Anomaly Detection of Distributed Denial of Service Attacks by Non-Liner Dynamics
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 very close to the point of origin (attacker). 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 these services to serve other users. One of the major problems for DDoS detection methods is difficulty of differentiate DDoS attack packets from legitimate packets [2]. This makes DDoS attacks are a very serious threat to computers users. Current DDoS research use both active and passive defence mechanisms [1].

In this paper, we developed a novel prediction algorithm that can not only detect DDoS attack packets, but also when did the attack start. This information is then used by a neural network trained filter to drop the DDoS attack packets and can be provided to 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. 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 collect real network traffic information to discover the self-similar pattern for legitimate traffic. We use this information as a benchmark and use our prediction algorithm to discover if any new traffic that enters the network is DDoS traffic or legitimate traffic. Our 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 with contains normal (X_n) and attack traffic (X_a).

\[ X_n + 1 = f(X_n) \] (1)
\[ X_a + 1 = f(X_a) \] (2)

Where \( f(X) \) maps the nonlinear function of 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:

\[ X_{n0}, X_{n1}, X_{n2}, \ldots, X_{nN} \] (3)
\[ X_{a0} + \Delta X_{a0}, X_{a1} + \Delta X_{a1}, \ldots, X_{aN} + \Delta X_{aN} \] (4)

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).

\[ X_{a0} + \Delta X_{a0}, X_{a1} + \Delta X_{a1}, \ldots, X_{aN} + \Delta X_{aN} \] (5)

We now consider the two points in space, legitimate traffic (self similar) = \( X_{a0}, \) and attack traffic = \( X_{a0} + \Delta X_{a0}. \) We assume that network traffic attracts to fixed points, which diminishes asymptotically with time \( \Delta X_n (X_{a0}, t) \). 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 \( \Delta X_a(X_{n0}, t) \) behaves ‘chaotically’ when new traffic enters the network, the function is change to \( \Delta X_a(X_{n0}, t) \) and the new traffic is assumed to be DDoS attack traffic.

### 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].

\[
\lambda_{\text{max}} = \lim_{x \to 0} \frac{1}{t} \ln \left( \frac{\Delta X(X_{n0}, t)}{\Delta X_{n0}} \right)
\]  

(6)

If \( \lambda_{\text{max}} < 1 \), 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 \( \lambda_{\text{max}} = 1 \), 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 \( \lambda_{\text{max}} > 1 \), 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 \( \Delta X_a(X_{n0}, t) \) changes to \( \Delta X_a(X_{n0}, t) \). 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 1.

### III. RESULTS AND ANALYSIS

We simulated our proposed anomaly prediction algorithm (table 1) 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 any anomalies 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 \( \lambda_{\text{max}} > 1 \).

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 (7)(8) [8], where \( V(x) \) is the Lyapunov Function candidate (and if \( V(x) \neq 0 \) or is not a negative \( V(x) \geq 0 \) equal to positive definite

\( V(x(t)) < 0 \) equal to negative definite

define (8)). Then we can say with some certainty about our predictions, that if the network continues to be attacked, the final resting state of the network will slow or collapse. This final resting state is called a strange attractor, which is clearly shown at the bottom left hand corner of figure 2.

With the strange attractor, we trained our 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 incremental increased by 0.1, and we know that it was trained successful, since we compared the attack curve with the trained strange attractor curve, 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. So to further our analysis of accuracy and time of detect and filtering of attack traffic by our neural network, we used our relative sensitivity (9), and false positives measures (10). Sensitivity (S) is measure by the number of detected attack packets (D) over the total number of packet, and the false positive rate (FPR) is measured by how many attack packets were detected as normal packets (ND), over the total number of attack packets.

\[
S = \frac{D}{T_D}
\]

(9)

\[
FPR = \frac{ND}{T_{ND}}
\]

(10)

<table>
<thead>
<tr>
<th>TABLE I</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETWORK ANOMALY PREDICTION ALGORITHM</td>
</tr>
<tr>
<td>1. Collect normal network traffic packets and flow information.</td>
</tr>
<tr>
<td>2. Calculate self similar traffic, based on f(t) time sequence.</td>
</tr>
<tr>
<td>3. Train neural network on self similar traffic.</td>
</tr>
<tr>
<td>4. New traffic enters the network and changes the orbit (anomaly).</td>
</tr>
<tr>
<td>5. Use Lyapunov Equation to predict the network anomaly:</td>
</tr>
<tr>
<td>( \text{If } \lambda_{\text{max}} &lt; 1 \text{ then traffic changes are due to legitimate traffic.} )</td>
</tr>
<tr>
<td>( \text{If } \lambda_{\text{max}} = 1 \text{ then recalculate point on new self similar traffic.} )</td>
</tr>
<tr>
<td>( \text{If } \lambda_{\text{max}} &gt; 1 \text{ then traffic changes are due to DDoS attack.} )</td>
</tr>
<tr>
<td>6. Train defense system on strange attractor traffic, ( \Delta X_a(X_{n0}, t) )</td>
</tr>
<tr>
<td>7. Filter DDoS attack packets.</td>
</tr>
</tbody>
</table>
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. What is curious, is the results at Point B and C, which shows ‘chunks’ of attack traffic that was filtered by our Neural Network, followed by attack traffic that was missed by our Neural Network. 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.

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 the 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