Anomaly Detection in Multilayer Networks

PIs: Rebecca Wright, Lazaros Gallos, and Nina Fefferman

International collaboration with the group of S. Havlin (Bar-Ilan University) funded by BSF in Israel

http://dimacs.rutgers.edu/~lgallos/SaTC_AnomalyDetection

Securing Cyberspace by Distributed Multilayer-Network Surveillance

Cascading anomalies within and across networks can compromise entire systems.

Early detection is the key to prevention/mitigation.

Anomalies in networks can take many forms.

In multilayer networks, the challenge increases because benign changes within single networks can act synergistically to compromise multilayer network function.

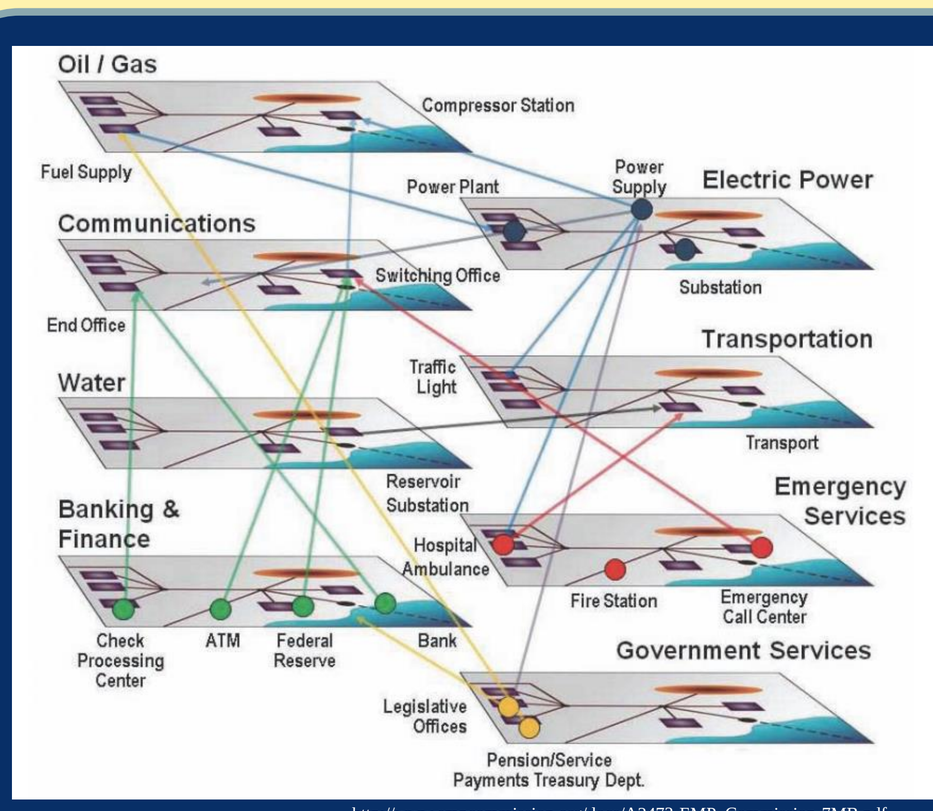
Extensive analysis shows that multilayer networks are conceptually very different than an aggregate of single networks, due to emergent phenomena.

Effective surveillance must be able to protect individual layers and whole systems.

A compromised node in Electrical Grid may impact function at multiple nodes in other networks (e.g. as Transportation, or Communications)

Each of these affected networks will then affect yet other networks (e.g. changes to Communications may affect Emergency Services)

(see Figure 1)



http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

Figure 1: A conceptual illustration of inter-dependence networks in critical infrastructure.

Approach

Extending Recent Advances for Anomaly Detection in Single Networks

- Recent methods for anomaly detection in single networks have proved fruitful, including the *Distributed Intrusion/Anomaly Monitoring for Nonparametric Detection* (DIAMoND) algorithm [M. Korczynski et al., ICCCN'15]
- We are working to adapt DIAMoND for use in multilayer networks
- We are developing a mathematical model and an algorithmic framework to combine cyber-security and network science results towards a rigorous understanding of multilayer functions.

The Theory Behind DIAMoND:

DIAMoND leverages non-parametric information from participating surveillance neighbors to update dynamic detection thresholds

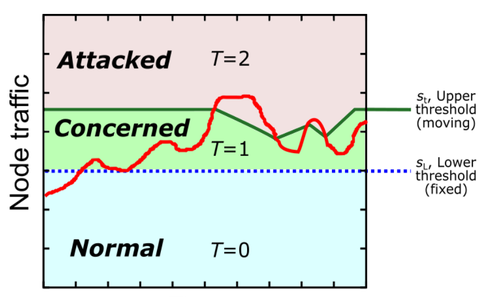


Figure 3: Coordination network-dependent dynamic surveillance threshold updates for each node

Reproduced from Korczynski et al. IEEE Com Mag 2016

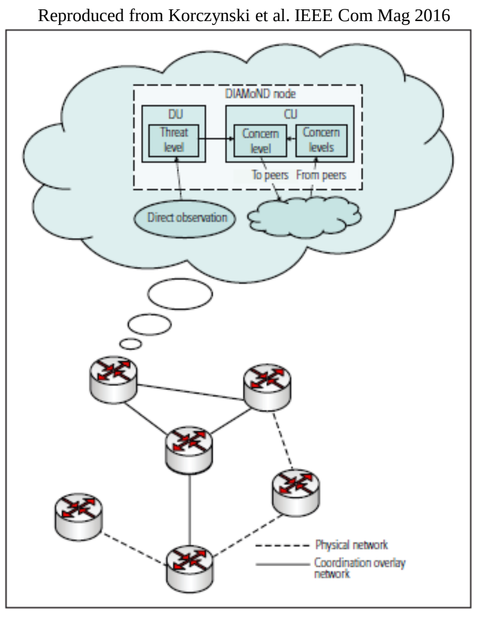


Figure 2: DIAMoND architecture in a single network

The challenge is to tailor this algorithm for multilayer networks!

Challenges Unique to Multilayer Networks

- Communication across layers may differ in nature/capacity
- Different connectivity patterns may alter which nodes are reachable
- Some threats/failures in one layer may not be able to propagate to other layers
- Trust among surveillance nodes can differ across layers
- Typical network traffic may be layer specific, so strong signals in one layer may be lost in noise in another
- An adversary may have layer-dependent ability to disrupt the detection mechanism itself

Interested in meeting the PIs? Attach post-it note below!

NSF 2017 Secure and Trustworthy Cyberspace Principal Investigators' Meeting
Jan. 9-11, 2017
Arlington, VA

National Science Foundation
WHERE DISCOVERIES BEGIN

RUTGERS THE UNIVERSITY OF TENNESSEE KNOXVILLE