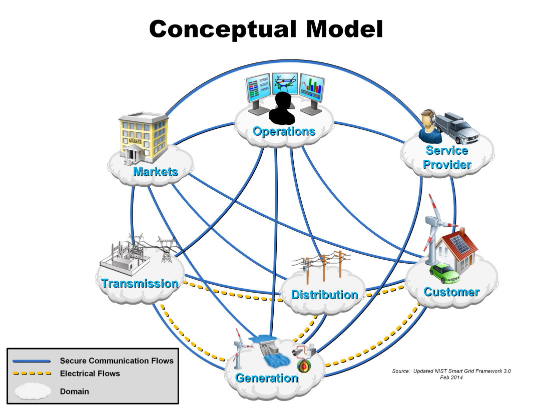
Honeypot Type Selection Games for Smart Grid Networks

Nadia Boumkhled, Sakshyam Panda, Stefan Rass, and Emmanouil Panaousis

29 Oct. 2019

Surrey Centre for Cyber Security
Department of Computer Science
University of Surrey, UK

Challenges in Protecting Smart Grids



NIST conceptual model of Smart Grid

Major Threats

- Physical attacks
- Cyber attacks
- Natural disasters

Motivation

Use of decoy systems

Source: https://earlyadopter.com/2018/06/13/active-defense-how-deception-has-changed-cybersecurity/

Common cyber decoy technique

Honeypots

Need to design appealing and believable decoy systems

Research Question

We investigate the defender's challenge in **choosing a type of system to install** with a

- security budget
- each type having some efficacy to deceive the adversary.

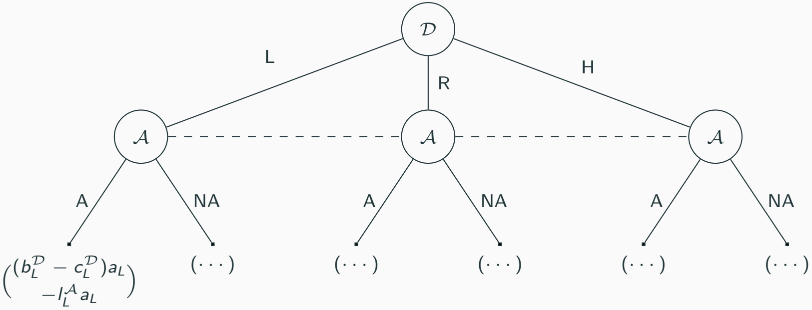
contribution

Efficacy parameter represents

the probability of a system to be recognised as a real system.

The analysis has been performed using this additional characteristic of the system.

Model



- $0 < a_L < 1 \longrightarrow$ efficacy of type-L system

Solution Space

	$\mathcal{U}^{\mathcal{D}}(L, NA) < \mathcal{U}^{\mathcal{D}}(H, NA)$	$\mathcal{U}^{\mathcal{D}}(L, NA) \geq \mathcal{U}^{\mathcal{D}}(H, NA)$
$\mathcal{U}^{\mathcal{D}}(L, A) \leq \mathcal{U}^{\mathcal{D}}(H, A)$	$(H, A;\ p_2 \geq \overline{p_2})$ $(R, NA;\ p_2 < \overline{p_2})$	$(L, A;\ p_1 \geq \overline{p_1})$ $(R, NA;\ p_1 < \overline{p_1})$ $(H, A;\ p_2 \geq \overline{p_2})$ $(R, NA;\ p_2 < \overline{p_2})$
$\mathcal{U}^{\mathcal{D}}(L, A) > \mathcal{U}^{\mathcal{D}}(H, A)$	$(L, A;\ p_1 \geq \overline{p_1})$ $(R, NA;\ p_1 < \overline{p_1})$ $(H, A;\ p_2 \geq \overline{p_2})$ $(R, NA;\ p_2 < \overline{p_2})$	$(L, A;\ p_1 \geq \overline{p_1})$ $(R, NA;\ p_1 < \overline{p_1})$

where $\overline{p_1} = \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$ and $\overline{p_2} = \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A} \longrightarrow \mathcal{A}$'s beliefs.

Remarks and Outlook

- GT gives better payoff than randomly choosing system type to deploy
- Our first step towards implementing game-theoretic strategies in smart grid networks as part of the H2020 SPEAR project.
- Various extensions are possible:
    i repeated game model with belief update scheme
    ii model with sophisticated attacker (e.g, with anti-honeypot techniques Wang et al. [2017]).

Thank you for your kind attention

Questions?

References

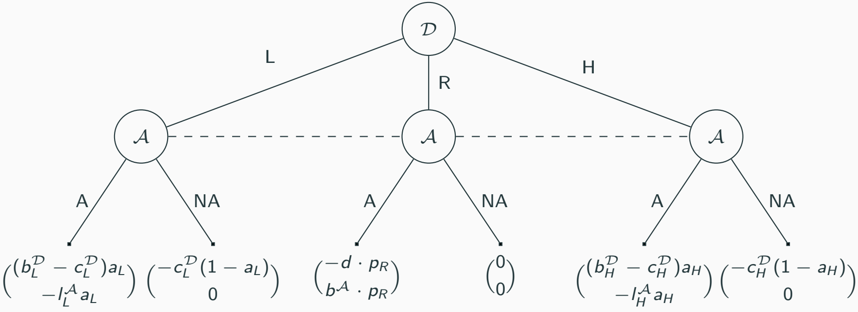
Thomas E Carroll and Daniel Grosu. A game theoretic investigation of deception in network security. *Security and Communication Networks*, 4(10):1162–1172, 2011.

Hongxia Li, Xiaoqiong Yang, and Lianhua Qu. On the offense and defense game in the network honeypot. In *Advances in Automation and Robotics, Vol. 2*, pages 239–246. Springer, 2011.

Jeffrey Pawlick and Quanyan Zhu. Deception by design: evidence-based signaling games for network defense. *arXiv preprint arXiv:1503.05458*, 2015.

Kun Wang, Miao Du, Sabita Maharjan, and Yanfei Sun. Strategic honeypot game model for distributed denial of service attacks in the smart grid. *IEEE Transactions on Smart Grid*, 8(5):2474–2482, 2017.

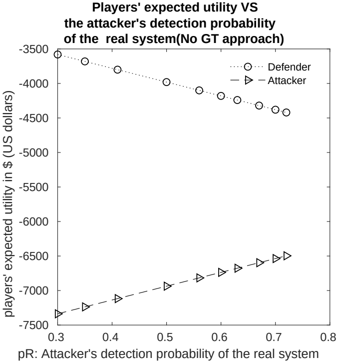
Model

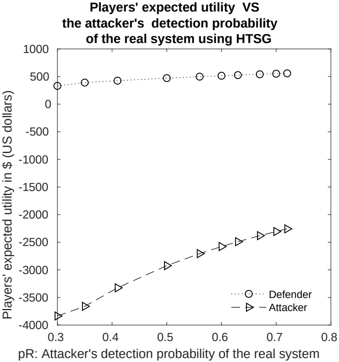

$\mathcal{D}$
L
R
H
$\mathcal{A}$
$\mathcal{A}$
$\mathcal{A}$
A
NA
A
NA
A
NA
$\binom{(b_L^{\mathcal{D}} - c_L^{\mathcal{D}})a_L}{-l_L^{\mathcal{A}} a_L}$
$\binom{-c_L^{\mathcal{D}}(1 - a_L)}{0}$
$\binom{-d \cdot p_R}{b^{\mathcal{A}} \cdot p_R}$
$\binom{0}{0}$
$\binom{(b_H^{\mathcal{D}} - c_H^{\mathcal{D}})a_H}{-l_H^{\mathcal{A}} a_H}$
$\binom{-c_H^{\mathcal{D}}(1 - a_H)}{0}$

Symbols

Symbols	Condition/Range	Description
a_H	$0 < a_H < 1$	Efficacy of type-H system
a_L	$0 < a_L < a_H$	Efficacy of type-L system
$b^{\mathcal{A}}$	$b^{\mathcal{A}} > 0$	Attacker's benefit on attacking type-R system
$b_H^{\mathcal{D}}$	$b_H^{\mathcal{D}} \geq c_H^{\mathcal{D}}$	Defender's benefit when type-H system attacked
$b_L^{\mathcal{D}}$	$c_L^{\mathcal{D}} \leq b_L^{\mathcal{D}} < b_H^{\mathcal{D}}$	Defender's benefit when type-L system attacked
$c_H^{\mathcal{D}}$	$c_H^{\mathcal{D}} > 0$	Cost of running type-H system
$c_L^{\mathcal{D}}$	$0 < c_L^{\mathcal{D}} < c_H^{\mathcal{D}}$	Cost of running type-L system
d	$d > b_H^{\mathcal{D}}$	Defender's loss when type-R system attacked
$l_H^{\mathcal{A}}$	$l_H^{\mathcal{A}} > 0$	Attacker's loss on attacking type-H system
$l_L^{\mathcal{A}}$	$0 < l_L^{\mathcal{A}} < l_H^{\mathcal{A}}$	Attacker's loss on attacking type-L system
p_R	$0 < p_R \leq 1$	Efficacy of type-R system

Results





Players' expected utility for different attacker's detection capability.

Motivation from Literature

- The game motivated from *Carroll and Grosu [2011]* and *Pawlick and Zhu [2015]* with refined strategies to include type-H, type-L and type-R system, rather than just honeypot and normal system.
- The types of parameter have been inspired from Li et al. [2011].