Attacker-Defender Investment Strategies in Cybersecurity

Columbia University
Data Science Institute

Austin Ebel, Debasis Mitra
Department of Electrical Engineering | Columbia University

1. Motivation

Malicious cyber activity cost the US economy between $57 and $109 billion in 2016. Consequently, there has been considerable investments and research on cybersecurity, especially in technical defenses (encryption, intrusion detection, etc.). Yet there remains a significant need to better understand how firms should allocate these investments.

Our contributions are *two-fold*:

- Generalize from a one-shot optimal investment allocation for cyber defense to an iterative framework between attackers and defenders.
- Extend existing models[1,2] of optimal investments to protection of multiple assets in more realistic network structures..

2. Gordon & Loeb Model

- Defines a *security breach probability function,* $\boldsymbol{S_D(z,v)}$, indicating how investments in information security, z, can decrease the vulnerability of the information, v.
- Optimal investments depend on the information's **value.**

$$z_D^* = \arg\min_{z\geq 0} \quad L\cdot S_D(z,v)+z \qquad (1)$$

- Shows that optimal investments may not always increase with increasing vulnerability.
- Provides guidelines for firms investing in information security to avoid paying more than ~37% of the information's expected loss.

3. Generalization to Networks

How might we extend the Gordon & Loeb model to account for multiple vulnerabilities and assets?

- *Represent network as a directed acyclic graph defining entry, intermediate, and leaf nodes.*

Let $\mathcal{R}$ be the set of all paths from entry node to leaf, and $\mathcal{E}$ be the set of all edges in the graph. For $r\in\mathcal{R}$ and $e\in\mathcal{E}$:

- $L^{(r)}$ is the loss associated with the leaf node in path r.
- $S^{(r)}(\boldsymbol{z},\boldsymbol{v})$ defines how investments along path r decrease its vulnerability.
- p_e is the probability of taking edge e at a node.

$$\begin{aligned}\min_{\mathbf{z}} \quad & u \\ \text{subject to} \quad & L^{(r)}\cdot S^{(r)}(\mathbf{z},\mathbf{v})\leq u \quad r\in R \\ & \mathbf{1}\cdot\mathbf{z}=I_{MAX} \\ & \mathbf{z}\succeq 0\end{aligned}$$

$$S^{(r)}(\mathbf{z},\mathbf{v})=\prod_{e\in r} p_e\cdot S_e(z_e,v_e)$$

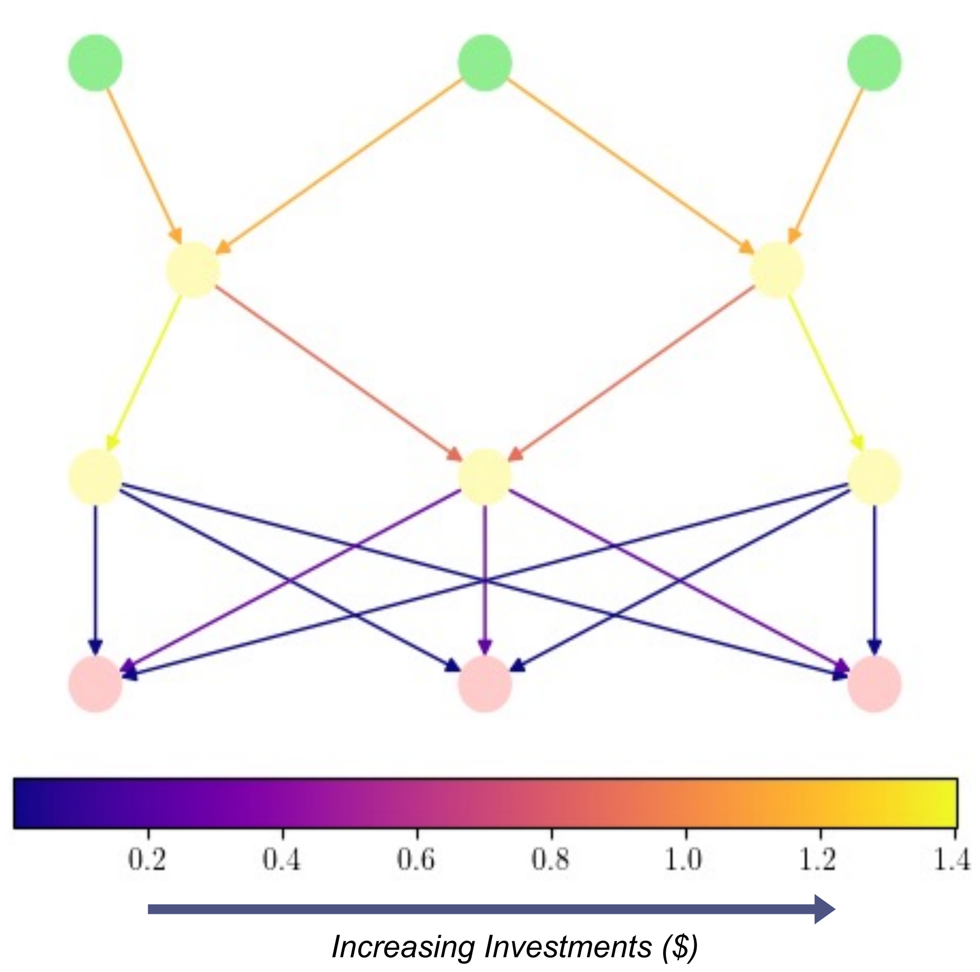

Figure 1: *Optimal network investments. Entry nodes in green, leaf nodes in red.*

4. Attacker-Defender Model & Results

- Allow attackers to invest in *increasing* breach likelihood.
  - $S_D(z,v)$ vs. $S_A(z,v)$

$$z_A^* = \arg\max_{z\geq 0} \quad G\cdot S_A(z,v)-z \qquad (2)$$

- Attackers and defenders allocate $T_A\leq G$ and $T_D\leq L$ respectively and alternate investing a fraction of their remaining funds $R_{A,i}$, and $R_{D,i}$ at iteration i.
- Define MDP $\mathcal{M}=(S,A,P,R,\gamma)$ to find an optimal policy $\pi_*(s|a)$ that exploits rational attacker investments and minimizes breach likelihood across the iterative process.
- Deep reinforcement learning required.

Iterative Process:

- For $i=1,2,3$ ...

$$v_{D,i}=S_D(z_{D,i}^*,v_{A,i-1})$$
$$v_{A,i}=S_A(z_{A,i}^*,v_{D,i})$$

- Where $z_{D,i}^*\leftarrow\pi_*(a|s)$ is the optimal defender investment given state s, and $z_{A,i}^*$ is the rational attacker investment that results from solving *Eq. (2)* for $z\in[0,R_{A,i}]$.
- We then update the remaining funds for each party as:

$$R_{D,i+1}=R_{D,i}-z_{D,i}^*$$
$$R_{A,i+1}=R_{A,i}-z_{A,i}^*$$

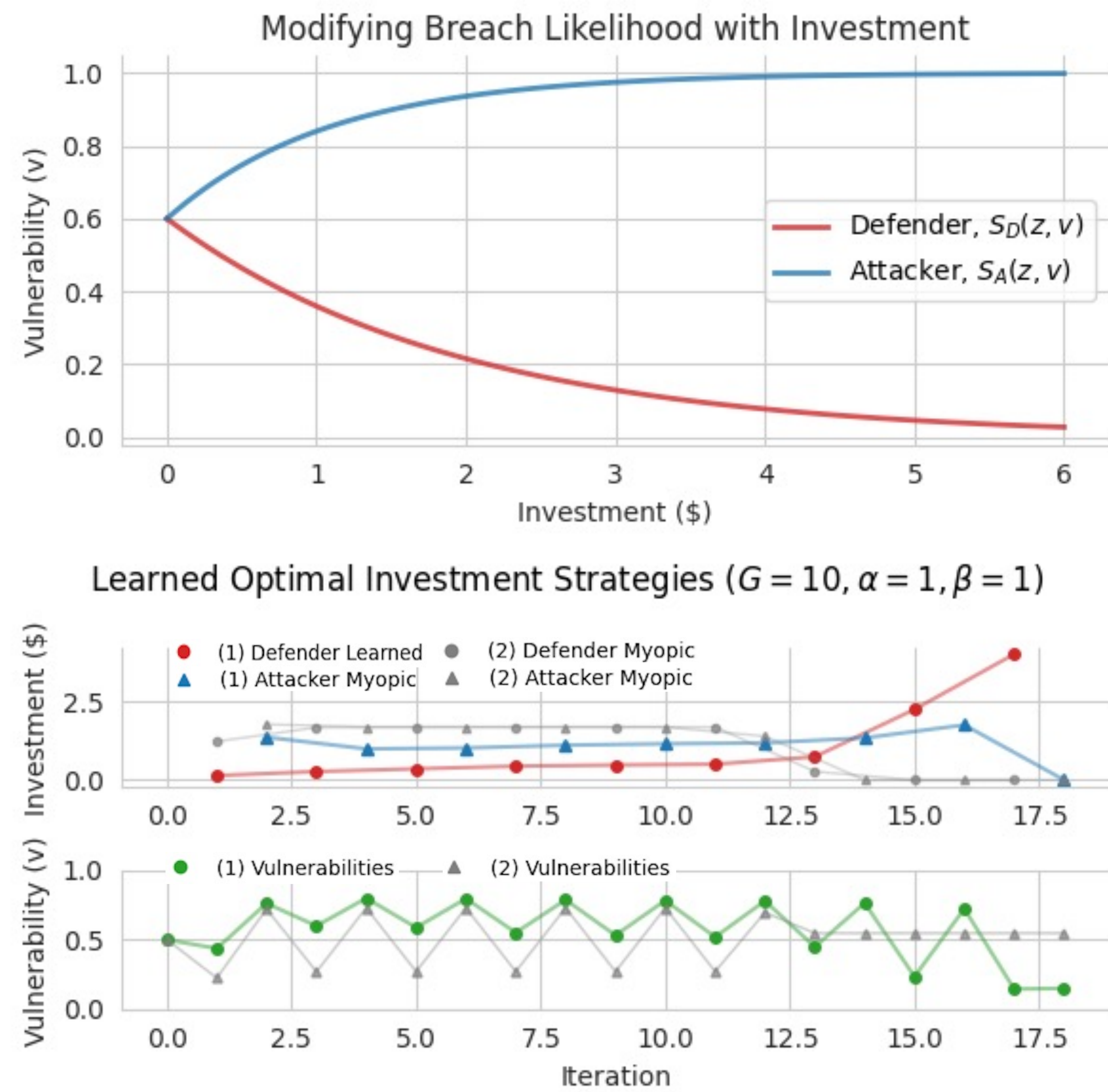

Figure 2: *Optimal Investments and Vulnerabilities*

5. Further Work

- *Multi-Agent Reinforcement Learning* – Can we train an intelligent *attacker* to increase the robustness and generalizability of our defender model?
- *Imperfect Information* – In practice, defenders may not have perfect knowledge of attacker investment allocations and strategies.
- *Generalizations of the Attacker-Defender model to networks* – Just as we have generalized the Gordon & Loeb model, is it possible to extend our attacker-defender model to interactions and strategies in arbitrarily large networks?

6. Acknowledgements

We thank Vladimir Marbukh (NIST) for his insights and the benefit of discussions. DM acknowledges the support of NIST.

7. References

1. Lawrence A. Gordon and Martin P. Loeb (2002) "The economics of information security investment.", ACM Trans. Inf. Syst. Secur. 5, 4 (November 2002), 438–457.
2. Y. Liu and H. Man, "Network Vulnerability Assessment Using Bayesian Networks," Proc. SPIE, vol. 5812, pp. 61-71, 2005.