DETECTING THE INCEPTION OF A NETWORK LAYER DOS ATTACK WITH A GRAPH-BASED APPROACH

Ramesh Paudel
Peter Harlan
Dr. William Eberle
■ Introduction
■ Methodology
■ Dataset
■ Experiments & Results
■ Discussion & Future Work
Denial of Service (DOS) Attack

- **Denial of Service (DOS) attack**: malicious act with the goal of interrupting the access to a computer network.

- **Motivation**: include but are not limited to revenge, prestige, politics, or money [1].

- **Goal**: overflow server/network with messages that have invalid return addresses → overwork the targeted network [2].
Motivation

- Imagine a world in which DoS attacks do not exist
  - Saves companies time and money
  - Allows user access to their contents without interruption

However, the majority of the techniques used to identify DoS are too late... the damage has already occurred

- How do we exterminate DoS attacks?
  - Locate DoS attacks at its inception
  - Take action to prevent further damage

- Goal:
  - Identify the DoS attack earlier in the process
Contribution

- Use graph-based approach for detecting DoS Attack.
- Detect DoS attack at its inception (quicker than the installed IDS in company’s network).
Graph-Based Anomaly Detection

- Find normative pattern $S$ (highly compressing pattern using MDL principal)
- Find closely-matching instances $S_A$ of $S$
  - Missing nodes/edges (gathered along the way)
  - Additional nodes/edges (search a bit further)
  - Modified labels among structural matches
- $P_r(SA) = \frac{\text{# particular } SA}{\text{# all } SA's}$
- Anom. score $= Pr(SA) \times D(SA, S)$
- GBAD (www.gbad.info)
Dataset

- **Visual Analytics Science and Technology (VAST) 2011**, mini challenge 2
- Multiple logs (firewall, IDS, etc) from All Freight Corporation’s computer network
- Only firewall log used for this work
- Although there were three days of data, the DoS attack occurs at 11:39:51 am on day one on an external web server.
- DoS attack carried by 5 devices: 10.200.150.<201, 206, 207, 208 and 209>
- IDS log did not flag the DoS attack until 11:43:29 (3 minute and 39 seconds delay)
Data Preparation

- Parsed the firewall log into graphs.
- Devices on network grouped by type instead of IP (helps establish clear pattern).
- Connections (edges) labeled by volume of traffic (e.g., “mid” and “high”).
- Individual graphs correspond to different time intervals.
Experimental setup

- 0 sec interval resulted in too many graphs with a small graph to vertex ratio ($\approx 1:8$) resulting in insignificant patterns.
- Similarly, 8-second intervals generalized the data too much (graph to vertex ratio 1:26), resulting in uninteresting and larger normative patterns.
- 5-sec intervals (middle ground) was chosen for the testing process

<table>
<thead>
<tr>
<th>Single Graph Interval</th>
<th># of Vertices</th>
<th># of Edges</th>
<th># XP/file</th>
<th># of Graphs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal</td>
<td>DoS</td>
<td>Total</td>
<td>Normal</td>
</tr>
<tr>
<td>0 Sec</td>
<td>68,267</td>
<td>59,588</td>
<td>8,478</td>
<td>7,801</td>
</tr>
<tr>
<td>1.25 Sec</td>
<td>49,197</td>
<td>45,007</td>
<td>4,629</td>
<td>4,295</td>
</tr>
<tr>
<td>2.5 Sec</td>
<td>42,032</td>
<td>39,957</td>
<td>3,201</td>
<td>2,962</td>
</tr>
<tr>
<td>5 Sec</td>
<td>33,544</td>
<td>34,543</td>
<td>1,691</td>
<td>1,580</td>
</tr>
<tr>
<td>8 Sec</td>
<td>29,607</td>
<td>32,282</td>
<td>1,140</td>
<td>1,066</td>
</tr>
</tbody>
</table>

Fig: Number of connection from internet to web server

Table: Graph topology based on time intervals and graph counts
Results

Fig: Normative Pattern I and anomalous addition (extra node and edge)

<table>
<thead>
<tr>
<th>Graph Interval</th>
<th>Anom. Graph Reported</th>
<th>Attack Source Reported</th>
<th>Detection Delay</th>
<th>Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Sec</td>
<td>6.35%</td>
<td>5</td>
<td>31</td>
<td>482</td>
</tr>
<tr>
<td>1.25 Sec</td>
<td>4.2%</td>
<td>4</td>
<td>612</td>
<td>289</td>
</tr>
<tr>
<td>2.5 Sec</td>
<td>18.4%</td>
<td>3</td>
<td>31</td>
<td>257</td>
</tr>
<tr>
<td><strong>5 Sec</strong></td>
<td><strong>96.4%</strong></td>
<td><strong>5</strong></td>
<td><strong>23</strong></td>
<td><strong>118</strong></td>
</tr>
<tr>
<td>8 Sec</td>
<td>1.35%</td>
<td>0</td>
<td>4</td>
<td>102</td>
</tr>
</tbody>
</table>

Table: Performance of on different graph topology

<table>
<thead>
<tr>
<th>Actual (DoS)</th>
<th>Predicted (DoS)</th>
<th>Predicted (Normal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual (DoS)</td>
<td>107 (TP)</td>
<td>4 (FN)</td>
</tr>
<tr>
<td>Actual (Normal)</td>
<td>0 (FP)</td>
<td>1580 (TN)</td>
</tr>
</tbody>
</table>

Table: Confusion matrix for 5 second graph using normative pattern shown in the left
Results

- To reduce the DoS attack detection delay.
- Use another subgraph shown above (left side) as a normative pattern.
- Two anomalous instances (right) were found.
- Anomalous pattern - unusual for the web server on All Freight’s computer network to communicate to the DNS servers.
- The anomaly topology was discovered at 11:39:56 am.
- The first flag was raised 5 seconds after the DoS attack begins (DoS attack starts at 11:39:51 am).

Fig: Normative Pattern II and anomalous addition (extra node and edge)
Discussion

■ We argue that these anomalies are justifiable and logical
■ The goal of DoS attack is to squander network resources.
■ It is done by sending a high amount of traffic (which is reflected by the first normative pattern)
■ The direct repercussion of a high amount of traffic:
  – Create factious return addresses
  – Web servers must perform a DNS quarry to find address it does not know
  – This was flagged as an anomaly using the second normative pattern.
Conclusion & Future Work

- Installed IDS picked DoS attack after 3 minute and 39 seconds.
- However, the proposed graph-based approach raised the first flag in 5 seconds after the DoS attack begins.
- Issues
  - Took ~100 seconds to run the algorithms
  - Need to be able to run in real-time, scalability
- Possibilities
  - Sliding window protocol, break down the dataset into smaller chunks instead of analyzing all data at once
  - Process graphs in parallel
Acknowledgements

This work is supported by US National Science Foundation under the grant number 1560434.
References


[10] https://www.ebuyer.com/blog/2015/06/ddos-attacks-explained/ddos-attack/
Questions?