A Non-Cooperative Game based Model for the Cybersecurity of Autonomous Systems

Farha Jahan*, Weiqing Sun*, and Quamar Niyaz†
*College of Engineering, The University of Toledo, Toledo, OH 43606, USA
†College of Engineering and Sciences, Purdue University Northwest, Hammond, IN 46323, USA
farha.jahan@rockets.utoledo.edu, weiqing.sun@utoledo.edu, qniyaz@pnw.edu

***Abstract*—Autonomous systems (AS) would soon revolutionize the way we live and work. The days are not so far when these systems, from delivery drones to driverless cars, would be seen around us. These systems are connected and rely heavily on the communication network for the information exchange, hence prone to several attacks. Human lives will be at risk if these systems are compromised. Cybersecurity modeling and attack analysis of AS needs the utmost attention of the research community. Primarily, a typical AS has three modules – perception, cognition, and control – and each one of them comes with their own vulnerabilities. In this work, we propose a new AS architecture that may prove useful in AS cybersecurity modeling. We also model the attacks on them, and defense mechanisms applied to these modules using a non-cooperative non-zero sum game. Finally, we solve this game to obtain optimal strategies to maintain a secure system state.**

***Index Terms*—autonomous systems, cybersecurity, game theory, Nash Equilibrium**

I. Introduction

The world is progressing towards the era of AS. Autonomous operations with voluminous data processing, integrated AI, and high definition imaging would develop new areas of applications for UAVs (Unmanned Autonomous Vehicles) that would change the outlook of this booming industry. These AS would increase efficiency and task productivity with improved safety in work environments. For example, any accident investigation that could manually take three hours to collect information could be done in less than an hour using a drone, reducing the traffic delays and saving time and money [1]. The driverless cars are estimated to save around millions of lives worldwide by avoiding accidents caused by human errors [2]. As the level of autonomy of these systems moves towards full automation, attack vectors and their impact would increase as well, which may result in deadly consequences [3]. Attacks with increased complexity are on the rise in recent days. It is critical to consider the security of these systems and explore the solutions thereby. Also, the research community lacks generalized modeling of cyberattacks on AS. One approach could be to apply game theory in this regard [4].

The main contributions of this paper are multi-fold. First, we model a generalized AS architecture based on common modules of AS such as a driverless car, robot, and drones. An attack on an autonomous system can be on any of its modules, and, based on the defensive measures, the impact would vary accordingly. Second, we propose a strategic *non-cooperative non-zero sum* game for modeling attacks on an AS to numerically compute the mixed strategies that achieve the Nash Equilibrium (NE) and the expected payoffs of the players. The AS would act as a defender while an adversary could be an individual attacker, a network node, or another AS. A game-theoretic framework can be used to analyze the system's response and payoffs for both the players in an attack situation when certain measures are in action. Third, we have taken into account the probability of a successful attack in defense and no defense scenarios and the cost of damage in our computation. In addition, we consider the game as a 'non-zero sum', which maps to the real world more realistically than the works of [5], [6]. Fourth, we extend the works in [7] to a $n \times n$ bimatrix game represented in a normal form. This method is easier than the algebraic/differential method to calculate the mixed strategies of $n \times n$ games where $n > 2$. Although various works have analyzed the threat and attack modeling of these systems individually, the research community lacks a generalized security modeling of these systems. Also, Section II discuss various cyber attack-defense game, but to the best of our knowledge, none has proposed a game related to the security of the autonomous system.

The rest of the paper is organized as follows. A summary of related work is provided in Section II. In Section III, we discuss the high-level architecture of an AS. The architecture will give us an idea to design the game, proposed in Section IV for which we evaluate the payoffs and Nash equilibrium. In Section V, we validate our approach through a case study. Finally, we conclude the paper in Section VI.

II. Related Work

Various game models have been applied in network security to model attacks as well as propose secure design or operation for specific cyber-physical systems (CPS). However, there are limited works that attempt to address the cybersecurity issue of AS. An early work from 2015 developed a game-based security framework for multi-agent AS [8]. The work leverages the cyber-physical nature of AS to formulate a min-max model-based predictive control (MPC) problem and proposes a dynamic signaling game model to solve it. Another relevant work in 2018 applied a robust deep reinforcement learning (DRL) model in combination with long-short term memory (LSTM) and game theory for security and safety in autonomous vehicle systems [9]. Several works have attempted to apply game theory principles to secure design, operation,

DOI 10.1109/SPW50608.2020.00049

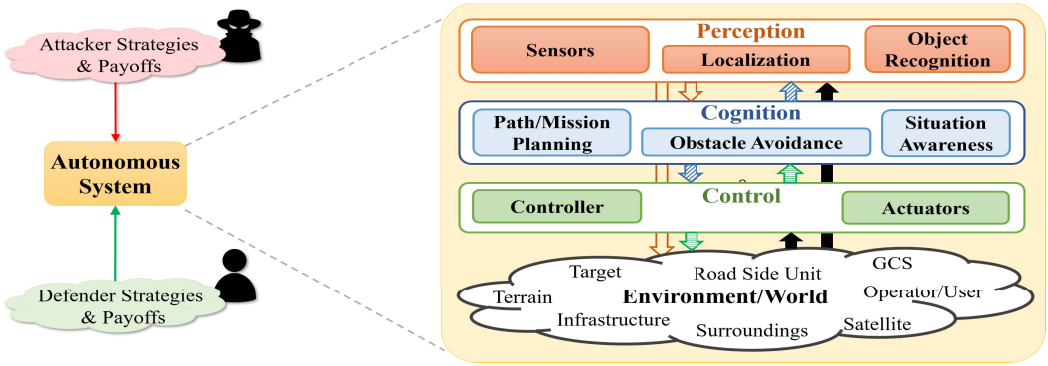

Fig. 1. Autonomous System Game Model and Architecture

or control of CPS, not necessarily, autonomous. Such CPSs include train control system [10], drone delivery system [11], and smart grid [12]. The application domain where game theory has been applied most is the security of computer networks. The nature of the computer network makes it more attractive to apply the game theory that may result in higher payoffs. In the past decade, several works have focused on modeling, design, simulation, and analysis of game-theory based defense mechanisms to protect (i) computer networks against DoS/DDoS attacks [13], [14], (ii) software-defined networks (SDN), Cloud or IoT environments [15], [16], and (iii) wireless sensor networks against intrusions [17]. A notable recent work attempts to propose a non-cooperative zero-sum attacker-defender dynamic game that allows players to choose between 3 levels of actions (No action, low-intensity action, high-intensity action) [5].

III. Autonomous System (AS) Architecture

It is essential to understand the high-level architecture of an AS and the functions of each module [18] before we move to the design and instructions of the game. In [19], Berntorp et al. gave a high-level control architecture of autonomous vehicles, which includes motion planning, vehicle control, and actuator control along with sensing and mapping as major blocks. Petnga et al. discuss a high-level architecture of a UAV reflecting the interactions between cyber (command, control, communication) and physical (sensors and actuators) components of these systems [20]. Based on these studies, we identify three major modules common to popular AS i) perception, ii) cognition, and iii) control. Fig. 1 shows a high-level architecture of an AS.

An AS senses the environment through sensors that act as eyes/ears for the AS. The *perception* module combines data from various sensors to create a picture of the environment through a sophisticated algorithm. As discussed in [21], there are two types of sensors: Exteroceptive and Proprioceptive sensors. Exteroceptive sensors are those that give information about robot workspaces like LASERs, LiDAR, and cameras. Proprioceptive sensors are those that measure value internally to the system, such as compass, gyroscope, potentiometers. The sensors have private information about the owner or the status of the machine itself, hence poses high-security risks if the system gets compromised. The sensor data fusion not only helps in localization and grid mapping for navigation, but it also helps to detect dynamic objects and recognize them, such as pedestrians and traffic signs [22]. An attack on the perception of the AS would disrupt the understanding of its environment leading to wrong decision making [23].

Cognition is the ability of a system to make complex decisions based on the systems intelligence algorithms on the data it receives from the perception module and the hardware. An AS with a high-level of autonomy would have to make a more complex analysis of the data for mission planning with many unknown factors. It has to assess the complexity of the given task and the environment, level of autonomy, risks, costs, and the broader mission before making effective decisions [18]. For example, an autonomous vehicle would need to make judgments of the best route, be aware of its surroundings, and avoid collision to reach its destination. Also, the cognition module should perform a threat assessment to ensure the security of the system and detect any malicious activities. Application layer attacks such as GPS jamming/spoofing and Sybil attacks may cause the system to make erroneous decisions [24].

Control can be described as the ability of the AS to execute the decisions made by the cognition module through physical or digital means [18]. In 2015, A remote attack on the actuators of Jeep Cherokee was launched that took over the controls of the steering wheel and brake systems [25]. Guo et al. proposed a mobile robot intrusion detection system for the detection of sensor and actuator attacks [26]. Hwang et al. modeled the attack and analyzed the security of the system for deception attack on sensors, actuators, or both [27].

The effects and consequences of cyberattacks on perception, cognition, or/and control module will vary with the system (driverless car, robot, U*X*Vs where X could be *air, underwater, or ground*) and subsystem (e.g., navigation, communication, network) under attack, the criticality of the mission, and the operating environment. For instance, an attack on a system designed for operation in a highly critical environment will

have more impact on the surroundings than on the one working in a relatively less critical environment. An attack on the navigation module of a Roomba vacuum cleaner wouldn't yield much to the attacker than on a UAV or a driverless car. However, it still may cause inconvenience to the owner, like cleaning the same area again and again or going in circles. The degree of autonomy may also vary based on the severity or motive of the cyber attack. The attack may even disconnect the user from the system or deny requests for support.

IV. Strategic Game Model

In this section, we introduce the autonomous system security game model, define the payoff functions based on the optimal actions for a given set of conditions of rational players and then, reach a state of equilibrium. Fig 1 shows the game model.

A. Autonomous System (AS) Security Game Representation

A **non-cooperative** game is one in which the players don't cooperate with each others' strategy. They try to bring down other player's payoff. It is a non-zero sum game as there would always be some loss to the defender. We represent the game using normal form and Nash equilibrium is reached. The security game model is represented by $\mathcal{G} =< \mathcal{N}, \mathcal{S}^{\mathrm{j}} | \mathrm{j} \in \mathcal{N}, \mathcal{U}^{\mathrm{j}} | \mathrm{j} \in \mathcal{N} >$ where $\mathcal{N}$ is the set of players $\{a, d\}$, $\mathcal{S}^{\mathrm{j}}$ is the strategy space and $\mathcal{U}^{\mathrm{j}}$ is the utility for $j \in N$. In an attack scenario, the players, their actions and the payoffs are discussed as follows.

1) Players: There are two players involved in this game; the attacker and the defender.

Attacker- An attacker could be a malicious individual/party, attack node(s) in the network, or another AS(s) who would benefit from the maximum damage caused by the attack to the target AS. There is a possibility that the attacker plans to attack more than one module simultaneously. The attacker action set would include no attack, attack on one or more modules.

Defender- The other player is called the defender whose actions would minimize the vulnerability of the system and take security measures in case of an attack. Such an entity would include system administrator, developer, or the system itself. Defender action set would include no defense, defense on one or more modules.

2) Strategy Space: Strategy space $\mathcal{S}^{\mathrm{t}} = \{S_i^t | t \in \mathcal{N}, i \in 1 \text{ to } z\}$ is the action set of all the possible strategies of the players, z is the sum of all possible combinations of attack/defense. For an autonomous system with three major modules, $n = 3$, there will be $z = ({}^3C_1 +^3 C_2 +^3 C_3)$ action strategies. The possible attack and defense strategies are enumerated in Table I. Each module is represented by 0s and 1s. For the attacker, 0 means no attack, and 1 means the system is under attack. Similarly, for defender 0 means no defense, and 1 means there is a defense on that module. For example, from an attacker's perspective, S_7^t indicates all the three modules are under attack, and from the defender's perspective, all the three modules have a defense mechanism.

TABLE I
Enumeration of Attack/Defense Strategies

Strategies	Perception (P)	Cognition (Cg)	Control (Cn)
S_1^t(P)	1	0	0
S_2^t(Cg)	0	1	0
S_3^t(Cn)	0	0	1
S_4^t(CgCn)	0	1	1
S_5^t(PCn)	1	0	1
S_6^t(PCg)	1	1	0
S_7^t (PCgCn)	1	1	1

TABLE II
Enumeration of Possible Cases of Attack and Defense

Case	Attack Status	Condition	Probability
0	no attack		
1	successful	$m_k \neq m_l$	p_k
2	unsuccessful	$m_k \neq m_l$	$1 - p_k$
3	successful	$m_k = m_l$	q_k
4	unsuccessful	$m_k = m_l$	$1 - q_k$

B. Payoff Calculation

In game theory, each strategy results in a payoff to the players. The security breach can result in loss of data, communication, or the system itself. The attacker would incur the cost of attacking. We denote the cost associated with implementing these attacks as C_A. The defender would employ strategies to block or mitigate the attacks. For example, AS would switch to Inertial Navigation System (INS) and other sensors if the navigation system is down. The cost incurred by the defender for implementing defending measures is denoted by C_D. The costs considered here are the monetary measure of the time, effort, or resources used. The damage or the impact incurred by the attack is represented by W.

The impact of a simple attack on a single module of an autonomous system could be high enough to cause a cascading failure effect, from few crashes to traffic jams, to loss of business and trust of the end-users. Such political, social, and environmental impacts of the attack are difficult to quantify and are beyond the scope of our work. For the sake of simplicity, we consider the economic value of the damage directly related to the defender.

Let p_k be the probability of a successful attack when no defense has been applied on that module, i.e, $m_k \neq m_l$ where $0 < k \leqslant n, 0 < l \leqslant n$, m_k, m_l represents the modules that the attacker decides to attack and the defender decides to defend, respectively. And q_k be the probability of a successful attack when the defensive measures are active, i.e., $m_k = m_l$. Table II enumerates all the possible scenarios of an attack which should be taken into account when calculating the damage caused by the attack. Case 1 indicates that the module that was attacked, was not the one that was defended. This leaves the module in a vulnerable state and so there is a probability p_k that the attack was successful. And probability $1 - p_k$ the attacker was not successful in exploiting the vulnerability of the module. For case 3, the module that was attacked had defenses but failed to counter the attack with a probability q_k.

Let $a = 1$ represents 'attack successful' and $a = 0$ represents 'attack unsuccessful'. Therefore, for each module k, the probability of each case is given by:

$$b_k = \begin{cases} p_k, & \text{if } m_k \neq m_l, a = 1 \\ 1 - p_k, & \text{if } m_k \neq m_l, a = 0 \\ q_k, & \text{if } m_k = m_l, a = 1 \\ 1 - q_k, & \text{if } m_k = m_l, a = 0 \end{cases} \quad (1)$$

Let C_k be the cost of damage incurred by the module that was successfully attacked. When attack was unsuccessful (a=0), $C_k = 0$ as there is no loss or damage of the property. Suppose, attacker plans strategy $S_4^a = \{0, 1, 1\}$ and defender plans $S_2^d = \{0, 1, 0\}$. Let s be an element of the set of all possible outcomes, $S = \{(H0, H3, H1), (H0, H3, H2), (H0, H4, H1), (H0, H4, H2)\}$ if the game of attack and defend is played, where H'X' indicates the cases from Table II. The total economic loss for the defender can be calculated as the summation over all possible outcomes, the product of the probabilities of each attacked module and total cost of damage [28]:

$$W_i = \sum_{s \in S} \left(\left(\prod_{k=1 | S_i^a(k)=1}^{n} b_k \right) \cdot \left(\sum_{k=1|a=1}^{n} C_k \right) \right) \quad (2)$$

We have not considered the situation of no attack and completely no defense, as this will yield zero payoffs to the attacker. If the attacker succeeds in his attack, he will cause damage to W to the defender. His payoff would benefit minus the cost of attack. If the defender has defending measures, the attack would cost him the amount of damage as well as the amount he spent on defending the system. The payoffs of both the players corresponding to the possible strategies of the attacker (S_i^a) and the defender(S_j^d) (refer to the Table I) for a **non-zero sum** is given by:

$$u_{ij} = -C_{Ai} + W_i, R_D - W_i - C_{Dj} \text{ if } 1 \leq i, j \leq z \quad (3)$$

where, R_D is the total cost of the modules, C_{Ai} is the sum of cost of attack on individual modules ($\sum_{k=1}^{n} C_{Ak}$) and C_{Dj} is the sum of cost of defense on individual modules ($\sum_{k=1}^{n} C_{Dk}$). In case the attack is unsuccessful, from equation (2), $W_i = 0$.

Based on eqn(3), Table III shows the 3x3 ordered pair of payoff matrices [A, D] for a non-cooperative non-zero-sum bimatrix game for autonomous system in case the attacker attacks only one module at a time.

C. Nash Equilibrium Calculation

Let X be a set of all mixed strategies of the attacker which is reduced to a vector $x = (x_1, x_2, ..., x_z)$, satisfying

$$x_i > 0 \text{ and } \sum_{i=1}^{z} x_i = 1 \quad (4)$$

Similarly, let Y represent the set of defender's mixed strategies. For a bimatrix game $[A, B]$ where $A = [a_{ij}]$ and $D = [d_{ij}]$, if the attacker chooses the mixed strategy x and the defender chooses y, the expected payoff of the attacker and the defender would be

TABLE III
PAYOFF MATRICES FOR THE AS SECURITY GAME

Attacker/ Defender	S_1^d	S_2^d	S_3^d
S_1^a	$-C_{A1} + W_1$, $R_D - W_1 - C_{D1}$	$-C_{A1} + W_1$, $R_D - W_1 - C_{D2}$	$-C_{A1} + W_1$, $R_D - W_1 - C_{D3}$
S_2^a	$W_2 - C_{A2}$, $R_D - W_2 - C_{D1}$	$W_2 - C_{A2}$, $R_D - W_2 - C_{D2}$	$-C_{A2} + W_2$, $R_D - W_2 - C_{D3}$
S_3^a	$-C_{A3} + W_3$, $R_D - W_3 - C_{D1}$	$-C_{A3} + W_3$, $R_D - W_3 - C_{D2}$	$-C_{A3} + W_3$, $R_D - W_3 - C_{D3}$

$$A(x, y) = \sum_{i=1}^{z} \sum_{j=1}^{z} x_i y_j a_{ij}, D(x, y) = \sum_{i=1}^{z} \sum_{j=1}^{z} x_i y_j d_{ij} \quad (5)$$

As discussed in [7], if the expected payoff value of the attacker is $v(a)$, we have

$$x_1 y_1 a_{11} + x_1 y_2 a_{12} + ... + x_z y_z a_{zz} = v(a)$$

or,

$$\begin{gathered} x_1(y_1 a_{11} + y_2 a_{12} + ... + y_z a_{1z}) + \\ x_2(y_1 a_{12} + y_2 a_{22} + ... + y_z a_{2z}) + \\ \vdots \\ + x_z(y_1 a_{1z} + y_2 a_{z2} + ... + y_z a_{zz}) = v(a) \end{gathered}$$

For the above and equation 4 to hold simultaneously, the coefficients of x_i in the above equation must be $\leq v(a)$. Since $x_i > 0$, these coefficients must be equal to $v(a)$ for equation 4 to hold, as shown below:

$$\begin{gathered} x_1 v(a) + x_2 v(a) + ... + x_z v(a) = v(a) \\ v(a)(x_1 + x_2 + ... + x_z) = v(a) \\ x_1 + x_2 + ... + x_z = 1 \end{gathered}$$

Hence,

$$\begin{gathered} y_1 a_{11} + y_2 a_{12} + ... + y_z a_{1z} = v(a) \\ y_1 a_{12} + y_2 a_{22} + ... + y_z a_{2z} = v(a) \\ \vdots \\ y_1 a_{1z} + y_2 a_{z2} + ... + y_z a_{zz} = v(a) \end{gathered}$$

In matrix form, the above equation can be written as below where J is the z-vector (1,1, ..., 1)

$$Ay^T = \begin{pmatrix} v(a) \\ v(a) \\ \vdots \\ v(a) \end{pmatrix} = v(a). \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = v(a).J^T$$

We will have ,

$$y^T = v(a) A^{-1} J^T \quad (6)$$

Since, sum of the components of y, i.e., yJ^T must be 1 (or, $Jy^T = 1$), we can write,

$$v(a) J A^{-1} J^T = 1 \implies v(a) = \frac{1}{J A^{-1} J^T}$$

Therefore, substituting for v(a) in equation (6),

$$y^T = \frac{A^{-1}J^T}{JA^{-1}J^T} \tag{7}$$

Since, $A^{-1} = \frac{A^*}{|A|}$, y can be written as

$$y = (\frac{A^*J^T}{JA^*J^T})^T \tag{8}$$

Similarly, if the the expected payoff value of the defender is $v(d)$ We can see that

$$\begin{gathered} y_1(x_1d_{11} + x_2d_{12} + ... + x_zd_{1z}) + \\ y_2(x_1d_{12} + y_2d_{22} + ... + y_zd_{2z}) + \\ \vdots \\ +y_z(x_1d_{1z} + x_2d_{z2} + ... + x_zd_{zz}) = v(d) \end{gathered}$$

And since, $y_i > 0$ and $y1 + y2 + ... + y_z = 1$,

$$\begin{gathered} x_1d_{11} + x_2d_{12} + ... + x_zd_{1z} = v(d) \\ x_1d_{12} + y_2d_{22} + ... + y_zd_{2z} = v(d) \\ \vdots \\ x_1d_{1z} + x_2d_{z2} + ... + x_zd_{zz} = v(d) \end{gathered}$$

In matrix form, it can be written as

$$xD = (v(d), v(d), ..., v(d)) = v(d)J$$

We will have ,

$$x = v(d)JD^{-1} \tag{9}$$

On solving similarly, we get,

$$x = \frac{JD^*}{JD^*J^T} \tag{10}$$

Hence, for a $n \times n$ bimatrix game, the unique equilibrium strategies for the defender and the attacker are given by equations (8) and (10), respectively, and the expected payoffs of the players can be given by [7],

$$v(a) = \frac{|A|}{JA^*J^T}, v(d) = \frac{|D|}{JD^*J^T} \tag{11}$$

where A^*, D^* is the adjoint of A and D, $|A|, |D|$ is the determinant of A and D, respectively and J is a z-vector (1, 1, ..., 1)

V. Case Study

This section presents a case study to validate the applicability of the game proposed. We consider an autonomous system with the three modules and quantify the cost of the attacker and the defending action taken by the system, as shown in Table IV. Table V shows the payoff matrix of the game, taking the best-case scenario for the attacker where all his attacks are successful. Equation (3) calculates the payoffs of the players.

For both attacker/defender's strategy $S_1^{a/d} = \{1, 0, 0\}$, the possible outcomes are $\{\{H3, H0, H0\}, \{H4, H0, H0\}\}$. For this particular example, from table IV, the probability of a successful attack with defense is $q_k = 0$. Using equation (2),

TABLE IV
Quantification of actions for the AS Security Game

	Perception (module 1)	**Cognition (module 2)**	**Control (module 3)**
Attack Cost (C_{Ai})	5	10	15
Defend Cost (C_{Dj})	6	10	12
Module Cost (C_k)	10	20	30
Attack success prob, no defense (p_k)	1	1	1
Attack success prob, defended (q_k)	0	0	0

TABLE V
Payoff Matrices for the AS Security Game

Attacker/ Defender	S_1^d	S_2^d	S_3^d
S_1^a	-5, 54	5, 40	5, 38
S_2^a	10, 34	-10, 50	10, 28
S_3^a	15, 24	15, 20	-15, 48

$W_1 = 0$. Attacker's payoff will be -5. If defender's strategy is S_2^d for attacker's strategy S_1^a, the probability of attack of the defended module, $p_k = 1$. The rest of the cells of the bimatrix is calculated likewise. From the payoff matrix [A,B] (Table V),

$$A = \begin{pmatrix} -5, & 5, & 5 \\ 10, & -10, & 10 \\ 15, & 15, & -15 \end{pmatrix} \text{ and } D = \begin{pmatrix} 54, & 40, & 38 \\ 34, & 50, & 28 \\ 24, & 20, & 48 \end{pmatrix}$$

$$JD^* = \big(360, 400, 340\big), (A^*J^T)^T = \big(250, 400, 450\big)$$

$$\text{and } JA^*J^T = JD^*J^T = 1100$$

$$|A| = 3000 = 2.72, \text{and } |D| = 41200 = 37.45$$

Therefore, the Nash equilibrium of the game is

$$x = (18/55, 4/11, 17/55), \text{and } y = (5/22, 4/11, 9/22).$$

And, the expected payoffs of the attacker and the defender are $v(a) = 30/11 = 2.72, \text{and } v(d) = 412/11 = 37.45$, respectively.

Figure 2 shows the variation of expected payoffs of the players with q_k. If the value of q_k is changed to 0.5 for Perception (module 1), this will change the value of the first cell of the payoff matrix (-5, 54) to (0,49). The expected payoff of the attacker would increase to 3.5, with minimal change for the defender; his payoff would be 37.64. When the value of q_k for module 2 is changed to 0.5, the attacker's payoff is 4.28, and the defender's payoff is decreased to 34.85. It clearly shows that the control module needs to be better defended than the perception module or the cognition module. This way, the defender could analyze the payoffs and then decide to distribute and prioritize the resources among the modules accordingly. Admittedly, the attack cost and probability of a successful attack is an estimation.

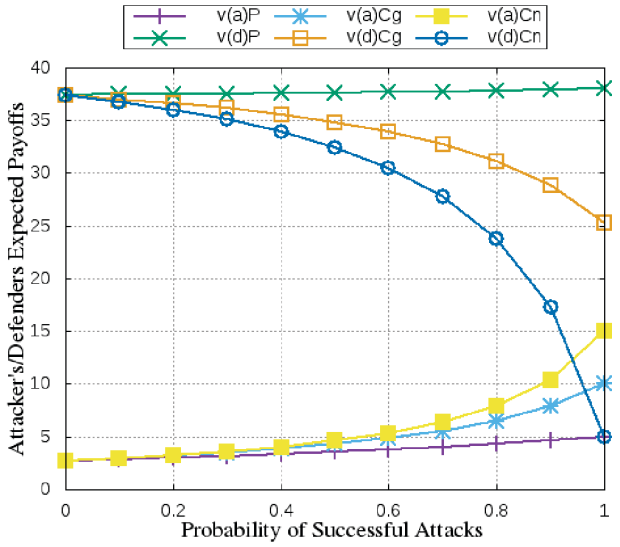

Fig. 2. Variation in Expected Payoffs of the players with probability of successful attack (q_k).

VI. Conclusion

In this paper, a game-theory based framework has been proposed to model an attack on an autonomous system. The proposed framework can be used to analyze the strategies of the attacker and the defender. We evaluate the cost of damage or loss of resources based on the probability of a successful attack. We propose a matrix method for calculating the Nash equilibrium for a $n \times n$ bimatrix game. For the sake of simplicity, we analyze a game based on three strategies of the attacker and the defender. The game considers attack/defense on only one module at a time. Future work would include the analysis of attacks on multiple modules. We acknowledge that our work is preliminary, and we plan to simulate our model in our future work.

References

[1] Jon Walker , "The Self-Driving Car Timeline Predictions from the Top 11 Global Automakers," 2019. [Online]. Available: https://tinyurl.com/y9uaosuu

[2] Teena Maddox, "How autonomous vehicles could save over 350K lives in the US and millions worldwide," 2018. [Online]. Available: https://tinyurl.com/y6me578b

[3] D. J. Atkinson, "Emerging cyber-security issues of autonomy and the psychopathology of intelligent machines," in *2015 AAAI Spring Symposium Series*, 2015.

[4] F. Jahan, W. Sun, Q. Niyaz, and M. Alam, "Security modeling of autonomous systems: A survey," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, p. 50, 2019.

[5] A. Attiah, M. Chatterjee, and C. C. Zou, "A game theoretic approach to model cyber attack and defense strategies," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–7.

[6] A. Ferdowsi, W. Saad, and N. B. Mandayam, "Colonel blotto game for secure state estimation in interdependent critical infrastructure," *arXiv preprint arXiv:1709.09768*, 2017.

[7] G. Owen, *Game theory*, 4th ed. Bingley, England: Emerald Group Publishing, 2013.

[8] Z. Xu and Q. Zhu, "A cyber-physical game framework for secure and resilient multi-agent autonomous systems," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 5156–5161.

[9] A. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust deep reinforcement learning for security and safety in autonomous vehicle systems," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2018, pp. 307–312.

[10] Z. Xu and Q. Zhu, "A game-theoretic approach to secure control of communication-based train control systems under jamming attacks," in *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*. ACM, 2017, pp. 27–34.

[11] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[12] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, 2017.

[13] Q. Wu, S. Shiva, S. Roy, C. Ellis, and V. Datla, "On modeling and simulation of game theory-based defense mechanisms against dos and ddos attacks," in *Proceedings of the 2010 spring simulation multiconference*. Society for Computer Simulation International, 2010, p. 159.

[14] H. S. Bedi, S. Roy, and S. Shiva, "Game theory-based defense mechanisms against ddos attacks on tcp/tcp-friendly flows," in *2011 IEEE symposium on computational intelligence in cyber security (CICS)*. IEEE, 2011, pp. 129–136.

[15] Y. Wang, Y. Zhang, L. Zhang, L. Zhu, and Y. Liu, "Game based ddos attack strategies in cloud of things," in *6th International Conference on Information Engineering for Mechanics and Materials*. Atlantis Press, 2016.

[16] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal load distribution for the detection of vm-based ddos attacks in the cloud," *IEEE Transactions on Services Computing*, 2017.

[17] E. M. Kandoussi, I. El Mir, M. Hanini, and A. Haqiq, "Modeling an anomaly-based intrusion prevention system using game theory," in *International Conference on Innovations in Bio-Inspired Computing and Applications*. Springer, 2017, pp. 266–276.

[18] R. Department of Defense and Engineering, "Technical Assessment: Autonomy," Office of Technical Intelligence, Office of the Assistant Secretary of Defense for Research and Engineering, Tech. Rep., 2015.

[19] K. Berntorp, T. Hoang, R. Quirynen, and S. Di Cairano, "Control architecture design for autonomous vehicles," in *2018 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE, 2018, pp. 404–411.

[20] L. Petnga and H. Xu, "Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks," in *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2016, pp. 811–819.

[21] F. J. R. Lera, C. F. Llamas, Á. M. Guerrero, and V. M. Olivera, "Cybersecurity of robotics and autonomous systems: Privacy and safety," in *Robotics-Legal, Ethical and Socioeconomic Impacts*. IntechOpen, 2017.

[22] J. Kocić, N. Jovičić, and V. Drndarević, "Sensors and sensor fusion in autonomous vehicles," in *2018 26th Telecommunications Forum (TELFOR)*. IEEE, 2018, pp. 420–425.

[23] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "Darts: Deceiving autonomous cars with toxic signs," *arXiv preprint arXiv:1802.06430*, 2018.

[24] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *arXiv preprint arXiv:1905.12762*, 2019.

[25] A. Greenberg. (2015) Hackers Remotely kill a Jeep on the Highway-With me in it. [Online]. Available: http://tinyurl.com/o9coyn4

[26] P. Guo, H. Kim, N. Virani, J. Xu, M. Zhu, and P. Liu, "Exploiting physical dynamics to detect actuator and sensor attacks in mobile robots," *arXiv preprint arXiv:1708.01834*, 2017.

[27] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *2013 American control conference*. IEEE, 2013, pp. 3344–3349.

[28] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of malicious attacks against power systems," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 39, no. 5, pp. 1074–1085, 2009.