Research Article

Bound Maxima as a Traffic Feature under DDOS Flood Attacks

Jie Xue,[1] Ming Li,[2] Wei Zhao,[3] and Sheng-Yong Chen[4]

[1] *Jiangsu Electronic Information Products Quality Supervision & Inspection Research Institute,*
China National Center for Quality Supervision and Test for the Internet of Things Products & Systems,
No. 100, Jin-Shui Road, Wuxi 214073, China

[2] *School of Information Science & Technology, East China Normal University, No. 500, Dong-Chuan Road,*
Shanghai 200241, China

[3] *Department of Computer and Information Science, University of Macau Av. Padre Tomas Pereira, Taipa,*
Macau SAR, P.R., China

[4] *College of Computer Science, Zhejiang University of Technology, Hangzhou 310023, China*

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

This paper gives a novel traffic feature for identifying abnormal variation of traffic under DDOS flood attacks. It is the histogram of the maxima of the bounded traffic rate on an interval-by-interval basis. We use it to experiment on the traffic data provided by MIT Lincoln Laboratory under Defense Advanced Research Projects Agency (DARPA) in 1999. The experimental results profitably enhance the evidences that traffic rate under DDOS attacks is statistically higher than that of normal traffic considerably. They show that the pattern of the histogram of the maxima of bounded rate of attack-contained traffic greatly differs from that of attack-free traffic. Besides, the present traffic feature is simple in mathematics and easy to use in practice.

1. Introduction

People nowadays are heavily dependent on the Internet that serves as an infrastructure in the modern society. However, distributed denial-of-service (DDOS) flood attackers remain great threats to it. By consuming resources of an attacked site, the victim may be overwhelmed such that it denies services it should offer or its service performances are significantly degraded. Therefore, intrusion detection system (ISD) for detecting DDOS flood attacks has been greatly desired.

There are two categories regarding IDSs. One is misuse detection and the other anomaly detection. Attacking alerts given by misuse detection is primarily based on a library of known signatures to match against network traffic, see, for example, [1–5]. Thus, attacking
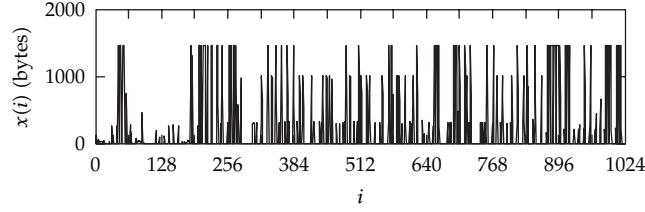
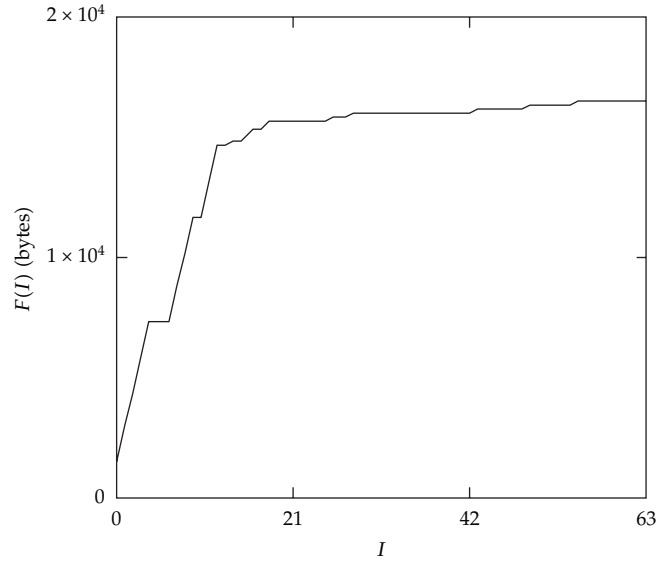**Figure 1:** Time series: OM-W1-1-1999AF for the first 1024 points.

Figure 2: Traffic upper bound of OM-W1-1-1999AF for $0 \leq I \leq 63$.

with unknown signatures from new variants of an attack can escape from being detected by signature-based IDSs with the probability one, see, for example, [6], making such a category of IDSs at the protected site irrelevant. However, based on anomaly detection, abnormal variations of traffic are identified as potential intrusion so that this category of IDSs are particularly paid attention to for identifying new attacking, see, for example, [7–13]. For the simplicity, in what follows, the term IDS is in the sense of anomaly detection.

Noted that the detection accuracy is a key issue of an anomaly detector, see, for example, [14, 15]. To be effective, IDSs require appropriate features for accurately detecting an attack and distinguishing it from the normal activity as can be seen from [10, Section IV]. Hence, developing new traffic features for anomaly detection is essential.

The reference papers regarding traffic features for IDS use are wealthy. For example, 86 features for clustering normal activities are discussed in [9]. Note that a selected feature is methodology-dependent. In this regard, [16] uses packet head data. The paper [17] utilizes autocorrelation function of long-range dependent (LRD) traffic time series in packet size and [18] employs the Hurst parameter. Scherrer et al. adopt scaling properties of LRD traffic [19].

The traffic models used in [17–23] are in the sense of fractal. In general, fractal models might be somewhat complicated in practical application in engineering in comparison with the traffic feature proposed in this paper.
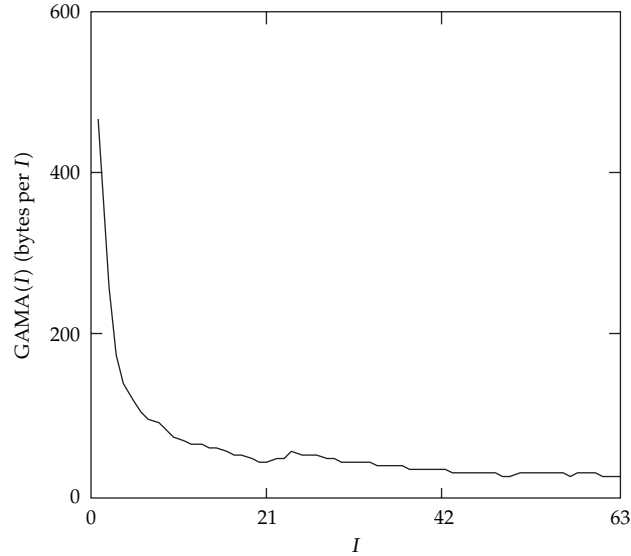
Figure 3: Traffic rate bound of OM-W1-1-1999AF for $0 \leq I \leq 63$.
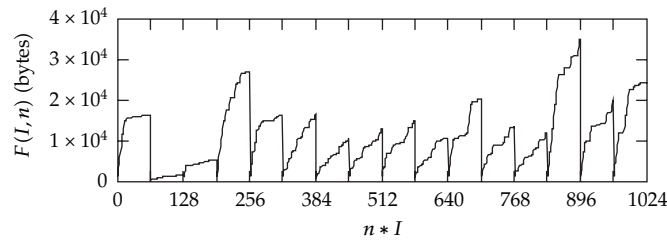

Figure 4: Traffic upper bound series for OM-W1-1-1999AF.

Recall that there are two categories in traffic modeling [24, Section XIV]. One is statistical modeling (e.g., LRD processes). The other bounded modeling, which has particular applications to modeling traffic at connection level, see, for example, [25–30]. Bounded models, in conjunction with a class of service disciplines, are feasible and relatively efficient in applications, such as connection admission control (CAC) in guaranteed quality-of-service (QoS). In addition, such models are simple in mathematics and relatively easy to be used in practice in comparison with fractal models. This paper aims at providing a new traffic feature for anomaly detection based on bounded modeling of traffic. The main contributions in this paper are as follows.

    (i) We present the histogram of the maxima of bounded traffic rate on an interval-by-interval basis as a traffic feature for exhibiting abnormal variation of traffic under DDOS flood attacks.

    (ii) The experimental results exhibit that the maxima of rate bound of attack-contained traffic is statistically greater than that of attack-free traffic drastically.

The rest of paper is organized as follows. Experimental data and related work are briefed in Section 2. The histogram of the maxima of traffic rate bound is proposed
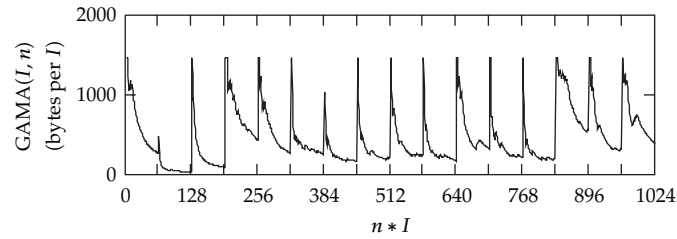
Figure 5: Traffic rate bound series for OM-W1-1-1999AF.
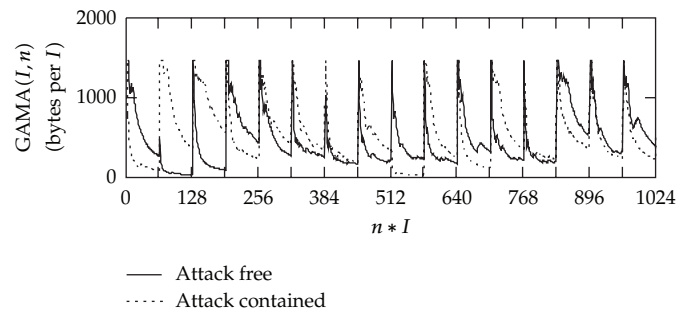

—— Attack free

····· Attack contained

Figure 6: Traffic rate bound series. Solid lines for attack-free traffic OM-W1-1-1999AF. Dot lines for attack-contained traffic OM-W1-1-1999AC.

in Section 3. Experimental results are demonstrated in Section 4, which is followed by discussions and conclusions.

2. Experimental Data and Related Work

2.1. Experimental Data

While DDOS attacks continue to be a problem, there is currently not much quantitative data available for researchers to study the behaviors of DDOS flood attacks. The data in the 1998-1999 DARPA (http://www.ll.mit.edu/IST/ideval) are valuable but rare for public use though there are points worth further discussion [31]. Those data were obtained under the conditions of realistic background traffic and mean examples of realistic attacks [32, 33]. The used data sets in 1999 contain more than 200 instances and 58 attacks types, see, for details [34]. Two data sets are explained below.

2.1.1. Set One: Attack-Free Traffic (1999 Training Data—Week 1)

The first set of data containing 5 traces. We name them by OM-W1-i-1999AF (i = 1, 2, 3, 4, 5), meaning Outside-MIT-week1-i-1999-attack-free. Table 1 indicates the actual times at which the first packet and last one were extracted for each trace.
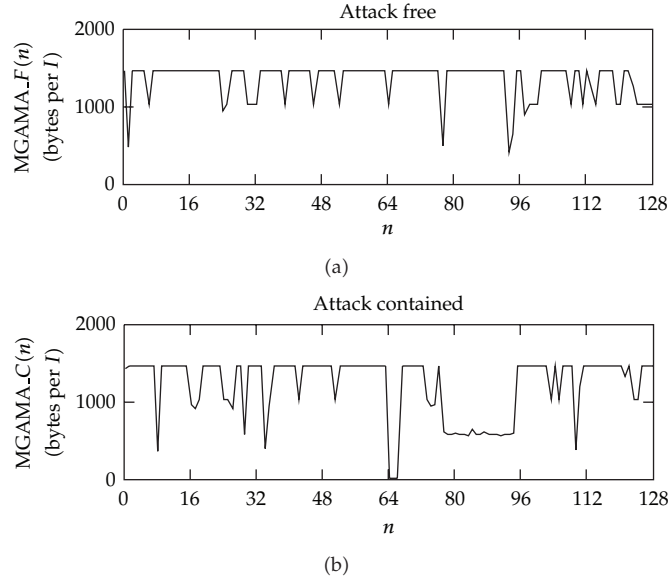
(a)

(b)

Figure 7: Maxima of traffic rate bound. (a) Maxima of $\mathrm{GAMA}(I, n)$ for OM-W1-1-1999AF. (b) Maxima of $\mathrm{GAMA}(I, n)$ for OM-W2-1-1999AC.

Table 1: Data set for attack-free traffic.

	First Packet Time			Last Packet Time		Trace Name
Mon	Mar 1	08:00:02	Tue	Mar 2	06:00:02	OM-W1-1-1999AF
Tue	Mar 2	08:00:02	Wed	Mar 3	06:00:01	OM-W1-2-1999AF
Wed	Mar 3	08:00:03	Thu	Mar 4	06:00:01	OM-W1-3-1999AF
Thu	Mar 4	08:00:03	Fri	Mar 5	06:00:02	OM-W1-4-1999AF
Fri	Mar 5	08:00:02	Sat	Mar 6	06:00:02	OM-W1-5-1999AF

2.1.2. Set Two: Attack-Contained Traffic (1999 Training Data—Week 2)

Five traces are included in the second data set. They are named as OM-W2-i-1999AC ($i = 1, 2, 3, 4, 5$), implying Outside-MIT-week2-i-1999-attack contained. The actual times at which the first packet and last one were extracted for each trace are listed in Table 2.

2.2. Traffic Rate under DDOS Flood Attacks

Roughly, high rate is the radical feature of attack-contained traffic. The paper [35] reported the real events in 2000. He noticed that "the attacks inundated servers with 1 gigabit per second of incoming data, which is much more traffic than they were built to handle [35, page 12]." The analysis given by Moore et al. says that "to load the network, an attacker generally sends small packets as rapidly as possible since most network devices (both routers and NICs) are limited not by bandwidth but by packet processing rate [36, Section 2.1]." They infer that traffic rate is usually the best measure of network load during an attack. In short, computer scientists consider high rate as a basic feature of attack-contained traffic, also see, for example, [37–42]. The experimental results in this paper are simply for the data of the 1999 DARPA in the case of high-rate attacks.
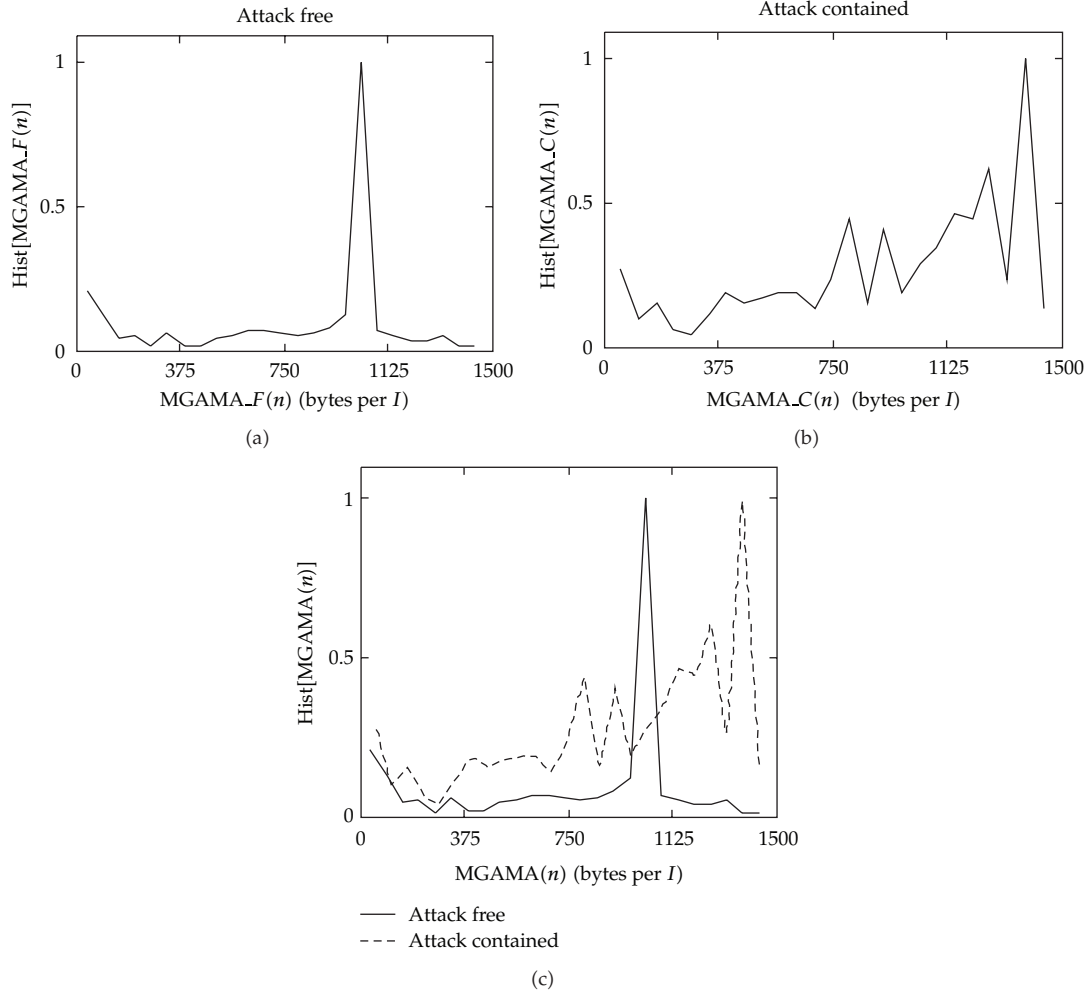
(a)

(b)

(c)

Figure 8: Histograms. (a) Hist[MGAMA_$F(n)$] of OM-W1-1-1999AF. (b) Hist[MGAMA_$C(n)$] of OM-W1-1-1999CF. (c) Comparison: Corr_FC = 0.01751.

Table 2: Data set for attack-contained traffic.

	First Packet Time			Last Packet Time			Trace Name
Mon	Mar 8	08:00:01	Tue	Mar 9	06:00:49	OM-W2-1-1999AC
Tue	Mar 9	08:00:01	Wed	Mar 10	06:00:59	OM-W2-2-1999AC
Wed	Mar 10	08:00:03	Thu	Mar 11	06:00:01	OM-W2-3-1999AC
Thu	Mar 11	08:00:03	Fri	Mar 12	06:00:00	OM-W2-4-1999AC
Fri	Mar 12	08:00:02	Sat	Mar 13	06:00:00	OM-W2-5-1999AC

2.3. Traffic Bounds

In this subsection, we brief the deterministic bounds for accumulated traffic and traffic rate with the help of demonstrations using traffic traces OM-W1-1-1999AF and OM-W1-1-1999CF.
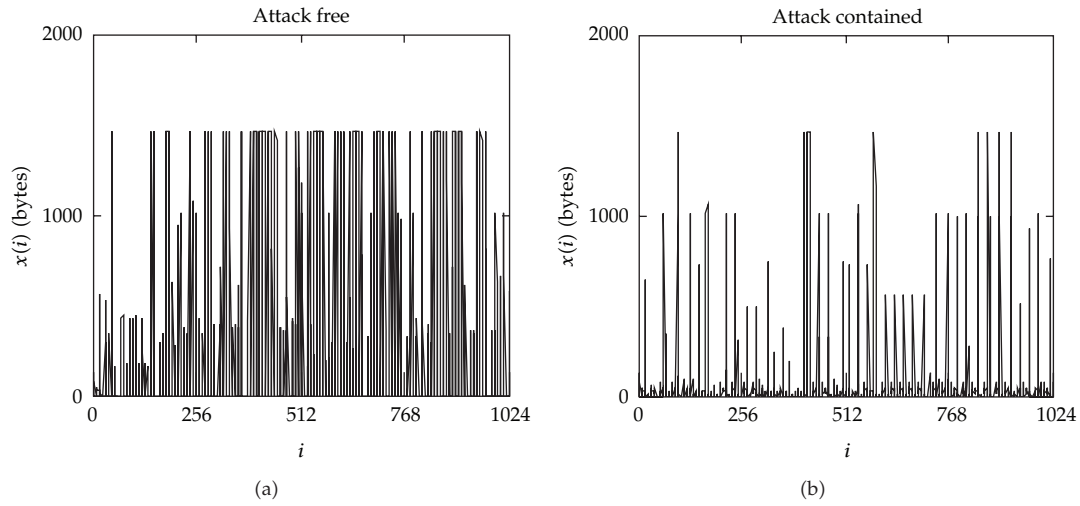
Figure 9: Time series of traffic traces. (a) The first 1024 points of OM-W1-2-1999AF. (b) The first 1024 points of OM-W2-2-1999AC.
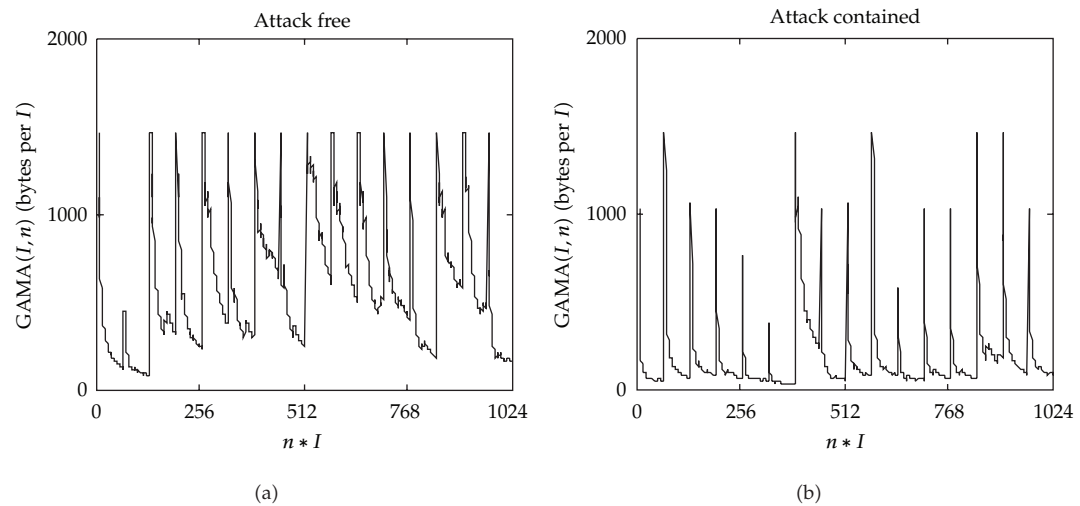

Figure 10: Series of traffic rate bound. (a) For OM-W1-2-1999AF. (b) For OM-W2-2-1999AC.

Let $x(t_i)$ be the series, indicating the number of bytes in the ith packet ($i = 0, 1, \ldots$) of arrival traffic at time t_i. Then, $x(i)$ is a discrete series, indicating the number of bytes in the ith packet of arrival traffic. Figure 1 shows a plot of $x(i)$ for the first 1024 points of OM-W1-1-1999AF.

According to [27, 43], an upper bound of arrival traffic $x(i)$ is given below.

Definition 2.1. Let $x(i)$ be the arrival traffic function. Then,

$$F(I) = \max_{i \geq 0}[x(i + I) - x(i)], \quad \text{for } i > 0, \ I > 0, \tag{2.1}$$

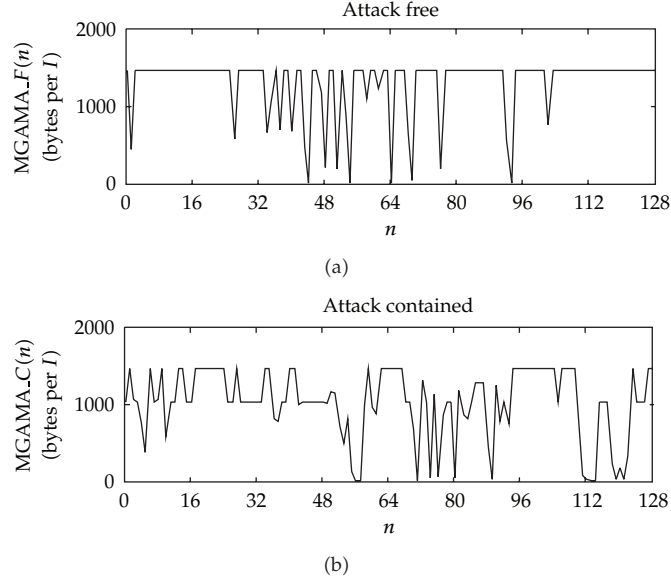is called traffic upper bound of $x(i)$ over the duration of length I.

(a)

(b)

Figure 11: Series of the maxima of traffic rate bound. (a) For OM-W1-2-1999AF. (b) For OM-W2-2-1999AC.

Note 1. The physical meaning of $F(I)$ is that the accumulated amount of arrival traffic $x(i)$ over the duration of length I is upper bounded by $F(I)$. The unit of $F(I)$ is bytes. $F(I)$ is an increasing function in terms of I. Figure 2 indicates $F(I)$ of OM-W1-1-1999AF for $0 \leq I \leq 63$.

Definition 2.2. Let $x(i)$ be the arrival traffic function. Then,

$$\text{GAMA}(I) = \frac{F(I)}{I} = \frac{\max_{i \geq 0}[x(i+I) - x(i)]}{I}, \quad \text{for } i > 0, \ I > 0, \tag{2.2}$$

is called upper bound of traffic rate (traffic rate bound for short) of $x(i)$.

Note 2. Equation (2.2) specifies that $\text{GAMA}(I)$ is the maximum arrival rate at a specific point in the network over any duration of length I. The unit of $\text{GAMA}(I)$ is defined as Bytes per I. $\text{GAMA}(I)$ is a decreasing function in terms of I. Figure 3 demonstrates $\text{GAMA}(I)$ of OM-W1-1-1999AF for $0 \leq I \leq 63$.

3. Histogram of Maxima of Traffic Rate Bound: A Feature for Identifying Abnormal Variation of Traffic under DDOS Attacks

In this section, we first introduce the time series of traffic rate bound. Then, we establish the maxima of traffic rate bound. Finally, we achieve the histogram of the maxima of traffic rate bound. The demonstrations with the experimental data are used for facilitating the discussions.
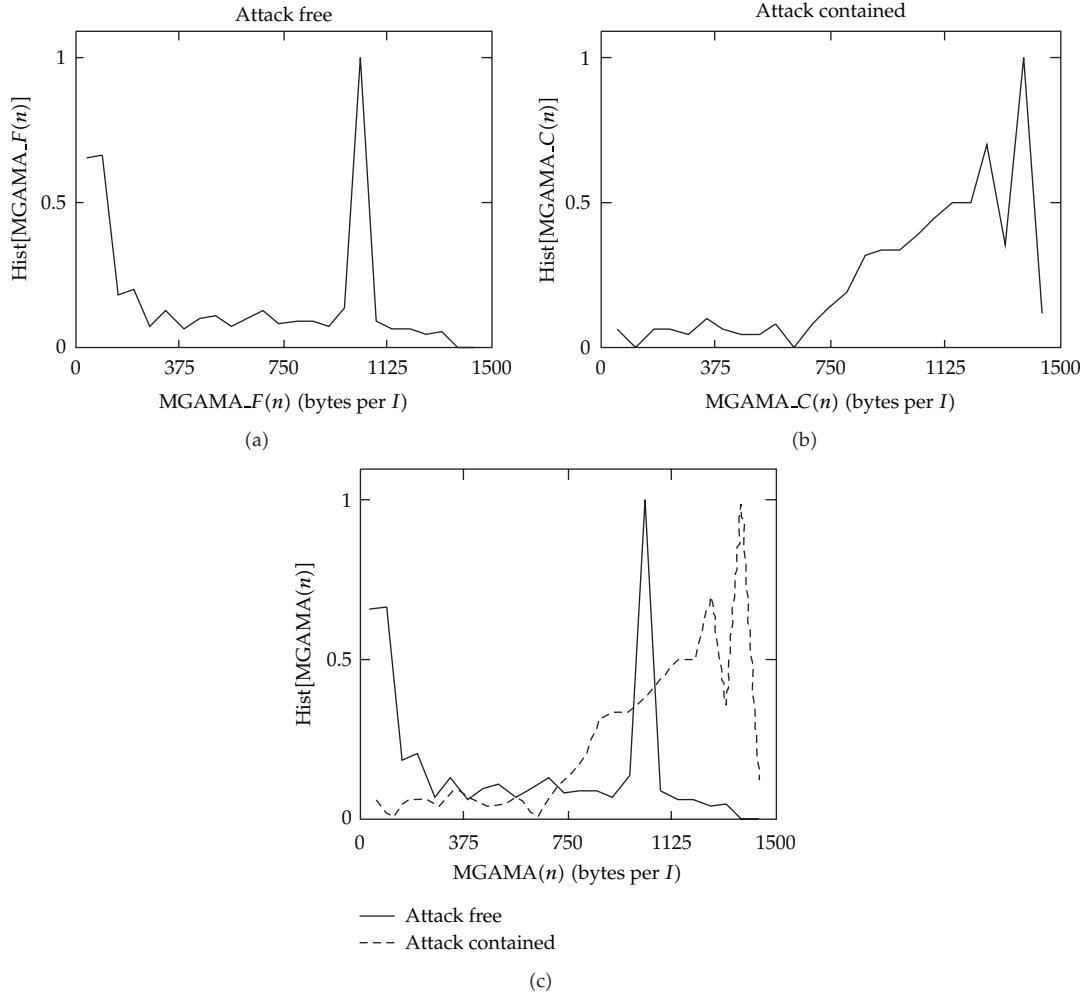
Figure 12: Histograms of the maxima of traffic rate bound. (a) For OM-W1-2-1999AF. (b) For OM-W2-2-1999AC. (c) Comparison: Corr_FC = 0.163261.

3.1. Traffic Bound Series

Theoretically, I can be any positively real number. In practice, however, I is selected as a finite positive integer. Fix the value of I and observe traffic bounds in the interval $((n-1)I,\ nI)$, $n = 1, 2, \ldots, N$. Then, we express traffic bounds as a function in terms of the interval index n. Considering the index n, we express traffic upper bound by $F(I, n)$, which is a series.

Note that $x(i)$ is a stochastic series and so is $F(I, n)$. That is, $F(I, m) \neq F(I, n)$ for $m \neq n$. We term $F(I,\ n)$ traffic upper bound series. Similarly, we use $\text{GAMA}(I, n)$ to represent traffic rate bound series. Figure 4 shows the traffic upper bound series. Figure 5 plots the rate bound series.

Since $\text{GAMA}(I, n)$ is random, identification in a single interval is not enough. We use Figure 6 to explain this point of view. From Figure 6, we see that the rate bound of attack-contained traffic is greater than that of attack-free traffic in some intervals, for example, in the second and third intervals. However, it is less than the rate bound of attack-free traffic
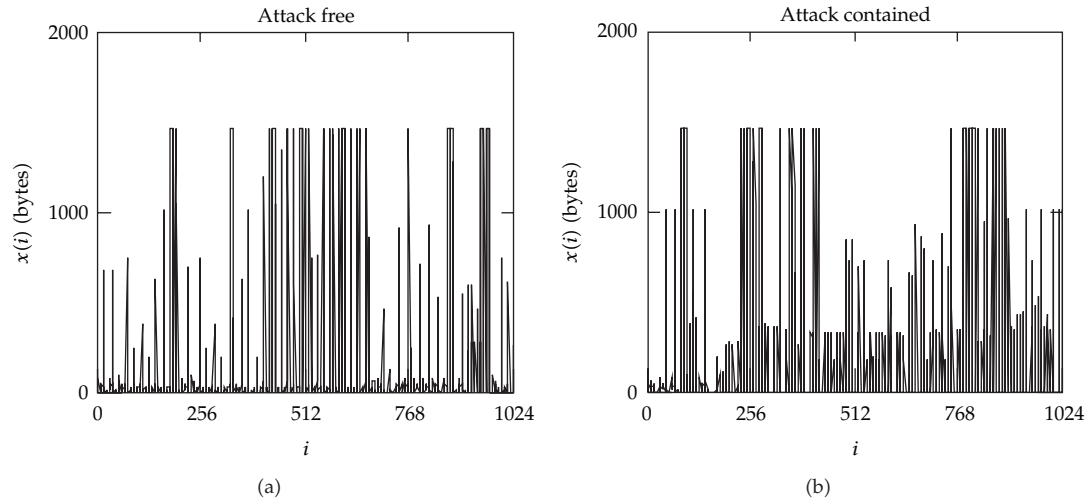
Figure 13: Time series of traffic traces. (a) The first 1024 points of OM-W1-3-1999AF. (b) The first 1024 points of OM-W2-3-1999AC.
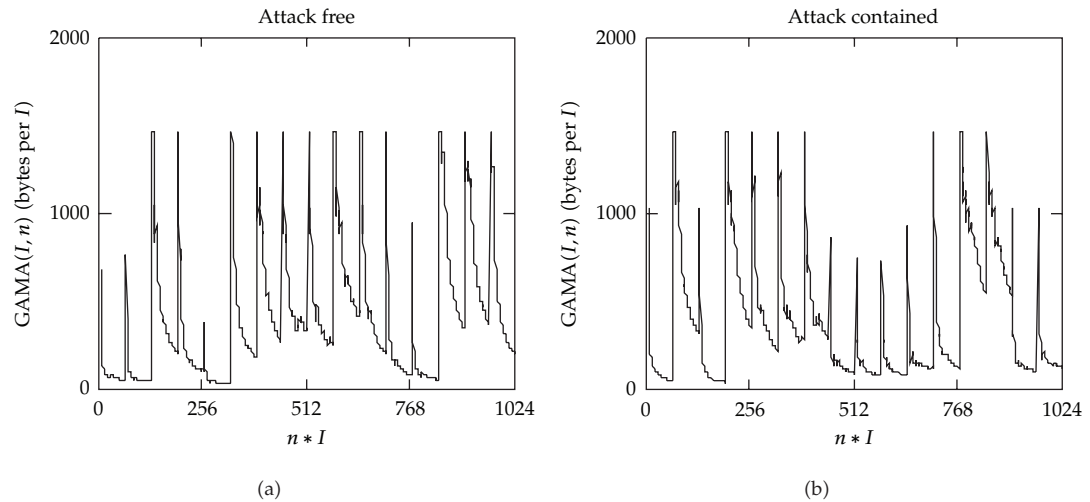

Figure 14: Series of traffic rate bound. (a) For OM-W1-3-1999AF. (b) For OM-W2-3-1999AC.

in some intervals, for example, in the first and fourth intervals. Therefore, we will study the issue how the bound series of traffic rate statistically varies under DDOS flood attacks. For this reason, we study the maxima of traffic rate bound.

3.2. Maxima of Traffic Rate Bound

Denote that

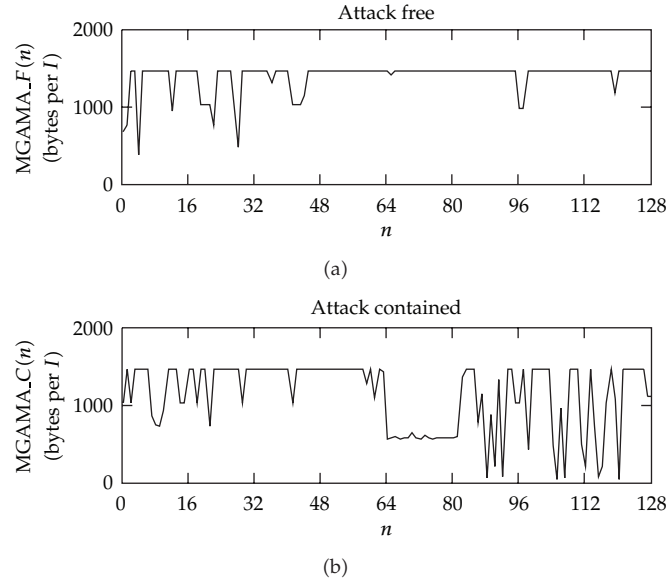$$\text{MGAMA}(n) = \text{Max}[\text{GAMA}(I, n)], \tag{3.1}$$

(a)

(b)

Figure 15: Series of the maxima of traffic rate bound. (a) Maxima of $GAMA(I, n)$ for OM-W1-3-1999AF. (b) Maxima of $GAMA(I, n)$ for OM-W2-3-1999AC.

over the index I in each interval $[(n - 1)I, \; nI]$. Then, MGAMA(n) represents a series to describe the maximum value of $GAMA(I, n)$ in each interval $[(n - 1)I, \; nI]$. In other words, MGAMA(n) stands for the maxima of $GAMA(I, n)$. The unit of MGAMA(n) is the same as that of $GAMA(I, n)$. Here and below, we use the notation MGAMA_F(n) for attack-free traffic and MGAMA_C(n) for attack-contained traffic. Figures 7(a) and 7(b) give the plots of MGAMA_F(n) and MGAMA_C(n) for OM-W1-1-1999AF and OM-W2-1-1999AC, respectively.

3.3. Histogram of Maxima

Denote Hist[MGAMA_F(n)] and Hist[MGAMA_C(n)] as the histograms of MGAMA_F(n) and MGAMA_C(n), respectively. Then, they represent empirical distributions of MGAMA_F(n) and MGAMA_C(n). Figures 8(a) and 8(b) indicate the Hist[MGAMA_F(n)] and Hist[MGAMA_C(n)] for OM-W1-1-1999AF and OM-W1-1-1999CF, respectively. From Figure 8(c), we see that the pattern of Hist[MGAMA_F(n)] considerably differs from that of Hist[MGAMA_C(n)]. To investigate this phenomenon quantitatively, we need a measure to describe the similarity or dissimilarity between the pattern of Hist[MGAMA_F(n)] and that of Hist[MGAMA_C(n)], which will be explained in the next subsection.

3.4. Correlation Coefficient Used as a Similarity Measure for Pattern Matching

There are many measures to characterize the similarity or the dissimilarity of two patterns in the field of pattern matching, see, for example, [44, 45]. Among them, the correlation
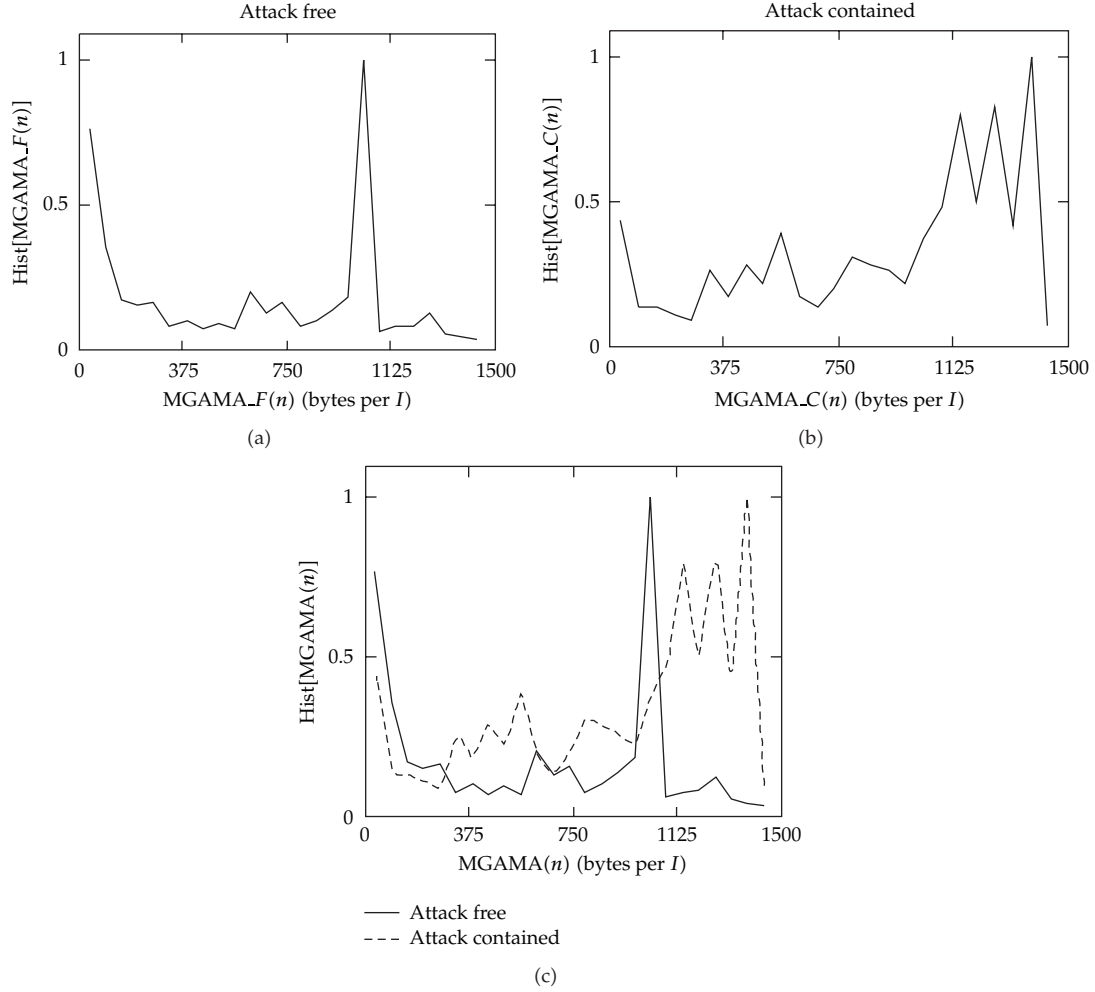
Attack free

Attack contained

(a)

(b)

(c)

— Attack free
--- Attack contained

Figure 16: Histograms of the maxima of traffic rate bound. (a) For OM-W1-3-1999AF. (b) For OM-W2-3-1999AC. (c) Comparison: Corr_FC = 0.045515.

coefficient between two patterns is commonly used in engineering, see, for example, [46]. We use it to measure the pattern similarity in this research. Denote that

$$\text{Corr}_{\text{FC}} = \left| \text{corr}\left\{ \text{Hist}\left[\text{MGAMA}_{\text{F}(n)}\right], \ \text{Hist}\left[\text{MGAMA}_{\text{C}(n)}\right] \right\} \right|, \tag{3.2}$$

where corr implies the correlation operation.

It is known that $0 \leq \text{Corr\_FC} \leq 1$. The larger the value of Corr_FC the more similar between the pattern of Hist[MGAMA_F(n)] and that of Hist[MGAMA_C(n)]. Mathematically, the case of Corr_FC = 1 implies that the pattern of Hist[MGAMA_F(n)] is exactly the same as that of Hist[MGAMA_C(n)]. On the contrary, Corr_FC = 0 means that the pattern of Hist[MGAMA_F(n)] is totally different from that of MGAMA_C(n). From the point of view of engineering, however, the extreme case of either Corr_FC = 1 or Corr_FC = 0 does not make much sense due to errors and uncertainties in measurement and digital
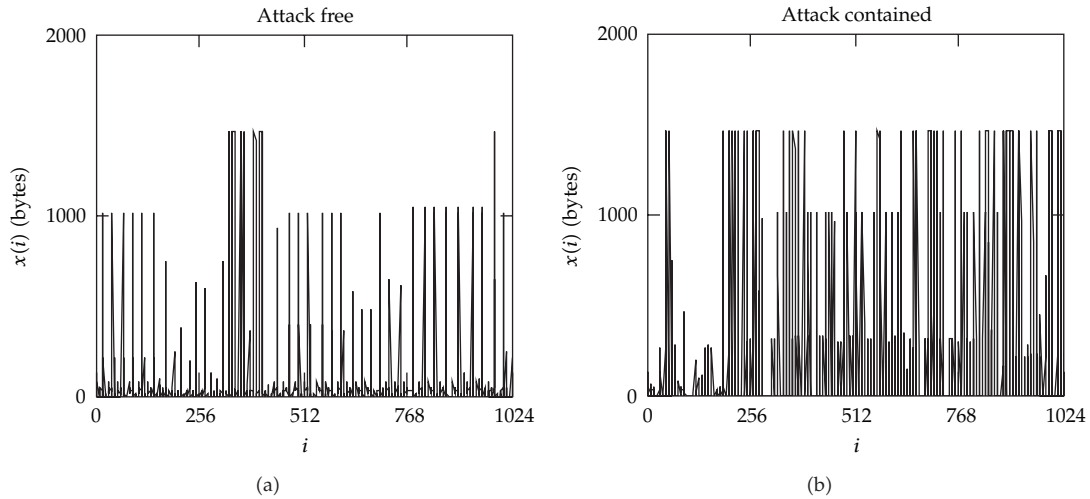
Figure 17: Time series of traffic traces. (a) The first 1024 points of OM-W1-4-1999AF. (b) The first 1024 points of OM-W2-4-1999AC.
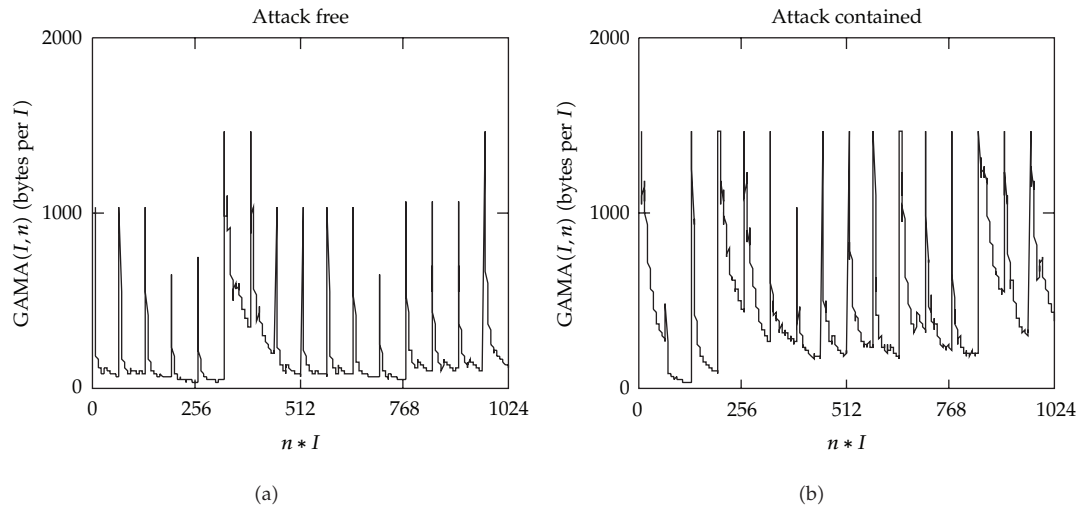

Figure 18: Series of traffic rate bound. (a) For OM-W1-4-1999AF. (b) For OM-W2-4-1999AC.

computation. In practical terms, one uses a threshold for Corr_FC to evaluate the similarity between two. The concrete value of the threshold depends on the requirement designed by researchers that but it is quite common to take 0.7 as the smallest value of the threshold for the pattern patching purpose. Suppose that we consider 0.8 as the threshold value. Then, we say that the pattern of Hist[MGAMA_F(n)] is similar to that of Hist[MGAMA_C(n)] if Corr_FC ≥ 0.8 and dissimilar otherwise.

By computing, we obtain Corr_FC = 0.01751 for OM-W1-1-1999AF and OM-W2-1-1999CF, implying the pattern of Hist[MGAMA_F(n)] considerably differs from that of Hist[MGAMA_C(n)] as indicated in Figure 8(c). We will further demonstrate this interesting phenomenon in the next section.
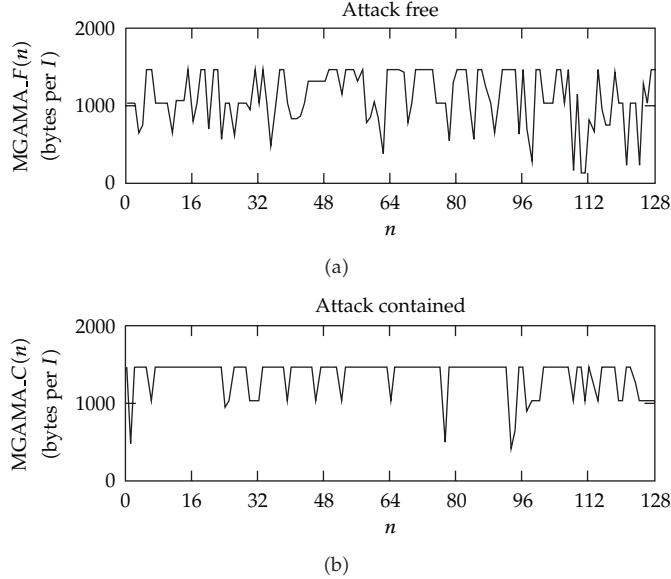
Figure 19: Series of the maxima of traffic rate bound. (a) Maxima of $GAMA(I, n)$ for OM-W1-4-1999AF. (b) Maxima of $GAMA(I, n)$ for OM-W2-4-1999AC.

4. Experimental Results

The value of Corr_FC for OM-W1-1-1999AF and OM-W2-1-1999CF has been mentioned above. In this section, we illustrate experimental results describing Corr_FC for OM-W1-2-1999AF and OM-W2-2-1999CF. The plots to illustrate Corr_FC for OM-W1-3-1999AF and OM-W2-3-1999CF, OM-W1-4-1999AF and OM-W2-4-1999CF, OM-W1-5-1999AF and OM-W2-5-1999CF and are listed in the appendices.

Figures 9(a) and 9(b) are the plots of the first 1024 points of OM-W1-2-1999AF and OM-W2-2-1999CF, respectively. Figures 10(a) and 10(b) indicate the series of traffic rate bound for OM-W1-2-1999AF and OM-W2-2-1999CF for $n = 0, 1, \ldots, 16$ with $I = 64$, respectively. Figures 11(a) and 11(b) demonstrate the maxima of rate bound for both traffic traces for $n = 0, 1, \ldots, 128$. Figures 12(a) and 12(b) show the histograms of the maxima of traffic rate bound for both traces. Figure 12(c) gives the comparison between two. By computation, we have Corr_FC = 0.163261, meaning that the pattern of Hist[MGAMA_F(n)] considerably differs from that of Hist[MGAMA_C(n)] for OM-W1-2-1999AF and OM-W2-2-1999AC.

Note that the values of Corr_FC for other three pairs of test traces, see Figures 16(c), 20(c), and 24(c), also exhibit that the pattern of Hist[MGAMA_F(n)] is noticeably different from that of Hist[MGAMA_C(n)]. We summarize the values of Corr_FC of all five pairs of traces in Table 3, which shows that Corr_FC < 0.2 for all pairs of test traces.

5. Discussions and Conclusions

The maxima of rate bound of attack-contained traffic is not always higher than that of attack-free traffic, see Figure 7. Statistically, however, it is higher than that of attack-free traffic
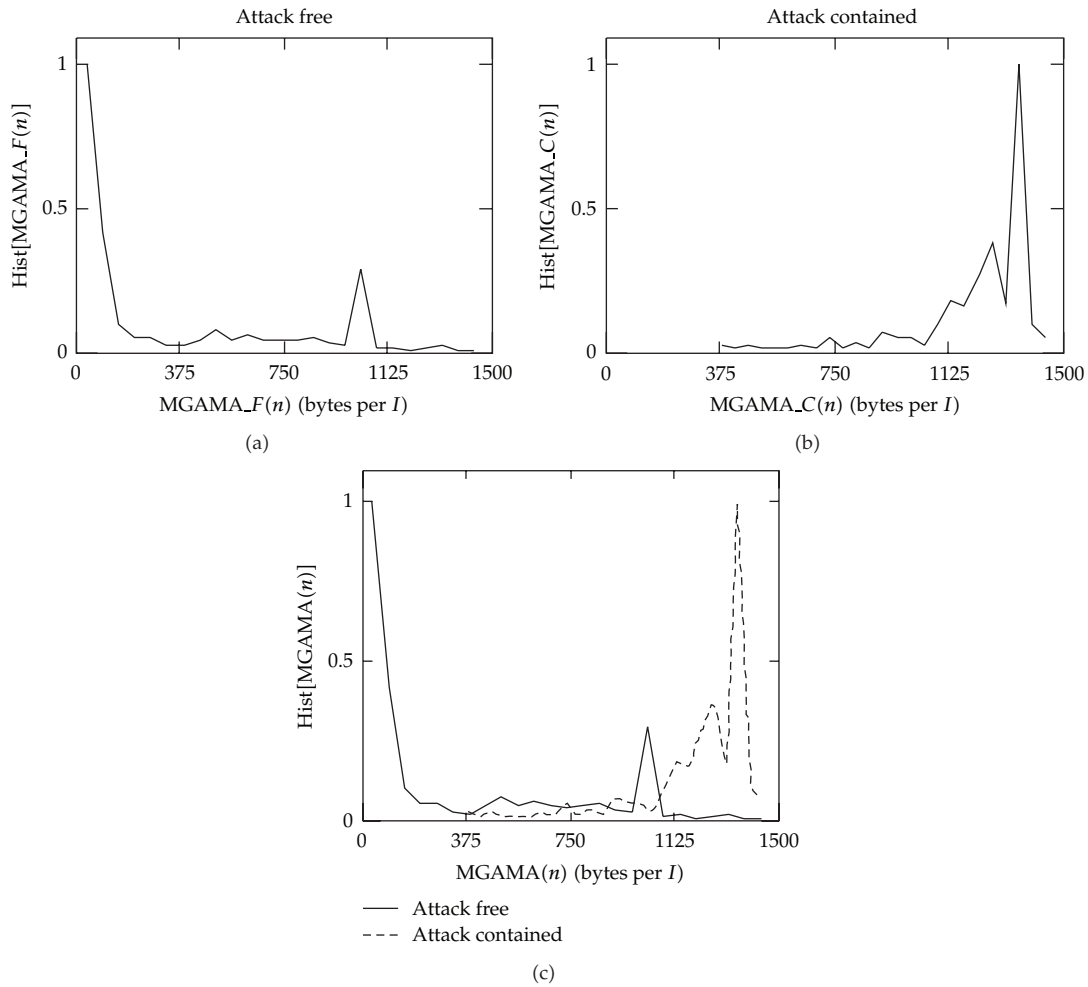
Figure 20: Histograms of the maxima of traffic rate bound. (a) For OM-W1-4-1999AF. (b) For OM-W2-4-1999AC. (c) Comparison: Corr_FC = 0.141885.

significantly as can be seen from the experimental results illustrated by Figures 8(c), 12(c), 16(c), 20(c), and 24(c). In addition, the results expressed in Table 3 indicate that the pattern of Hist[MGAMA_F(n)] is obviously different from that of Hist[MGAMA_C(n)]. Thus, the results in this paper suggest that the histogram of the maxima of traffic rate bound may yet be a traffic feature to distinctly identify abnormal variation of traffic under DDOS flood attacks.

In comparison with fractal model of traffic as discussed in [18, 19, 43], the present feature has an apparent advantage. Recall that statistical models like LRD processes, see, for example, [18, 19], are usually for traffic in the aggregate case, but there is lack of evidence to use them to characterize statistical patterns of real traffic at connection. As a matter of fact, finding statistical patterns of traffic at connection may be a tough task. To overcome difficulties in describing traffic at connection level, bounded modeling is introduced [25–29]. Thus, if we let $x_{j,k}(t)$ be all flows going through server k from input link j and let $F_{j,k}(I)$ be the maximum traffic constraint function of $x_{j,k}(t)$, the present analysis method of traffic
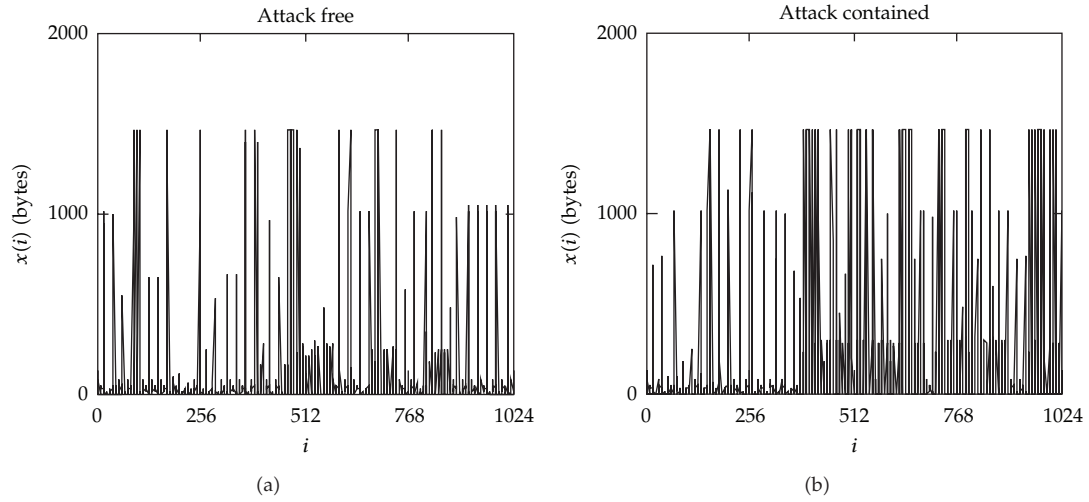
(a)

(b)

Figure 21: Time series of traffic traces. (a) The first 1024 points of OM-W1-5-1999AF. (b) The first 1024 points of OM-W2-5-1999AC.
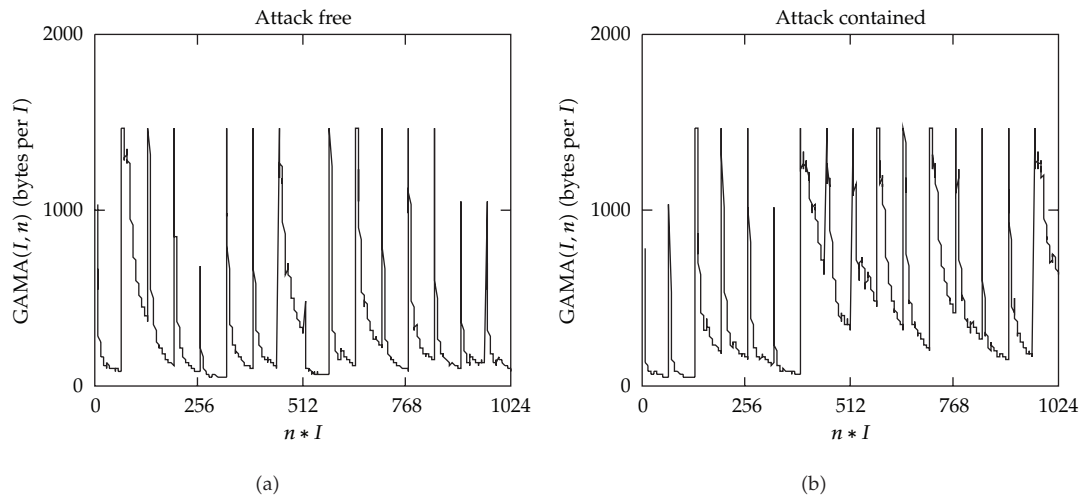

(a)

(b)

Figure 22: Series of traffic rate bound. (a) For OM-W1-5-1999AF. (b) For OM-W2-5-1999AC.

Table 3: Correlation coefficients between the pattern of Hist[MGAMA_F(n)] and that of Hist[MGAMA_C(n)] for 5 pairs of test traces.

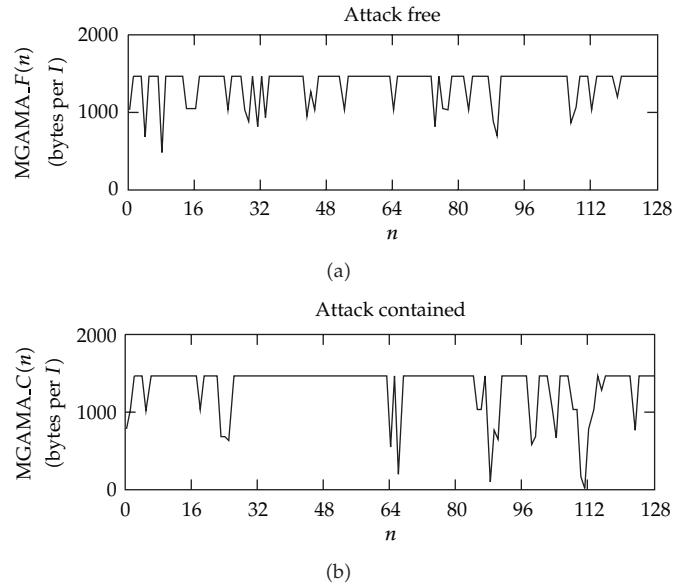| Attack-free traffic traces	Attack-contained traffic traces	Corr_FC
OM-W1-1-1999AF	OM-W2-1-1999AC	0.01751
OM-W1-2-1999AF	OM-W2-2-1999AC	0.163261
OM-W1-3-1999AF	OM-W2-3-1999AC	0.045515
OM-W1-4-1999AF	OM-W2-4-1999AC	0.141885
OM-W1-5-1999AF	OM-W2-5-1999AC	0.177468

(a)

(b)

Figure 23: Series of the maxima of traffic rate. (a) Maxima of $\text{GAMA}(I, n)$ for OM-W1-5-1999AF. (b) Maxima of $\text{GAMA}(I, n)$ for OM-W2-5-1999AC.

is technically sound and usable for $x_{j,k}(t)$ but fractal models may not. Since the bounded models of traffic are mainly used at connection level in some applications, such as real-time admission control, it is clear that the present traffic feature for identifying abnormal variation of traffic under DDOS flood attacks can be extracted at early stage of attacks.

Appendices

These appendices gives experimental results for three pairs of traces. They are OM-W1-3-1999AF and OM-W2-3-1999CF, OM-W1-4-1999AF and OM-W2-4-1999CF, and OM-W1-5-1999AF and OM-W2-5-1999CF. The values of Corr_FC for each pair of traces are given in the captions of Figures 16(c), 20(c), and 24(c), respectively.

A. Experiments for OM-W1-3-1999AF and OM-W2-3-1999CF

See Figures 13, 14, 15, and 16.

B. Experiments for OM-W1-4-1999AF and OM-W2-4-1999CF

See Figures 17, 18, 19, and 20.

C. Experiments for OM-W1-5-1999AF and OM-W2-5-1999CF
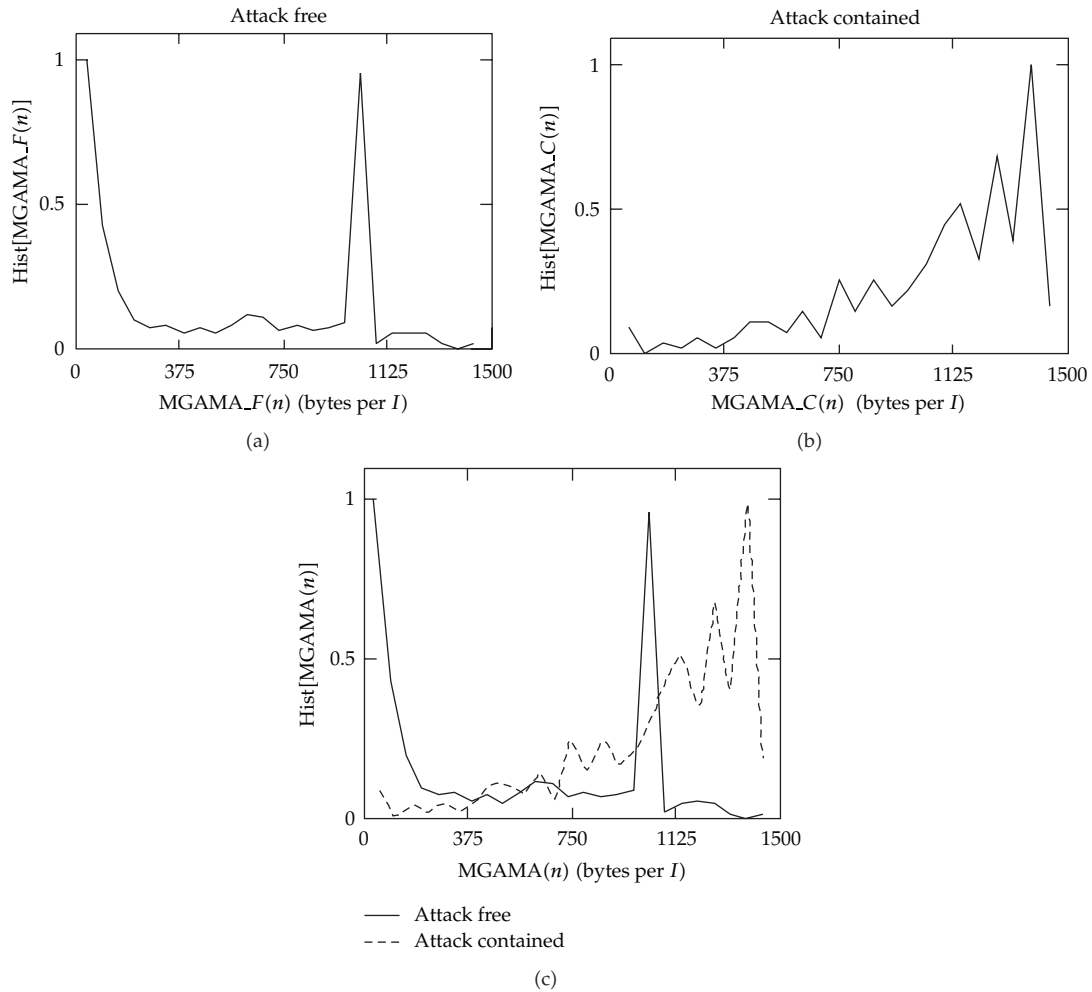
See Figures 21, 22, 23, and 24.

(a)

(b)

(c)

Figure 24: Histograms of the maxima of traffic rate bound. (a) For OM-W1-5-1999AF. (b) For OM-W2-5-1999AC. (c) Comparison: Corr_FC = 0.177468.

Acknowledgments

References

[1] R. Shirey, *Internet Security Glossary*, RFC 2828, 2000.
[2] N. Hussain, *Measurement and spectral analysis of denial of service attacks*, Ph.D. dissertation, University of Southern California, 2005.
[3] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," *Computers & Security*, vol. 24, no. 4, pp. 295–307, 2005.

[4] E. G. Amoroso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response*, Intrusion.Net Books, 1999.

[5] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall, 2004.

[6] K. Liston, "Intrusion Detection FAQ: can you explain traffic analysis and anomaly detection?" 2004, http://www.sans.org/security-resources/idfaq/anomaly_detection.php.

[7] E. Schultz, "Intrusion prevention," *Computers and Security*, vol. 23, no. 4, pp. 265–266, 2004.

[8] J. Leach, "TBSE—an engineering approach to the design of accurate and reliable security systems," *Computers and Security*, vol. 23, no. 1, pp. 265–266, 2004.

[9] S. H. Oh and W. S. Lee, "An anomaly intrusion detection method by clustering normal user behavior," *Computers and Security*, vol. 22, no. 7, pp. 596–612, 2003.

[10] F. Gong, "Deciphering detection techniques: part III denial of service detection," White Paper, McAfee Network Security Technologies Group, 2003.

[11] S. Sorensen, "Competitive overview of statistical anomaly detection," White Paper, Juniper Networks, 2004.

[12] S. B. Cho and H. J. Park, "Efficient anomaly detection by modeling privilege flows using hidden Markov model," *Computers and Security*, vol. 22, no. 1, pp. 45–55, 2003.

[13] S. Cho and S. Cha, "SAD: web session anomaly detection based on parameter estimation," *Computers and Security*, vol. 23, no. 7, pp. 312–319, 2004.

[14] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," *Computer*, vol. 35, pp. 27–30, 2002.

[15] E. E. Schultz, "Representing information security fairly and accurately," *Computers and Security*, vol. 25, no. 4, p. 237, 2006.

[16] S. S. Kim, A. L. Narasimha Reddy, and M. Vannucci, "Detecting traffic anomalies through aggregate analysis of packet header data," *Lecture Notes in Computer Science*, vol. 3042, pp. 1047–1059, 2004.

[17] M. Li, "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition," *Computers and Security*, vol. 23, no. 7, pp. 549–558, 2004.

[18] M. Li, "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks," *Computers and Security*, vol. 25, no. 3, pp. 213–220, 2006.

[19] 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.

[20] B. Tsybakov and N. D. Georganas, "Self-similar processes in communications networks," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 44, no. 5, pp. 1713–1725, 1998.

[21] M. Li, "Modeling autocorrelation functions of long-range dependent teletraffic series based on optimal approximation in Hilbert space-A further study," *Applied Mathematical Modelling*, vol. 31, no. 3, pp. 625–631, 2007.

[22] M. Li and S. C. Lim, "Modeling network traffic using generalized Cauchy process," *Physica A*, vol. 387, no. 11, pp. 2584–2594, 2008.

[23] M. Li and W. Zhao, "Detection of variations of local irregularity of traffic under DDOS flood attack," *Mathematical Problems in Engineering*, vol. 2008, Article ID 475878, 2008.

[24] H. Michiel and K. Laevens, "Teletraffic engineering in a broad-band era," *Proceedings of the IEEE*, vol. 85, no. 12, pp. 2007–2032, 1997.

[25] R. L. Cruz, "A calculus for network delay—I: network elements in isolation," *IEEE Transactions on Information Theory*, vol. 37, no. 1, pp. 114–131, 1991.

[26] J.-Y. Le Boudec, J. Yves, and T. Patrick, *Network Calculus, A Theory of Deterministic Queuing Systems for the Internet*, vol. 2050 of *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 2001.

[27] S. 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.

[28] M. Li and W. Zhao, "Representation of a stochastic traffic bound," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, Article ID 5342414, pp. 1368–1372, 2010.

[29] M. Li and W. Zhao, "A model to partly but reliably distinguish DDOS flood traffic from aggregated one," *Mathematical Problems in Engineering*, vol. 2012, Article ID 860569, 12 pages, 2012.

[30] M. Li and W. Zhao, "Asymptotic identity in min-plus algebra: a report on CPNS," *Computational and Mathematical Methods in Medicine*, vol. 2012, Article ID 154038, 11 pages, 2012.

[31] J. McHugh, "Testing intrusion detection systems: a critique of the 1988 and 1999 DARPA intrusion detection system evaluations as performed by lincoln laboratory," *ACM Transactions Information System Security*, vol. 3, no. 4, pp. 262–294, 2000.

[32] J. W. Haines, L. M. Rossey, R. Lippmann, and R. K. Cunningharm, "Extending the DARPA off-line intrusion detection evaluations," in *Proceedings of the DARPA Information Survivability Conference and Exposition II*, vol. 1, pp. 77–88, IEEE, Anaheim, Calif, USA, 2001.

[33] 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, 2003.

[34] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," *Computer Networks*, vol. 34, no. 4, pp. 579–595, 2000.

[35] L. Garber, "Denial-of-service attacks rip the internet," *Computer*, vol. 33, no. 4, pp. 12–17, 2000.

[36] D. Moore, G. M. Veolker, and S. Savage, "Inferring internet denial-of-service activity," in *Proceedings of the 10th USENIX Security Symposium*, 2001.

[37] R. Mahajan, S. M. Bellovin, and S. Floyd, "Controlling high bandwidth aggregates in the network," vol. 32, no. 3, pp. 62–73.

[38] A. Lakhina, M. Crovella, and C. Diot, "Characterization of network-wide anomalies in traffic flows," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC '04)*, pp. 201–206, Sicily, Italy, October 2004.

[39] P. Barford and D. Plonka, "Characteristics of network traffic flow anomalies," in *Proceedings of the 1st ACM SIGCOMM Internet Measurement Workshop (IMW '01)*, pp. 69–73, San Francisco, Calif, USA, November 2001.

[40] V. A. Siris and F. Papagalou, "Application of anomaly detection algorithms for detecting SYN flooding attacks," *Computer Communications*, vol. 29, no. 9, pp. 1433–1442, 2006.

[41] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 1530–1539, New York, NY, USA, June 2002.

[42] M. Li, J. Li, and W. Zhao, " Simulation study of flood attacking of DDOS," in *Proceedings of the IEEE 3rd International Conference on Internet Computing in Science and Engineering (ICICSE '08)*, pp. 289–293, Harbin, China, 2008.

[43] R. Bettati, W. Zhao, and D. Teodor, "Real-time intrusion detection and suppression in ATM networks," in *Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, pp. 111–118, 1999.

[44] K. S. Fu, Ed., *Digital Pattern Recognition*, Springer, 2nd edition, 1980.

[45] M. Basseville, "Distance measures for signal processing and pattern recognition," *Signal Processing*, vol. 18, no. 4, pp. 349–369, 1989.

[46] M. Li, "An iteration method to adjusting random loading for a laboratory fatigue test," *International Journal of Fatigue*, vol. 27, no. 7, pp. 783–789, 2005.