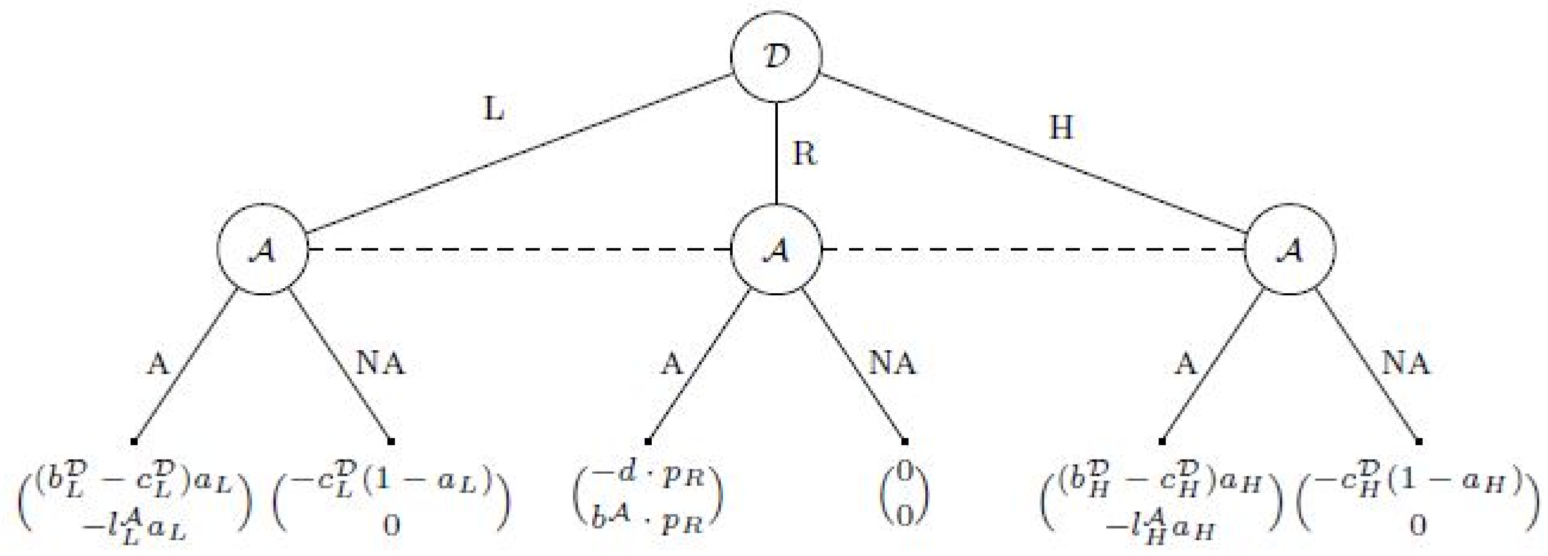
HONEYPOT TYPE SELECTION GAMES FOR SMART GRID NETWORKS

Nadia Boumkhled[1], Sakshyam Panda[1], Stefan Rass[2], Emmanouil Panaousis[3]

[1] University of Surrey [2] Universität Klagenfurt [3] University of Greenwich

The Model



- Single-shot Bayesian game with complete but imperfect information.
- Defender decides to install a system with high-interaction honeypot (H), or low-interaction honeypot (L), or no honeypot (R); with each having its costs and benefits.
- Attacker deciding whether to attack a target in the presence of information asymmetry.
- motivated from [1] and [3] $\longrightarrow$ refined strategies to include L, H and R rather than just honeypot and normal system.

Novelty

L, H and R has efficacy ($a_L < a_H < p_R$) which reflects a system's ***probability of being recognised as a real system*** during reconnaissance.

Assumptions and Payoffs

- type-L and type-H systems have additional costs and benefits to type-R system.
- The aggregated cost includes the deployment, maintenance and operational costs of having a honeypot in the network.
- type-H system $\longrightarrow$ higher threat intelligence but expensive.
- Attacker, similar to the defender, has loss and benefits ($b^{\mathcal{A}} > -l_L^{\mathcal{A}} > -l_H^{\mathcal{A}}$) based on her choice of action.

List of symbols

Symbols	Condition/Range	Description
$b^{\mathcal{A}}$	$b^{\mathcal{A}} > 0$	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

Solution: Bayesian Equilibria

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

where $\overline{p_1} = \frac{a_L \cdot l_L^A}{p_R \cdot b^A + a_L \cdot l_L^A}$ and $\overline{p_2} = \frac{a_H \cdot l_H^A}{p_R \cdot b^A + a_H \cdot l_H^A}$

Remarks and Outlook

- Game-theoretic approach gives better payoff than randomly choosing system type to implement.
- Our first step towards implementing game-theoretic strategies in smart grid networks as a part of the **H2020 SPEAR project**.
- [2] considers a *decoy parameter* for honeypots which could be *conceived as the efficacy* for each type of system in our model.
- Various extensions are possible:
  - repeated game model with belief update schemes,
  - model with sophisticated attacker (e.g, with anti-honeypot techniques [4]).

References

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

[2] Yang Li, Leyi Shi, and Haijie Feng. A game-theoretic analysis for distributed honeypots. *Future Internet*, 11(3):65, 2019.

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

[4] 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.