Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 26 (2018) 1255–1264

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

46th SME North American Manufacturing Research Conference, NAMRC 46, Texas, USA

A game theory based cybersecurity assessment model for advanced manufacturing systems

Alireza Zarreh[a], Can Saygin[a,b]*, HungDa Wan[a,b], Yooneun Lee[a,b], Alejandro Bracho[a]

[a] Department of Mechanical Engineering, University of Texas at San Antonio, San Antonio, Texas 78249, USA
[b]Center for Advanced Manufacturing and Lean Systems, University of Texas at San Antonio, San Antonio, Texas 78249, USA

* Corresponding author. Tel.: +1-210-458-5194; fax: +1-210-458-6504.
E-mail address: can.saygin@utsa.edu

Abstract

This paper presents a method to create and solve a game theory model to address cybersecurity issues specifically for advanced manufacturing systems with high-level computer-controlled integration. This method introduces a unique approach to defining the contents of the game payoff matrix by incorporating maintaining of defense strategies, production losses, and recovery from attacks as part of a cost function that effectively represents the reality in the manufacturing systems domain. Once the cost function is developed to define the payoff matrix, the game is run for all possible combinations to find the best possible combination of the strategies. Finally, a case study is presented to illustrate the application. The proposed method can be applied to different domains, other than automated manufacturing systems, by customizing cost components in the utility function.

Peer-review under responsibility of the scientific committee of the 46th SME North American Manufacturing Research Conference.

Keywords: Game Theory; Cybersecurity in Manufacturing; Best Strategy for Defense

1. Introduction

Advancement in manufacturing technology and its integration with IT technology has introduced new terminology to the manufacturing world like smart manufacturing and cloud manufacturing [1–4]. Moreover, support tools development for Internet-based Computer-Aided Engineering (CAE) such as cloud computing and software as a service (SaaS) are being increasingly popular across manufacturing [2], [5, 6]. While these advancements have improved the productivity, agility, and sustainability of manufacturing systems, they make manufacturing systems more vulnerable to the new type of threats.

According to the newest Verizon Data Breach Investigations report in 2017 [7], the manufacturing sector has been the most targeted one for cyberattacks in 2016, more than the public sector and higher than

2351-9789
Peer-review under responsibility of the scientific committee of the 46th SME North American Manufacturing Research Conference.
10.1016/j.promfg.2018.07.162

utilities and education. Moreover, Deloitte [8] reports that the cybersecurity instances in the manufacturing sector have been constantly increasing in recent years since 2011. It categorizes these malicious attacks into six major themes including executive and board level engagement, talent and human capital, intellectual property, industrial control systems, connected products, and industrial ecosystem. Another report by Deloitte [9] tries to identify motivations behind these attacks and classify types of attackers. According to this report, motivations could range from money and revenge to competitive advantage and strategic disruption. It also brings three scenarios to attack manufacturing systems including hacking employee log-in credentials, gaining control of industrial plants, and access and theft of intellectual properties. However, despite the increasing trend in existence of these threats to manufacturing systems only few studies have been led to address these issues.

In order to deal with these cyber security vulnerabilities, there are two basic approaches that could be utilized: reactive approach and proactive approach.

Reactive Approaches

In reactive approaches, the previous attacks are taken into account to address current attacks. As shown in figure 1, when a hacker develops a technique and tests it successfully against security systems, other hackers adopt and use it widely. The security communities, at this point, eventually respond with proper countermeasures that encourage attackers to develop new techniques, and the cycle continues again from the beginning. This approach in fact is a retrospective approach and it is effective against novice attacker but it is inadequate for Advanced Persistent Threats (APTs) and sophisticated cyber weapons against manufacturing systems.

Proactive Approaches

Proactive approach attempts to reliably forecast cyber-attacks by predicting likely behavior of attackers and estimate attackers' capabilities in order to launch proper countermeasures. These countermeasures could range from taking infected system offline, reinstalling system, or performing more invasive "checkups" on systems likely to be attacked. More specifically for manufacturing systems, rescheduling could also be considered as a countermeasure to eliminate or reduce the damage of an attack.

Forecasting cyber security in manufacturing systems however is not a simple task to do. Modeling

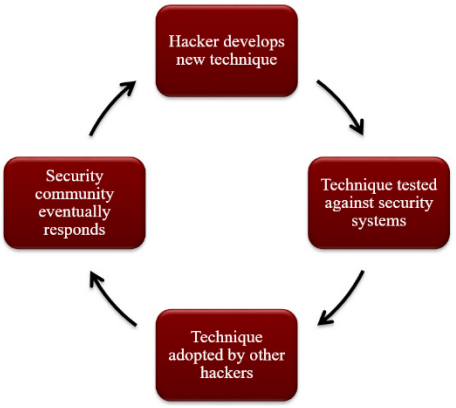

Fig. 1: Reactive approach cycle

interaction of attackers and cyber system in an analytical framework to forecast cyber-attacks is challenging and complicated. Moreover, computational complexity of analyzing such a model is another challenge that should be taken into account.

This research introduces a novel approach to address manufacturing cyber physical security issues by forecasting likelihood of possible attacks and analyzing them to obtain best defense policy using game theory to model behavior of the system in the presence of potential threats.

The remainder of this paper is organized as follows. Section 2 discusses related work in the field of vulnerability assessment and relevant commercial tools for cyber-physical systems. Section 3 consists of two components of cyber-attack forecasting; modeling of a manufacturing system and analyzing the model using game theory approach. In Section 4, a case study is illustrated for further understanding of the model, and finally, Section 5 concludes this paper by summarizing its main contributions and highlights possible future work to be undertaken to further improve the performance and the usability of the model.

2. Literature Review

2.1. Cybersecurity in manufacturing

Cybersecurity concerns in manufacturing areas as a type of cyber-physical systems have increased as a result of integration with internet network and also the introduction of the internet of things (IoT) and software as a service (SaaS) into the manufacturing

world. Recent incidents demonstrate the impact of these cybersecurity threats.

One of the oldest known attacks on cyber-physical systems is the logic bomb which affected gas pipeline infrastructure in Siberia and caused an explosion in 1982 [10]. However, the most well-known incident in recent years is the attack on the Iranian uranium enrichment facilities between 2009 and 2010. According to the Institute for Science and International Security report [11], the Stuxnet virus was responsible for destroying about 1,000 centrifuges in the Fuel Enrichment Plant at Natanz. Another recent example is the effort of hackers to infect the industrial control system of an unnamed steel company in Germany [12]. As the result, the system could not shut down the furnace blast and caused serious damage to the company.

Even though in the aforementioned incidents, infection of industrial control systems was the critical point, they are not the only vulnerability in manufacturing systems. Some studies demonstrate the risk of producing flawed parts under cyber-attacks. Wells et al. [13] mention some specific characteristics of manufacturing systems and their difference with other cyber-physical systems and highlight the importance of having specifically designed tools for cybersecurity issues in manufacturing systems. Sturm et al. [14] focus on the vulnerabilities of additive manufacturing (AM), one of the most trending type of manufacturing procedure, and emphasize its weaknesses in using STL files during the process. Another research on additive manufacturing by Zeltmann et al. [15] demonstrate the significant effect of alteration of printing orientation in the mechanical behavior of the specimens in AM as a result of cyber-attack while all specimens look identical.

DeSmit et al. [16] proposed an approach for assessing vulnerabilities of cyber-physical systems in manufacturing areas. They suggest that the intersection of main elements of manufacturing systems including cyber, physical, cyber-physical, and human are vulnerable, and then by evaluating the characteristics of these intersections assess the vulnerabilities of the system.

Moreover, the security challenges of Supervisory Control and Data Acquisition (SCADA) systems that has been highly utilized in advance manufacturing systems in recent decades [17] as well as other critical national infrastructure like communication, energy, transportation, water, and power have been studied in several research [18, 19]. Ten et al. [19] proposed a vulnerability assessment framework for SCADA systems and demonstrate the impact of cybersecurity intrusion in power systems.

While most of the researchers focus on identifying vulnerabilities and risks in manufacturing systems, Vincent et al. [20] suggest a real-time detection method to compensate the imperfection and weaknesses of quality control systems, using the side-channel scheme to detect Trojans (alien melodious logic) attacks. Mainly, in the above-described studies, the research objectives are relatively limited into the qualitative analysis rather than quantitative methods to address aforementioned threats. For this reason, a game theory solution is proposed to deal with this problems.

2.2. Application of Game Theory in Cybersecurity

The lack of quantitative decision-making method is the main shortcoming in traditional solutions for network security. At present, game theory has been utilized in dealing with the cyber-security issues, and a few researches have been conducted utilizing game theory approach to address this weakness [21–23]. This method mainly focuses on finding the optimal defense strategy to encounter cyber threats.

The optimal defense strategy could be used to design an optimal controller for cyber-physical systems under attack. Niu and Jagannathan [24] use the game theory approach to find an optimal defense strategy and then design a controller for cyber-physical systems under attack while cyber section and physical section of the system could affect each other mutually. Zhu and Martinez [25] also model a coupled decision-making process as a two-level receding-horizon Stackelberg game with rational players whose strategies are highly correlated with the control system operator.

Sallhammar et al [26] present a two-player stochastic zero-sum game model as a mathematical tool to predict the behavior of attackers in computer networks, considering attacker and security mechanism as the two players of the game. In another research [27], the same approach is applied to provide operational tools to measure the trustworthiness of a system, regardless of causes of failure. In fact, the authors use optimal strategy for attackers as probabilities of expected attacker behavior for the transition between states in a Markov Chain Model.

In conclusion, to the best knowledge of the authors, even though game theory approach has been used to identify best defense strategy in cyber physical systems, no effort has been reported in the literature in developing a game theory framework specifically for manufacturing systems. The main barrier creating such a framework is to have a realistic payoff function (see section 3) considering specific characteristics of the manufacturing systems and understanding how cybersecurity threats could affect these systems. To find the Nash equilibrium (also see Section 3) and optimal strategies of the players, tools such as value iterations to solve Markov decision processes (MDP) [28], minimax-Q [29], and Q-learning [24] were applied.

3. Cyber-Attackers' Behavior Forecasting

In this section, the premise of game theory is identified to aid the understanding of the games and later use it to model the manufacturing system to forecast cyber-attacks. Game theory illustrates the interaction between several decision makers where each one can choose various actions that result differently. The players try to choose the best possible actions to increase their possible rewards while anticipating actions from other rational players.

Nomenclature

π	Probability of attack
φ	Probability of defense
Γ	Game value, payoff matrix
D	Set of strategies for the defense
A	Set of actions for attacker
n	Number of action types for attacker
m	Number of defense strategies
E	Matrix of effectiveness
s	Cost of implementing and maintaining
S	Matrix of spending
G	Matrix of gain
p	Rate of the loss in production for each type of attacks
P	Matrix of production lost
r	Cost of recovery from each type of attacks
R	Matrix of cost of recovery
T	Total production

In cybersecurity, since there are two decision makers, defender and attacker, and one of the purposes is to predict likely behavior of attacker in order to make good decision for defending the system against cyber-attack, the game theory could be utilized. Game theory provides a mathematical decision framework to model cyber-physical system regardless of the complexity of interaction among attacker and defender. Moreover, it helps analyzing this interaction between decision makers and predict the likely actions of an adversary and recommend appropriate actions to defend.

To forecast cyber-attack in a manufacturing system, two tasks have to be fulfilled. First the system should be modeled using its characteristic regarding cybersecurity and then, game theory approach is utilized to analyze the model and understand the likely behaviors of attacker and their consequences on the system in the long run to find the best response from the defender's standpoint.

3.1 Modeling a Manufacturing System

To model any relation or competition as a game, three elements are needed: players, actions for each player, and payoff matrix [30]. A player is a basic entity in a game that is tasked with making choices for actions. A player can represent a person, machine, or group of people within a game. An action constitutes a move in the given game. And finally, the payoff is the positive or negative reward to a player for a given action within the game [21]. So, to form the model as a game the following elements needs to identify:

Players: In this paper, two players are considered as the decision maker; attacker and defender. Attacker can be a group of human individuals, governments or organizations [31] which benefits from harming a manufacturing system. On the other side, defender is a system or an organization that utilize countermeasures to defend the system and reduce the harms of an attack.

Action sets: The next step to form the game is to construct the sets of actions for each of the players. The actions for the defender are the all possible defense mechanism and is shown as $D = \{d_1, d_2, \dots, d_m\}$ where m is the number of available mechanism. On the other side, all malicious actions that could harm vulnerabilities in a manufacturing system are considered as the action set for the attacker and shown as $A = \{a_1, a_2, \dots, a_n\}$ where n is the number of vulnerabilities in the system.

Reward function (payoff matrix): to model the attackers' motivation, a reward and cost concept is used which assign values (γ_{ij}) to each combination of attack and defensive actions. This function could be shown as a $n \times m$ matrix when it is a two-players game

in which row player is the attacker and column player is the defender.

$$\Gamma = \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1m} \\ \vdots & \ddots & \vdots \\ \gamma_{nm} & \cdots & \gamma_{nm} \end{bmatrix} \quad (1)$$

Reward and cost are generic concepts, which can be used to quantify the payoff of the actions in terms of both abstract values, such as social status and satisfaction versus disrespect and disappointment, as well as real values, e.g. financial gain and loss. For instance, in [32] the reward of a successful attack action is the expected amount of recovery effort required from the system administrator and in [33] the reward is the degree of bandwidth occupied by a DDoS attack. In contrast to [32] and [33, 27] uses the cost as an alternative outcome of the game to represent the fact that risk averse attackers may sometimes refrain from certain attack actions due to the possible consequences of detection.

In this research, the game is considered as a zero-sum game which means the attacker objective inverse of the defender. In other words, if the attacker and the defender use action i and j respectively, (γ_{ij}) is the amount that attacker gains, and the defender at the same time loses the same amount. Now to form the reward function, the characteristic of the manufacturing systems regarding cybersecurity are considered.

$$\gamma_{\mathrm{ij}} = s_j - \left(s_i \times e_{ij}\right) + \mathrm{T} \times p_i \times \left(1 - e_{ij}\right) + r_i \times \left(1 - e_{ij}\right), \quad \forall\, \mathrm{i,\ j} \quad (2)$$

The reward function consists of three parts: maintenance cost of a defense mechanism, cost of production loss, and cost of recovery for the system to its initial good state from an attack.

The first two elements of the function is regarding of the maintenance cost of defense mechanism. Let $s=\{s_1, s_2, \ldots, s_m\}$ be the set that includes the cost of implementing and maintaining each of the defense strategies. Looking at the function from game theory's perspective, when a defense mechanism is effective there should not be a positive amount on that element. So, for each function element, costs that are not effective is the gain for the attacker.

Each defense mechanism could be effective either fully or partially for one or more attack actions and could be described as a matrix (equation 3). In this matrix if the element e_{ij} is equal to 1, it means that the defense strategy j is fully effective to prevent action i by the attacker. On the other hand, if the element is equal to 0, it means that the effectiveness of defense j to prevent the action i is zero and it cannot be considered as a strategy to defend for action i from the attacker. Therefore, the bigger number in each element, the bigger effect it could have to prevent a specific type of attack.

$$E = \begin{matrix} \\ a_1 \\ \vdots \\ a_n \end{matrix} \begin{matrix} \begin{matrix} d_1 & \ldots & d_m \end{matrix} \\ \begin{bmatrix} e_{11} & \cdots & e_{1m} \\ \vdots & \ddots & \vdots \\ e_{n1} & \cdots & e_{nm} \end{bmatrix} \end{matrix} \quad , 0 \le e_{ij} \le 1 \quad (3)$$

The third element of reward function is related to amount of money that a manufacturer would lose due to an attack. In manufacturing systems the most important attributes are integrity, availability, and consistency of the production, and one of the main purposes of any attacker is to disturb it. if T is total production and p_i is the rate of the loss in production for attack type i that can be shown as $p = \{p_1, p_2, \ldots, p_n\}$, $0 \le p \le 1$, by multiplying total production and rate of the loss with ineffectiveness of different mechanism, the production loss considering all types of defense mechanism due to different attack action is calculated.

The last part of the reward function is constructed by the recovery cost of an attacked manufacturing system and bring it back to its good state assuming that the recovery costs could be described as a set $r = \{r_1, r_2, \ldots, r_n\}$, in which each one demonstrates the recovery cost due to a specific attack.

Strategies: likelihood of attack which is the probability of using different actions for each of the players in a mixed strategy game called strategy of the players that for the attacker is shown as $\pi(a_i) = \{ \pi(a_1), \pi(a_2), \ldots, \pi(a_n)\}$, and for the defender is $\varphi(d_j) = \{ \varphi(d_1), \varphi(d_2), \ldots, \varphi(d_m)\}$. If a player always chooses only one of the actions, that means the probability of that action is one hundred percent and this game called pure strategy (saddle points). This could be interpreted as what might happen in repeated play or could be described as the population dynamics that means each players chosen from a population in which all have deterministic strategies.

$$\sum_{i=1}^{n} \pi(a_i) = 1, \qquad \sum_{j=1}^{m} \varphi\left(d_j\right) = 1 \quad (4)$$

Global utility (game value): in mixed strategy games global utility illustrates the trustworthiness of a system. It represents the amount of the reward or gain for the players in the long run, and it is defined as the

sum of probability that attacker and defender play *i* and *j* respectfully (likelihood of actions), multiplied by according element of reward function.

$$U\left(\pi(a_i), \varphi(d_j)\right) = \sum_{j=1}^{m} \sum_{i=1}^{n} \pi(a_i)\varphi(d_j)\gamma_{ij} \quad (5)$$

The game is considered as stochastic zero-sum game with rational players and complete information. The rationality means each players is trying to maximize their global utility and as the result they choose actions with better payoff considering the other players' behavior. Moreover, complete information means both players know about the consequence (reward) of each action.

3.2 *Analyzing the Model Using Game Theoretic Methods*

Having the model, to solve and analyze this model, it is formulated as a general optimization problem. In this problem each of the decision makers try to increase their own payoff by alternating actions. However, since the game is defined as a zero-sum, for the defender increasing the payoff is to minimize the damage.

To formulate this behavior of the players as an optimization problem minimax function is utilized. From the defenders standpoint since the attacker tries to increase his payoff, the defender should minimize the maximum payoff which could be gained by the attacker.

$$U^* = \min_{\varphi} \max_{\pi} U_{ij}(\pi(a_i), \varphi(d_j), \gamma_{ij}) \quad (6)$$

According to the Nash theorem, every finite game has an equilibrium called Nash equilibrium [34] and there is always at least a point in which each players cannot enhance their payoff further. This status, *U**, is called optimal mixed strategy and happens when the game reaches to its Nash Equilibrium. Feasible constraint is applied based on the definition to solve the game and can be expressed as follows.

$$U^* \geq U\ ,\ \forall\, U, \pi, \varphi \quad (7)$$

However, solving a two-player game is difficult when the order of the payoff matrix is more than three for each of the players (m≥3, n≥3). Neumann [35] for the first time discovered the connection of the game with linear programing. Moreover, Neumann and Morgenstern [36] proved that mixed strategy must exist for two-player zero-sum games.

So, to solve the game, it is formulated as a linear program, which is computationally more efficient to solve the problem. The model is converted to two sets of linear program to find the optimal mixed strategy.

$$\min \sum_i \pi_i$$
$$\begin{cases} \sum_i \gamma_{ij}\pi_i \geq 1 & (i = 1,2 \dots, n) \\ \pi_i \geq 0 & (j = 1,2 \dots, m) \end{cases} \quad (8)$$

and

$$\max \sum_j \varphi_j$$
$$\begin{cases} \sum_i \gamma_{ij}\varphi_j \leq 1 & (i = 1,2 \dots, n) \\ \varphi_j \geq 0 & (j = 1,2 \dots, m) \end{cases} \quad (9)$$

The optimization toolbox of the MATLAB is utilized to find the results. To further understand solving two-players zero-sum game by MATLAB the readers refer to [37].

To find the best strategy to defend the system, all combinations of defense mechanism should be considered. The total number of the combinations is $2^m - 1$where m is the number of available defense mechanism. Then by comparing the global utility of optimal mixed strategies for each combination and compare it with the maintenance cost of them, the best combination could be decided.

4. Numerical case study

In this section, a numerical example is presented to further illustrate the approach introduced in the previous section. A manufacturing system will be analyzed to find the optimal defense strategy to encounter cyber threats by incorporating effectiveness of strategies, production losses, recovery cost, and maintenance cost of defense mechanism.

Based on the model explained in the previous section, the manufacturing system encounters four different types of attack regarding the vulnerabilities discussed in introduction and literature review, $A = \{a_1, a_2, a_3, a_4\}$ = *{theft of intellectual properties, hacking employee log-in credentials, infecting control systems, corruption of products}*, [8], [9]. To encounter the aforementioned threats, five potential mechanism

is considered to defend which is set $D = \{d_1, d_2, d_3, d_4, d_5\}$ in which the last one is doing nothing.

Maintaining these defense strategies incurs cost, $s = \{3, 50, 10, 300, 0\}$, respectively. Moreover, the production loss rate according to each attack action is $p = \{0.5, 0.1, 0.7, 1\}$, while the total production (T) is assumed to be 1000. If attacks are successful, the cost of recovery to bring back the system to its initial state is $r = \{15, 20, 100, 300\}$.

Furthermore, the matrix of effectiveness which describes the behavior of each defense mechanism encountering any of the actions is assumed as follows:

$$E = \begin{bmatrix} 1 & 0.1 & 0 & 0 & 0 \\ 0.98 & 0.5 & 0 & 0 & 0 \\ 0 & 0.3 & 0.98 & 0.8 & 0 \\ 0 & 0.92 & 0.7 & 0.98 & 0 \end{bmatrix} \quad (10)$$

Putting all variables into equation (2), the payoff matrix could be obtained.

$$\Gamma = \begin{bmatrix} 0 & 103.5 & 75 & 365 & 65 \\ 2.46 & 85 & 130 & 420 & 120 \\ 803 & 595 & 16.2 & 220 & 800 \\ 1303 & 108 & 393 & 32 & 1300 \end{bmatrix} \quad (11)$$

Having five defense policies, there are 31 (2^5-1) possible combinations as shown in table 1 in which each one should be solved and analyzed separately. As mentioned in previous section, to find the Nash equilibrium and optimal strategy for each combination, minimax optimization method is used. Then, the problem is defined as a linear programming and is solved by optimization toolbox in MATLAB.

As an example, if all of the defense mechanisms are considered, it can be seen that the game has no saddle point which means the players are going to alternate their choices to gain a better outcome. The global utility (game value) is 212.719, while the optimal strategies for each players are $\pi = \{0, 0.35, 0.23, 0.41\}$ and $\varphi = \{0, 0.21, 0.45, 0.32, 0\}$ for the attacker and the defender respectively.

Table 1 includes all of the combinations of defense strategies and demonstrates the global utilization for each row which is obtained by solving the optimization problem for that combination along with the maintenance cost for that strategies.

In general, it could be said the lower global utility with low maintenance cost is the better, but finding the best strategy is very dependent on company policies on what the best strategy is. For instance, for a big company with the continuous production line, the minimums losses (smaller global utility) in the long run could be a critical point to decide; while for a small or medium size company with batch production the maintenance cost could be the deciding point.

Table 1. The payoff values vs. maintaining costs for all combinations of defense strategies

d1	d2	d3	d4	d5	Global Utility	Maintaining Cost
0	1	1	1	0	213	360
0	1	1	1	1	213	360
1	1	1	1	0	213	363
1	1	1	1	1	213	363
0	0	1	1	0	247	310
0	0	1	1	1	247	310
1	0	1	1	0	247	313
1	0	1	1	1	247	313
0	1	1	0	0	269	60
0	1	1	0	1	269	60
1	1	1	0	0	269	63
1	1	1	0	1	269	63
0	1	0	1	0	326	350
0	1	0	1	1	326	350
1	1	0	1	0	326	353
1	1	0	1	1	326	353
1	0	0	1	0	337	303
1	0	0	1	1	337	303
0	0	0	1	1	352	300
0	0	1	0	0	393	10
0	0	1	0	1	393	10
1	0	1	0	0	393	13
1	0	1	0	1	393	13
0	0	0	1	0	420	300
0	1	0	0	0	595	50
0	1	0	0	1	595	50
1	1	0	0	0	595	53
1	1	0	0	1	595	53
0	0	0	0	1	1300	0
1	0	0	0	1	1300	3
1	0	0	0	0	1303	3

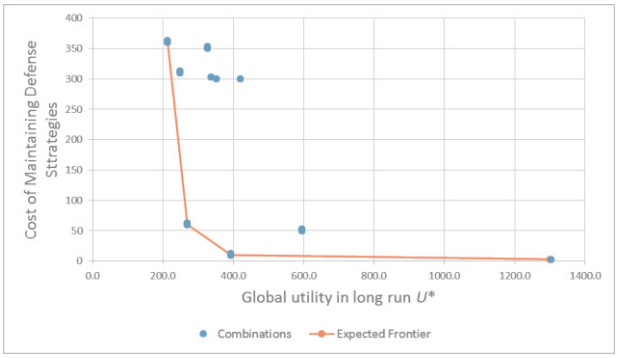

Fig. 2. Payoff from an attack in long time vs. cost of maintaining strategies

In figure 2 also, global utilities and maintenance costs are compared in which each point represents one of the combinations of defense mechanism. As can be seen in this diagram, the expected frontier line shows the limit of optimal strategies in which when the maintenance cost is at minimum amount the damage in the system (global utility) is at the maximum and vice versa. However, there are some points that both the maintenance cost and the global utility are relatively low. In other words, it can be said since the likelihood of different attack actions (attacker's strategy) could be predicted through game theory approach, expensive defense mechanism is not optimal to implement and keep when the likelihood of that attack action is low.

5. Conclusion and future work

The results of this study show that the game theory approach could apply to manufacturing domain to measure the trustworthiness of a system under cyber threats and analyze the different defense policies to encounter these attacks. This approach also provides a proper representation that characterizes the interplay between attackers and the defender in manufacturing areas to assist decision-making process for finding optimal defense strategy.

Moreover, three characteristics of manufacturing systems, i.e., cost of maintaining of a defense mechanism, cost of production losses due to an attack, and cost of recovery from an attack, were identified as the decision making base elements to form the payoff function and evaluate defending policies against cyber-attacks. Then the minimax method was used to calculate the Nash equilibrium and global utility. According to the definition of the game and the payoff matrix which was identified from attacker's perspective, the less the game value is the better, however, not always the minimum game value is the best since the cost of maintenance defense policies should be taken into the consideration.

Furthermore, a numerical case study was presented to further illustrate the proposed method. As seen, the optimal strategy could be different from the one with the lowest game value since the maintenance cost of a strategy could affect the decision-making process.

The first area identified for the future work is considering normal form games (non-zero-sum) with imperfect knowledge and irrational players. The approach in this paper only considered attacker and defender in the sense that they have perfect knowledge about each other's payoff regarding every one of their actions, while in reality of the cybersecurity it is not the case most of the times. Also, categorizing cybersecurity as a zero-sum game while the motivation behind each of the players' action could be different is just to simplify the calculation. In another word, the gain of the attackers is not necessarily the same as the defender's losses, hence the game should be considered as a non-zero-sum game.

Another aspect to investigate in future works is the effect of the initial cost of investment to implement a defense policy. This aspect could only be considered when the timeframe of the game has been taken into account as well since the effect of constant initial investment cost could be ignored in long run, while in short span of time it is a critical point for deciding the optimal strategy.

Finally, other methods to calculate the optimal strategy from the game such as Q-learning and quantal response equilibrium (QRE) which could reveal more information about the game could be considered if the initial condition of the game is different. Moreover, simulation of the system under cyber threats with all its cyber and physical manufacturing components and considering attackers and defender as players of the game would broaden our understanding of the system with similar circumstances.

References

[1] G. Adamson, L. Wang, M. Holm, and P. Moore, "Cloud manufacturing–a critical review of recent development and future trends," *Int. J. Comput. Integr. Manuf.*, vol. 30, no. 4–5, pp. 347–380, 2017.

[2] D. Wu, D. W. Rosen, L. Wang, and D. Schaefer, "Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation," *Comput.-Aided Des.*, vol. 59, pp. 1–14, 2015.

[3] M. Helu and T. Hedberg, "Enabling smart manufacturing research and development using a product lifecycle test bed," *Procedia Manuf.*, vol. 1, pp. 86–97, 2015.
[4] J. Lee, E. Lapira, B. Bagheri, and H. Kao, "Recent advances and trends in predictive manufacturing systems in big data environment," *Manuf. Lett.*, vol. 1, no. 1, pp. 38–41, Oct. 2013.
[5] I. Horváth and R. W. Vroom, "Ubiquitous computer aided design: A broken promise or a Sleeping Beauty?," *Comput.-Aided Des.*, vol. 59, pp. 161–175, 2015.
[6] L. Kung, C. G. Cegielski, and H.-J. Kung, "An integrated environmental perspective on software as a service adoption in manufacturing and retail firms," *J. Inf. Technol.*, vol. 30, no. 4, pp. 352–363, 2015.
[7] "2017 DBIR: Understand Your Cybersecurity Threats," *Verizon Enterprise Solutions*. [Online]. Available: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.
[8] "Cyber risk in advanced manufacturing | Deloitte US," *Deloitte United States*. [Online]. Available: https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html.
[9] "Manufacturing - Cyber Executive Briefing | Deloitte | Analysis," *Deloitte Belgium*. [Online]. Available: https://www2.deloitte.com/be/en/pages/risk/articles/Manufacturing.html.
[10] A. A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems.," in *HotSec*, 2008.
[11] D. Albright, P. Brannan, and C. Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? | Institute for Science and International Security." [Online]. Available: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.
[12] "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *WIRED*. [Online]. Available: https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[13] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manuf. Lett.*, vol. 2, no. 2, pp. 74–77, 2014.
[14] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects," *J. Manuf. Syst.*, vol. 44, pp. 154–164, 2017.
[15] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3D printing," *Jom*, vol. 68, no. 7, pp. 1872–1881, 2016.
[16] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical vulnerability assessment in manufacturing systems," *Procedia Manuf.*, vol. 5, pp. 1060–1074, 2016.
[17] N. B. Portilla, M. H. de Queiroz, and J. E. Cury, "Integration of supervisory control with SCADA system for a flexible manufacturing cell," in *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*, 2014, pp. 261–266.
[18] B. Zhu, A. Joseph, and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 380–388.
[19] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, 2008.
[20] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," *Procedia Manuf.*, vol. 1, pp. 77–85, 2015.
[21] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010, pp. 1–10.
[22] S. Shiva, S. Roy, and D. Dasgupta, "Game theory for cyber security," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 2010, p. 34.
[23] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Game theory meets information security management," in *IFIP International Information Security Conference*, 2014, pp. 15–29.
[24] H. Niu and S. Jagannathan, "Optimal defense and control of dynamic systems modeled as cyber-physical systems," *J. Def. Model. Simul.*, vol. 12, no. 4, pp. 423–438, 2015.
[25] M. Zhu and S. Martinez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in *American Control Conference (ACC), 2011*, 2011, pp. 4063–4068.
[26] K. Sallhammar, S. J. Knapskog, and B. E. Helvik, "Using stochastic game theory to compute the expected behavior of attackers," in *Applications and the Internet Workshops, 2005. Saint Workshops 2005. The 2005 Symposium on*, 2005, pp. 102–105.
[27] K. Sallhammar, B. E. Helvik, and S. J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, 2006, p. 8–pp.
[28] K. Etessami and M. Yannakakis, "Recursive Markov Decision Processes and Recursive Stochastic Games," *J ACM*, vol. 62, no. 2, p. 11:1–11:69, May 2015.
[29] M. L. Littman, "Markov games as a framework for multi-agent reinforcement learning," in *Proceedings of the eleventh international conference on machine learning*, 1994, vol. 157, pp. 157–163.
[30] G. Owen, *Game theory. 1995*. Academic Press.
[31] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on future directions in cyber-physical systems security*, 2009, vol. 5.
[32] K. Lye and J. M. Wing, "Game strategies in network security," *Int. J. Inf. Secur.*, vol. 4, no. 1–2, pp. 71–86, 2005.
[33] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Trans. Inf. Syst. Secur. TISSEC*, vol. 8, no. 1, pp. 78–118, 2005.
[34] J. Nash, "Non-cooperative games," *Ann. Math.*, pp. 286–295, 1951.
[35] J. Von Neumann and O. Morgenstern, "Theory of games and economic behavior, 2nd rev," 1947.
[36] P. K. Dutta, *Strategies and games: theory and practice*. MIT press, 1999.

[37] Y. M. Yang, Y. Guo, L. C. Feng, and J. Y. Di, "Solving two-person zero-sum game by Matlab," in *Applied Mechanics and Materials*, 2011, vol. 50, pp. 262–265.