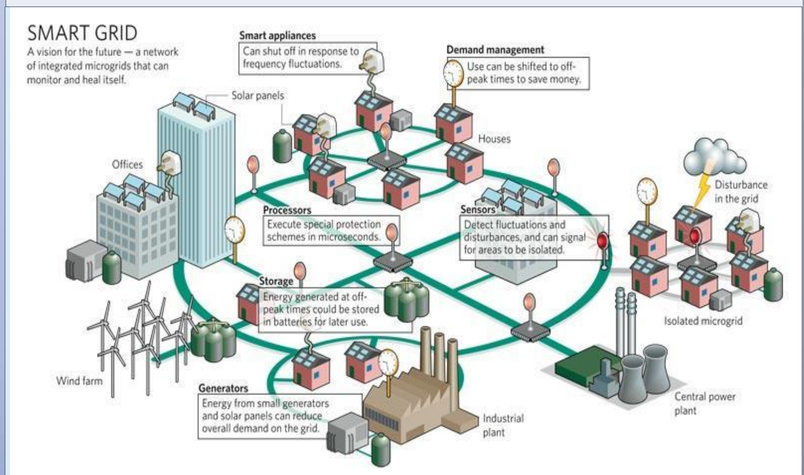
A Game-Theoretic Approach to Modeling Attacks and Defenses of Smart Grids

Giovanni Madejski[a], Xiaojun Shan[a], Jun Zhuang[a], Nageswara S. V. Rao[b]

a. Department of Industrial and Systems Engineering b. Oak Ridge National Laboratory

Abstract

As optimization, user capabilities, and data-taking abilities are incorporated into the power grid, the next generation power grid, or smart grid faces the new risk of cyber threats. With the current electrical grid, physical access is required to cause damage, while with the smart grid it will be possible for users to remotely attack and severely damage the grid. We propose the use of a game-theoretic model to model three-levels of defenses and attacks (Power Plants, Utility Companies, and Home Networks) in smart grid network security. To our knowledge, such an approach to smart grid network security has never been taken, our paper fills this gap by characterizing both the defender's and attacker's best response functions and the corresponding Nash equilibrium. We find that the defender's best response is not only a function of direct attacks but of the spread from connected networks. Sensitivity analysis of the equilibrium shows that when success probability of an attack against power plants reaches a certain threshold the defender increases defending efforts for power plants. In contrast, the attack effort at all network levels is not a function of this probability.



Smart Grid Diagram [3]

Network Topology

- Smart Grid is large complex network, Figure 1 shows a network schematic highlighting essential components [1]
- Power is generated at power plants (Grandfather network) then transmitted to Utility companies (Father Network) and then finally arrives at the Home network (Child Network).
- Advanced Metering Infrastructure (AMI) is the underlying structure of the smart grid, the function of which is to monitor real time power usage. This allows power generation and transmission to to be controlled based on real-time demand.
- Alternative energy sources such as solar panels, personal generators, and plug-in electric cars help curb peak-time demand.

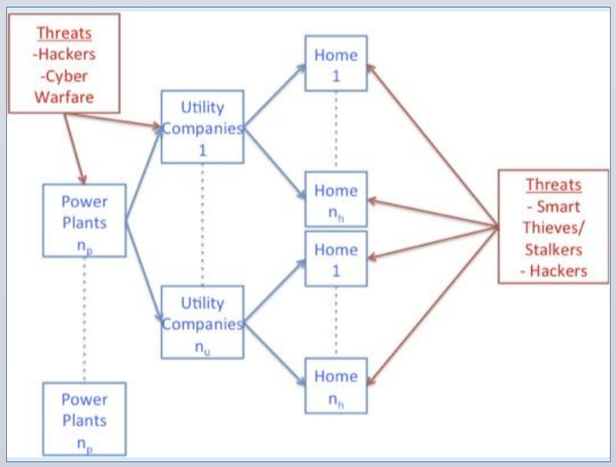


Figure 1 Network Schematic

Notation

a_k=0, 1,…, n_k - *Number of nodes in network of type k attacked*

d_k=0,1,…,n_k - *Number of nodes in network of type k defended*

P_k (a_k,d_k) - *Probability of Network of type k operating*

$I_{(ak>dk)}$ -Indicator function that attacks outweigh defenses at network of type k

U_D - *Defender's Utility function*

U_A - *Attacker's Utility function*

k= {p,u,h}-where k represents network type of {Power Plant, Utility company, Home Network}

n_k - Number of nodes in network of type k

m_k - Minimum number of nodes for network of type k to operate

s_k - Number of successful attacks against node of type k

p_k - Probability of successful attack against node of type k

V_k - Defender loss from successful attack against node of type k

v_k - Attacker gain from successful attack against node of type k

g_{kj} - Probability of spread of damage from network of type k to lower network j

C_k , c_k - Cost to defend or attack a node of type k

The Model

We characterize the defender's objective as follows

$$max\ P_pV_p\text{-}I_{ap>dp}g_{pu}V_u\text{+}P_uV_u\text{-}I_{au>du}g_{uh}V_h\text{+}P_hV_h\text{-}C_pd_p\text{-}C_ud_u\text{-}C_hd_h$$

- The defender's objective is to maximize the operating probability of the networks, while simultaneously minimizing the spread of damage and cost of defending the networks by deciding which nodes to protect

We characterize the attacker's objective as follows

$$max\ (1\text{-}Pp)vp\text{+}I_{ap>dp}g_{pu}v_u\text{+}(1\text{-}P_u)v_u\text{+}\ I_{au>du}g_{uh}v_h\text{+}(1\text{-}P_h)v_h\text{-}c_pa_p\text{-}c_ua_u\text{-}c_ha_h$$

- The attacker's objective is to maximize the failure probability of the different networks and the spread of failure, while minimizing the cost of attacks by deciding which nodes to attack

Illustrations

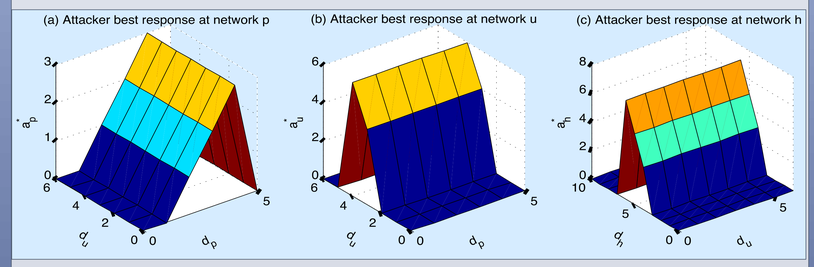


Figure 2 Attacker's Best Response

- Figures 2 (a)-(c) show the attacker's best responses at the network fronts of power plants, utility companies, and homes respectively.
- Figure 2(a) shows that the attacker's best response for attacking a power plant does not depend on the defense at the network of utility companies. This is intuitive since we assume the spread of damage is one directional.
- Figure 2(b) shows that the best-response function of the attacker completely depends on the defense of the intended target network of the attack. This would seem to imply that the spread of damage from parent networks does not affect the attacker choice.
- Figure 2 appears to imply that it is in the best interest of the attacker to directly attack their intended target and not to rely on spread to damage the connected network.

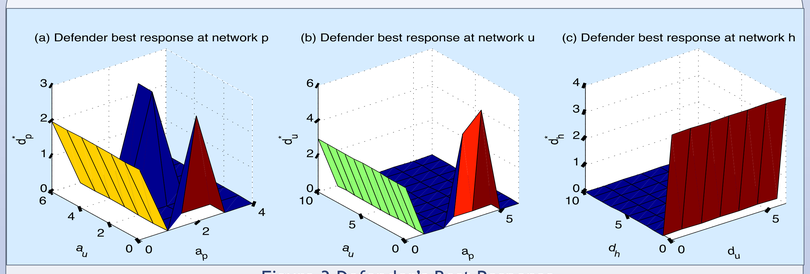


Figure 3 Defender's Best Response

- It appears that the defender's best response does depend on spread unlike the attacker. This is evident from the interdependent relationships illustrated in the power plant and utility company diagrams and missing from the home network as shown in Figure 3(a), (b), and (c), respectively.
- Since our model only considers one directional spread of damage, attacks on a single home cause negligible amount of damage to the smart grid. Therefore it is in the best interest of the defender to concentrate resources on utility companies and power plants, where the potential for greater damage is much higher.

Conclusions

- This research formulates for the first time a game-theoretic approach to modeling smart grid network interactions
- From the numerical illustrations we find that attacker's best response is not affected by the interdependent nature of the network, they should directly attack their target
- The defender's response is dictated by the interdependent relationships requiring them to spend resources at all three levels of interactions

Future Research Directions

There is a number of interesting future research directions.

- In the future, we plan to incorporate another parameter indicating the effectiveness of defense, which varies from 0 to 1
- In the current model, it appears that indirect attacks counting on spread are not complete; this result was rather counter-intuitive and requires further exploration.
- One way to do so is to consider continuous levels of attack and defense, which would generate an alternative and more complex optimization problem for both the defender and the attacker.
- Another is to allow decentralized defense so that the defender for power plant network and utility and the defender for homeowners are separate decision-makers. As a result, we would have three players in the strategic defender-attacker game.

References

[1] Sorebo, G., and Michael C. Echols. Smart Grid Security: An End-to-end View of Security in the New Electrical Grid. Boca Raton FL: CRC, 2012.

[2] Flick, Tony, Morehouse. Securing the Smart Grid: Next Generation Power Grid Security. Amsterdam: Syngress, 2011.

[3] http://blog.cas.suffolk.edu/shanettah/files/2012/02/smartgrid2.jpg Accessed March 2013

Acknowledgements

This work was funded by the Mathematics of Complex, Distributed, Interconnected Systems Program, Office of Advanced Computing Research, U.S. Department of Energy, and was performed in part at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725. This research was also partially supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under award number 2010-ST-061-RE0001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security, or CREATE.