A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks

Seyyed Meysam Tabatabaie Nezhad, Mahboubeh Nazari, and Ebrahim A. Gharavol

***Abstract*—This letter deals with the problem of detecting DoS and DDoS attacks. First of all, two features including number of packets and number of source IP addresses are extracted from network traffics as detection metrics in every minute. Hence, a time series based on the number of packets is built and normalized using a Box-Cox transformation. An ARIMA model is also employed to predict the number of packets in every following minute. Then, the chaotic behavior of prediction error time series is examined by computing the maximum Lyapunov exponent. The local Lyapunov exponent is also calculated as a suitable indicator for chaotic and nonchaotic errors. Finally, a set of rules are proposed based on repeatability of chaotic behavior and enormous growth in the ratio of number of packets to number of source IP addresses during attack times to classify normal and attack traffics from each other. Simulation results show that the proposed algorithm can accurately classify 99.5% of traffic states.**

***Index Terms*—DoS and DDoS detection, Chaos, Lyapunov exponent, Time series.**

I. Introduction

NETWORK attacks by a malicious node aiming to deny access to resources on computer networks are called availability based attacks. These forms of attacks are one of the most serious security threats affecting network resources [1]. They are commonly recognized as denial-of-service (DoS) attack. When the attack is launched by more than one attacker, it is called a distributed denial-of-service (DDoS) attack. During DoS attack, intruders destroy their target(s) by sending a large number of packets that prevent legal users from having access to network nodes. Usually, giant servers are capable enough to endure a basic DoS attack from a single machine without suffering performance losses [1]. The ability of an organization to detect and preserve itself against DoS and DDoS attacks is vital for its success. Without suitable detection and prevention methods, an organization would be damaged by DoS and DDoS attacks and suffers financial losses and reputational damages [1]. There has been much research on DoS and DDoS attacks in order to accurately detect them in computer networks. In the following, related papers are reviewed.

Chonka *et al.* [2] proposed a novel DDoS detection algorithm which uses self-similarity theory for network traffic modeling. The DDoS attack is detected by computing the local Lyapunov exponent. Furthermore, they claimed that a neural network could improve the detection rate of the network attacks. Frequently, time series models such as AR, ARMA, FARIMA, etc. are used as proper tools for time series forecasting [9]. Zhang *et al.* [3] proposed a prediction method based on an ARIMA model to predict DDoS attack through simulation studies with NS2. Yaacob *et al.* [4] introduce a novel algorithm through using an ARIMA technique to detect potential attacks that may occur in computer networks. Their method provide an early warning mechanism for the network administrator. Fachkha *et al.* [5] proposed an approach that is presented by a DDoS forecasting model. Anjali [6] and Chen *et al*. [7] -as the first step- perform preprocessing on the network traffic by calculating the cumulative average of time series values in the time domain. Then the local Lyapunov exponent is used as a suitable DDoS indicator. They also assumed that the prediction error of an AR model is chaotic. Furthermore, they used a neural network to improve the DDoS detection accuracy. Because the cumulative average cannot stabilize the variance of the data, it is not an appropriate input to an AR model [7]. In [8] Wu and Chen validate that the error of the traffic prediction has chaotic characteristics. They predict the network traffic using an exponential smoothing model instead of the forecasting method used in NADA [7]. The forecasting method based on exponential smoothing may be inefficient in terms of accuracy [9]. Ramaki *et al.* [11] proposed two real-time methods based on stream mining for the DDoS attack detection and predicting the next goal of the attacker. In the methods, a probabilistic approach based on the Bayesian network concept is used for learning the specification of DDoS attack pattern and detecting it in alert streams. In this letter, it is proposed to combine the Box-Cox based preprocessing, the ARIMA modeling, chaos based analysis, and applying defined rules of classification in order to improve the efficiency of DoS/DDoS detection. The remainder of the letter is organized as follows. Section II describes the proposed detection algorithm. Section III shows the experimental results. Finally, a conclusion is provided in Section IV.

II. The Proposed Detection Algorithm

In this section, the proposed algorithm, called TNA, is briefly reviewed in Algorithm 1. The detailed explanation is provided afterwards.

A. Feature Selection

According to the number of packets in every minute (x_i), the number of source IP addresses of network nodes in every minute (I_i), and dividing them to each other ($y_i = x_i/I_i$), two time series (x_i & y_i) are built as detection metrics Fig. 1 and Fig. 2 show these metrics, respectively.

Manuscript received September 2, 2015; revised December 29, 2015; accepted December 29, 2015. Date of publication January 13, 2016; date of current version April 7, 2016. The associate editor coordinating the review of this paper and approving it for publication was H. Otrok.

S. M. T. Nezhad and E. A. Gharavol are with the Electrical Engineering Department, Imam Reza International University, Mashhad 7917893349, Iran (e-mail: miysam.ucla2017@gmail.com).

M. Nazari is with the Department of Mathematics, Ferdowsi University of Mashhad, Mashhad 9177948974, Iran.

Digital Object Identifier 10.1109/LCOMM.2016.2517622

```
Algorithm 1. Network traffic classification steps
Require: $x_i$ (the number of packets in every minute) and $I_i$ (source IP addresses of network nodes in every minute)
  1: Data preprocessing using a Box-Cox transformation employing (1).
  2: Forecasting based on an ARIMA model and calculating the error based on (2).
  3: Chaotic and non-chaotic errors classification by applying a local Lyapunov exponent using (3) and (4).
  4: Proposed a set of rules using (5) and (6).
  5: Final decision based on (7).
```

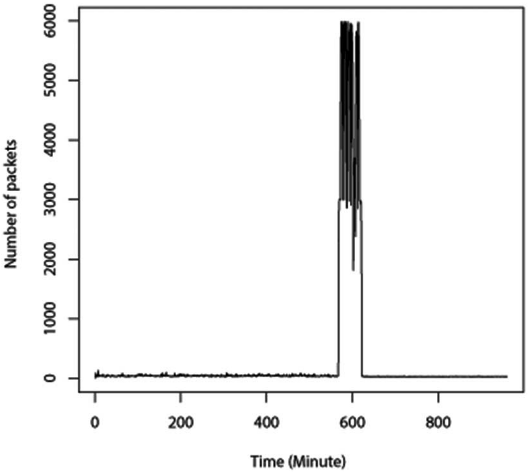

Fig. 1. A time series based on number of packets for time instants 1–960.

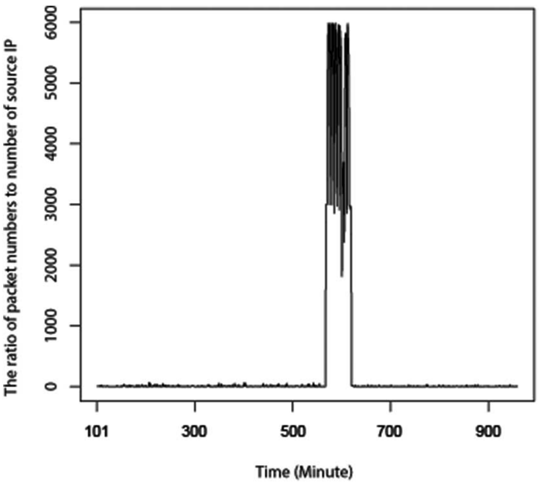

Fig. 2. The ratio of packet numbers to number of source IP for time instants 101–960.

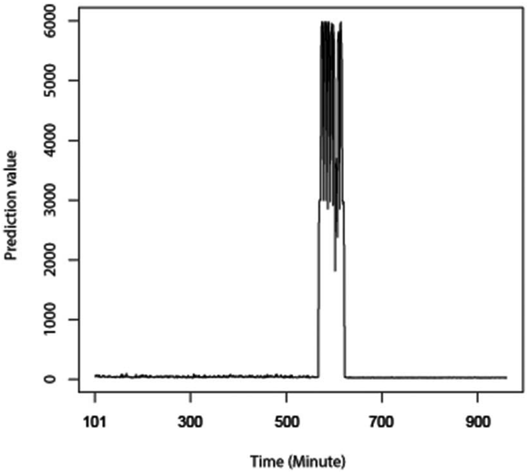

Fig. 3. Predicted values for time instants 101–960.

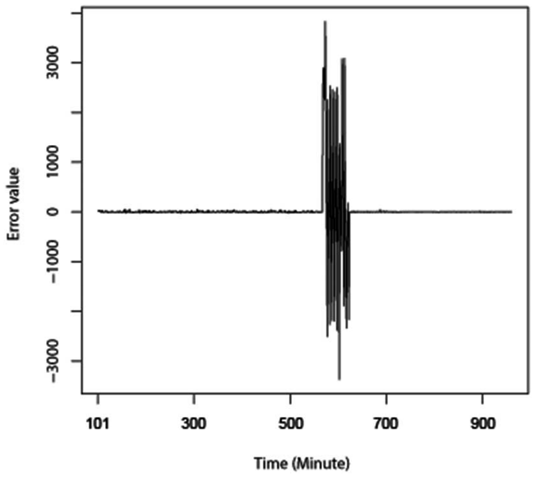

Fig. 4. Error of predicted values for time instants 101–960.

B. Data Preprocessing Using Box-Cox

Since the non-constant variance is quite common in the time series, data transformations are often used to improve the prediction accuracy. A very popular type of data transformation to deal with non-constant variance is the Boxtransformation. As a preliminary step before fitting an ARIMA model to time series, the Box-Cox transformation has been recommended in [9]. The one-parameter Box-Cox transformation of a time series x_i that depends on the power parameter α, is as follows:

$$x_i^{(\alpha)} = \begin{cases} (\frac{x_i^{(\alpha)}-1}{\alpha}), & \text{if } \alpha \neq 0; \\ \ln(x_i), & \text{if } \alpha = 0. \end{cases} \quad (1)$$

The preprocessed data is denoted using x_i.

C. Forecasting Based on an ARIMA Model and Calculating the Error

Predicting models are important tools in forecasting the time series. In order to better predict the normal traffic, an autoregressive integrated moving average (ARIMA) model [9] is applied. Empirically L=100 is chosen as the ARIMA model order. The first one-hundred samples of data are used for predicting 101st sample($\hat{x}_{101}$), and the data samples among 2–101 are employed for forecasting 102nd sample ($\hat{x}_{102}$). By continuing this process, the data samples among time indexes 101–960 are predicted. Finally, prediction error Δx_i is calculated by subtracting the real traffic x_i and the output of Inverse Box-Cox on predicted traffic ($\hat{x}_i$).

$$\Delta x_i = (x_i) - (\text{Inverse.Box.Cox}(\hat{x}_i)). \quad (2)$$

Fig. 3 and Fig. 4 demonstrate network traffic prediction and error values of forecasting, respectively. In aforementioned

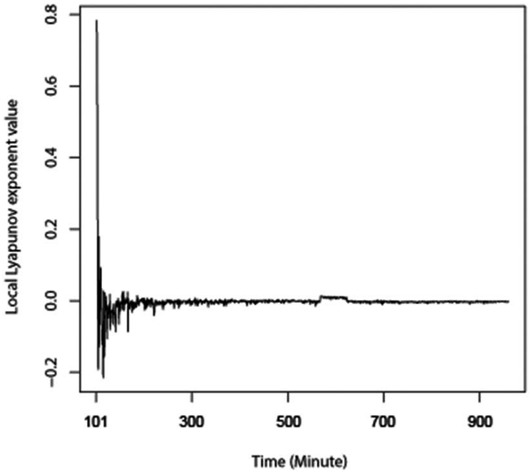

Fig. 5. The local Lyapunov exponent values for time instants 101–960.

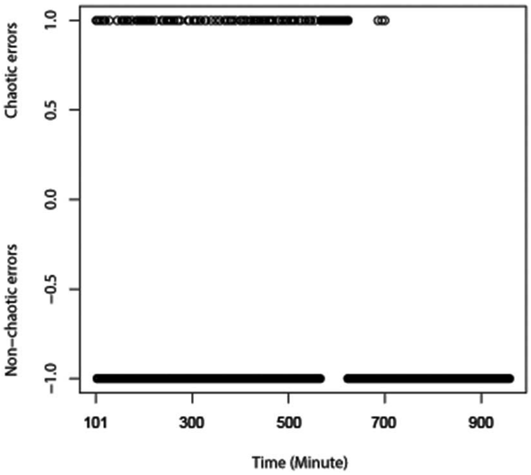

Fig. 6. Non-chaotic(-1) and chaotic(1) errors for time instants 101–960.

graphs, the first 100 samples are ignored because (2) is undefined for those samples.

D. Analysis of Chaotic Error in Time Series

Since error is inevitable in every forecasting system, it must be specifically analyzed. In order to determine whether the prediction error has chaotic behavior or not, the largest Lyapunov exponent is calculated [10]. As analyzed in [8], the existence of a positive maximum Lyapunov exponent shows that the chaotic behavior exists in prediction error values. This means that prediction error possesses complexity behavior in some time instants that can be further classified by computing the local Lyapunov exponent in the next step.

E. Chaotic and Non-chaotic Errors Classification by Applying a Local Lyapunov Exponent (Exponential Rate of Error)

In this step, error value Δx_i is analyzed to classify chaotic and non-chaotic errors, which is calculated using the local Lyapunov exponent formula [8]:

$$\lambda_i = \frac{1}{t_i} \ln \left| \frac{\Delta x_i}{\Delta x_1} \right|; \tag{3}$$

A positive value for λ_i demonstrates that the prediction error Δx_i has a complex behavior at this time instant. The predicted value $\hat{x}_i$ has much distance with respect to the real x_i that means a chaotic error. In fact, chaotic errors refer to abnormal behavior. Furthermore, the negative value of λ_i shows non-chaotic error on i-th time instant, because the prediction error is so small. Non-chaotic errors refer to normal behavior. The accuracy of the proposed procedure can be seen in Fig. 5. In this figure, only at 160 time instants there exist chaotic states which are clearly marked with a positive λ_i. Now, to clearly represent the chaotic and non-chaotic errors as shown in Fig. 6, a sign map is built to display the distinction, as follows:

$$N_1(i) = \begin{cases} -1, & \text{if } \lambda_i < 0; \\ 1, & \text{if } \lambda_i > 0; \end{cases} \tag{4}$$

clearly, $N_1(i) = -1$ and 1 present chaotic and non-chaotic errors, respectively. According to the dynamic characteristics of network traffic during attack time, all of the chaotic states do not lead to attack instant. Attack traffic will be detected in the next section.

F. Normal and Attack Traffics Detection Step

The ratio of packet numbers, x_i, to number of source IP addresses, I_i, in each time instant ($y_i = x_i/I_i$) is plotted in Fig. 2. It is clear that during attack times, this ratio enormously grows. This fact and positive values for λ_i are used to detect attack traffics. Following behaviors simultaneously happen:

1) During attack times, the ratio of y_i/y_1 enormously grows (exponential growth). It means $\alpha_i = \ln|\frac{y_i}{y_1}| > 1$
2) During attack times the dynamics of the traffic state attracts to a stable state [2]. According to this fact, one can consider $\beta_i = \ln|\frac{y_i}{y_{i-1}}| \leq 1$
3) As mentioned in section E, during attack times the Lyapunov exponent remains positive for a while, due to DoS/DDoS attacks nature. It is clearly shown in Fig. 1 as well. If it is assumed that this situation is repeated in at least K consecutive minutes, then $K = \sum_{j=i-k+1}^{i} N_j$. Considering the repetitive number K, if the attack happens at $i = i_0$, the system detects the attack with K-1 minutes of delay (cf. (5)). Hence, K should not be a large number. In this algorithm, $K = 4$ is selected.

Finally, based on (5), traffic states, including normal and attack are detected. The result is shown in Fig. 7.

$$A(i) = \begin{cases} 1, & \text{if } \lambda_i > 0, \sum_{j=i-3}^{i} N_1(j) = 4, \alpha_i > 1, \beta_i \leq 1; \\ 0, & \text{Otherwise}; \end{cases} \tag{5}$$

$A(i) = 0$ and 1 represent normal and attack traffics, respectively. Furthermore, if the data set contains both DoS and DDoS traffics, the number of source IP addresses can be used to differentiate between DoS and DDoS attacks. The following equation explores this issue:

$$D(i) = \begin{cases} 0, & \text{if } A_i = 1; I_i = 1 \\ 1, & \text{if } A_i = 1; I_i > 1; \end{cases} \tag{6}$$

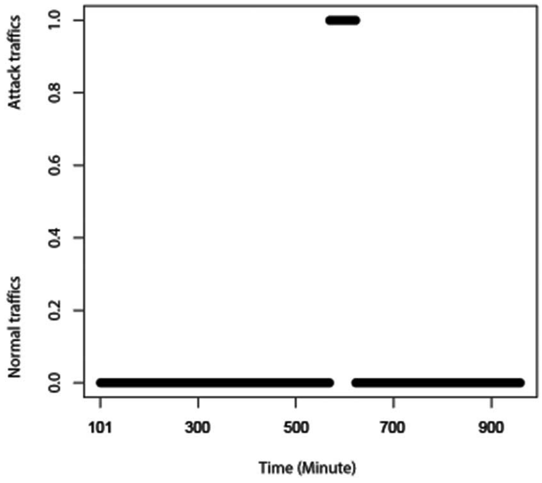

Fig. 7. Normal(0) and attack(1) traffics detection for time instants 101–960.

TABLE I
CONFUSION MATRIX

Number of False Negative(s)	Number of True Positive(s)
3	51
Number of True Negative(s)	Number of True Negative(s)
805	1

TABLE II
COMPARISON BETWEEN DETECTION RATES OF ALGORITHMS

Algorithms	Detection rate(%)
The proposed algorithm	99.5
Wu and Chen's algorithm [8]	98.4
Anjali's algorithm [6]	95
Chonka *et al.'s* algorithm [2]	94
Chen *et al.'s* algorithm [7]	93.75

Clearly, $D(i) = 0$ and 1 shows DoS and DDoS traffics, respectively. The above steps of the algorithm are summarized as follows:

$$FD(i) = \begin{cases} \text{Normal}, & \text{if } A_i = 0 \\ \text{DoS}, & \text{if } A_i = 1, D_i = 0 \\ \text{DDoS}, & \text{if } A_i = 1, D_i = 1. \end{cases} \tag{7}$$

III. EXPERIMENTAL RESULTS

In the proposed algorithm, attack times are 54 minutes long continuously and almost all of them (51 out of 54) are correctly detected. The proposed algorithm implemented on a Core i7 Laptop with 2.3 GHZ CPU and 8GB RAM, using R software environment. Furthermore, Box-Cox and ARIMA toolboxes are also used in the mentioned software. Table I shows the confusion matrix and Table II is the detection rate of the proposed and previous algorithms. Although there are new data sets such as Darknet and CAIDA, but in order to fairly compare the proposed algorithm with [8], Friday of week five is used in standard DARPA1998 data set [12].

IV. CONCLUSION AND FUTURE WORKS

In this letter, a novel DoS and DDoS detection algorithm is proposed, in which the number of packets time series variance is fixed using the Box-Cox transformation. This choice causes a better prediction based on an ARIMA model. In the next step, error chaotic characteristics of time series are explored and the local Lyapunov exponent classify chaotic and non-chaotic errors. Finally, based on the defined rules, normal and attack traffics are classified from each other. Although, in bursty time instants, the number of packets has a meaningfule difference with normal ones (they have positive Lyapanuv exponent), but they have not all properties of attack time instants such as features 1, 2, and 3 in the section F. Hence, classification of attack and bursty traffics from each other is an important issue. This fact is a good motivation to follow two goals in the future work. First, building a Darknet dataset with DRDoS attack and bursty time instants using more features (such as type of protocols, TTL values, geo-location of reflective IPs, etc.) and second, presenting an algorithm based on chaos theory to classify attack and bursty traffic states from each other.

REFERENCES

[1] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, Nov. 2013.

[2] A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Commun. Lett.*, vol. 13, no. 9, pp. 717–719, Sep. 2009.

[3] G. Zhang, S. Jiang, G. Wei, and Q. Guan, "A prediction-based detection algorithm against distributed denial-of-service attacks," in *Proc. Int. Conf. Wireless Commun. Mobile Comput.*, 2009, pp. 106–110.

[4] A. H. Yaacob, I. K. T. Tan, S. F. Chien, and H. K. Tan, "ARIMA based network anomaly detection," in *Proc. 2nd Int. Conf. Commun. Softw. Netw.*, 2010, pp. 205–209.

[5] C. Fachkha, E. Bou-Harb, and M. Debbabi, "Towards a forecasting model for distributed denial of service activities," in *Proc. IEEE 12th Int. Symp. Netw. Comput. Appl.*, 2013, pp. 110–117.

[6] M. Anjali, "Detection of DDoS attacks based on network traffic prediction and Chaos theory," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6502–6505, 2014.

[7] Y. Chen, X. Ma, and X. Wu, "DDoS detection algorithm based on preprocessing network traffic predicted method and Chaos theory," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 1052–1054, May 2013.

[8] X. Wu and Y. Chen, "Validation of Chaos hypothesis in NADA and improved DDoS detection algorithm," *IEEE Commun. Lett.*, vol. 17, no. 12, pp. 2396–2399, Dec. 2013.

[9] D. C. Montgomery, C. L. Jennings, and M. Kulahci, *Introduction to Time Series Analysis and Forecasting*. Hoboken, NJ, USA: Wiley, 2015.

[10] M. Rosenstein, J. Collins, and C. de Luca, "A practical method for calculating largest Lyapunov exponents from small data sets," *Phys. D-Nonlinear Phenom.*, vol. 65, nos. 1–2, pp. 117–134, 1993.

[11] A. A. Ramaki, M. Amini, and R. E. Atani, "RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection," *Comput. & Sec.*, vol. 49, pp. 206–219, 2015.

[12] MIT Lincoln Lab. (1998). DARPA Intrusion Detection Evaluation [Online]. Available: https://www.ll.mit.edu/ideval/data/1998/training/week5/index.html