Chaos Theory Based Detection against Network Mimicking DDoS Attacks

Ashley Chonka, *Member, IEEE,* Jaipal Singh, *Member, IEEE,* and Wanlei Zhou, *Member, IEEE*

***Abstract*—DDoS attack traffic is difficult to differentiate from legitimate network traffic during transit from the attacker, or zombies, to the victim. In this paper, we use the theory of network self-similarity to differentiate DDoS flooding attack traffic from legitimate self-similar traffic in the network. We observed that DDoS traffic causes a strange attractor to develop in the pattern of network traffic. From this observation, we developed a neural network detector trained by our DDoS prediction algorithm. Our preliminary experiments and analysis indicate that our proposed chaotic model can accurately and effectively detect DDoS attack traffic. Our approach has the potential to not only detect attack traffic during transit, but to also filter it.**

***Index Terms*—Distributed denial-of-service (DDoS), anomaly detection, chaotic models.**

I. Introduction

DENIAL of service (DoS) attacks are designed to disrupt network services, by intentionally blocking or degrading the available resources used by them. One of the major problems for DDoS detection methods is the difficulty of differentiating DDoS attack packets from legitimate packets [1], since attackers mimic their attack traffic amongst legitimate traffic in order to hide their attack. This makes DDoS attacks a very serious threat to computers users [2].

In this paper, we developed a novel prediction algorithm that can detect DDoS attack packets and give some certainty of when the attack started. This information is then used by a trained neural network to drop the DDoS attack packets and can be used by the relevant authorities to identify the attacker.

The organisation of this paper is as follows: Details of our proposed Network Anomaly Prediction Algorithm (NAPA) are provided in section II. Analysis of our simulated network experiments are discussed in section III. Section IV concludes the paper.

II. Network Anomaly Prediction Algorithm

The use of chaos models to represent network traffic is not new. Previous research has shown that TCP-based network traffic has self-similar characteristics [3], [4]. Algorithms to detect DDoS attack packets from legitimate packets, based on self-similar characteristics, have been proposed in [5].

In our approach, we use real network traffic information to discover the self-similar pattern for legitimate traffic, and use this information as a benchmark for our prediction algorithm, to determine if any new traffic that enters the network is DDoS traffic or legitimate traffic. Our trained neural network system will filter out any anomalous traffic that fits the DDoS characteristics. We present our self similar network traffic model and DDoS prediction algorithms in the following sections.

A. Self Similar Network Model

Our model requires that all network traffic be sampled so that a self similar phase space graph can be generated of the network. We pick the state of traffic that contains normal (X_n) and attack traffic (X_a).

$$X_n + 1 = f(X_n) \tag{1}$$

$$X_a + 1 = f(X_a) \tag{2}$$

Where $f(X)$ maps the nonlinear function dimension of the input variables, which is the same as the dimension of output variables.

From (1) and (2) we generate a sequence of the form:

$$X_{n0}, X_{n1}, X_{n2}, X_{n3}, \ldots, X_{nN} \tag{3}$$

$$X_{n0} + \Delta X_{n0}, X_{n1} + +\Delta X_{n1}, \ldots, X_{nN} + \Delta X_{nN} \tag{4}$$

$$X_{a0} + \Delta X_{n0}, X_{a1} + +\Delta X_{n1}, \ldots, X_{nN} + \Delta X_{aN} \tag{5}$$

The sequence (3) (4) are the orbit or trajectory of (1), representing normal traffic and changed traffic due to new traffic or bursty legitimate traffic. Equation (5) is the orbit or trajectory of normal traffic changes to attack traffic, given in (2).

We now consider the two points in space, legitimate traffic (self similar) = X_{n0}, and attack traffic = $X_{a0} + \Delta X_{n0}$. We assume that network traffic attracts to fixed points, which diminishes asymptotically with time $\Delta X_n(X_{n0}, t)$. We further assume in our model that at any time the normal traffic orbit diverges exponentially but eventually settles, it is either due to new traffic entering the system or a burst of legitimate traffic. This behavior is modeled in (4).

If the function $\Delta X_n(X_{n0}, t)$ behaves 'chaotically' when new traffic enters the network, the function is changed to $\Delta X_a(X_{a0}, t)$ and the new traffic is assumed to be IP spoofed DDoS attack traffic.

Manuscript received March 15, 2009. The associate editor coordinating the review of this letter and approving it for publication was C.-K. Wu.

A. Chonka and W. Zhou are with the School of Engineering and Information Technology, Deakin University, Melbourne, Australia (e-mail: {ashley, wanlei}@deakin.edu.au).

J. Singh is at the Digital Ecosystems and Business Intelligence Institute, Curtin University, Perth, Australia (e-mail: j.singh@cbs.curtin.edu.au).

This work is partially supported by the ARC Discovery Grant DP0773264 and ARC Linkage Grant LP0562156.

Digital Object Identifier 10.1109/LCOMM.2009.090615

TABLE I
NETWORK ANOMALY PREDICTION ALGORITHM

1.	Collect normal network traffic packets and flow information.
2.	Calculate self similar traffic, based on $f(x)$ time sequence.
3.	Train neural network on self similar traffic.
4.	New traffic enters the network and changes the orbit (anomaly).
5.	Use Lyapunov Equation to predict the network anomaly:
	If $\lambda_{max} < 1$ then traffic changes are due to legitimate traffic.
	If $\lambda_{max} = 1$ then recalculate point on new self similar traffic.
	If $\lambda_{max} > 1$ then traffic changes are due to DDoS attack.
6.	Train defense system on strange attractor traffic, $\Delta X_a(X_{a0}, t)$
7.	Filter DDoS attack packets.

B. Anomaly Prediction Algorithm

Based on the assumptions above, we study the mean exponential rate of divergence between these two close orbits (normal and new traffic to see if it is attack traffic) by using the Lyapunov Exponent [6].

$$\lambda_{max} = \lim_{x \to \infty} \frac{1}{t} \ln \frac{|\Delta X(X_{n0}, t)|}{|\Delta X_{n0}|} \tag{6}$$

If $\lambda_{max} < 1$, network traffic orbits attract to a stable fixed point from when they diverge due to new legitimate traffic, or bursty legitimate traffic, entering the system. This means that the change in the network phase space graph is not caused by DDoS attack traffic.

If $\lambda_{max} = 1$, the phase space graph is in a steady state (neural fixed point). This event means that the introduced network traffic has moved the self similar network traffic line either up and down, thus becoming the new standard for detecting attack traffic.

If $\lambda_{max} > 1$, the network traffic orbit is chaotic and unstable, which means the nearby points will diverge to any arbitrary separation. This is representation of attack traffic that was introduced by an attacker into the system. This means that $\Delta X_n(X_{n0}, t)$ changes to $\Delta X_a(X_{a0}, t)$. This network traffic is considered to be DDoS attack traffic and dropped by our neural network trained filters. We present our network anomaly prediction algorithm in Table I.

III. RESULTS AND ANALYSIS

We simulated our proposed anomaly prediction algorithm (Table I) by using a real DDoS dataset, DARPA LLS DDoS-1.0 dataset, available from MIT [7]. From this dataset, we generated a time series graph (Fig. 1) from the source IP address, which shows self-similar (Spoof free) traffic and attack traffic (Spoofed) in the network. From Fig. 1, we see that attack traffic closely follows the self similar (normal traffic) line, until the full attack commences, which diverges the line greatly at around 11.25pm. This clearly shows that the network is sensitive to the anomaly and since the attack line did not return to the steady state, we know this is some form of attack. This data fits with our Lyapunov prediction Equation $\Lambda_{max} > 1$.

To further our analysis, we insert our data into a phase space graph (Fig. 2), which gives us a clearer picture of network traffic. Fig. 2 displays normal traffic (top right hand corner) and the attack traffic in the bottom left hand corner. Using Lyapunov Stability 78 [8], where $V(x)$ is the Lyapunov Function candidate (and if $V(x) \neq 0$ or is not a negative definite 8). What can be said about our predictions is that if the attack continues against the network, then its final resting state will show a slow down, moving towards total collapse. This final resting state is called a strange attractor, which is clearly shown at the bottom left hand corner of Fig. 2.

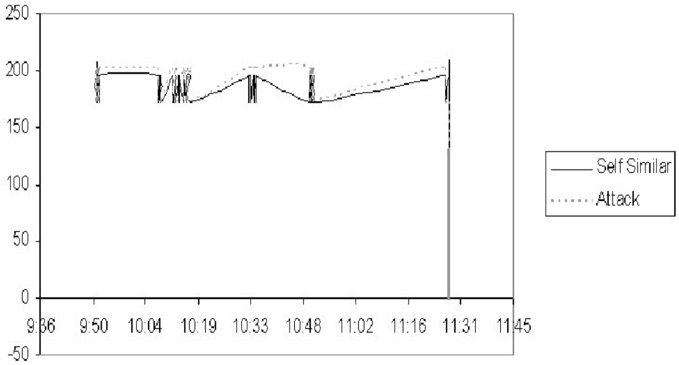

Fig. 1. Time series graph of self-similar normal traffic and DDoS attack traffic in the network.

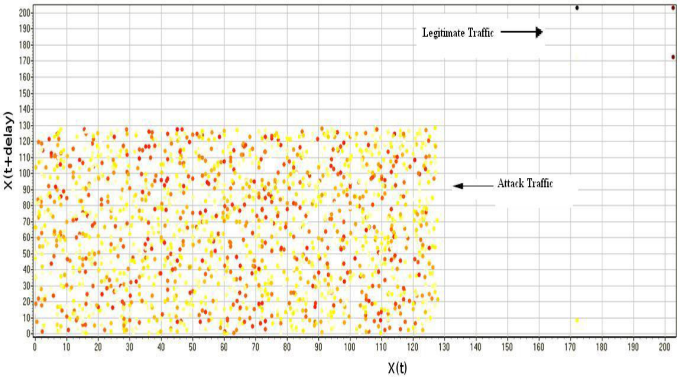

Fig. 2. Phase Space graph for DDoS flooding attack traffic in the network, where $X(t+$ delay$)$ over $X(t)$.

$$V(x) \geq 0 \text{ equal to positive definite} \tag{7}$$

$$V(x(t)) < 0 \text{ equal to negative definite} \tag{8}$$

With the strange attractor, we trained our back-propagation neural network to detect it, with the trained settings of 4 Neuron Layers (3,3,3,1), Learning Rate of 0.2, Momentum of 0.6, and a variable threshold of 0.1 to 0.9, which was incrementally increased by 0.1, and we know that it was trained successfully, since we compared the attack curve with the trained strange attractor curve shown in Bifurcation diagram (Fig. 3).

From the results in Fig. 3, we can see that our neural network follows the strange attractor curve quite accurately, with some slight variation. To further our analysis of accuracy, detection time and time to filter attack traffic by our neural network, we used our relative sensitivity 9 and false positives 10 measures. Sensitivity (S) is measured by the number of detected attack packets (D) over the total number of packets, and the false positive rate (FPR) is measured by how many

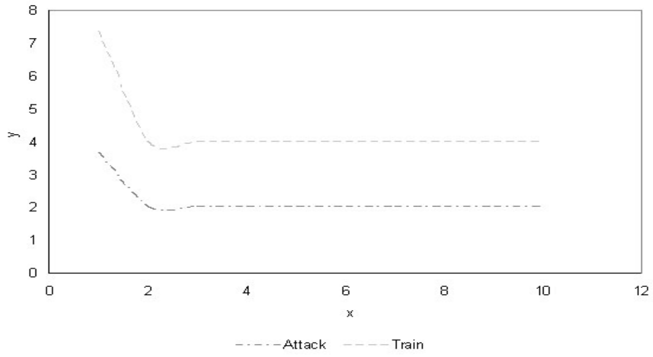

Fig. 3. Bifurcation diagram of trained Neural Network to detect strange attractor (attack) at r = 3.68.

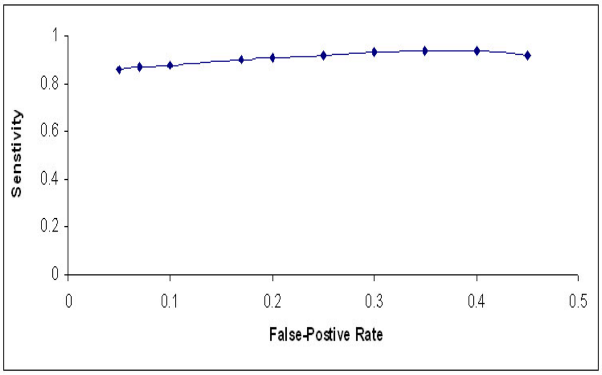

Fig. 4. Sensitivity of Neural Network, where the number of detected packets is over the total of number of packets scanned.

attack packets were detected as normal packets (ND), over the total number of attack packets.

$$S = \frac{D}{T_D} \tag{9}$$

$$FPR = \frac{ND}{T_{ND}} \tag{10}$$

Overall, our Neural Network performed remarkably well (Fig. 4) as expected, with the sensitivity range of 88% to 94%, with a false positive range 0.05% to 0.45%. We furthered our results with another phase space, Fig. 5, which displayed our best performance (94%) of filtering the attack traffic. Based on our simulations, we conclude, that with any large introduction of spoof network traffic (such as a DDoS flooding attack) it will alter the network phase space graph. With this alteration, we can use our Lyapunov Exponent, to predict if a strange attractor (DDoS attack) will develop. If one does, our trained Neural Network will assume that this is DDoS attack and filter the traffic to protect the system.

We further this conclusion by seeing at point A, in Fig. 5, confirms that detection of attack traffic starts within a few seconds of becoming aware that network traffic deviation, in which our neural network begins to filter the attack traffic out. One interesting result is at points B and C in Fig. 5, which displays these large gaps where our Neural Network had filtered the attack traffic. This suggests a possibility that our Neural Network could possible be re-trained and its settings re-adjusted to further filter out more of the attack traffic.

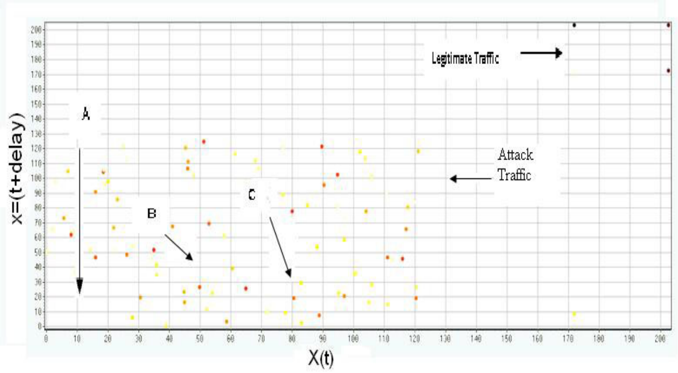

Fig. 5. Filtered DDoS attack traffic from our Neural Network. Point A displays where the Neural Network started to filter the attack traffic.

We further this conclusion by seeing at point A, in Fig. 5, confirms that detection of attack traffic starts within a few seconds of becoming aware of network traffic deviation, in which our neural network begins to filter the attack traffic out. One interesting result is at points B and C in Fig. 5, which displays these large gaps where our Neural Network had filtered the attack traffic. This suggests a possibility that our Neural Network could possibly be re-trained and its settings re-adjusted to further filter out more of the attack traffic.

IV. Conclusion

We have introduced a new algorithm that can predict the nature of network traffic in a dynamic system. Our algorithm detects whether a strange attractor caused by the introduced network traffic returns to the steady state, thus is bursty legitimate traffic, or greatly diverges from the steady state, identifying such traffic as caused by DDoS flooding attack. We have shown through simulations that DDoS attacks can be detected since they cause the network phase space to change. We are currently using neural networks to implement our prediction algorithm in order to filter DDoS attack traffic.

References

[1] K. Kumar, R. C. Joshi, and K. Singh, “A distributed approach using entropy to detect ddos attacks in isp domain,” in *Intl. Conf. in Signal Processing, Communications and Networking (ICSCN)*, 2007, pp. 331–337.

[2] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, “Denial-of-service attack-detection techniques,” *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[3] K. Park, G. Kim, and M. Crovella, “On the relationship between file sizes, transport protocols, and self-similar network traffic,” in *IEEE International Conference on Network Protocols*, 1996, pp. 171–180.

[4] K. Park and W. Willinger, *Self-similar network traffic and performance evaluation*. Wiley New York, 2000.

[5] Y. Xiang, Y. Lin, W. L. Lei, and S. J. Huang, “Detecting ddos attack based on network self-similarity,” *Communications, IEE Proceedings-*, vol. 151, no. 3, pp. 292–295, 2004.

[6] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, “Determining lyapunov exponents from a time series,” *Chaotic Oscillators: Theory and Applications*, vol. 160, pp. 285–317, 1992.

[7] MIT Lincoln Lab (DDoS 1.0):. [Online]. Available: http://www.ll.mit.edu/IST/ideval/data/2000/LLS_DDOS_1.0.html

[8] A. M. Lyapunov, *Stability of Motion*. Academic Press, 1966.