Is game theory a viable tool when fighting against threat actors in cybersecurity

Andrei-Ioan Ianău
University of Medicine, Pharmacology, Sciences and Technology “George Emil Palade”
from Târgu Mureș

Research Methodology

Instructor: Sándor Miklós Szilágyi

Date: 08.12.2022

Abstract

In answering the question of this literature review, my scope will be to determine the usefulness of game theory models in the decision making process regarding the cyber security space. To asses if the models may be fit to be used in different contexts, we must look into the economic side, risk taking and risk management side and also on the general client needs. As theory may sometimes not correspond with the practices found in the domain, the question is as hard to answer as fast-paced and dynamic the cyber security domain is. We find that some models are capable of some usages in the real world regarding general cybersecurity practices and there are papers that lay the taxonomy and ground work for future studies.

Keywords: game theory, cybersecurity

Discussion

In (Pawlick et al., n.d., 3) the authors present the current options regarding cybersecurity and their limitations and come up with a taxonomy of deception.

Firewalls, cryptography, and role-based access control, although essential components of any security strategy, are unable to fully address these new cybersecurity and privacy threats. Adversaries often gain undetected, insider access to network systems.

Perturbation in privacy and security

The first set of papers study the privacy that is obtained by perturbing sensitive data. (Chessa et al., 2015) model the interaction between a set of users who contribute data in order to identify mechanisms by which the learning agent can improve the quality of its estimation. The users have two options: wether to contribute at all, and the level of details to be contributed as information. There is a trade-off between privacy and the benefit of contributing to data analysis, although, this trade-off is hardly quantifiable on the economic side. The findings in this paper show that the users will gain more information if they choose to contribute a greater amount of details,

In their paper, (Alvim et al., 2017) study information privacy within the framework of information theory. They develop a model of information transmission and leakage using quantitative information flow. The sender has a secret, which the defender only knows with some prior probability. The sender transmits the secret through a channel, which leaks some information to the adversary. Using this information, the adversary forms an a posteriori belief about the secret. The posterior vulnerability of the secret is a measure of the adversary's knowledge, which can be quantified using the entropy of the posterior distributions or a general convex function. Alvim et al. observe that the expected utility becomes convex rather than linear in the mixed-strategy probabilities, which leads them to call the game an information leakage game. This formulation connects to the many tools available in information theory.

In their paper, (Theodorakopoulos et al., 2014) address the issue of privacy for location-based services (LBS). They argue that human locations do not occur at discrete spatial-temporal points but instead follow a trajectory. To protect the privacy of past, present, and future locations, as well as transitions between locations and locations between LBS queries, they propose user-centric location privacy preserving mechanisms (LPPMs) that send LBS pseudolocations. As the leader in a Bayesian Stackelberg game, the LPPM strategically sends a perturbed pseudolocation to the LBS to protect the user's exact real location. The privacy provided by the LPPM is measured by the error with which an adversary can deduce the real location of the target, and the quality is determined by how much the altered location data from the LPPM affects the functionality of the LBS. The authors evaluate their LPPM using mobility traces for taxi cabs in the San Francisco Bay area.

In (Feng et al., 2017), the authors study the use of moving target defense, a strategy where a defender of a network asset changes the security configuration of the system

periodically, to protect against an attacker. The authors model the interaction between the attacker and defender as a Stackelberg game, in which the defender chooses a defense strategy, and the attacker then chooses an attack. The authors use a Markov decision process to represent the security configurations of the system, and show that the problem can be expressed as a minimization problem. They propose an algorithm with $O(|V|^2 log|V|)$ complexity, where $|V|$ is the number of valid states, to solve this problem. The paper highlights that the defender's cost can be reduced more effectively by increasing the degree of the switching graph rather than reducing the costs of switching.

Obfuscation for defensive means

In (Zhu et al., 2012), the authors study the use of deception to protect against attackers in a network. The authors model the interaction between the defender and attacker as a Stackelberg game, in which the defender chooses the flow rates of deceptive and real traffic, and the attacker then chooses a path to attack. The authors consider situations in which the sources of information cooperate or do not cooperate to obfuscate their traffic, and model the effects of adding fake data on the network. The authors suggest that future work could explore other measures of the effectiveness of deception and an incomplete information model in which nodes have limited information about the attacker's cost and utility functions.

Pawlick & Zhu study the use of obfuscation to protect privacy. The authors model the interaction between a machine learning or tracking agent, who has the option to promise a level of differential privacy protection, and a user who chooses whether to obfuscate their data. In the first paper, the authors show that under certain conditions, it is incentive-compatible for the learning agent to promise some level of privacy protection in order to avoid user obfuscation (Pawlick & Zhu, 2016). In the second paper, the authors extend this scenario to multiple users through a mean-field game model, and show that under certain conditions, obfuscation does not motivate privacy protection from the learner but only results in data pollution (Pawlick & Zhu, 2017a). The authors suggest that future work could measure users' preferences in experimental or empirical settings.

Deception as a defensive tool in cybersecurity

Atackers obtain information about networks through reconnaissance, while defenders lack an understanding of the threats that they face. Deception is crucial to counteract this information asymmetry. Consider the following definition (Mahon, 2016): To deceive == to intentionally cause another person to acquire or continue to have a false belief, or to be prevented from acquiring or cease to have a true belief.

Using game theory, they create a quantitative framework to model the information structure, actors, actions, and duration of various types of defensive deception. As a systems science, this approach models the essential, transferable, and universal aspects of defensive deception, helping to build a science of security.

Another example of game theory applied to deception in cybersecurity is the work of (Chen, 2018), who studied the problem of secure network formation. In this problem, a group of nodes (such as computers or devices) must decide how to connect to each other to form a network. The nodes can choose to be either vulnerable or secure, and the cost of being secure depends on the number of connections a node has. Chen et al. used game theory to model the interactions between the nodes and showed that under certain conditions, the resulting network will be more secure than if the nodes had chosen their connections randomly.

Another example is the work of (Li et al, 2020), who studied the problem of cyber insurance. In this case, the players are the insurance company and the policyholder. The policyholder must decide whether to invest in cybersecurity measures, while the insurance company must decide how much to charge for their policies. Li et al. used game theory to model the interactions between the insurance company and the policyholder and showed that under certain conditions, the policyholder will choose to invest in cybersecurity measures, leading to a more secure overall system.

Conclusion

These examples show the potential of game theory for studying deception in cybersecurity. By modeling the interactions between the attacker and the victim, game theory can help us understand how deception works and how it can be countered. In the future, game theory could be used to develop more sophisticated models of deception, and to design new strategies for defending against it.

References

Alvim, M. S., Chatzikokolakis, K., Kawamoto, Y., & Palamidessi, C. (2017). Information Leakage Games.

Chen, J. (2018). Factored Markov Game Theory for Secure Interdependent Infrastructure Networks.

Chessa, M., Grossklags, J., & Loiseau, P. (2015). A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications.

Feng, X., Zheng, Z., Mohapatra, P., & Cansever, D. (2017). A Stackelberg Game and Markov Modeling of Moving Target Defense.

Li, R. (2020). Pricing of cyber insurance premiums using a Markov-based dynamic model with clustering structure.

Mahon, J. E. (2016). The Definition of Lying and Deception.

Pawlick, J., Colbert, E., & Zhu, Q. (n.d.). A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. *ACM*, *V*.

Pawlick, J., & Zhu, Q. (2016). A Stackelberg Game Perspective on the Conflict Between Machine Learning and Data Obfuscation.

Pawlick, J., & Zhu, Q. (2017a). A Mean-Field Stackelberg Game Approach for Obfuscation Adoption in Empirical Risk Minimization.

Theodorakopoulos, G., Shokri, R., Troncoso, C., Hubaux, J.-P., & Boudec, J.-Y. L. (2014). Prolonging the hide-and-seek game: Optimal trajectory privacy for location-based services.

Zhu, Q., Clark, A., Poovendran, R., & Basar, T. (2012). Deceptive routing games.