Game Theory-Based Defense Mechanisms of Cyber Warfare

Monica Ravishankar, D. Vijay Rao and C. R. S. Kumar

Abstract Threat faced by wireless network users is not only dependant on their own security stance but is also affected by the security-related actions of their opponents. As this interdependence continues to grow in scope, the need to devise an efficient security solution has become challenging to the security researchers and practitioners. We aim to explore the potential applicability of game theory to model the strategic interactions between these agents. In this paper, the interaction between the attacker and the defender is modeled as both static and dynamic game and the optimal strategies for the players are obtained by computing the Nash equilibrium. Our goal is to refine the key insights to illustrate the current state of game theory, concentrating on areas relevant to security analysis in cyber warfare.

Keywords Game theory · Static game · Dynamic game · Nash equilibrium

1 Introduction

Cyber technology, in contrast to making communication in the wireless network less obtrusive, has made privacy the most "often-cited criticism" [1]. Even though security systems are designed against the attacks of the highly skilled adversaries, they are still vulnerable to cyber threats [2]. Accordingly, advancements in technology have paved way for the growing risk of security concerns that are well exemplified by recent incidents. This list of security incidents is certainly inexhaustive; [3] gives a perception of this growing risk of cybercrimes. Recent studies reveal that defending against sophisticated antagonists is a challenging task which requires not only high technical skills, but also a keen understanding of incentives behind their attacks and different strategies used by them. Thus, being able to

M. Ravishankar (✉) · C. R. S. Kumar
Defence Institute of Advanced Technology, Pune 411 025, India
e-mail: monica_pcse14@diat.ac.in

D. Vijay Rao
Institute of Systems Studies & Analyses, Delhi 110054, India

D. Reddy Edla et al. (eds.), *Advances in Machine Learning and Data Science*,
Advances in Intelligent Systems and Computing 705,
https://doi.org/10.1007/978-981-10-8569-7_16

defend against and survive cyber attacks is still a great concern. Very aware of that, security researchers have analyzed a wide range of mechanisms for successful deterrence [4].

Of late, security decisions have been scrutinized analytically in a more meticulous way. Decisions made analytically are well grounded and persistent since it can be numerically implemented and checked experimentally with further improvements. Many mathematical models like Decision Theory, Machine Learning, Control Theory, Fuzzy Logic, and Pattern Recognition have been used to model, analyze, and solve the security decision problems. But among all the available approaches, game theory seems very effective whose models pave way for capturing the nature of adversaries related to security problem. Since game-theoretic methods stand out for their obstinacy, they have a striking virtue to anticipate and design defense against a sophisticated attacker, rather than responding randomly to a specific attack [5]. Furthermore, game theory can model issues of risk, trust, and other externalities (such as, beliefs) that arise in security systems.

2 Game Model

Our work focuses on mitigating cyber attacks using game-theoretic approach and validating the game models using network simulator for monitoring the network traffic and mitigating malicious flow. For illustration purpose, DoS/DDoS attacks are considered where the attacking nodes attempt to disrupt the network services by flooding with malicious traffic. The attack scenario is considered with an assumption on the network setting that the defender is uncertain about the normal flow and attack flow. The work presents a game model for the DoS attacks, in the form of interaction between the attacker and defender. In an attack scenario, the network traffic flow rate is given by

$$T = n \times r_n + a \times r_a \tag{1}$$

where r_n signifies normal traffic rate for the chosen n legitimate nodes and r_a signifies attack flow rate for the chosen number of a attack nodes. In case there is no defense mechanism in place, it is assumed that θ fraction of traffic pass the firewall to reach the destination and $(1-\theta)$ fraction of flow will be dropped without passing through the firewall. For the rate of each packet, θr, the average number of normal packets, which are able to reach the server, is given by

$$n_{avg} = \frac{n \times r_n}{n \times r_n + a \times r_a} \tag{2}$$

and the average of legitimate nodes deprived of the network services is estimated as

$$n_l = \frac{n - n_{avg}}{n} \tag{3}$$

The attacker's objective is to increase n_l, which will incur him some cost proportional to a. Accordingly, the attacker's net expected payoff is given by:

$$E_a = n_l - a \tag{4}$$

while the defender's expected payoff is defined as:

$$E_d = -n_l + a \tag{5}$$

Now assume a case where the network is configured with an appropriate defense mechanism such as firewall, which filters the incoming packets depending upon the flow rate X. The rate of filtering is given by fast sigmoid function as:

$$F(x) = 0.5 \times \left((x - X) \times \left[\frac{\delta}{1 + abs(x + \delta)} \right] \right) + 0.5 \tag{6}$$

Thus for the expected rate of normal traffic, the average rate of legitimate packets reaching the server through the firewall is given by

$$r_n^{'} = r_n \times (1 - F(r_n)) \tag{7}$$

while the average rate of attack flow reaching the server through the firewall is given by

$$r_a^{'} = r_a \times (1 - F(r_a)) \tag{8}$$

We then compute the attacker's and defender's payoff by replacing r_n by $r_n^{'}$ and r_a by $r_a^{'}$ in Eqs. (2) and (3). The attacker has to set optimal values for a and r_a, and the defender has to set optimal value for X in the fast sigmoid function used by the firewall, in order to maximize their payoffs. The notion of Nash equilibrium is used to determine the equilibrium state of the game which defines the best response strategies of the two players. For the given strategy profile of the two players, $\left(r_a^*, a^*, X^*\right)$, the Nash equilibrium is defined to satisfy the following two relations simultaneously.

$$\begin{aligned} E^a_{\left(r_a^*, a^*, X^*\right)} &\geq E^A_{(r_a, a, X^*)} \quad \forall\, r_a, a \\ E^d_{\left(r_a^*, a^*, X^*\right)} &\geq E^D_{\left(r_a^*, a^*, X\right)} \quad \forall\, X \end{aligned} \tag{9}$$

The discussed model is made dynamic, which allows the players to change their strategies based on his/her anticipation of the opponent's behavior. Assuming the game duration as the sequence of k time steps, attacker's and defender's total

expected payoff, over the entire game, is given by, $E_a = \sum_{t=1}^{k} E_a^t$ and $E_d = \sum_{t=1}^{k} E_d^t$ and denoted by the strategy profile $\left(r_a^t, a^t, X^t\right)$ at the tth step $\forall t = 1, \ldots, k$. For the given strategy profile, $\left(r_{a_t}^*, a_t^*, X_t^*\right)$, the Nash equilibrium is defined to satisfy the following two relations simultaneously.

$$\begin{aligned} E^a_{\left(r^*_{a_t}, a^*_t, X^*_t, \quad t=1,\ldots,k\right)} &\geq E^a_{\left(r_{a_t}, a_t, X^*_t, \quad t=1,\ldots,k\right)} \\ E^d_{\left(r^*_{a_t}, a^*_t, X^*_t, \quad t=1,\ldots,k\right)} &\geq E^d_{\left(r^*_{a_t}, a^*_t, X_t, \quad t=1,\ldots,k\right)} \end{aligned} \quad \begin{array}{l} \forall\, r_a, a \\ \forall\, X \end{array} \tag{10}$$

3 Discussions

Game theory is not about the prescription for the clever strategy but the search for effective decision. What game theory can elucidate is how an interaction proceeds, representation of these interactions as mathematical models that allow a meticulous analysis of the problem, and to help analysts to predict each other's behavior for real-world attacks and defenses. Attackers have their own selection criteria over their targets and are sound enough to alter their attack strategies based on the available defensive schemes. But traditional security approaches which uses heuristic solutions fail to capture this fact in their decision model and prefer the strategy of the attacker alone as an input to the model. Whereas in game-theoretic model, both the defense strategies and the hacker's actions are endogenously realized. This signifies that there is the potential for game theory to play a significant role in cyber warfare.

References

1. Kotenko, I., Chechulin, A.: A cyber attack modeling and impact assessment framework. In: Podins, K., Stinissen, J., Maybaum, M. (Eds.) Proceedings of the Fifth International Conference on Cyber Conflict. 2013 © NATO CCD COE Publications, Tallinn
2. Nagurney, A., Nagurney, L.S., Shukla, S.: A supply chain same theory framework for cyber security investments under network vulnerability in computation, cryptography, and network security, pp 381–398. Springer International Publishing Switzerland (2015)
3. US-CERT: Technical Cyber Security Alerts. http://www.uscert.gov/cas/techalerts/index.html. Dec 2010
4. Lim, S.-H., Yun, S., Kim, J.-H.: Prediction model for botnet-based cyber threats. In International Conference on Convergence, pp. 340–341. IEEE Press, Jeju Island (2012)
5. Bier, V.M., Naceur Azaiez, M. (eds.): Game Theoretic Risk Analysis of Security Threats. Springer, New York (2009)