Security and Safety, Vol. 3, 2023028 (2024)
https://doi.org/10.1051/sands/2023028
sands.edpsciences.org

Commentary OPEN ACCESS

Industrial Control

Optimal DoS attack on multi-channel cyber-physical systems: A Stackelberg game analysis

Zhuping Wang[1,2], Haoyu Shen[1], Hao Zhang[1,2,*], Sheng Gao[1], and Huaicheng Yan[3]

[1] *Department of Control Science and Engineering, Tongji University, Shanghai 200092, China*
[2] *Shanghai Research Institute for Intelligent Autonomous Systems, Shanghai 201210, China*
[3] *School of Information Science and Engineering, East China University of Science and Technology, Shanghai 200237, China*

Received: 17 March 2023 / Revised: 19 June 2023 / Accepted: 17 August 2023 / Published online: 23 January 2024

Citation Wang ZP, Shen H, Zhang H, Gao S and Yan H. Optimal DoS attack on multi-channel cyber-physical systems: A Stackelberg game analysis. Security and Safety 2024; **3**: 2023028. https://doi.org/10.1051/sands/2023028

1 Problem formulation

1.1 System model and communication channel

Consider a simplified model of a cyber-physical system (CPS) with a physical plant, m wireless sensors, and a remote estimator, which has been widely applied in existing literature [1–3]. It is assumed that there exists a Denial-of-Service (DoS) attacker in the environment. The information CPS states that $x_k \in \mathbb{R}^{n_x}$ may be blocked or congested by the attacker at any time. For this reason, the information received by the estimator satisfies

$$\hat{x}_k^i = \begin{cases} \hat{x}_k^{s,i} & \text{channel } i \text{ is safe (without DoS attack),} \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

where $\hat{x}_k^{s,i} \in \mathbb{R}$ is the value of a certain state at time k. The value is measured by sensor i in real-time. s is the abbreviation of the sensor.

Along with DoS attacks, network transmission is also susceptible to attenuation and interference, which causes data packet dropouts. The signal-to-interference-and-noise ratio (SINR) is introduced as a way to assess the integrity of data after transmission.

$$\pi_i = \mathrm{SINR}_i = \frac{\alpha_i \lambda_i}{\sigma_{\mathrm{bgn}} + \beta_i \theta_i}, \quad i \in \mathcal{M}, \tag{2}$$

where $\mathcal{M} = \{1, 2, \ldots, m\}$. m is the number of channels. The fading channel gain of the defender or attacker for the ith channel is denoted by $\alpha_i, \beta_i > 0$. The level of background noise is described by σ_{bgn}. The energy assigned by the defender or attacker to the ith channel is denoted by $\lambda_i, \theta_i \geq 0$. If the attacker does not launch DoS attacks, the SINR can be simplified to signal-to-noise ratio (SNR), which is indicated by ρ_i.

$$\rho_i = \mathrm{SNR}_i = \frac{\alpha_i \lambda_i}{\sigma_{\mathrm{bgn}}}, \quad i \in \mathcal{M}. \tag{3}$$

* Corresponding authors (email: zhang_hao@tongji.edu.cn)

1.2 Reward function and strategy

Suppose the probability that there is only background noise in the channel is γ, and both players know the total energy of each other, which are $\bar{\lambda}_M$ and $\bar{\theta}_M$. The rewards for the defender and the attacker are given as follows

$$J_d(\lambda,\theta)=\gamma\langle\mathbf{1_m},\rho\rangle+(1-\gamma)\langle\mathbf{1_m},\pi\rangle-\eta_d\langle\mathbf{1_m},\lambda\rangle, \tag{4}$$

$$J_a(\lambda,\theta)=-\langle\mathbf{1_m},\pi\rangle-\eta_a\langle\mathbf{1_m},\theta\rangle+\eta_d\langle\mathbf{1_m},\lambda\rangle, \tag{5}$$

where $\rho=[\rho_1,\ldots,\rho_m]^\top,\pi=[\pi_1,\ldots,\pi_m]^\top,\lambda=[\lambda_1,\ldots,\lambda_m]^\top,\theta=[\theta_1,\ldots,\theta_m]^\top,\mathbf{1_m}=[1,\ldots,1]^\top_{1\times m}$ and η_d,η_a refer to the cost of unit energy consumed by defender and attacker, respectively. $\langle\cdot\rangle$ denotes the standard inner product in n-dimensional Euclidean space.

The goal of the defender and the attacker is to maximize their reward value. Hence, strategies should be their real-time decisions on energy allocation. The strategy sets $\mathcal{R}_d,\mathcal{R}_a$ are given for defender and attacker, respectively. $\bar{\lambda}_M,\bar{\theta}_M$ refer to the total energy available for both sides of the game.

$$\mathcal{R}_d=\left\{(\lambda_1,\ldots,\lambda_m)|\sum_{i=1}^{m}\lambda_i=\bar{\lambda}_M,\lambda_i\geq 0\right\}, \tag{6}$$

$$\mathcal{R}_a=\left\{(\theta_1,\ldots,\theta_m)|\sum_{i=1}^{m}\theta_i=\bar{\theta}_M,\theta_i\geq 0\right\}. \tag{7}$$

2 Main results

In the following contents, theoretical results of Stackelberg equilibrium in static Stackelberg game [5] and strategies for both defender and attacker in dynamic Stackelberg game are given.

2.1 Static game analysis

Given that both sides' total energy is known, the following optimization problem can be solved to determine the optimal DoS attack strategy for the attacker. Theorem 1 is the theoretical conclusion reached by utilizing the Karush-Kuhn-Tucker (KKT) conditions [6].

$$\begin{aligned}&\max_{\theta\in\mathcal{R}_a}-\langle\mathbf{1}_m,\pi\rangle\\ s.t.\ &\langle\mathbf{1}_m,\theta\rangle-\bar{\theta}_M=0,\\ &-\theta_i\leq 0,i\in\mathcal{M}.\end{aligned} \tag{8}$$

Theorem 1. *Suppose that the defender's strategy is known as λ. The optimal strategy of energy allocation obtained by the attacker to respond to the defender's defensive scheme is*

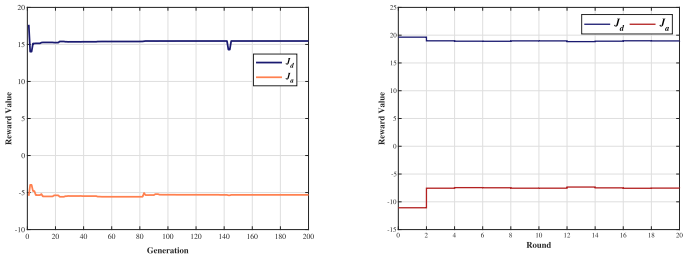
$$\theta_i(\lambda)=\max\left\{\frac{1}{\beta_i}(\sqrt{\frac{\alpha_i\beta i\lambda_i}{\bar{\mu}}}-\sigma_{\text{bgn}}),0\right\},\ i\in\mathcal{M}, \tag{9}$$

where $\bar{\mu}$ is the solution of the following equation

$$\sum_{i=1}^{M}\max\left\{\frac{1}{\beta_i}(\sqrt{\frac{\alpha_i\beta_i\lambda_i}{\bar{\mu}}}-\sigma_{\text{bgn}}),0\right\}=\bar{\theta}_M. \tag{10}$$

Proof. See Appendix A for details.

Meanwhile, a non-convex optimization problem can be solved to determine the defender's best course of action. The numerical result of Stackelberg Equilibrium is proposed to be found using a self-adaptive particle swarm optimization (PSO). Appendix B contains a complete list of the steps.



(a) (b)

Figure 1. Reward value of both sides. (a) Self-adaptive PSO. (b) Dynamic game

Table 1. Optimal strategy for both sides in static game and dynamic game

Game type	Defender's optimal strategy				Attacker's optimal strategy			
	λ_1	λ_2	λ_3	λ_4	θ_1	θ_2	θ_3	θ_4
Static game	7.5308	2.138	1.3259	0.0053	3.3922	4.5128	1.5200	0
Dynamic game	7.8595	3.1405	0	0	2.8810	1.1730	0	0

Remark 1. The attack-defence model in CPS constructed in this commentary can be extended to the Stackelberg game with multiple attackers and defenders. It has been proved [7, 8] that there exist equilibrium points as long as the reward function of both sides guarantees certain convexity requirements. The procedures of proving the static equilibrium and obtaining the optimal attack strategy are similar [9]. The differences in attack strategy between work [9] and this commentary lie in the physics scene and mathematical modeling. Attackers' unknown energy is emphasized in work [9], while the probability of launching DoS attacks is considered in this commentary.

2.2 Dynamic game

In mathematical form, the reward function for the defender is undoubtedly a linear function with respect to λ. To express it in vector form, $J_d = \varphi^\top \lambda$. As a result, the defender can adopt the optimal defensive strategy based on the following theorem.

Theorem 2. *Given the attacker's strategy θ, the optimal response for the defender is to allocate all of its limited energy to the channel with the maximum weight factor φ_i, which is the index of the maximum item in the weight factor vector. If there is not a unique index with the maximum weight factor, then the optimal response for the defender is a set of channels with equal weight factors*

$$\{(\lambda_{i_1}, \cdots, \lambda_{i_k}) | \Sigma_{r=1}^{k} \lambda_{i_r} = \bar{\lambda}_M\}. \tag{11}$$

Proof. See Appendix C for details.

Based on Theorem 1 and 2, a computational algorithm can be designed for the evolution of the strategies of both attackers and defenders in a dynamic Stackelberg game.

3 Simulation results

The probability of the attacker's existence is chosen as $\gamma = 0.4$. For simulation, consider the network parameters selected in [3], where $m = 4$, $\bar{\lambda}_M = 11$, $\bar{\theta}_N = 10$, $\eta_a = \eta_d = 0.3$, $\sigma_{\text{bgn}} = 0.2$, $\alpha = [0.8, 0.7, 0.6, 0.5]^\top$ and $\beta = [0.2, 0.3, 0.4, 0.5]^\top$. The static equilibrium of energy allocation for both the defenders and the attackers is depicted in Figure 1a. In the dynamic game scenario, after 10 000 Monte Carlo simulations, it is found that the energy allocation pattern varies. The reward values are plotted in Figure 1b. Table 1 summarizes the optimal strategies for both defenders and attackers. It is observed that compared to the static equilibrium scenario, even if the amount of energy allocated to each

channel and the resulting reward values vary, both defenders and attackers still allocate the majority of their resources to Channel 1 and Channel 2. The additional details of the simulations are included in Appendix E. To further strengthen the novelty of the proposed PSO, a set of comparative experiments is included in the supporting information, as shown in Appendix F.

4 Conclusion

In this commentary, a Stackelberg game framework for a multi-channel CPS consisting of one DoS attacker and one defender is introduced. Simulation results demonstrate that both offline and online strategies demonstrate a tendency to allocate energy to specific channels. In the dynamic game setting, the defender and attacker energy allocation strategies follow a repeating pattern, with the average values approaching static equilibrium levels. Future work will focus on extending the proposed framework to investigate false data injection attacks and replay attacks.

Authors' Contributions

Zhuping Wang provided the core idea behind this paper. Haoyu Shen was a co-author and driving force behind the creation of this commentary. Hao Zhang provided feedback and corrected errors in the text and was also a co-author. Sheng Gao contributed by verifying theoretical derivations and assisting with simulation experiments. Huaicheng Yan oversaw the completion of the commentary and provided suggestions for future research directions.

Funding

This work is supported by the National Natural Science Foundation of China (62273255, 62088101), Shanghai International Science and Technology Cooperation Project (22510712000, 21550760900), Shanghai Municipal Science and Technology Major Project (2021SHZDZX0100) and Fundamental Research Funds for the Central Universities.

Supporting Information

The supporting information is available online at https://sands.edpsciences.org/10.1051/sands/2023028/olm. The supporting information is published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

[1] Li Y, Shi L and Cheng P et al. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. IEEE Trans Autom Control 2015; **60**: 2831–2836
[2] Li Y, Mehr AS and Chen T. Multi-sensor transmission power control for remote estimation through a sinr-based communication channel. Automatica 2019; **101**: 78–86
[3] Liu H. SINR-based multi-channel power schedule under dos attacks: A stackelberg game approach with incomplete information. Automatica 2019; **100**: 274–280
[4] Proakis JG and Salehi M. Digital Communications (5th ed). New York: McGraw-Hill, 2007
[5] Fujiwara-Greve T. Non-cooperative Game Theory. Tokyo: Springer, 2015
[6] Boyd SP and Vandenberghe L. Convex Optimization. Cambridge: Cambridge University Press, 2004
[7] Fiez T, Chasnov B and Ratliff L. Implicit learning dynamics in stackelberg games: Equilibria characterization, convergence analysis, and empirical study. Proc 37th Int Conf Mach Learn (PMLR) 2020; **119**: 3133–3144
[8] Sherali HD. A multiple leader stackelberg model and analysis. Oper Res 1984; **32**: 390–404
[9] Wang Z, Shen H and Zhang H, et al. Optimal DoS attack strategy for cyber-physical systems: A Stackelberg game-theoretical approach. Inf Sci 2023; **642**: 119134