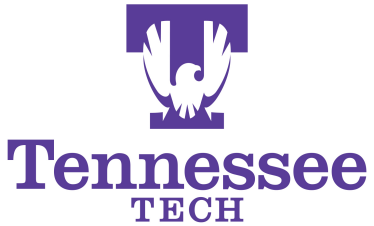
FLAIRS 2019 – Main Track

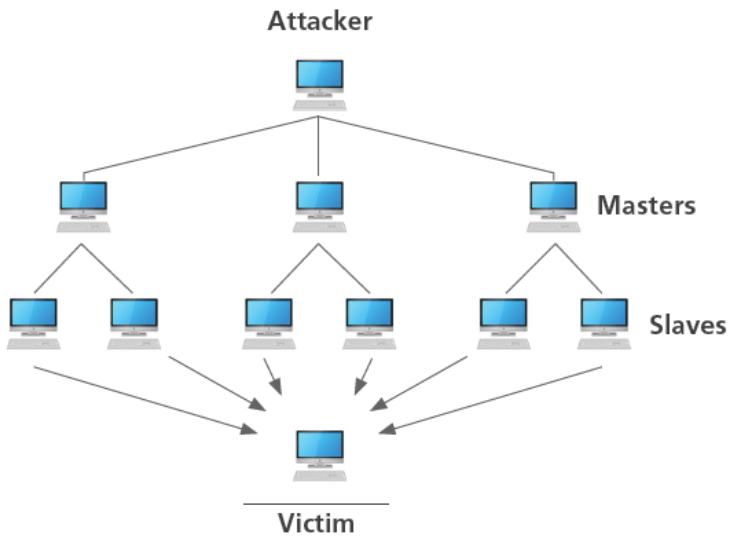


DETECTING THE INCEPTION OF A NETWORK LAYER DOS ATTACK WITH A GRAPH-BASED APPROACH

Ramesh Paudel
Peter Harlan
Dr. William Eberle

- Introduction
- Methodology
- Dataset
- Experiments & Results
- Discussion & Future Work

Denial of Service (DOS) Attack



[10]

- **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

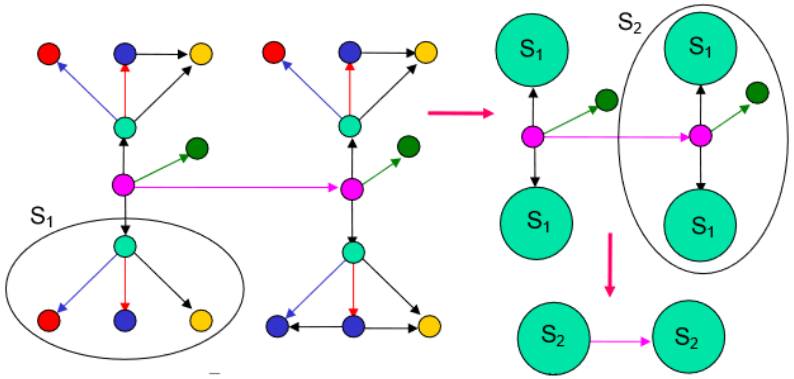
- **How do we exterminate DoS attacks?**
  - *Locate DoS attacks at its inception*
  - *Take action to prevent further damage*
- **Goal:**
  - ***Identify the DoS attack earlier in the process***

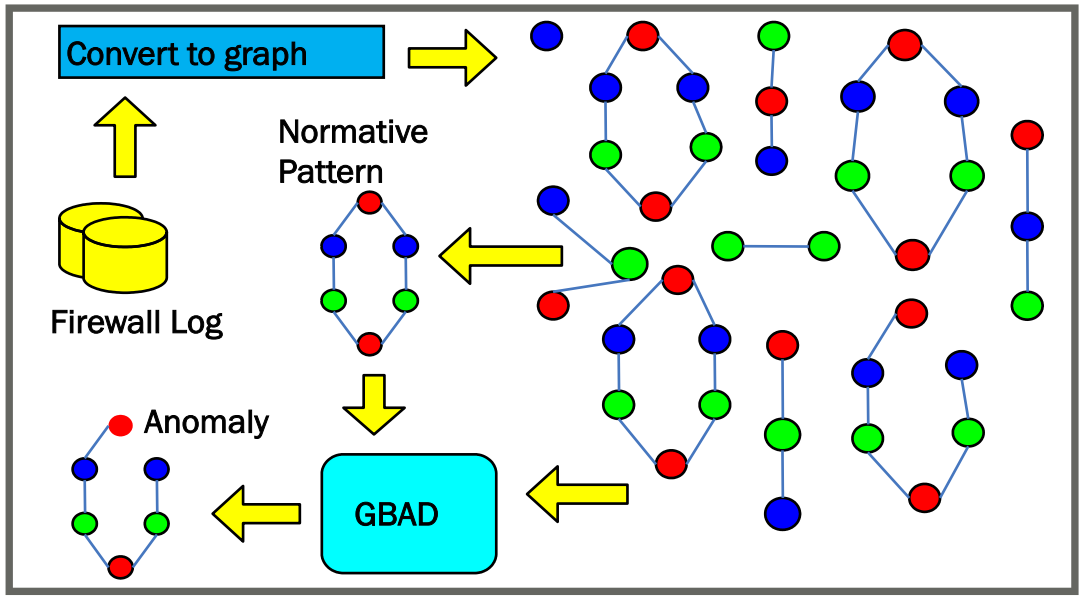
Contribution

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

Graph-Based Anomaly Detection

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

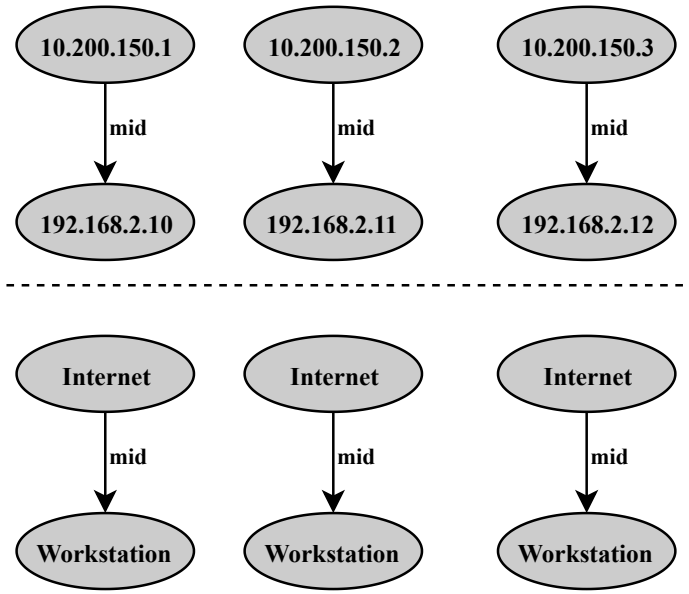




Dataset

- **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 (≈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**

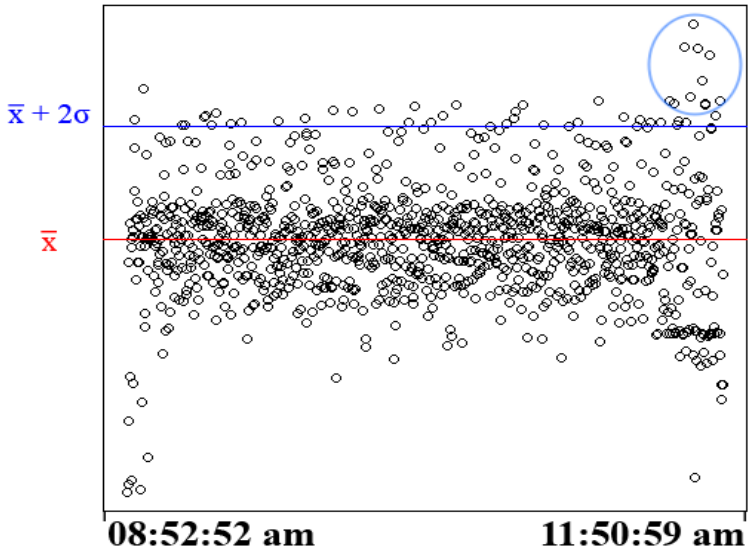


Fig: Number of connection from internet to web server

Single Graph Interval	# of Vertices	# of Edges	# XP/file	# of Graphs		
				Normal	DoS	Total
0 Sec	68,267	59,588	8,478	7,801	677	8,478
1.25 Sec	49,197	45,007	4,629	4,295	344	4,629
2.5 Sec	42,032	39,957	3,201	2,962	239	3,210
5 Sec	33,544	34,543	1,691	1,580	111	1,691
8 Sec	29,607	32,282	1,140	1,066	74	1,140

Table: Graph topology based on time intervals and graph counts

Results

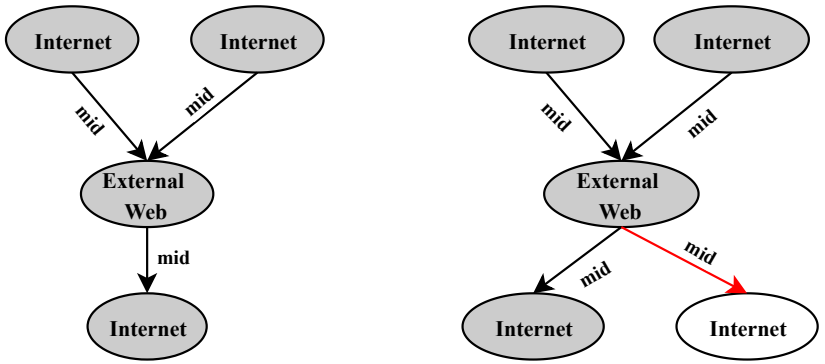


Fig: Normative Pattern I and anomalous addition (extra node and edge)

Graph Interval	Anom. Graph Reported	Attack Source Reported	Detection Delay	Runtime
0 Sec	6.35%	5	31	482
1.25 Sec	4.2%	4	612	289
2.5 Sec	18.4%	3	31	257
5 Sec	**96.4%**	**5**	**23**	**118**
8 Sec	1.35%	0	4	102

Table: Performance of on different graph topology

	Predicted (DoS)	Predicted (Normal)
Actual (DoS)	107 (TP)	4 (FN)
Actual (Normal)	0 (FP)	1580 (TN)

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

Results

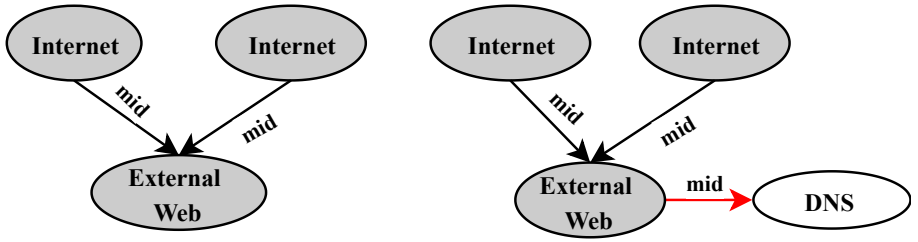


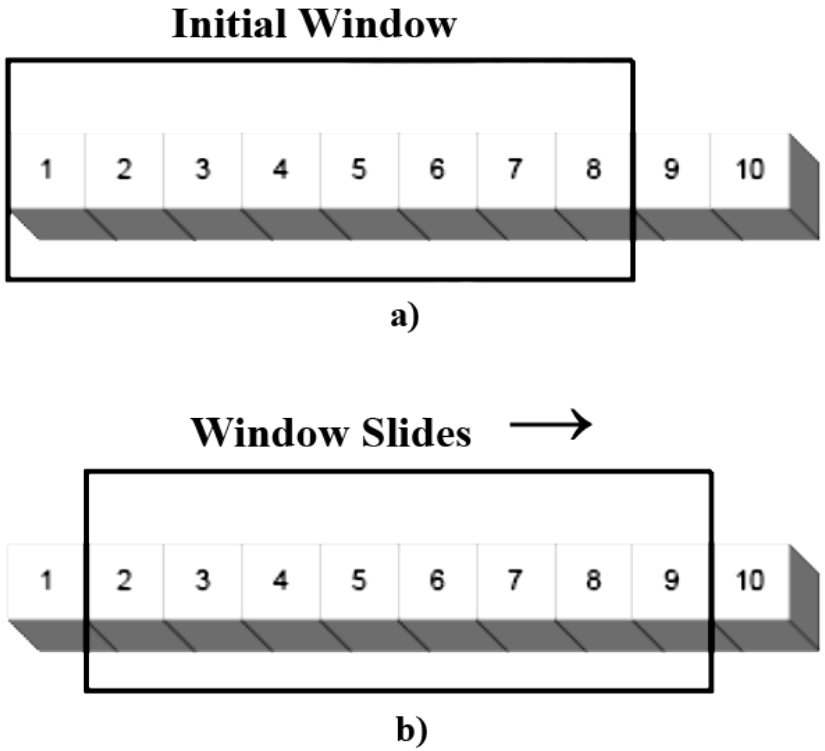
Fig: Normative Pattern II and anomalous addition (extra node and edge)

- 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).

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

[1] G. Carl, G. Kesidis, R. Brooks and S. Rai, "Denial-of-Service Attack Detection Techniques," IEEE Internet Computing, vol. 10, no. 1, pp. 82-89, 2006.

[2] K. Singh and T. De, "Analysis of Application Layer DDoS Attack Detection Parameters Using Statistical Classifiers," Internetworking Indonesia Journal, vol. 9, no. 2, pp. 23-32, 2017.

[3] "A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks," IEEE Communications Letters, vol. 20, no. 4, pp. 700-703, 2016.

[4] N. Weiler, "Honeypot for Distributed Denial of Service Attacks," Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002.

[5] A. Mairh, D. Barik, K. Verma and D. Jena, "Honeypot in Network Security: A Survey," Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 600-605, 2011.

[6] C. Navenna and R. Sasikala, "Analyse Honey Pot Traffics to Detect DoS Attacks Using Support Vector Machine," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 6, pp. 326-329, 2017.

[7] C. Harshaw, R. Bridges, M. Lannacone, J. Reed and J. Goodall, "GraphPrints: Towards a Graph Analytic Method for Network Anomaly Detection," 2016.

[8] B. Miller, L. Stephens and N. Bliss, "GOODNESS-OF-FIT STATISTICS FOR ANOMALY DETECTION IN CHUNG–LU RANDOM," 2012 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 25-30, 2012.

[9] W. Eberle and L. Holder, "Anomaly Detection in Data Represented as Graphs," Intelligent Data Analysis, vol. 11, no. 6, pp. 663-689, 2007.

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

Questions?