Computer Networks and Security Management

-- Visual Analytics, Data Mining and Economic Approaches

CMU CENTRAL MICHIGAN UNIVERSITY

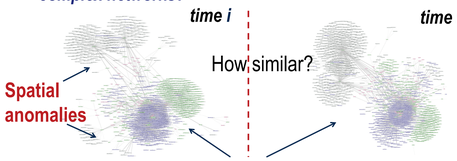
Dr. Qi Liao

Department of Computer Science

College of Science and Technology

A Visualization Approach

➢ *Can we detect spatial and temporal anomalies in complex networks?*

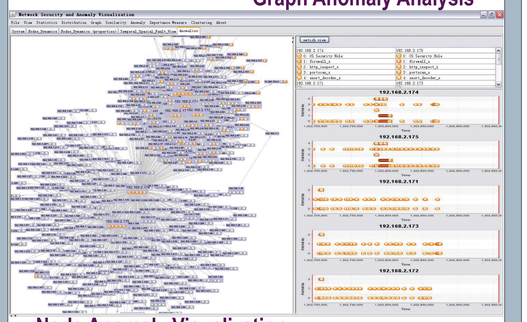


Large-scale networks are complex, typically involving thousands of users and applications, terabytes of data, and millions of connections. How do we know precisely what is going on in our network? If there are intrusions and attacks, can we quickly detect and find who is responsible? Some attacks are noisy and therefore easier to detect, such as port scans and DDoS. What about less obvious intrusions from advanced and persistent attackers? To understand anomalies and their underlying reasons, we need to ask a few key questions:

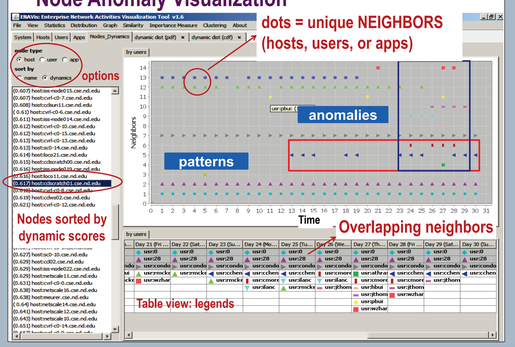
- What are the *changes* between snapshot network graphs?
- What are the *variance* and *invariance*?
- How *similar* (or *different*) are day-to-day network activities?
- What changes are *normal* / *abnormal*?
- How to quantify and visualize the *evolution* of changes?

Our network graph anomaly visual analytic tools and algorithms [1-3] can help network operators gain situation awareness as well as provide a time-efficient alternative to find the causes of problems in network performance diagnosing, troubleshooting and security management.

Graph Anomaly Analysis

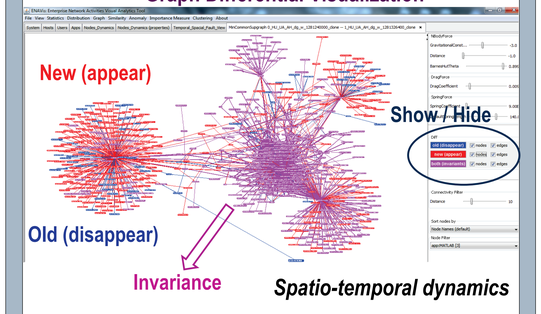


Node Anomaly Visualization



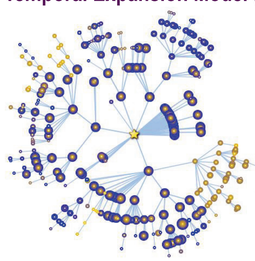
A Visualization Approach

Graph Differential Visualization

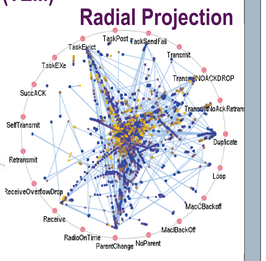


Spatio-temporal dynamics

Temporal Expansion Model (TEM)



Correlation-based Radial Projection



Graph Distances

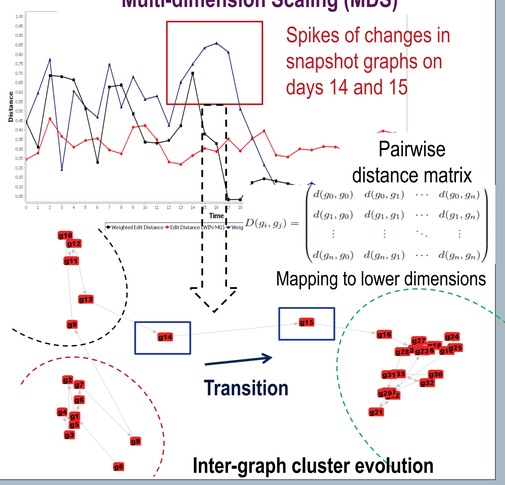
Maximum common subgraphs (MCS) based:

$$d(g_1,g_2) = 1 - \frac{|\,mcs(g_1,g_2)\,|}{\max(|\,g_1\,|,|\,g_2\,|)}$$

Graph edit distance (GED) based:

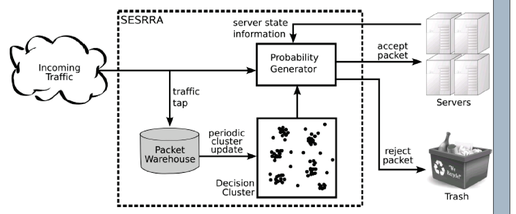
$$d(g_1,g_2) = \frac{|\,g_1\,| + |\,g_2\,| - 2\,|\,mcs(g_1,g_2)\,|}{|\,g_1\,| + |\,g_2\,|}$$

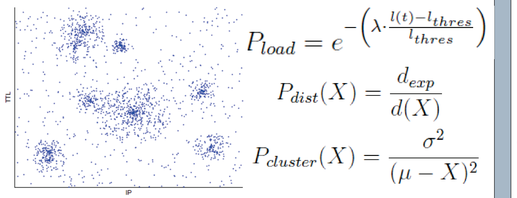
Multi-dimension Scaling (MDS)



A Data Mining Approach

➢ *Can we distinguish which connection requests are from legitimate users?*





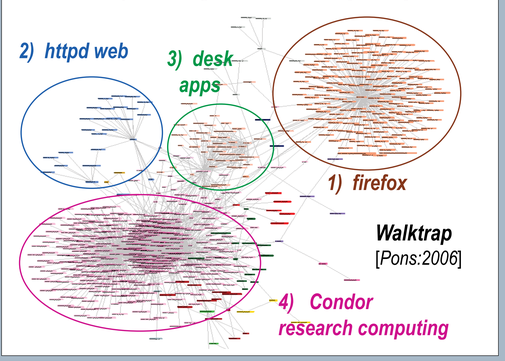
$$P_{load} = e^{-\left(\lambda \cdot \frac{l(t)-l_{thres}}{l_{thres}}\right)}$$

$$P_{dist}(X) = \frac{d_{exp}}{d(X)}$$

$$P_{cluster}(X) = \frac{\sigma^2}{(\mu - X)^2}$$

Distributed Denial of Service (DDoS) attacks originating from botnets can quickly bring normally effective web services to a screeching halt. We propose SESRAA (SElective Short-term Randomized Acceptance Algorithms) [4], an adaptive scheme for maintaining web service despite the presence of multifaceted attacks in a noisy environment. In contrast to existing solutions that rely upon "clean" training data, we presume that a live web service environment makes finding such training data difficult if not impossible. SESRAA functions much like a battlefield surgeon's triage: focusing on quickly and efficiently salvaging good connections with the realization that the chaotic nature of the live environment implicitly limits the accuracy of such detections. SESRAA employs an adaptive *k*-means clustering approach using short-term extraction and limited centroid evolution to defend the legitimate connections in a mixed attack environment. We present the SESRAA approach and evaluate its performance through experimental studies in a diverse attack environment. The results show significant improvements against a wide variety of DDoS configurations and input traffic patterns.

Graph Mining and Community Analysis

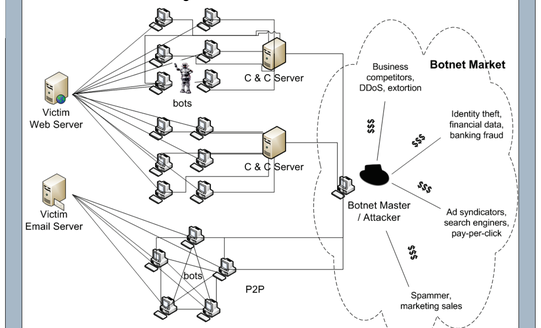


An Economic Approach

➢ *Can we fight botnets with economic uncertainty?*

A **botnet** is a collection of compromised computers (bots) that can do much harms to the health of the Internet. For example, bots can be used for launching distributed denial-of-service attacks (DDoS) against important websites, fraudulent ad clicks, sending spam, stealing credit card numbers and people's identity, etc.

Botnets have become an increasing security concern in today's Internet. Since current technological defenses against botnets have failed to produce results, it has become necessary to think about different strategies.



$$\max_{N^v,k^v} (\text{profit}) = M_1 - c * k^v$$

$$s.t. \quad (1 - p_v)\{V + (N^v - V) * U\} \geq n^e$$

$$k^v \geq \frac{N^v}{q}$$

Given that money is perhaps the single determining force driving the growth in botnet attacks, we propose an interesting economic approach [5] to take away the root cause of botnet, i.e., the financial incentives. We model botnet-related cyber crimes as a result of profit-maximizing decision-making optimization problem from the perspective of botmasters. By introducing the *uncertainty* level created by the *virtual bots*, we make determining the optimal botnet size infeasible for the botnet operators, and consequently the botnet profitability can fall dramatically. The theoretical model we developed has a large potential to fight off botnet-related attacks of varying revenue patterns.

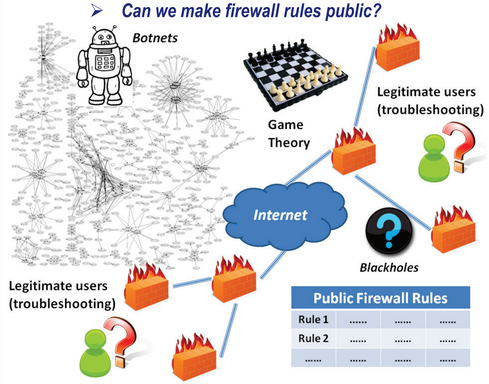
Contact information

Qi Liao, Ph.D.
Pearce Hall 417
Department of Computer Science
Central Michigan University
Mount Pleasant, MI 48859
Tel: (989) 774 4419, Fax: (989) 774 3728
Email: qi.liao@cmich.edu

We want smart students like you to work on our research projects. Visit http://cps.cmich.edu/liao1q for more information.

A Game Theoretical Approach

➢ *Can we make firewall rules public?*



Public Firewall Rules			
Rule 1	.....	.....	.....
Rule 2	.....	.....	.....
.....	.....	.....	.....

Firewalls are among the most important components in network security. Traditionally, the rules of the firewall are kept private under the assumption that privacy of the ruleset makes attacks on the network more difficult. We posit that this assumption is no longer valid in the Internet of today due to two factors: the emergence of botnets reducing probing difficulty and second, the emergence of distributed applications where private rules increase the difficulty of troubleshooting. We argue that the enforcement of the policy is the key, not the secrecy of the policy itself. We demonstrate [6] through the application of game theory that *public* firewall rules when coupled with false information (lying) are actually better than keeping firewall rules private, especially when taken in the larger group context of the Internet. Interesting scenarios arise when honest, public firewalls are socially insured by other lying firewalls and networks adopting public firewalls become mutually beneficial to each other. The equilibrium under multiple-network game is socially optimal because the percentage of required lying firewalls in social optimum is much smaller than the percentage in single-network equilibrium and the chance of attack through firewalls is further reduced to zero.

Publications

[1] Qi Liao, Andrew Blaich, Dirk VanBruggen, and Aaron Striegel. **Managing networks through context: graph visualization and exploration**. *Computer Networks, Special Issue: Managing Emerging Computing Environments*, 54(16):2809-2824, November 15 2010.

[2] Qi Liao, Aaron Striegel, and Nitesh Chawla. **Visualizing graph dynamics and similarity for enterprise network security and management**. In *ACM Proceeding of the 7th International Symposium on Visualization for Cyber Security (VizSec'10)*, pages 34-46, Ottawa, Canada, September 14 2010.

[3] Qi Liao, Andrew Blaich, Aaron Striegel, and Douglas Thain. **ENAVis: Enterprise Network Activities Visualization**. *In Proceedings of the USENIX 22nd Large Installation System Administration Conference (LISA '08)*, San Diego, CA, November 9-14, 2008. **USENIX BEST PAPER AWARD.**

[4] Qi Liao, David A. Cieslak, Aaron D. Striegel, Nitesh V. Chawla. **Using Selective, Short-Term Memory to Improve Resilience versus DDoS Exhaustion Attacks.** *Journal of Security and Communication Networks*, Volume 1, Issue 4, Wiley InterScience, page 287-299, July/August 2008, doi: 10.1002/sec.22.

[5] Zhen Li, Qi Liao, Andrew Blaich, and Aaron Striegel. **Fighting Botnets with Economic Uncertainty.** *Journal of Security and Communication Networks*, Volume 4, Wiley InterScience, page 1104-1113, 2011, doi: 10.1002/sec.235.

[6] Qi Liao, Zhen Li, and Aaron Striegel. **Information Game of Public Firewall Rules.** The *Fifth Workshop on Secure Network Protocols (NPSEC '09) in conjunction with the 17th IEEE International Conference on Network Protocols (ICNP '09)*, Princeton, NJ, October 13-16, 2009, doi: 10.1109/NPSEC.2009.5342253.