Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2012, Article ID 860569, 12 pages
doi:10.1155/2012/860569

Research Article

A Model to Partly but Reliably Distinguish DDOS Flood Traffic from Aggregated One

Ming Li[1] and Wei Zhao[2]

[1] *School of Information Science & Technology, East China Normal University, No. 500, Dong-Chuan Road, Shanghai 200241, China*
[2] *Department of Computer and Information Science, University of Macau, Avenue Padre Tomas Pereira, Taipa, Macau SAR, China*

Correspondence should be addressed to Ming Li, ming_lihk@yahoo.com

Received 23 April 2011; Accepted 7 June 2011

Academic Editor: Shengyong Chen

Reliable distinguishing DDOS flood traffic from aggregated traffic is desperately desired by reliable prevention of DDOS attacks. By reliable distinguishing, we mean that flood traffic can be distinguished from aggregated one for a predetermined probability. The basis to reliably distinguish flood traffic from aggregated one is reliable detection of signs of DDOS flood attacks. As is known, reliably distinguishing DDOS flood traffic from aggregated traffic becomes a tough task mainly due to the effects of flash-crowd traffic. For this reason, this paper studies reliable detection in the underlying DiffServ network to use static-priority schedulers. In this network environment, we present a method for reliable detection of signs of DDOS flood attacks for a given class with a given priority. There are two assumptions introduced in this study. One is that flash-crowd traffic does not have all priorities but some. The other is that attack traffic has all priorities in all classes, otherwise an attacker cannot completely achieve its DDOS goal. Further, we suppose that the protected site is equipped with a sensor that has a signature library of the legitimate traffic with the priorities flash-crowd traffic does not have. Based on those, we are able to reliably distinguish attack traffic from aggregated traffic with the priorities that flash-crowd traffic does not have according to a given detection probability.

1. Introduction

Attackers may take the advantages of the principles [1] of distributed systems (i.e., the internet), such as openness, resources sharing, assessability, and so on, to launch distributed denial of service (DDOS) attacks. The threats of DDOS attacks to the individuals are severe. For instance, any denial of service of a bank server implies a loss of money, disgruntling or losing customers.

According to the classification of the CERT Coordination Center (CERT/CC), DDOS attacks are divided into three categories [2]: (1) flood (i.e., bandwidth) attacks, (2) protocol attacks, and (3) logical attacks. This paper considers flood attacks. DDOS flood attacks consume resources (e.g., bandwidth) by sending flood packets in order to shut down the target or significantly degrade its performance. The flood packets may be generated by hundreds or thousands of machines distributed all over the world.

A network-based intrusion detection system (IDS) monitors the traffic on its network as a data source [3]. In this regard, there are two main approaches. One is misuse detection and the other anomaly detection. Solutions given by misuse detection are primarily based on a library of known signatures to match against network traffic. Hence, unknown signatures from new variants of an attack mean 100% miss positives. As a matter of fact, the form in which an attack takes place is usually determined by a large number of details many of which are unknown. This is particularly true for DDOS attacks [4]. Hence, anomaly detectors play a role in DDOS detection [2, 3, 5–12]. Anomaly detectors cannot replace signature-based systems [2, 3]. From a practical view, therefore, the combination of a signature-based system and anomaly detector is worth noting [2].

A traffic series is a packet flow. A packet consists of a number of fields, such as protocol, source IP, destination IP, ports, flag setting (in the case of TCP or UDP), message type (in the case of ICPM), timestamp, and length (packet size). Each may serve as a feature of a packet for statistical detection purpose, see for example, [8, 13–15]. In addition, there are other available features of traffic, such as flow rate [16], the number of connections [17], and so on [6, 11, 12]. This paper takes traffic series in packet size (traffic series for short) as a monitored objective.

Usually, detections are expected to be adaptable to a wide range of network environments (e.g., [7, 8, 11–17]). Nevertheless, it is obviously worth studying detections that are environment dependent. This paper studies detecting signs of DDOS flood attacks in the underlying network to use static-priority schedulers.

As known, two tough issues in detecting DDOS flood attacks are (1) reliable detection as can be seen from [2, 3, 5, 7, 9, 10], and (2) distinguishing attack traffic from aggregated traffic [7, 9, 16]. The solution to the first issue is crucial to practical applications because false positives can lead to inappropriate responses that cause denial of service to legitimate traffic. In addition, it is the basis to find the solution to the second.

It is noted that flash-crowd traffic and DDOS flood traffic may have similar statistics from a network view. DDOS flood is malicious but flash crowds legitimate. Flash crowds happen when a huge number of users try to access the same server simultaneously for some specific events (e.g., the NASA Pathfinder mission) [16]. Because an attacker aims at attacking the target such that it denies services of all legitimate traffic, we assume DDOS flood traffic has all priorities in all classes. On the other hand, according to the nature of differentiated services, we assume that flash-crowd traffic does not have all priorities. Further, we suppose that the protected site is equipped with a sensor that has a signature library of the legitimate traffic with the priorities flood crowds do not have. In these cases, DDOS flood attack traffic can be distinguished, according to a given detection probability, from aggregated traffic with the priorities flash crowds do not have.

The rest of paper is organized as follows. Section 2 introduces the randomized traffic regulator for feature extraction of arrival traffic. Section 3 considers the principle. A case study is demonstrated in Section 4; discussions are given in Section 5 and conclusions in Section 6.

2. Traffic Regulator and Its Randomization

There are two major areas of traffic modeling. One is based on random processes, see for example, [6, 8, 18–30]. The other is deterministically modeling, for example, traffic regulator [18, 30–33]. We take traffic regulator to characterize traffic in this research.

Definition 2.1 (see [31, 33]). Let $y(t)$ be the instantaneous rate of arrival traffic at time t. Then, the amount of traffic generated in the interval $[t_1, t_2]$ is upper bounded by

$$\int_{t_1}^{t_2} y(t)dt \le \sigma + \rho(t_2 - t_1), \tag{2.1}$$

where σ and ρ are constants and $t_2 > t_1$. This property is written as $y \sim (\sigma, \rho)$ that is called traffic regulator.

Practically, traffic is considered in the discrete case on an interval-by-interval basis. Thus, we generalize Definition 2.1 as follows.

Definition 2.2. Let $y(t)$ be the instantaneous rate of arrival traffic at t. Then, the amount of traffic generated in the nth interval $[(n-1)I, nI]$ $(n = 1, 2, \ldots, N)$ is upper bounded by

$$\sum_{t=(n-1)I}^{nI} y(t) \le \sigma(n, I) + \rho(n, I)I, \tag{2.2}$$

where $(\sigma(I, n), \rho(I, n))$ represents the traffic regulator in the nth interval, and I is a positively real number.

For the simplicity, denote $F(I, n) = \sigma(I, n) + \rho(I, n)I$.

Definition 2.3. Let $y^i_{p,j,k}(t)$ be the instantaneous rate of all flows of class i with priority p going through server k from input link j at t. Then, the amount of $y^i_{p,j,k}(t)$ generated in the nth interval $[(n-1)I, nI]$ $(n = 1, 2, \ldots, N)$ is upper bounded by $F^i_{p,j,k}(I, n)$. That is, $\sum_{y=(n-1)I}^{nI} y^i_{p,j,k}(t) \le F^i_{p,j,k}(I, n)$.

Definition 2.3 provides a feature of arrival traffic $y^i_{p,j,k}(t)$ on an interval-by-interval basis. Theoretically, I can be any positively real number. In practice, however, I is selected as a finite positive integer.

Usually, $F^i_{p,j,k}(I, n) \ne F^i_{p,j,k}(I, q)$ for $n \ne q$. Therefore, $\{F^i_{p,j,k}(I, n)\}$ $(n = 1, 2, \ldots)$ is a random process. Computing the sample mean of $F^i_{p,j,k}(I, n)$ in terms of I yields

$$\frac{1}{I}\sum_{m=1}^{I} F^i_{p,j,k}(m, n) = \overline{F}^i_{p,j,k}(n). \tag{2.3}$$

Usually, $\overline{F}^i_{p,j,k}(n_1) \ne \overline{F}^i_{p,j,k}(n_2)$ for $n_1 \ne n_2$. In practice, if $I \ge 10$, $\overline{F}^i_{p,j,k}(n)$ quite accurately follows Gaussian distribution regardless of the distribution of $F^i_{p,j,k}(I, n)$ [34]. Denote $A = \mathrm{Var}[\overline{F}^i_{p,j,k}(n)]$ and $B = E[\overline{F}^i_{p,j,k}(n)]$, where Var and E are operators of variance and mean, respectively. Then, one can use the sample distribution of $\overline{F}^i_{p,j,k}(n)$ as follows: $[B - \overline{F}^i_{p,j,k}(n)]/\sqrt{A} = z$, where z follows the standard Gaussian distribution. Thus,

$$\overline{F}^i_{p,j,k}(n) \sim \frac{1}{\sqrt{2\pi A}} e^{-[\overline{F}^i_{p,j,k}(n) - B]^2/2A}. \tag{2.4}$$

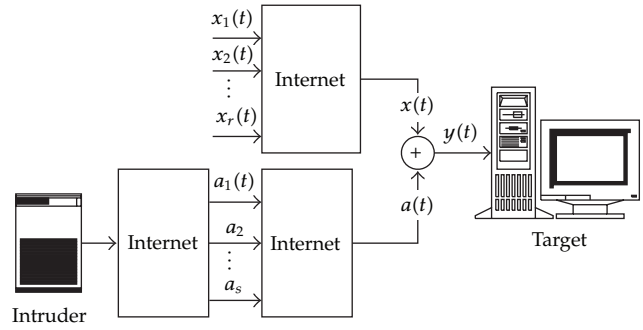

Figure 1: Illustration of DDOS flood attacks.

3. Principle

3.1. Detection Probability and Miss Probability

Normally, a server serves for a number of connections (clients) concurrently. Figure 1 illustrates a server that serves for r connections of normal traffic and s connections of attack traffic. Aggregated traffic $y(t)$ consists of normal traffic $x(t)$ and attack one $a(t)$.

In the case of $I \geq 10$, one has

$$\text{Prob}\left[z_{1-\alpha/2} < \frac{\overline{F}^{i}_{p,j,k}(n) - B}{\sqrt{A}} \leq z_{\alpha/2}\right] = 1 - \alpha, \tag{3.1}$$

where $(1 - \alpha)$ is called confidence coefficient. Let $C^{i}_{p,j,k}(\alpha)$ be the confidence interval with $(1 - \alpha)$ confidence coefficient. Then,

$$C^{i}_{p,j,k}(\alpha) = \left(B - \sqrt{A}z_{\alpha/2}, B + \sqrt{A}z_{\alpha/2}\right). \tag{3.2}$$

The above expression exhibits that B is a template of $\overline{F}^{i}_{p,j,k}(n)$. Thus, we have $(1 - \alpha)\%$ confidence to say that $\overline{F}^{i}_{p,j,k}(n)$ normally takes the value of B as its approximation with the variation less than or equal to $\sqrt{A}z_{\alpha/2}$.

Denote that $\xi(n) = \xi = \overline{F}^{i}_{p,j,k}(n)$. Then,

$$\text{Prob}\left(\xi > B + \sqrt{A}z_{\alpha/2}\right) = \frac{\alpha}{2}. \tag{3.3}$$

On the other hand,

$$\text{Prob}\left(\xi \leq B - \sqrt{A}z_{\alpha/2}\right) = \frac{\alpha}{2}. \tag{3.4}$$

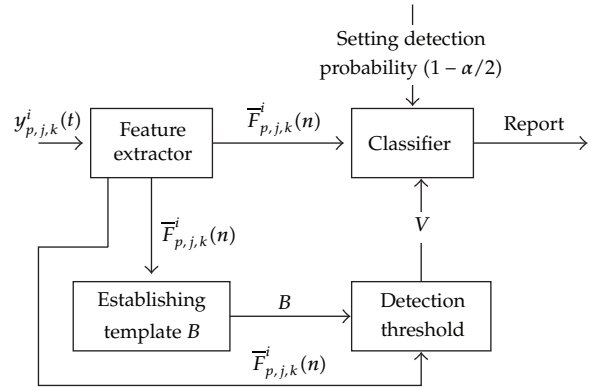

Figure 2: Diagram of detection model.

For facilitating the discussion, two terms are explained as follows. Correctly recognizing an abnormal sign means *detection* and failing to recognize it *miss*. We explain the detection probability and miss probability by the following theorem.

Theorem 3.1 (Detection probability). *Let*

$$V(\alpha) = V = B + \sqrt{A} z_{\alpha/2} \tag{3.5}$$

be the detection threshold. Denote $P_{\text{det}} = P\{V < \xi < \infty\}$ *as detection probability. Denote* P_{miss} *as miss probability. Then,*

$$P_{det} = P\{V < \xi < \infty\} = \left(1 - \frac{\alpha}{2}\right), \tag{3.6}$$

$$P_{miss} = \frac{\alpha}{2}. \tag{3.7}$$

Proof. The probability of $\xi \in C^i_{p,j,k}(\alpha)$ is $(1-\alpha)$. Accordingly, the probability of $\xi \leq V$ is $(1-\alpha/2)$. Therefore, the detection probability for $\xi > V$ is $(1-\alpha/2)$. Hence, (3.6) holds. Since $P_{\text{det}} + P_{\text{miss}} = 1$ [8], $P_{\text{miss}} = \alpha/2$. □

In the case of $P_{\text{det}} = 1$ and the computation precision being 4, one has

$$V = B + 4\sqrt{A}. \tag{3.8}$$

The diagram of our detection is indicated in Figure 2.

3.2. About False Alarm

False alarm means mistakenly recognizing a normal as abnormal. In this mechanism, detection criterion is $\overline{F}^i_{p,j,k}(n) > V(\alpha)$ with $P_{\text{det}} = (1-\alpha/2)$ and $P_{\text{miss}} = \alpha/2$. Therefore, if

$\overline{F}^i_{p,j,k}(n) > V(\alpha)$ happens in the case that $\overline{F}^i_{p,j,k}(n)$ comes from normal traffic and an alert is fired, then this alert will be a false alarm, which has the probability $\alpha/2$. Therefore,

$$P_{\text{false}} = P_{\text{miss}}. \tag{3.9}$$

In the case of $P_{\text{det}} = 1$, one has $P_{\text{false}} = P_{\text{miss}} = 0$.

3.3. Partly Distinguishing Attack Traffic

For the simplicity, suppose that traffic has two priorities p_1 and p_2. We further suppose that flash-crowd traffic has the priority p_1 but does not have p_2. Non-flash-crowd normal traffic has both p_1 and p_2 and DDOS flood traffic has both p_1 and p_2. Then, $\overline{F}^i_{p_2,j,k}(n) > V(\alpha)$ implies a detection that the traffic $y^i_{p_2,j,k}(t)$ contains attack traffic of class i at the server k from the link j in the nth interval. The detection probability is $(1 - \alpha/2)$.

Denote $y^i_{p_2,j,k}(t) = {}_x y^i_{p_2,j,k}(t) + {}_a y^i_{p_2,j,k}(t)$, where ${}_x y^i_{p_2,j,k}(t)$ and ${}_a y^i_{p_2,j,k}(t)$ are normal traffic and attack traffic with p_2, respectively. Note that ${}_x y^i_{p_2,j,k}(t)$ does not have the components of flash-crowd traffic.

Usually, a signature-based sensor is designed such that it has a library that contains signatures of attack traffic. In the present mechanism, however, we use a signature-based sensor that has a library to contain signatures of legitimate traffic with the priorities that flash-crowd traffic does not have. In this way, traffic whose signatures cannot be matched by this signature-based sensor may be taken as flood traffic or suspicious. Thus, if $\overline{F}^i_{p_2,j,k}(n) > V(\alpha)$ occurs, the flows that are in $y^i_{p_2,j,k}(t)$ and cannot be matched by the signature-based sensor are flood traffic of class i with p_2 at the server k from the link j in the nth interval. The reason to use a signature library of legitimate traffic instead of attack one is that attackers make efforts to create new variants of signatures but legitimate users usually do not. Figure 3 indicates the process of distinguishing attack traffic ${}_a y^i_{p_2,j,k}(t)$ from $y^i_{p_2,j,k}(t)$.

4. A Case Study

We consider fractional Gaussian noise (FGN), which is an approximation model of traffic time series [18, 19, 21, 22, 35, 36]. The autocorrelation function of discrete FGN is given by

$$R(l) = 0.5\sigma^2\left[||l| + 1|^{2H} - 2|l|^{2H} + ||l| - 1|^{2H}\right], \tag{4.1}$$

where $\sigma^2 = (\Gamma(2 - H)\cos(\pi H))/\pi H(2H - 1)$ is the strength of FGN [37], l is an integer, $\Gamma(\cdot)$ is the Gamma function, and $H \in (0.5, 1)$ the Hurst parameter.

In Figures 4, 5, 6, and 7, subscripts and superscripts of y and F are omitted. Consider TCP traffic series $y(t)$ $(40 \le y \le 1500$ (Bytes)), indicating the number of bytes in a packet at t. By simulating FGN, we have a series with $H = 0.6$ as shown in Figure 4. According to Definition 2.2, we obtain $F(I, n)$ (Bytes) as shown in Figure 5 $(n, I = 1, 2, \ldots, 16)$. Figure 6 indicates $\xi(n)$ (Bytes). The histogram of ξ is given in Figure 7.

From Figure 7, we attain $\mu_\xi = 3{,}105$ and $\sigma_\xi = 344.402$. Under the condition of $P_{\text{det}} = 1$, one has the interval [1720, 4467] and the threshold $V = 4{,}467$.

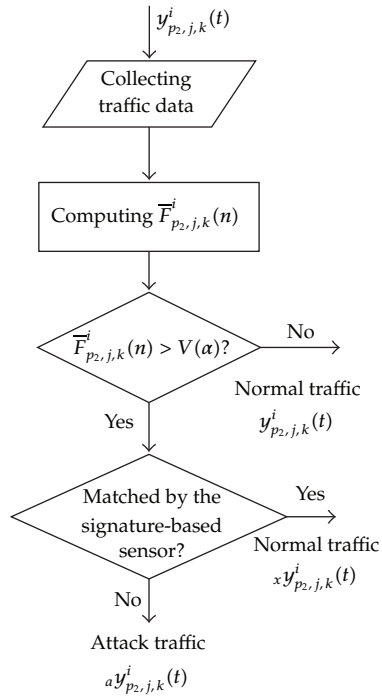

Figure 3: Distinguishing attack traffic.

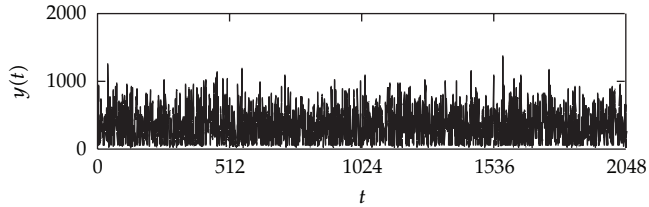

Figure 4: Synthesized FGN series.

5. Discussions

5.1. DiffServ Architecture: A Flexible Foundation

The above explanations only take the simple case of two priorities. In fact, there may be several priorities in a DiffServ domain, where applications are differentiated by their classes, and a certain portion of bandwidth is reserved for each class traffic [38]. Usually, all the flows in a class are assigned the same priority on each router. However, it is also available that the flows in a class may be assigned different priorities, and flows from different classes may have the same priority as can be seen from [32, Paragraph 5, Section 1, page 327]. This paper considers a class to be assigned different priorities. On the other side, the DiffServ architecture distinguishes two types of routers (edge routers and core routers) [32, Paragraph 2, Section 3, page 327]. Thus, a detector can be installed with either edge routers or core ones. Consequently, the DiffServ architecture provides a flexible foundation to design effective IDS to distinguish flood traffic from aggregated one. This paper is simply a beginning on this track.

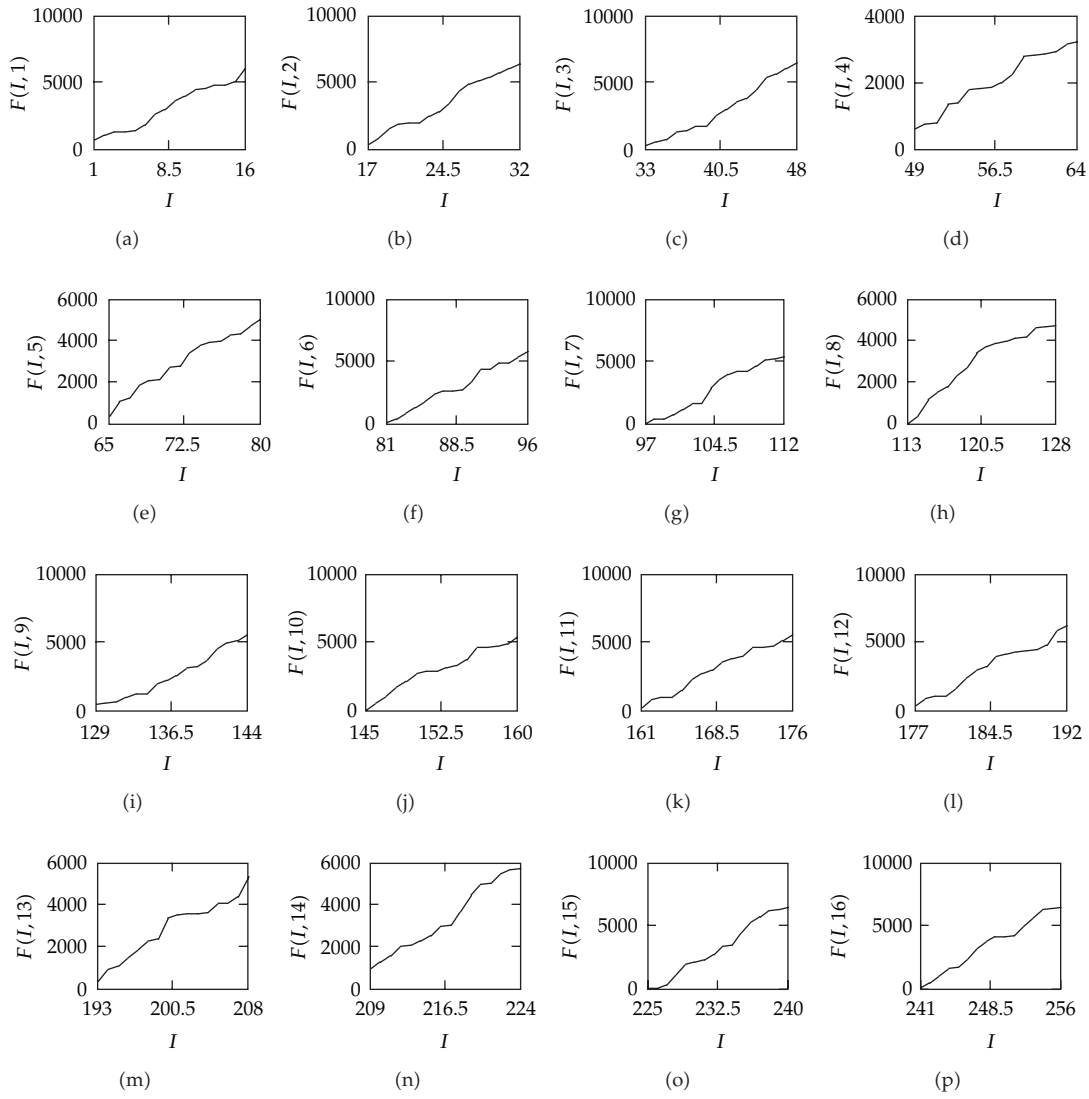

Figure 5: Illustrations of traffic regulators in different intervals.

5.2. Applicability

Mathematical properties of traditionally aggregated traffic time series have been studied deeply in a way, see for example, [18–22, 35]. However, math properties of aggregated traffic time series on a class-by-class basis for different priorities in the DiffServ domain are rarely seen. That is a main reason we use traffic regulator proposed by [33] because it is a tool particularly applicable in a flow-unaware environment. In addition to that, the traffic regulator is simple. Let T_m and T_c be the time for recording data and data processing, respectively. Suppose that we record a packet per 10 microsecond. Then, $T_m = 10^{-5}Q$ (second), where Q is the length of the series involved in computations. In the above case study, $Q = 16 \times 16 = 256$. Thus, $T_m = 2.56$ ms. One the other hand, T_c for a series of 256 length

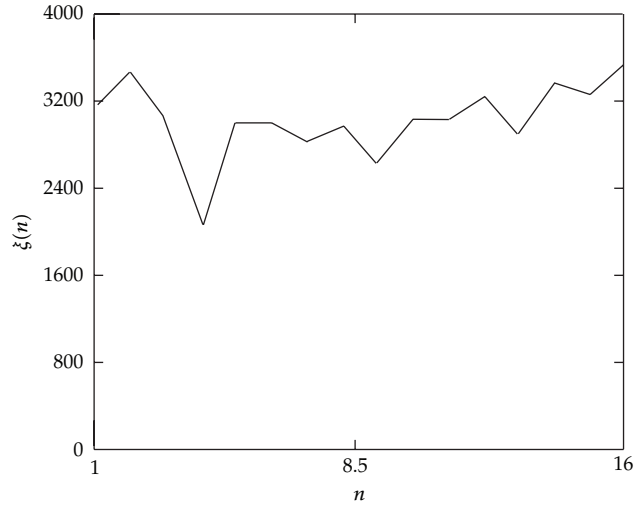

Figure 6: The sample mean of $\xi(n)$.

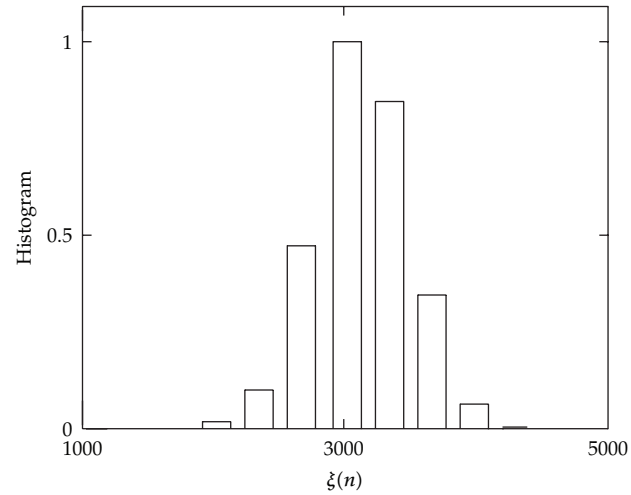

Figure 7: Histogram of ξ.

on an average Pentium IV PC is neglectable in comparison with T_m. This exhibits that the detection time is short enough to meet real-time use in practice.

It is worth noting that $\overline{F}^i_{p,j,k}(n)$ is a traffic pattern. In the present method, signs of DDOS flood attacks are identified by $\overline{F}^i_{p,j,k}(n) > V$, meaning traffic pattern under attacking must be significantly different from that of normal traffic. As a matter of fact, if an attacker were able to attack a target such that it would be overwhelmed by creating the floods that well mimic or be near to normal traffic, the target would be overwhelmed at its normal state even if there were no flood packets. This is obviously impossible even if the attacker knows normal traffic pattern exactly before attacking.

5.3. Future Work

The previous presentation is quite academic in the following senses. The detection mechanism previously exhibited was discussed based on postulated traffic models without analyzing real-traffic data. For this reason, we shall work on the traffic models in this paper with real-traffic data for anomaly detections. In addition, we will derive a general mechanism to reliably identify and distinguish attack traffic from aggregated traffic for the flows of class i with all priorities. In addition to that, we shall explore statistical learning methods discussed in other fields, see for example, [39–49].

6. Conclusions

This paper suggests a reliable method to detect signs of DDOS flood attacks in the DiffServ environment with static-priority schedulers. The present method can, with the combination of a signature-based sensor, partly but reliably distinguish attack traffic from aggregated traffic at a given server for a given link in a given time interval according to a predetermined detection probability. Given that static-priority schedulers are widely supported in current routers, it is our belief that this approach may be practical and effective in engineering.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China (NSFC) under the project Grant nos. 60873264, 61070214, and the China national 973 plan under the project number 2011CB302801/2011CB302802.

References

[1] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed Systems: Concepts and Design*, Addison-Wesley, 3rd edition, 2001.
[2] K. Liston, "Intrusion Detection FAQ: Can You Explain Traffic Analysis and Anomaly Detection?" July 2004, http://www.sans.org/security-resources/idfaq/anomaly_detection.php.
[3] E. Schultz, "Intrusion prevention," *Computers & Security*, vol. 23, no. 4, pp. 265–266, 2004.
[4] W. W. Streilein, D. J. Fried, and R. K. Cunninggham, "Detecting flood-based denial-of-service attacks with SNMP/RMON," in *Proceedings of the Workshop on Statistical and Machine. Learning Techniques in Computer Intrusion Detection*, George Mason University, September 2003.
[5] J. Leach, "TBSE—an engineering approach to the design of accurate and reliable security systems," *Computers & Security*, vol. 23, no. 1, pp. 22–28, 2004.
[6] S. H. Oh and W. S. Lee, "An anomaly intrusion detection method by clustering normal user behavior," *Computers & Security*, vol. 22, no. 7, pp. 596–612, 2003.
[7] F. Gong, *Deciphering Detection Techniques: Part III Denial of Service Detection, White Paper*, McAfee Network Security Technologies Group, 2003.
[8] M. Li, "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition," *Computers & Security*, vol. 23, no. 7, pp. 549–558, 2004.
[9] S. Sorensen, *Competitive Overview of Statistical Anomaly Detection, White Paper*, Juniper Networks, 2004, http://www.juniper.net.
[10] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview, supplement to computer," *IEEE Security & Privacy*, vol. 35, no. 4, pp. 27–30, 2002.
[11] S. B. Cho and H. J. Park, "Efficient anomaly detection by modeling privilege flows using hidden markov model," *Computers & Security*, vol. 22, no. 1, pp. 45–55, 2003.
[12] S. Cho and S. Cha, "SAD: web session anomaly detection based on parameter estimation," *Computers & Security*, vol. 23, no. 4, pp. 312–319, 2004.
[13] S. S. Kim, A. L. N. Reddy, and M. Vannucci, "Detecting traffic anomalies at the source though aggregate analysis of packet header data," in *Proceedings of the Networking*, vol. 3042 of *Lecture Notes in Computer Science*, pp. 1047–1059, Springer, Athens, Greece, May 2004.

[14] B. Bencsath and I. Vajda, "Protection against DDoS attacks based on traffic level measurements," in *Proceedings of the International Symposium on Collaborative Technologies and Systems*, W. W. Smari, Ed., William McQuay, 2004.
[15] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in *Proceedings of the DARPA Information Survivability Conference and Exposition*, vol. 1, pp. 303–314, Washington, DC, USA, April 2003.
[16] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," *Computer Communication Review*, vol. 32, no. 3, pp. 62–73, July 2002.
[17] J. B. D. Cabrera, B. Ravichandran, and R. K. Mehra, "Statistical modeling for network intrusion detection," in *Proceedings of the 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, San Francisco, Calif, USA, August-september 2000.
[18] H. Michiel and K. Laevens, "Teletraffic engineering in a broad-band era," *Proceedings of the IEEE*, vol. 85, no. 12, pp. 2007–2033, 1997.
[19] V. Paxson and S. Floyd, "Wide area traffic: the failure of poisson modeling," *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226–244, 1995.
[20] I. W. C. Lee and A. O. Fapojuwo, "Stochastic processes for computer network traffic modeling," *Computer Communications*, vol. 29, no. 1, pp. 1–23, 2005.
[21] J. Beran, *Statistics for Long-Memory Processes*, Chapman and Hall, New York, NY, USA, 1994.
[22] M. Garetto and D. Towsley, "An efficient technique to analyze the impact of bursty TCP traffic in wide-area networks," *Performance Evaluation*, vol. 65, no. 2, pp. 181–202, 2008.
[23] M. Li, "Change trend of averaged hurst parameter of traffic under DDOS flood attacks," *Computers & Security*, vol. 25, no. 3, pp. 213–220, 2006.
[24] H. G. Sun, Y. Q. Chen, and W. Chen, "Random-order fractional differential equation models," *Signal Processing*, vol. 91, no. 3, pp. 525–530, 2011.
[25] A. Scherrer, N. Larrieu, P. Owezarski, P. Borgnat, and P. Abry, "Non-gaussian and long memory statistical characterizations for internet traffic with anomalies," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 56–70, 2007.
[26] R. Delgado, "A reflected fBm limit for fluid models with ON/OFF sources under heavy traffic," *Stochastic Processes and their Applications*, vol. 117, no. 2, pp. 188–201, 2007.
[27] C. Cattani, "Harmonic wavelet approximation of random, fractal and high frequency signals," *Telecommunication Systems*, vol. 43, no. 3-4, pp. 207–217, 2010.
[28] C. Cattani, "Fractals and hidden symmetries in DNA," *Mathematical Problems in Engineering*, vol. 2010, Article ID 507056, 31 pages, 2010.
[29] E. G. Bakhoum and C. Toma, "Dynamical aspects of macroscopic and quantum transitions due to coherence function and time series events," *Mathematical Problems in Engineering*, vol. 2010, Article ID 428903, 2010.
[30] M. Li and W. Zhao, "Representation of a stochastic traffic bound," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1368–1372, 2010.
[31] C. S. Chang, "On deterministic traffic regulation and service guarantees: a systematic approach by filtering," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1097–1110, 1998.
[32] S. Q. Wang, D. Xuan, R. Bettati, and W. Zhao, "Providing absolute differentiated services for real-time applications in static-priority scheduling networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 2, pp. 326–339, 2004.
[33] R. Cruz, "A calculus for network delay. II. Network analysis," *IEEE Transactions on Information Theory*, vol. 37, no. 1, pp. 132–141, 1991.
[34] J. S. Bendat and A. G. Piersol, *Random Data: Analysis and Measurement Procedure*, John Wiley & Sons, 2nd edition, 1991.
[35] B. B. Mandelbrot, *Gaussian Self-Affinity and Fractals*, Springer, New York, NY, USA, 2002.
[36] Y. Q. Chen, R. Sun, and A. Zhou, "An improved hurst parameter estimator based on fractional fourier transform," *Telecommunication Systems*, vol. 43, no. 3-4, pp. 197–206, 2010.
[37] H. Sheng, H. Sun, Y. Q. Chen, and T. Qiu, "Synthesis of multifractional gaussian noises based on variable-order fractional operators," *Signal Processing*, vol. 91, no. 7, pp. 1645–1650, 2011.
[38] S. Black, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "Architecture for differentiated services," Tech. Rep. 2475, IETF, 1998.
[39] J. Chen, C. Hu, and Z. Ji, "An improved ARED algorithm for congestion control of network transmission," *Mathematical Problems in Engineering*, vol. 2010, Article ID 329035, 2010.
[40] M. Dong, "A tutorial on nonlinear time-series data mining in engineering asset health and reliability prediction: concepts, models, and algorithms," *Mathematical Problems in Engineering*, vol. 2010, Article ID 175936, 2010.

[41] M. Dong, "A novel approach to equipment health management based on auto-regressive hidden semi-Markov model (AR-HSMM)," *Science in China*, vol. 51, no. 9, pp. 1291–1304, 2008.
[42] Z. Liao, S. Hu, D. Sun, and W. Chen, "Enclosed laplacian operator of nonlinear anisotropic diffusion to preserve singularities and delete isolated points in image smoothing," *Mathematical Problems in Engineering*, vol. 2011, Article ID 749456, 15 pages, 2011.
[43] S. Hu, Z. Liao, D. Sun, and W. Chen, "A numerical method for preserving curve edges in nonlinear anisotropic smoothing," *Mathematical Problems in Engineering*, vol. 2011, Article ID 186507, 14 pages, 2011.
[44] W. Mikhael and T. Yang, "A gradient-based optimum block adaptation ICA technique for interference suppression in highly dynamic communication channels," *Eurasip Journal on Applied Signal Processing*, vol. 2006, Article ID 84057, 2006.
[45] S. Y. Chen, Y. F. Li, and J. W. Zhang, "Vision processing for realtime 3D data acquisition based on coded structured light," *IEEE Transactions on Image Processing*, vol. 17, no. 2, pp. 167–176, 2008.
[46] D. She and X. Yang, "A new adaptive local linear prediction method and its application in hydrological time series," *Mathematical Problems in Engineering*, vol. 2010, Article ID 205438, 2010.
[47] J. Chen, C. Hu, and Z. Ji, "Self-tuning random early detection algorithm to improve performance of network transmission," *Mathematical Problems in Engineering*, vol. 2011, Article ID 872347, 17 pages, 2011.
[48] H. Dong, Z. Wang, D. W. C. Ho, and H. Gao, "Variance-constrained H_∞ filtering for a class of nonlinear time-varying systems with multiple missing measurements: the finite-horizon case," *IEEE Transactions on Signal Processing*, vol. 58, no. 5, pp. 2534–2543, 2010.
[49] B. Shen, Z. Wang, and X. Liu, "Bounded H_∞ synchronization and state estimation for discrete time-varying stochastic complex networks over a finite horizon," *IEEE Transactions on Neural Networks*, vol. 22, no. 1, pp. 145–157, 2010.