ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp05.pdf

A Novel Syn Flood Detection Mechanism for Wireless Network

Neethu Raj P, Dr. S Suresh Babu, Prof. Nishanth N
PG student, TKM college of engineering, Kollam, Kerala University, India, neethurajpunathil@gmail.coml
Professor, TKM college of engineering, Kollam, Kerala University, India, drssbtkm@gmail.com
Assistant professor, TKM college of engineering, Kollam, Kerala University, India, nishtkm@gmail.com

Abstract-SYN flood attack is a distributed denial of service attack (DDoS). This paper presents an effective and more accurate mechanism to detect synflood attack. In the proposed SYN-flood defense mechanism, different transport layer parameters are used to characterize attack, like abnormal increase in SYN packet,SYN-ACK packets, and increase in SYN/FIN rate. Proposed mechanism uses preprocessing and prediction using AR model to predict the traffic. Lyapunov exponent developed using prediction error is used as a threshold to detect attack. Out of the three parameters analyzed using same method, at least two results must be same which is taken as the final decision. To analyze validity of proposed scheme, syn flood attack was created using NS2. Data extracted from trace file, given as an input to the detection scheme developed by MATLAB. Probability of false alarm will be very less, since all the parameters do not show abnormality at the same time in a normal traffic.

Keywords- *SYN-flood;DDoS attack; Transport layer; Prediction; Chaos.*

INTRODUCTION

Wireless networks like Mobile Adhoc network (MANET) is infrastructure-less network, or there is no centralized controller [1]. It consists of mobile nodes which are free to move independently in any direction. Nodes can join and leave the network at any time, and so links are changing frequently. Due to the dynamic nature of MANET and since the nodes act asrouters MANET is vulnerable to different attacks. Since nodes can join and leave at any time, and can move in any direction it is difficult to detect attack.

In the TCP three- way handshake, when the server receives a client's SYN request, it replies with a SYN/ACK packet and then waits for the client to send the ACK to complete the three-way handshake. While waiting for the final ACK, the server maintains a half-open connection. But the attacker never sends final ACK, and the server maintains half open connection for the entire duration of normal ideal TCP connection which is 75s normally. SYN flood attack leads to denial of service. As a result of SYN flood attack, the number of half open connections in a node is increasing. Since the connections are half open the server cannot provide service to good nodes that request for new connection. Thus the services provided by the server are denied. It is important to detect SYN-flood attacks at an early stage before there are a large number of half-open connections maintained by the protected server.

Algorithms like CUSUM [2] used to defend SYN flood attack, is complex. Trace-back mechanism uses the network layer or MAC layer abnormalities to characterize the SYN flood attack. After detecting the presence of attack, a search process is initialized by the victim to trace the attacker. Defending mechanisms which detect and defend attack at an early stage is more efficient. It should also inform other nodes about the attack. Many Detection algorithms like the algorithm based on chaos theory uses the network traffic for characterizing and detecting SYN flood attack. Some detection mechanisms use MAC layer abnormalities for detection. Abnormalities may occur in a layer due to delay, increased traffic etc.Many detection algorithms are proposed to detect syn flood attack. Still a perfect solution is not yet developed.

If each node monitor different symptoms of SYN flood attack in transport layer like abnormal increase in transport layer packet, abnormal increase in SYN-FIN rate and abnormal increase in SYN-ACK rateand make a decision based on majority, detection will be more accurate. Every node monitors all the three parameters.Based on the collected information each parameter independently process and detects the presence of SYN flood attack. Victim takes a decision based on the majority result obtained.

The organization of thesis is as follows. This section introduces to the main properties of the problem identified. In section 2, a brief review of several research papers related to the thesis are given. Parameters used and proposed work of this thesis is included in chapter sections 3 and 4. Section 5 includes result analysis and conclusion of the work is given in section 6.

RELATED WORK

Researchers suggested different methods to defend SYN flood attack. Still a perfect solution is not yet developed. To prevent SYN flood attack, *Improving The Functionality of SYN Cookies* [4] was suggested. In his approach, when the server receives SYN, it computes a normal SYN-ACK reply,gets a cookie for the server's ISN, and sends it as a pure SYN (with the ACK bit disabled).

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp05.pdf

Anomaly detection algorithms for detecting SYN flooding attacks [2] proposed two algorithms- adaptive threshold algorithm and an algorithm based on the CUSUM change point detection scheme. Adaptive threshold algorithm is adaptively set using recent traffic measurements. The algorithm signals an alarm when the measurements exceed some threshold for a number of consecutive intervals. Algorithm based on the CUSUM change point detection, signalsan alarm when the accumulated volume of measurements up to are above some traffic threshold exceeds an aggregate volume threshold the CUSUM algorithm considers the excess volume sent above the normal volume, hence accounts for the intensity of the violations. CUSUM based algorithm is complex in nature.

Traceback along with IDPF (Inter Domain Packet Filter-used to identify spoofed nodes) is proposed to detect DDoS in network. Attacker traceback determine real attack sources and full path taken by attack sources. Attacker Traceback mechanism should be scalabe, efficient, and show robustness to address spoofing, collusion and topology change. Under attack, abnormality is observed consistently on route from attacker to victim. Victim node initiates efficient search process. *SWAT: Small World-based Attacker Traceback in Ad-hoc Networks* [5] is a lightweight in terms of information gathering. Traffic shows abnormal pattern or volume. Extended Small World Based Contact is used to search for the nodes that observe similar traffic signature. In *ATTENTION: ATTackErTraceback using MAC Layer AbNormalityDetecTION* [6] attack signature is characterized by MAC layer abnormality. *ZSBT (Zone- Sampling Based Attacker Trace-back Algorith) - A Novel Algorithm for Tracing DoS Attackers in MANETs* [7], the network is partitioned into several zones and assign a unique zone ID for each zone, which helps to traceback the attacker. *CATCH: A protocol framework for cross-layer attacker traceback in mobile multi-hop networks* [8] uses network layer and MAC layer activity to characterize attack. There are course-grained (network layer and MAC layer) abnormality monitoring and fine-grained (network layer and MAC layer) abnormality monitoring.

Attacking signatures are captured using an active probing method DARB in *An autonomous defense against SYN flooding attacks: Detect and throttle attacks at the victim side independently* [9]. It obtains the routers delay values by sending packets containing special TTL set at the IP headers. The results of the probing are used to perform SYN flooding detection.

A collaborative defense mechanism against SYN flooding attacks in IP networks [10] was proposed to protect a spoofed network from syn flood attack and reduce the ARP traffic, a matching table is that keeps track of initiated sessions is used. The matching table identifies a session by a combination of the source IP, destination IP, source port, destination port, and the time the connection was requested.

PARAMETERS USED TO CHARACTERIZE SYN FLOOD ATTACK

To detect SYN-flood attack each nodes monitors different transport layer parameters. Some nodes monitor number of SYN packets with time, some other nodes SYN-ACK packets, and increase in SYN/FIN rate. For monitoring these abnormalities each node collects traffic and flow information in transport layer. Based on the collected information each nodes independently check for the presence of SYN-flood attack. When victim node observes the presence of SYN-flood attack, it seeks the help from other nodes. Other nodes use the same mechanism and inform their opinion to victim. Victim node combine the opinion of others using Un-normalized Dempster's combination rule.

SYN traffic

It uses SYN packet count information for characterizing transport layer traffic. Chaos theorem can be used to predict and analyze abnormality, to detect SYN flood attack. Victim nodes continuously monitor traffic pattern collect transport layer traffic packets and flow information. Sample all the traffic and get a sequence of samples, x_1,x_2,……x_k,x_n where x_n represents state of traffic. Then carry out preprocessing method and Chaos theory.

SYN/FIN rate.

To initiate a TCP connection client must first send a SYN packet to the server. To terminate a TCP connection the client must send a FIN packet. For a normal connection for every SYN packet there must be a FIN packet. So the SYN-FIN rate must be 1. But in a time interval, due to network traffic, delay, and variable connection time SYN-FIN rate must have some variations. If the variation is much more, the abnormal variations in SYN-FIN rate can be concluded as attack. Nodes that monitor transport layer will continuously check for the SYN-FIN rate and detect presence of attack.

Abnormalities in SYN-ACK rate

To begin a TCP connection, client will send a SYN packet to server. Server allocates buffer and a port for the client and sends back a SYN-ACK packet to the client, and wait for ACK. Whenever the timeout event occurs, TCP retransmits the not-yet acknowledged segment with the smallest sequence number. But each time TCP retransmits, it sets the next timeout interval to twice the previous value.

When server receives a SYN packet, it will send SYN-ACK to the client. Let the time out is defined as 3RTT (Round Trip Time). If the server didn't get ACK after 3RTT, again retransmit SYN-ACK and set the timeout to 6RTT[11]. After 6RTT, if ACK is not obtained retransmit SYN-ACK and set timeout to 12RTT. This process continues till a maximum timeout set. After that the half open connection will be terminated. Rate of SYN-ACK transmission will increase in

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp05.pdf

this way. DDoS attack (SYN flood attack) can be characterized by the abnormal increase in the SYN-ACK rate.

PROPOSED DDoSSYN FLOOD DETECTION SCHEME

SYN flood detection method

Each node monitors any one of the above mentioned parameters to detect the presence of SYN-flood attack. Collected samples

$$x_1, x_2, \ldots\ldots x_k, \ldots x_n$$

where x_n represent the state of traffic. Here we use three different transport layer parameters. And analyze them separately to detect syn flood attack. When the syn packets is used for analyzing, x_n represents number of syn packets received per second. When syn-ack packet is used for detection, x_n is the number of syn-ack packets send per second. Or x_n may be syn/fin rate per second.

For accurate prediction traffic must be relatively stable. Preprocessing by calculating cumulative average of x_n with a time range, makes the traffic relatively stable[12,13].

$$\tilde{X}_k = {(x_1 + x_2 + \cdots + x_k)}/{t_k} \qquad (1)$$

Use AR (Auto Regressive) model to predict the future value, of preprocessed traffic [14].

$$\tilde{X}_j = \sum_{k=1}^{m} a_k \tilde{X}_{j-k} \qquad (2)$$

Where $$a_k = \frac{\sum_{t=1}^{n-k}(\tilde{X}_t - \bar{X})(\tilde{X}_{t+k} - \bar{X})}{\sum_{t=1}^{n}(\tilde{X}_t - \bar{X})^2} \qquad (3)$$

We know that

$$\tilde{X}_{k-1} = {(x_1 + x_2 + .. + x_{k-1})}/{t_{k-1}} \text{ and}$$

$$\tilde{X}_k = {(x_1 + x_2 + \cdots + x_k)}/{t_k}$$

From the prediction of preprocessed data prediction of x_k can be obtained using the following equation.

$$\hat{x}_k = t_k \tilde{X}_k - t_{k-1} \tilde{X}_{k-1} \qquad (4)$$

Exact prediction can- not be done always. So there will be some prediction error. The prediction error can be obtained by using the equation,

$$\Delta x_k = x_k - \hat{x}_k \qquad (5)$$

Δx_k represents changed traffic due to additional new traffic busty legitimate traffic or attack traffic.

For the server, however, it is hard to tell which is caused by congestion and which by attack. As a result, the victim server will wait until time is out and will try several times by resending 'ACK/SYN' packets. It is important to refer to half-open connections of this type as *abnormal half-open* connections.

$\{\Delta x_k\}$ is the divergence between predicted traffic $\{\hat{x}_k\}$ and real time traffic $\{x_k\}$. Using the obtained divergence, obtain Lyapnov exponent as follows[15].

$$\lambda_k = {\{\ln({\Delta x_k}/{\Delta x_0})\}}/{t_k} \qquad (6)$$

If $\lambda_k > 0$, Δx_k is still chaotic. The change is due to new traffic. The change is not caused by DDoS attack.

If $\lambda_k = 0$, Δx_k is in steady state. The network traffic is not moved to new one. Thus there is no attack traffic entering.

If $\lambda_k < 0$, Δx_k is not chaotic. It represents legitimate abrupt traffic entering the system, or DDoS attack traffic that may be introduced by an attacker entering the system.

Working of Syn flood detection scheme

1. Each node collect the information, number of SYN packets received per second, number of SYN-ACK packets send per second, and SYN/FIN rate per second.
2. Nodes monitor the traffic and take a decision, about the abnormal increase in traffic.
   i. Collect traffic packets and flow information in real time.
   ii. Preprocess the collected information with (2) and then predict with (3) and (4)
   iii. Based on chaos theory distributed above analyze prediction error and then detect abnormal traffic.
3. If analysis of at least two parameters shows abnormality, the node confirms presence of syn flood attack.

RESULT ANALYSIS

To analyze the validity of proposed SYN flood detection scheme, trace files for normal traffic and SYN flood attack traffic for slow and fast attack are extracted using NS2. From the trace file required, parameters are extracted. Validation of the detection scheme was conducted using MATLAB.

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp05.pdf

Normal traffic behaviour

For a normal network, without any attack, syn arrival depends only on the connection requests from legitimate nodes. Normally number of SYN packets received per second varies between 0 and 50. Seasonal variations cause an increase in syn arrival, but this will not persist for a long time.

After the season syn arrival also becomes normal. Result obtained while analyzing the syn detection scheme using a normal traffic is shown in Fig.1. Here number of syn packets arrived during a second is always below 80. Normally syn arrival varies between 0 and 50. Syn arrival becomes 70 two times which may be due to seasonal variations. Preprocessed data, predicted traffic, prediction error, Lyupunov exponent and attack detection are plotted against time. From the graph it is clear that Lyupunov exponent never goes negative. Which indicate the absence of attack.

SYN flood detection

To evaluate relevance of the proposed algorithm in detecting syn flood attack syn arrival details extracted and verified the algorithm. At first syn flood attack with a syn arrival rate 100 syn/sec created. Proposed algorithm evaluated using, SYN arrival traffic. Analysis result is shown in Fig.2. The network behaves normally for first twenty seconds. After thirty second syn arrival increases slowly. SYN arrival varies between 100 and 200. Preprocessed traffic increases the stability of detection. Predicted data is shown in the graph. Prediction error, which is obtained by comparing actual traffic and predicted traffic, is very high compared to prediction error in normal traffic. Lyupunov exponent obtained using prediction error, which is used as the threshold becomes negative and attack is detected at a time 50s. It takes 20 seconds to detect attack.

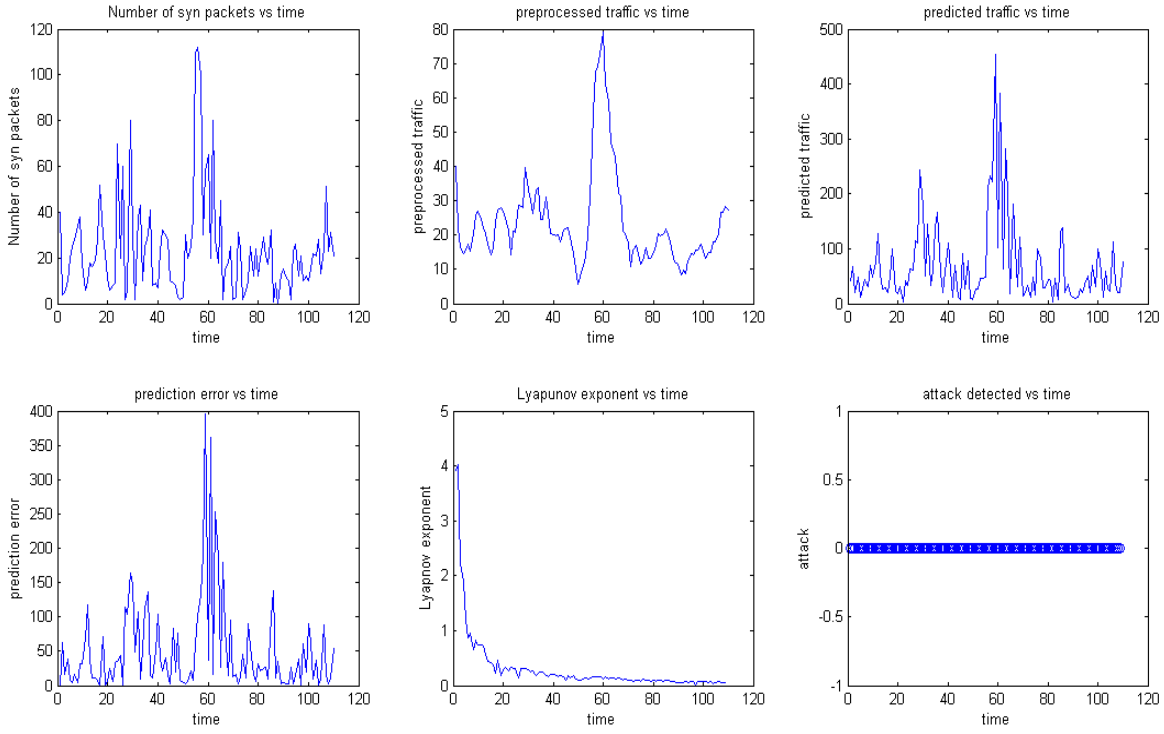

Fig.1. SYN arrival, preprocessed data, predicted traffic, prediction error, Lyupunov exponent and attack detection for normal network.

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp05.pdf

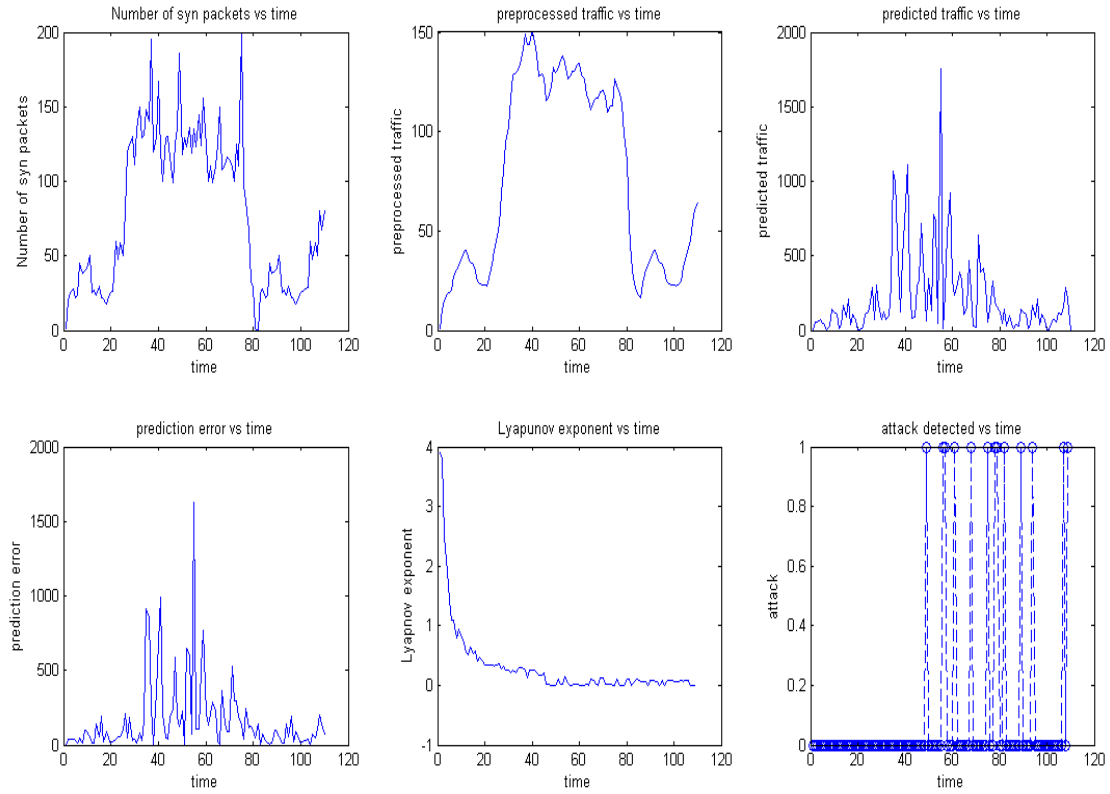

Fig.2. SYN arrival, preprocessed data, predicted traffic, error, Lyupunov exponent and attack detection for network with SYN flood attack

CONCLUSION

SYN flood attack is one of the major security issues in infrastructure less network like MANET. The defense mechanism uses different transport layer abnormalities. Each node uses algorithm based on preprocessing network traffic predicted method and Chaos Theory to detect syn flood attack. Victim node combines opinion of other nodes and take a decision about the presence of attack. The method is less vulnerable to false alarm. False alarm is reduced by monitoring three different parametersand analyzing the using same method simultaneously. Final decision is made based on majority result. The proposed mechanism is a better mechanism to defend SYN flood attack in MANET compared to the existing mechanisms.

REFERENCES

[1]. PriyankaGoyal, VintiParmar , Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM, January 2011 Volume-. 11, pp 32-37

[2]. Vasilios A. Siris and FotiniPapagalou, "Application of Anomaly Detection Algorithms forDetecting SYN Flooding Attacks", FORTH,2003[3]. Sunil Gupta, Harsh K Verma, A L Sangal, "Security Attacks

& Prerequisite for Wireless Sensor Networks", IJEAT, June 2013, Volume-2, Issue-5, pp 558-566.

[4].Andr_eZ_uquete, "Improving the functionality of syn cookies", ACM, 2002, pp 57-77.

[5]. Yongjin Kim and Ahmed Helmy, "*SWAT*: *S*mall *W*orld-based *A*ttacker *T*raceback in Ad-hoc Networks", IEEE, Proc. 2005.

[6]. Yongjin Kim, Ahmed Helmy, "ATTENTION: ATTackErTraceback using MAC Layer

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 22 - 27 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp05.pdf

AbNormalityDetecTION", Electrical Engineering Dept.– Systems University of Southern California, California, U.S.A.

[7]. Xin Jin, Yaoxue Zhang, Yi Pan, and YuezhiZhou,"ZSBT - A Novel Algorithm for Tracing DoS Attackers inMANETs",EURASIP Journal onWirelessCommun and Networking,2006, pp 1–9.

[8]. Yongjin Kim, Ahmed Helmy, "CATCH: A protocol framework for cross-layer attacker traceback in mobile multi-hop networks", ELSEVIER, 2009, pp 193–213

[9]. B.Xiao,Wei Chen, Yanxiang He and Edwin H.-M, "An autonomous defense against SYN flooding attacks: Detect and throttle attacks at the victim side independently", Science direct, 2008, pp456 – 470.

[10] HaidarSafa, and MohamadChouma, "ACollaborative Defense mechanism against SYN flooding attacks in IP networks",Science direct, 2008, pp 509–534.

[11] B J Kwak, Nah-Oak Song, and Leonard E. Miller, "Performance Analysis of Exponential Backoff", IEEE/ACM transactions on networking, VOL. 13, NO. 2, APRIL 2005

[12] Yonghong Chen, Xinlei Ma, Xinya Wu, "DDoS Detection Algorithm Based on Preprocessing Network Traffic Predicted Method and Chaos Theory", IEEE communications letters, VOL. 17, NO. 5, MAY 2013, pp-1052-105.

[13] 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, 2009.

[14] T. Vafeiadis, A. Papanikolaou, C. Ilioudis, and S. Charchalakis, "Realtime network data analysis using time series models," *Simulation ModellingPractice and Theory*, pp. 173–180, 2012.

[15] A. Wolf, J. B. Swift, H. L. Swinneyt, and J. A. Vastano, "Determining Lyapunov exponents from a time series," Chaotic Oscillators: Theory and Applications, vol. 160, pp. 285–317, 1992.