Applying game theory for improving security in the process industries: a discussion

Zhang, Laobing; Reniers, Genserik

DOI
10.18757/jiss.2018.1.2033

Publication date
2018

Document Version
Final published version

Published in
Journal of Integrated Security Science

Journal of Integrated Security Science

APPLYING GAME THEORY FOR IMPROVING SECURITY IN THE PROCESS INDUSTRIES: A DISCUSSION

Laobing Zhang [1,*], Genserik Reniers [1,2,3]

1. Safety and Security Science Group, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands

2. Antwerp Research Group on Safety and Security (ARGoSS), University Antwerpen, 2000 Antwerp, Belgium

3. Faculty of Economics and Management, KULeuven, 1000 Brussels, Belgium

Background

Game theory has been introduced to the chemical security community in recent years. Talarico et al. (2015) developed the so-called 'MISTRAL' game for optimizing resources' allocation in a multiple modal chemical transportation network. Rezazadeh et al. (2017) employed game theory for randomly but strategically scheduling patrolling for pipelines. Zhang and Reniers (2016) proposed a chemical plant protection (CPP) game based on the physical intrusion detection system in chemical plants. Feng et al. (2016) introduced a game theoretic approach for allocating security resources among multiple chemical plants within a city. These game theoretic models are innovative on the one hand since taking into consideration strategic adversaries, and on the other hand since they provide quantitative recommendations on how to allocate limited security resources.

Why should game theory be introduced and used in the chemical security practitioners?

Security risks are initiated by deliberate behaviours for certain goals. For instance, thieves intentionally intrude a plant for stealing valuable materials, or terrorists maliciously set a fire on a chemical facility to cause societal fear. Initiators of security events (henceforth, attackers) would intelligently observe the defender's defence plan and then schedule their attack accordingly. Powell (2007) illustrated how resources can be mis-allocated if intelligent interactions between the defender and the attacker are not considered. Game theory was invented in the economic domain for modelling both the cooperative and competitive behaviours in a multiple actors system. In the last 100 years, game theory has been theoretically improved and practically applied to various domains, such as the evolutionary biology, the nuclear balance, computer science etc. These researches have demonstrated the capability of game theory in modelling intelligent interactions.

Industrial managers need quantitative recommendations to support their decision making. Conventional security risk assessment methodologies (e.g., the API SRA framework (API, 2013)), being good at studying security systematically, are not able to provide quantitative insights.

* Corresponding author: Laobing Zhang
Email address: Laobing.Zhang@tudelft.nl

ISSN: 2468-4546

Moreover, results of these conventional methodologies are not repeatable which means that applying the same methodology to the same plant, different analysts may come to different conclusions. Some quantitative security risk assessment models, for instance, by employing a Bayesian Network framework (e.g., Argenti et al. (2018); Landucci et al. (2017); Fakhravar et al. (2017)), can provide quantitative and repeatable results as well. Nevertheless, these models fail on modelling the intelligent interactions between the defender and the attacker. Game theory, conversely, has a rigorous mathematical foundation and models the intelligent interactions. A game theoretic model explicitly indicates 1) who is involved in the game; 2) what actions can each participant take; 3) what results (numbers) will each participant obtain, for each participants' strategy combination; 4) how much information that each participant has about the game. Furthermore, outputs of a game theoretic model (i.e., equilibrium) clearly and quantitatively indicates what should the participants do (i.e., the equilibrium strategy) and what will each participant obtain (i.e., the equilibrium payoff).

A critical issue is that industrial managers often prefer a qualitative approach and they have difficulties on understanding (the physical meaning of) the quantitative outputs of a game theoretical model. This issue can be addressed by requiring game developers to do a further step work by also translating/mapping their quantitative outputs to qualitative descriptions, and the latter should be expressed in terminologies that industrial practitioners are familiar with. Figure 1 illustrates the idea.

How can game theory be employed to improve chemical security?

Game theory can be employed to improve chemical security from various perspectives, some of which have already been investigated while others still need more research input.

From a single plant point of view, game theory can be used to study how to optimally allocate security resources to better defend the plant from intentional attacks. Non-cooperative games are most likely to be suitable in these cases. See for instance, the Chemical Plant Protection game proposed by Zhang and Reniers (2016), which studied how to optimally set security alert levels at entrances and zones of a chemical plant.

From a cluster point of view, game theory can be used to design a better mechanism that stimulates security investments from each single plant. Plants in one chemical park on the one hand may benefit from the security investment from their neighbour plants, and on the other hand they may suffer a loss from an attack taking place in their neighbour plants (due the existence of domino effects). A good cluster-level security mechanism will stimulate plants to invest in security while a bad mechanism will stop plants from investing in security. Cooperative and multiple players games are suitable for these cases. For instance, Reniers and Soudan (2010) studied the security investment game within chemical industrial parks.

Other applications of game theory in the chemical security domain can be, for instance, optimizing patrolling within each plant as well as in a cluster level. Furthermore, in Europe, high hazardous (from a safety point of view) chemical facilities are regulated by the SEVESO Directive (European Commission (2012)), and therefore the government and legislation have roles in the safety enhancement of these facilities. However, no specific regulations exists yet w.r.t to the security enhancement of these SEVESO sites. Game theory may play a role in the procedure of designing security regulations that fits benefits of different stakeholders (the chemical industries, the

surrounded residents, the government etc.), as well as in the auditing procedure of the compliance of security regulations in chemical plants.

What obstacles are there?

Game theory, although being invented for modelling strategic behaviours, is not widely employed in the chemical industrial security domain yet. Several criticisms are there.

Game theoretic models need massive (and mostly quantitative) input data, being the first obstacle that prevents its popularity among industrial managers. As we mentioned before, the basic components of a game theoretic model are players, strategies, and payoffs. In a game against terrorism, the players and strategies modelling should be based on the threat and attractiveness analysis, for instance, to know what kind of threat the plant is facing (players modelling), and to know what kind of attack scenarios that the attacker may use (strategies modelling). However, terrorist attacks are normally happening unexpectedly in time, place, and means, as also pointed out by Pasman (2017) "Failing to see a possibility can be fatal, but completeness is almost impossible…", and by Baybutt (2017) "The number of threat scenarios is unbounded and is limited only by the imagination of attackers." Therefore, to enumerate all the possible players and each player's strategies can be a difficult task. Moreover, payoffs in a game theoretic model are quantitative numbers, and they can be quite difficult to obtain, especially payoffs of the attackers. For instance, under a certain defence plan and a certain attacker intrusion path, how likely is it (a probability) that the attacker would successfully pass all the security barriers and reach the target? Furthermore, attackers may have different estimations of the probability, both with respect to the defender and with respect to different types of attackers.

Game theoretic models are based on several strict assumptions, limiting the use of game theoretic models in industrial practice. The most frequently used assumptions are the rationality assumption and the common knowledge assumption. The rationality assumption requires that players are rational at maximizing their own payoff. In reality, human beings are not machines, and some of our decisions are emotions-based, especially in case of terrorists. The common knowledge assumption says that each player in the game knows i) its own information (i.e., rationality, strategies, payoffs, preferences etc.); ii) all other players' information; iii) that other players know that they know other players' information; and so forth. In reality, industrial security managers find it difficult to know the information even of themselves (e.g., how severe an attack would be?). For the information of the attackers, and also regarding whether the attackers know the defender's information, the common knowledge assumption is intuitively unacceptable.

How to remove these obstacles?

Baybutt (2017) suggests "SVA (Security Vulnerability Analysis) practitioners to identify threat scenarios that are representative of unidentified scenarios?", to meet the difficulty of completely enumerating all the players' strategies. Zhang et al. (2018) propose a framework in which the API SRA methodology should act as the data provider while game theory should be the data processor, as shown in Figure 1. Zhang et al. (2017b) propose a chemical plant protection game to deal with inputs with distribution-free uncertainties (the Interval CPP game). The Interval CPP game does not need the exact numerical values of the input parameters (e.g., a probability of 0.1), instead, it only requires an interval that the value will be situated in (e.g., the probability is situated in the interval [0.05,0.2]) while how the value is distributed in the interval does not matter either.

Behaviour modelling has a long history of being integrated into game theoretic models. Players with a different rationality level (e.g., epsilon-optimal players, level-k thinking players, quantal response players etc.) can be modelled by different behaviour models. Zhang et al. (2017a) introduce a chemical plant protection game which incorporates bounded rationality attackers, for instance. For relaxing the common knowledge assumption, on the one hand, the so-called "Bayesian Game" (Harsanyi, 2004) can be employed, on the other hand, in a typical defender-attacker sequential game (Tambe, 2011), the common knowledge assumption is actually not required. Furthermore, besides the "Bayesian Game" approach, a methodology called "adversarial risk analysis" (Rios and Insua, 2012) is also suitable for relaxing the common knowledge assumption in a simultaneous game.

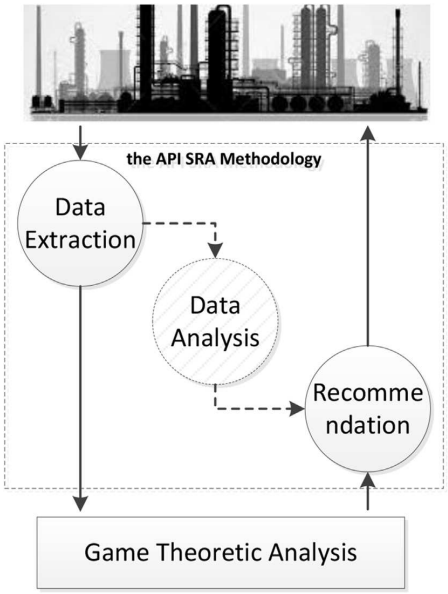

Figure 1. Integration of the API SRA methodology and game theory (adopted from Zhang et al. (2018))

Conclusions

Game theory fills the gap that conventional security assessment methodologies are not able to deal with. Strategic adversaries are considered and highly quantitative recommendations can be provided. Research opportunities exist in the use of game theory to improve the security of chemical industrial activities. However, modelling challenges also exist.

References

API. (2013). Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. In A. R. P. 780 (Ed.).

Argenti, F., Landucci, G., Reniers, G., & Cozzani, V. (2018). Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. *Reliability Engineering & System Safety, 169*, 515-530.

Baybutt, P. (2017). Issues for security risk assessment in the process industries. *Journal of Loss Prevention in the Process Industries, 49*(Part B), 509-518. doi: https://doi.org/10.1016/j.jlp.2017.05.023

Commission, E. (2012). *Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC text with EEA relevance*. Off J Eur Union 2012.

Fakhravar, D., Khakzad, N., Reniers, G., & Cozzani, V. (2017). Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network. *Process Safety and Environmental Protection, 111*, 714-725.

Feng, Q., Cai, H., Chen, Z., Zhao, X., & Chen, Y. (2016). Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. *Journal of Loss Prevention in the Process Industries, 43*, 614-628.

Harsanyi, J. C. (2004). Games with incomplete information played by "Bayesian" players, i–iii: part i. the basic model&. *Management science, 50*(12_supplement), 1804-1817.

Landucci, G., Argenti, F., Cozzani, V., & Reniers, G. (2017). Assessment of attack likelihood to support security risk assessment studies for chemical facilities. *Process Safety and Environmental Protection, 110*, 102-114.

Pasman, H. (2017). Safety and security: what are the parallels, and why research is needed? *Journal of Integrated Security Science, 1*(1), 29-31.

Powell, R. (2007). Defending against terrorist attacks with limited resources. *American Political Science Review, 101*(03), 527-541.

Reniers, G., & Soudan, K. (2010). A game-theoretical approach for reciprocal security-related prevention investment decisions. *Reliability Engineering and System Safety, 95*(1), 1-9. doi: 10.1016/j.ress.2009.07.001

Rezazadeh, A., Zhang, L., Reniers, G., Khakzad, N., & Cozzani, V. (2017). Optimal patrol scheduling of hazardous pipelines using game theory. *Process Safety and Environmental Protection, 109*, 242-256.

Rios, J., & Insua, D. R. (2012). Adversarial risk analysis for counterterrorism modeling. *Risk Analysis, 32*(5), 894-915.

Talarico, L., Reniers, G., Sörensen, K., & Springael, J. (2015). MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. *Reliability Engineering and System Safety, 138*, 105-114. doi: 10.1016/j.ress.2015.01.022

Tambe, M. (2011). *Security and game theory: algorithms, deployed systems, lessons learned*: Cambridge University Press.

Zhang, & Reniers. (2016). A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. *Risk Analysis, 36*(12), 2285-2297.

Zhang, L., Reniers, G., Chen, B., & Qiu, X. (2017a). A Chemical Plant Protection Game Incorporating Boundedly Raitonal Attackers and Distribution-free Uncertainties *Submitted to Chemial Engineering Science*.

Zhang, L., Reniers, G., Chen, B., & Qiu, X. (2018). Integrating the API SRA methodology and game theory for improving chemical plant protection. *Journal of Loss Prevention in the Process Industries, 51*(Supplement C), 8-16. doi: https://doi.org/10.1016/j.jlp.2017.11.002

Zhang, L., Reniers, G., & Qiu, X. (2017b). Playing chemical plant protection game with distribution-free uncertainties. *Reliability Engineering & System Safety*. doi: https://doi.org/10.1016/j.ress.2017.07.002