IP packets with the highest cross-correlation with the attack signals are canceled.

As shown in the Figure 12, as the packets are entered, the number of filtered packets increases. At the same time, the number of remaining packets in the flow decreases. After one million input packets enter, the proportion of packets received by the system dropped to less than 99 percent. However, after three million input packets enter, the proportion of packets received by the system is still higher than 97 percent. By comparing the input flow and output flow, we can find that data is filtered. At the beginning, the curve will drop faster and then stabilize at a value.

After cleaning, it can be clearly seen that some packets in the data stream are filtered. On the one hand, because the proportion of attacker in the actual flow cannot be known, the efficiency of flow cleaning cannot be determined. On the other hand, the experiment can show that this method has filtering and cleaning effects for attack flow actually.

5. Conclusions

In the study, we place the server's historical data throughout the time domain so that the flow data is treated as a finite signal in the time domain. Through the time attribute of the TCP flow, we directly construct the appropriate simulated attack flow signal according to the system related settings. The proposed simulated attack flow signal has the characteristics of periodic, lower maximum, and normal fragment flow.

We compare the simulated attack flow with Gaussian white noise, single-door function, and actual attack flow. We find that they cannot be distinguished by the value of the time domain. Then we calculate the cross-correlation in the time domain. The cross-correlation coefficient between the simulated attack flow and the actual attack flow is high and the cross-correlation coefficient with the other two signals is low. It helps us to distinguish the attack flow from the normal users.

We carried out the Fourier transform of the three signals to obtain their representation in the frequency domain. We calculate the frequency domain functions of these three signals and can also obtain the correlation coefficient. Then we can get the same conclusion in the frequency domain and time domain. When multiple signals are superimposed, the system will get a mathematical mean of the cross-correlation coefficients of single signals. It shows that when users use linear superposition of these two flows, the method can effectively distinguish between the normal users and the attackers.

We also test the method in real environment. As shown in the test, attacker is continuously filtered while flow is stabilized at a normal value without affecting normal users.

Data Availability

The test data used to support the findings of this study have not been made available because these data belong to the ISP (Internet Service Provider).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61571290, 61831007, and 61431008), National Key Research and Development Program of China (2017YFB0802900, 2017YFB0802300, and 2018YFB0803503), the NSFC Zhejiang Joint Fund for the Integration of Industrialization and Informationization under grant (U1509219), Shanghai Municipal Science and Technology Project under grants (16511102605, 16DZ1200702), Information Network Security Key Laboratory of the Ministry of Public Security Open Project Support (C18611), and NSF grants 1652669 and 1539047.

References

[1] S. Latha and S. J. Prakash, "A survey on network attacks and Intrusion detection systems," in *Proceedings of the 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017.

[2] E. M. Chakir, "A real-time risk assessment model for intrusion detection systems using pattern matching," in *Proceedings of the International Conference on Information Technology and Communication Systems*, 2017.

[3] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, Y. Gong, D. J. Parish, and J. A. Chambers, "Using pattern-of-life as contextual information for anomaly-based intrusion detection systems," 2017.

[4] S. Iannucci, H. A. Kholidy, A. D. Ghimire, R. Jia, S. Abdelwahed, and I. Banicescu, "A comparison of graph-based synthetic data generators for benchmarking next-generation intrusion detection systems," in *Proceedings of the IEEE CLUSTER*, 2017.

[5] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069–1083, 2014.

[6] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *Journal of Network and Computer Applications*, vol. 59, no. 1, pp. 325–332, 2016.

[7] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "A denial of service attack in advanced metering infrastructure network," in *Proceedings of the 2014 IEEE International Conference on Communications (IEEE ICC 2014)*, Sydney, Australia, 2014.

[8] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web phishing detection using a deep learning framework," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–9, 2018.

[9] T. Zhu, S. Xiao, Y. Ping, D. Towsley, and W. Gong, "A secure energy routing mechanism for sharing renewable energy in smart microgrid," in *Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm 2011)*, pp. 17–20, Brussels, Belgium, 2011.

[10] P. Yi, T. Zhu, J. Ma, and Y. Wu, "An intrusion prevention mechanism in mobile ad hoc networks," *Ad-Hoc & Sensor Wireless Networks*, vol. 17, no. 3-4, pp. 269–292, 2013.

[11] P. Yi, T. Zhu, N. Liu, Y. Wu, and J. Li, "Cross-layer detection for black hole attack in wireless network," *Journal of Computational Information Systems*, vol. 8, no. 10, pp. 4101–4109, 2012.

[12] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. 2014, Article ID 240217, 8 pages, 2014.

[13] P. Yi, Y. Wu, and J. Chen, "Towards an artificial immune systems in detection of anomalies in wireless mesh networks," *China Communications*, vol. 8, no. 3, pp. 107–117, 2011.

[14] P. Yi, Y. Wu, N. Liu, and Z. Wang, "Intrusion detection for wireless mesh networks using finite state machine," *China Communications*, vol. 7, no. 5, pp. 40–48, 2010.

[15] P. Yi, X. Jiang, and Y. Wu, "Distributed intrusion detection for mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 19, no. 3, pp. 851–859, 2008.

[16] P. Yi, F. Zou, X. Jiang, and J. Li, "Muti-agent cooperative intrusion response in mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 18, no. 4, pp. 785–794, 2007.

[17] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "Green firewall: an energy-efficient intrusion prevention mechanism in wireless sensor network," in *Proceedings of IEEE Global Communications Conference(GLOBECOM 2012)*, Anaheim, Calif, USA, 2012.

[18] X. D. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.

[19] P. Yi, Y. Wu, F. Zou, and N. Liu, "A survey on security in wireless mesh networks," *IETE Technical Review*, vol. 27, no. 1, pp. 6–14, 2010.

[20] P. Yi, F. Zou, Y. Zou, and Z. Wang, "Performance analysis of mobile ad hoc networks under flooding attacks," *Journal of Systems Engineering and Electronics*, vol. 22, no. 2, pp. 334–339, 2011.

[21] K. Satpathi, Y. M. Yeap, A. Ukil, and N. Geddada, "Short-time fourier transform based transient analysis of vsc interfaced point-to-point dc system," *IEEE Transactions on Industrial Electronics*, 2017.

[22] H. Chen, Y. Chen, D. H. Summerville, and Z. Su, "An optimized design of reconfigurable PSD accelerator for online shrew DDoS attacks detection," in *Proceedings of the IEEE INFOCOM*, pp. 1780–1787, 2013.

[23] H. Chen and Y. Chen, "A novel embedded accelerator for online detection of shrew DDoS attacks," in *Proceedings of the International Conference on Networking, Architecture, and Storage*, pp. 365–372, 2008.

[24] J. Jiao, B. Ye, Y. Zhao et al., "Detecting tcp-based ddos attacks in baidu cloud computing data centers".

[25] Y. Yuan, L. Huo, and D. Hogrefe, "Two layers multi-class detection method for network intrusion detection system," in *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)*, 2017.

[26] V. V. Kumari and P. R. K. Varma, "A semi-supervised intrusion detection system using active learning SVM and fuzzy c-means clustering," in *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017.

[27] D. R. Pereira, F. A. D. Silva, H. Molinasapia, E. M. Kakihata, and R. T. Oiakawa, "Intrusion detection system based on flows using machine learning algorithms," *IEEE Latin America Transactions*, vol. 15, no. 10, p. 1998, 2017.

[28] J. Luo and X. Yang, "The newShrew attack: a new type of low-rate TCP-Targeted DoS attack," in *Proceedings of the IEEE International Conference on Communications*, pp. 713–718, 2014.

[29] H. Rastegarfar, M. Glick, N. Viljoen et al., "TCP flow classification and bandwidth aggregation in optically interconnected

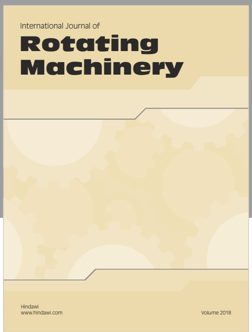
data center networks," *IEEE/OSA Journal of Optical Communications Networking*, vol. 8, no. 10, pp. 777–786, 2016.

[30] Y. Chen, H. Kai, and Y. K. Kwok, "Filtering of shrew ddos attacks in frequency domain," in *Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary*, pp. 786–793, 2005.

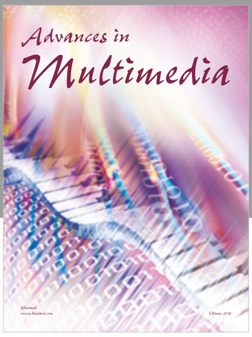
[31] Z. G. Liu, X. C. Yin, and H. J. Lee, "A new network flow grouping method for preventing periodic shrew ddos attacks in cloud computing," in *proceedings of the International Conference on Advanced Communication Technology*, pp. 66–69, 2016.

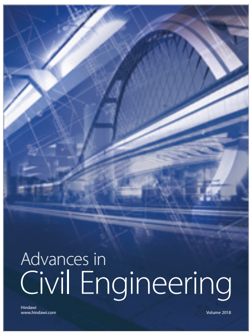
Journal of
Engineering

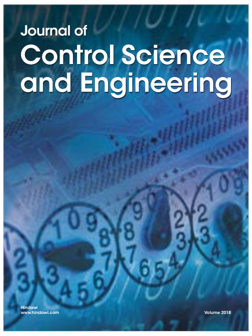
The Scientific World Journal


International Journal of
Rotating Machinery

Journal of
Sensors

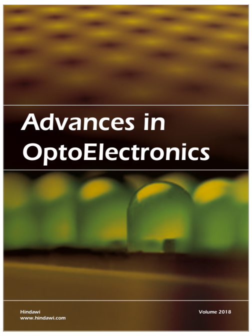

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science and Engineering

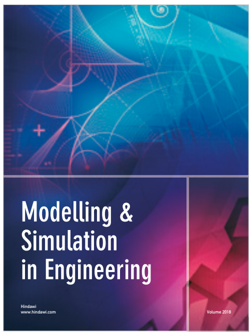
Journal of
Robotics

Journal of
Electrical and Computer Engineering

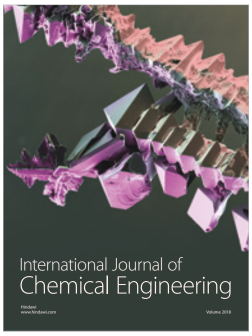

Advances in
OptoElectronics

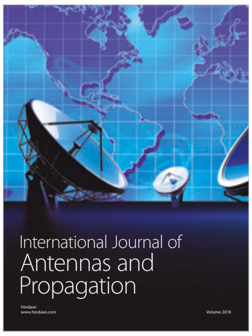
VLSI Design

International Journal of
Navigation and Observation

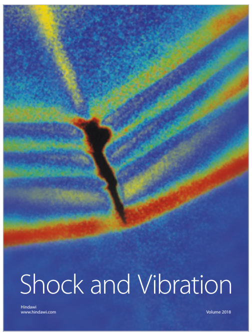

Modelling & Simulation in Engineering

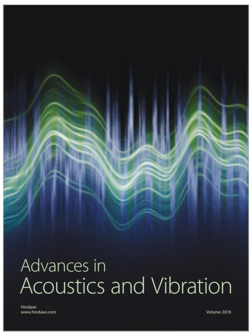
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration