Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 134 (2018) 283–288

Procedia Computer Science

www.elsevier.com/locate/procedia

The 13th International Conference on Future Networks and Communications (FNC 2018)

Optimal Resource Allocation in Cyber-Security: A Game Theoretic Approach

Abderrahmane Sokri*

DRDC CORA, 60 Moodie Dr., Ottawa, ON K2H 8G1, Canada

Abstract

The increased reliance on the information and communication technologies has drastically changed the definition of security and the nature of war. Many critical infrastructures such as airports, hospitals, and oil pipelines have become potentially vulnerable to intentional cyber-attacks. A growing body of literature recognizes game theory as a sound theoretical foundation for modeling the strategic interactions between attackers and defenders. This paper explores the main challenging issues in the application of security games in cyberspace. A new game formulation combining simulation and game-theoretic approaches is proposed and illustrated.

Keywords: Game theory; Cyber-defence; Cyber-attack; Cyber-Security; Common knowledge; Uncertain observability.

1. Introduction

While Information and Communication Technologies (ICT) have allowed military decision makers to have the right information at the right time, they have brought many changes to the nature of war. Cyberspace has become the new battlespace where the weapons are social engineering, upgraded viruses, Trojan horses, worms, flooding Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) or botnets, and advanced persistent threat (APTs) [1], [2]. Cyber-attacks do not directly lead to a lethal effect, but can cause abuse of, malfunctions, or the destruction of equipment [3], [4].

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: Abderrahmane.Sokri@drdc-rddc.gc.ca

10.1016/j.procs.2018.07.172

In cyberspace, the weapon arsenal is built by finding more exploitable vulnerabilities in the target's defence. A vulnerability is a weakness in system security procedures, design, internal controls, or implementation that could be exploited by a threat source [5]. The dynamic nature of vulnerabilities implies that they are constantly changing over time. Detecting a vulnerability by the defender has two main implications on cyber weapons: (1) It makes the attacker's weapon exploiting the vulnerability ineffective and (2) enhances the target's defence (Czosseck and Podins, 2012)[4].

Many scholars including Roy et al. (2010) [6], Kiekintveld et al. (2015) [7] and Tambe (2011) [8] recognize game theory as a sound theoretical foundation for modeling the strategic interactions between attackers and defenders in cyberspace. Game theory has been applied to myriad topics including resource allocation, network security, and cooperation models. The problem of resource allocation commonly referred to as the allocation game is a typical game in the cyber domain [9]. In this game the defender and the attacker make the decision as to where to allocate their respective resources. The defender resources may be the security infrastructure such as firewalls. A network administrator, for example, may want to find the optimal resource allocation that minimizes risk of attack as well as the unnecessary associated cost [10]. The attacker may not only have limited resources, but can also run the risk of being traced back and punished.

The aim of this paper is to show how a resource allocation problem can be formulated in cyberspace using a game theoretic approach. More specifically, the paper discusses the challenging concept of common knowledge and suggests a solution to the uncertain observability problem.

The paper is organized into five sections. Following the introduction, section 2 offers a succinct review of literature on resource allocation games. Section 3 presents a new game formulation combining simulation and game-theoretic approaches. In section 4, a case study using a resource allocation game is presented to illustrate the suggested approach. Some concluding remarks and open research questions are indicated in section 5.

2. Literature review

The development of resource allocation algorithms in physical security domains has been an active research area in the last decade [6], [8], [11], [12]. Allocation games were used, for example, to randomize checkpoints at the Los Angeles International Airport (LAX), to assign limited security resources [7], [14], [15].

A growing body of literature tries to adapt the physical security algorithms to cybersecurity [16]. In the cyber world, defenders face more complex and sophisticated attacks. The digital attacks are often imperceptible to the human senses, not limited by geography and political boundaries, and highly dynamic and distributed [11].

Bloem et al. (2007) [17], for example, analyzed intrusion response in access control systems as a resource allocation problem. The authors modeled the interaction between an attacker and a distributed Intrusion Detection System (IDS) as a non-cooperative non-zero sum game. They developed an algorithm for optimal allocation of the system administrator's time treated as a scarce resource.

Vanek et al. (2012) [18] examined a game where an attacker tries to harm multiple vulnerable computers by sending malicious packets from multiple entry points of the network. The defender seeks to optimally allocate the available resources to maximize the probability of malicious packet detection under network latency constraints. The authors formulated the problem as a graph-based security game with multiple resources of heterogeneous capabilities and propose a mathematical program for finding optimal solutions.

Fielder et al. (2014) [19] analyzed the interactions between an omnipresent attacker and a team of system administrators. The authors used a game theoretic model to optimally allocate cyber security resources such as administrators' time across different tasks. They found, in this two-player, non-cooperative static game, that the defender's strategy was optimal independently from the attacker's strategy.

Game theory is also used to determine the optimal allocation of the total defensive budget over the various components of the system in order to minimize the success probability of a potential attack or to maximize its expected cost. Azaiez and Bier (2007) [20], for example, used a game where the defender attempts to deter attacks by making them as costly as possible to the attacker. The authors characterized the optimal attack and defence strategies.

In continuous time, Van Dijk et al. (2013) [21] suggested a two player dynamic game, termed Flipit, where the defender and attacker fight over control of a given resource. Depending on the setting being modeled, the resource may be a password or an entire infrastructure. Flipit is characterized by the idea of stealthy moves or stealthy takeover (Rasouli et al., 2014) [22]. Bowers et al. (2012) [23] demonstrated the application of Flipit to a broad range of real-world security problems including password reset policies and cloud auditing. The authors concluded that the model has countless uses in a world where no system is safe and the assumptions of security system designers can no longer be taken for granted.

The existing literature relies on the assumption of certain observability. In real-world, the common knowledge on payoffs may be missing. This paper combines simulation and game-theoretic approaches to deal with this situation. A case study is presented and discussed to illustrate the methodology.

3. Game Theoretic Formulation

Following the work done by Tambe (2011) [8] and Paruchuri et al. (2008) [13] in the physical world, we consider a security game between an attacker a and a defender d in a cyberinfrastructure system. Let $T = \{t_1, t_2, \dots, t_n\}$ be a set of n targets at risk of being attacked and $S = \{s_1, s_2, \dots, s_m\}$ a set of resources to cover the targets. In the physical world, targets and resources may be flights and air marshals. In the cyber world they may be security vulnerabilities in Internet-connected systems and the security infrastructure such firewalls.

The attacker's mixed strategy can be represented by the vector $\langle a_t \rangle$ where a_t is the probability of attacking the target t. The defender's mixed strategy is the vector $\langle p_t \rangle$ where p_t is the marginal probability of protecting the target t. Mixed strategies allow the two players to play probability distributions over their pure strategies ([12], [15]). A strategy profile ⟨a, p⟩ is a combination of strategies that the attacker and the defender may play.

Let $r_d(t)$ be the defender's reward if the attacked target t is covered and $c_d(t)$ his cost if the target is uncovered. Similarly, denote by $r_a(t)$ the attacker's reward if the attacked target t is uncovered and by $c_a(t)$ the attacker's cost if the attacked target t is covered. When the strategy profile $\langle a, p \rangle$ is played, the expected payoffs of the two players are given by:

$$U_d(a,p) = \sum_{t \in T} a_t \left(p_t r_d(t) - (1-p_t) c_d(t)\right) \quad (1)$$

$$U_a(a,p) = \sum_{t \in T} a_t \left((1-p_t) r_a(t) - p_t c_a(t)\right) \quad (2)$$

The payoffs in equations 1 and 2 depend only on the attacked targets and their coverage. Those that are not attacked are not considered in the payoffs. If the players move simultaneously, the solution is a Nash equilibrium [12]. If the game is sequential where the defender moves first and commits to a strategy and the attacker reacts, the standard solution in this leader-follower interaction is called Stackelberg equilibrium [16], [19].

Stackelberg games rely on the assumption that the leader knows his own payoffs and the payoffs of the follower. The follower needs not only to know his own payoffs but also the strategy to which the leader committed to. In most real-world cyber-security problems this assumptions is not always true. The players are generally unable to exactly evaluate their own payoffs and the payoffs of their opponents. Using deterministic values of payoffs makes the committed strategies ineffective [12].

To solve this problem, this paper suggests randomizing the payoffs using stochastic simulation. This new approach places uncertainty on each reward and cost by changing their static values to a range of values. Different approaches may be used to assess the likely fluctuation of the rewards and costs. Applying three-point estimates (optimistic, most likely, and pessimistic) for each variable seems to be particularly suitable to this end.

Given a leader's policy p, the follower's optimization problem can be presented as follows:

$$Max_a \sum_{t \in T} a_t \left((1-p_t) r_a(t) - p_t c_a(t)\right) \quad (3)$$

$$\text{s.t. } \sum_{t \in T} a_t = 1 \quad (4)$$

$$a_t \geq 0, \quad \forall t. \quad (5)$$

Equation 3 maximizes the follower's expected payoff given p. Equations 4 and 5 define the follower's set of feasible solutions as a probability distribution over the set of targets T. It is straightforward to see that it is optimal to assign 1 to any a_t associated with a maximal value of

$$U_a(t,p) = (1-p_t)r_a(t) - p_t c_a(t), \quad \forall t \in T \tag{6}$$

The corresponding dual problem that has the same optimal solution can be formulated as follows:

$$Min\ u \tag{7}$$

$$u \geq U_a(t,p), \quad \forall t \in T \tag{8}$$

The complementary slackness condition can be written as follows:

$$a_t\big(u - U_a(t,p)\big) = 0, \quad \forall t \in T \tag{9}$$

If we complete the leader's problem by including the follower's optimality conditions, the two programs can be formulated as a single Mixed-Integer Quadratic Problem [12].

$$Max_p \ \textstyle\sum_{t\in T} a_t \left(p_t r_d(t) \ - (1-p_t)c_d(t)\right) \tag{10}$$

$$\textstyle\sum_{t\in T} p_t \leq m \tag{11}$$

$$\textstyle\sum_{t\in T} a_t = 1 \tag{12}$$

$$0 \leq u - U_a(t,p) \leq (1-a_t)M, \forall t \in T \tag{13}$$

$$p_t \in [0,1], \quad \forall t \in T \tag{14}$$

$$a_t \geq 0, \quad \forall t. \tag{15}$$

$$u \in R \tag{16}$$

In this formulation, equation 10 maximizes the leader's expected payoff. Equation 11 limits the coverage to the available resources (m) and equation 14 restricts the coverage vector to [0, 1]. The two constraints enforce the leader's mixed strategy to be feasible. Equation 13, where M is a large number, is the complementary slackness condition. It indicates that the follower's payoff u is optimal for every pure strategy with $a_t > 0$.

A recent survey of the existing game-theoretic approaches for cyber security can be found in [24].

4. Illustration

To illustrate the suggested approach, consider the game in normal form shown in Table 1, adapted from the physical security literature [14], [25].

In this game, there are 4 targets and two resources that can cover any of the two targets. For each target, there are two payoffs: the payoff of the defender and the payoff of the attacker. Each payoff consists of two parts: a reward and a cost. The defender can cover a target and get a reward if the target is attacked. He can also leave the target uncovered and incur a cost if it is attacked. The attacker can attack a target and get a reward if the target is uncovered. He can also incur a cost if the target is covered.

Table 1: Payoff table

	Defender		Attacker	
	Reward	Cost	Reward	Cost
Target 1	4	3	9	6
Target 2	3	2	7	6
Target 3	6	4	10	8
Target 4	3	2	12	6

Instead of using single deterministic values of payoffs, uncertainty is incorporated using a three-point estimate (minimum, most likely, and maximum) approach. This approach places uncertainty on each variable in Table 1 by changing its static values to a range of values.

The following feasible solution has satisfied all the constraints as well as the numerical convergence criterion

$$\langle p=(0.5549, 0.4994, 0.3411, 0.6025), a=(0,0,0,1)\rangle.$$

After many iterations, the objective did not move significantly. The attacker preferred to attack the most valuable target even if it is heavily defended. This result is on par with the existing literature. It is particularly consistent with the studies conducted by Jain et al. (2010) [14] and An et al. (2011) [25].

Figure 1 depicts the cumulative distribution function (CDF) of the most likely payoffs, under the found solution. It shows the probability for each player to have a payoff less than a given value. For example, the median of the defender's average payoff is approximately 0.95. This means that the probability that the defender's average payoff will be less than 0.95 would be 50%. The minimum and maximum values for this variable would be 0.4261 and 1.5166, respectively.

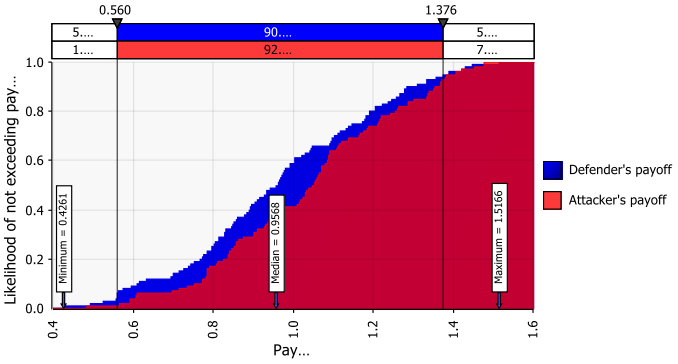

Figure 1: Distribution of the payoffs

5. Conclusion

While Stackelberg games have been recognized as a sound theoretical framework for modeling the strategic interactions between attackers and defenders, their application is still facing many challenges in cyberspace. One of the main challenging issues is the common knowledge concept. It is assumed in these games that the defender knows his own payoffs and the payoffs of the follower. The follower is also assumed to know his own payoffs and the strategy to which the leader committed to. In real-world cyber-security problems, the players are not able to exactly evaluate these payoffs which may make their strategies ineffective. A stochastic simulation is suggested in this paper to solve this uncertain observability problem. This new approach incorporates uncertainty on each imprecise variable by changing its static value to a range of values. An illustrative example is provided and some preliminary results are presented and discussed.

Further efforts will be undertaken to explore possible extensions of this framework to other real-world situation. These situations include (but are not limited to):

- A dynamic formulation of the problem where recent attacks are built upon previous attacks
- A formulation that includes other factors that determine the objective function
- A game where the defender faces multiple attackers
- A game with irrational attackers

References

[1] Bernier M, LeBlanc S, and Morton B. (2012). "Metrics Framework of Cyber Operations on Command and Control". Proceedings of the 11th European Conference on Information Warfare and Security, Laval, France, p. 53-62.

[2] Aslanoglu R, Tekir S. (2012). "Recent Cyberwar Spectrum and its Analysis". Proceedings of the 11th European Conference on Information Warfare and Security, Laval, France: 45-52.

[3] Ziolkowski K. (2010). "Computer network operations and the law of armed conflict". *Military Law and Law of War Review*, 49 (2): 47-94.

[4] Czosseck C and Podins K. (2012). "A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict". *International Journal of Cyber Warfare and Terrorism*, 2 (1): 14–26.

[5] NIST (2002). "Risk Management Guide for Information Technology Systems". NIST Special Publication: 800-30.

[6] Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V., and Wu Q. (2010). "A Survey of Game Theory as Applied to Network Security". Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS).

[7] Kiekintveld C, Lisy V, and Pibil R. (2015). "Game-theoretic foundations for the strategic use of honeypots in network security". In *Cyber Warfare*. Springer: 81–101.

[8] Tambe, M. (2011). "*Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned"*. Cambridge University Press.

[9] Bier VM, Cox LA, and Azaiez M.N. (2009). "Why Both Game Theory And Reliability Theory Are Important in Defending Infrastructure Against Intelligent Attacks" (Chapter 1). In: *Game Theoretic Risk Analysis of Security Threats*, Bier, V.M. and Azaiez, M.N. (eds) Springer: New York: p. 1–11.

[10] Acquaviva JR. (2017). "Optimal Cyber-Defense Strategies for Advanced Persistent Threats: A Game Theoretical Analysis". Master Thesis, the Pennsylvania State University.

[11] Moisan F and Gonzalez C. (2017). "Security under Uncertainty: Adaptive Attackers Are More Challenging to Human Defenders than Random Attackers". *Frontiers in Psychology*, 8.

[12] Coniglio S. (2014). "Algorithms for Finding Leader-Follower Equilibrium with Multiple Followers". Ph.D. Thesis, Politecnico di Milano.

[13] Paruchuri P, Pearce J, Marecki J, Tambe M, Ordonez F, and Kraus S. (2008). "Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games". Proceedings of the International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS): 895–902.

[14] Jain M, Tsai J, Pita J, Kiekintveld C, Rathi S, Ordone, F, and Tambe, M. (2010). "Software assistants for randomized patrol planning for the LAX airport police and the Federal Air Marshals Service". *Interfaces*, 40 (4): 267–290.

[15] Kiekintveld C, Jain M, Tsai J, Pita J, Ordonez F, and Tambe M. (2009). "Computing optimal randomized resource allocations for massive security games". Proceedings of the 8th International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS), Budapest, Hungary: 689–696.

[16] Sinha A, Nguyen TH, Kar, D, Brown M., Tambe M and Xin Jiang AX. (2015). "From physical security to cybersecurity". *Journal of Cybersecurity*, 1 (1): 19-35.

[17] Bloem M, Alpcan T, and Basar T. (2006). "Intrusion Response as a Resource Allocation Problem". IEEE Conference on Decision and Control.

[18] Vanek O, Yin Z, Jain M, Boransky B, Tambe M, Pechouceky M. (2012). "Game-Theoretic Resource Allocation for Malicious Packet Detection in Computer Networks". Proceedings of the 11th International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS).

[19] Fielder A, Panaousis E, Malacaria P, Hankin C, and Smeraldi F. (2014). "Game Theory Meets Information Security Management". Information Security and Privacy Conference, 2014, p. 15–29.

[20] Azaiez N. and Bier VM. (2007). "Optimal Resource Allocation for Security in Reliability Systems". *European Journal of Operational Research*, 181 (2): 773–786.

[21] Van Dijk M, Juels A, Oprea A., and Rivest RL. (2013). "Flipit: The Game of Stealthy Takeover". *Journal of Cryptology*, 26 (4): 655-713.

[22] Rasouli M, Miehling E, and Teneketzis D. (2014). "A Supervisory Control Approach to Dynamic Cyber-security". In *Decision and Game Theory for Security*, Poovendran, R. and Saad, W. Eds., Springer International Publishing: 99-117.

[23] Bowers KD, van Dijk M, Griffin R, Juels A, Oprea A, Rivest RL., Triandopoulos, N. (2012). "Defending Against the Unknown Enemy: Applying Flipit to System Security". In: Grossklags, J., Walrand, J. (eds.) *GameSec* 2012. LNCS, Springer, Heidelberg, 7638: 248–263.

[24] Do CT, Tran NH, Hong C, Kamhoua CA, Kwiat KA, Blasch E, Ren S, Pissinou N, and Iyengar SS. (2017). "Game Theory for Cyber Security and Privacy". *ACM Computing Surveys* (CSUR), 50 (2): 30.

[25] An B, Tambe M, Ordonez F, Shieh E, and Kiekintveld C. (2011). "Refinement of strong Stackelberg equilibria in security games". Proceedings of the 25th Conference on Artificial Intelligence: 587–593.