# Modeling Cyber Attack and Defense Strategies in Vehicular Networks using Game Theory

Luca Agosti[†], Aidin Attar[‡], Alberto Coppi[⋆]

***Abstract*—Game theory is a powerful tool for analyzing the interactions between different entities in a network, and it has recently been applied to the field of vehicular network security. In this paper, we propose a game-theoretic approach to analyze the cybersecurity of vehicular networks (VANETs). Our approach models the strategic decision-making of vehicles and attackers in the VANET as a non-cooperative game, and uses this model to analyze the security of the network. We show that game theory can be used to analyze the effectiveness of different security mechanisms and identify vulnerabilities in the network. Furthermore, we propose a game-theoretic modeling of the VANET learning process to improve its defense mechanism. By considering the actions and reactions of both vehicles and attackers, our approach allows for a more comprehensive analysis of the network's security. Our proposed model is validated through simulations and experiments. The results show that our proposed models and solutions can effectively improve the security of VANETs. For example, our approach can identify the optimal security mechanisms for different scenarios. Additionally, our game-theoretic modeling of the VANET learning process can improve the network's defense mechanism by allowing it to adapt to changing attack patterns.**

## I. Introduction

Vehicular networks, also known as VANETs (Vehicular Ad-hoc Networks), are a rapidly growing area of research that has the potential to revolutionize the transportation industry. VANETs are wireless networks that enable communication between vehicles and between vehicles and road-side infrastructure. The primary goal of VANETs is to improve road safety, traffic efficiency, and driver comfort by providing real-time information about road conditions, traffic congestion, and other important factors.

As previously reported in the literature, the deployment of VANETs is driven by the increasing number of connected vehicles on the road, as well as the increasing demand for intelligent transportation systems, as discussed in [1]. The communication infrastructure for VANETs is based on various wireless technologies, such as Dedicated Short-Range Communications (DSRC) and Long-Range Wide-Area Networks (LoRaWAN). The data generated by VANETs can be used to support a wide range of applications, such as traffic management, emergency services, and in-car entertainment.

The success of VANET has led to various security and privacy challenges, such as malicious attacks, data integrity, and confidentiality. To address these challenges, researchers have proposed various security and privacy mechanisms, such as cryptography, secure communication protocols, and intrusion detection systems. Game theory has been used to analyze the interactions between different entities in a network and it has been applied to the field of vehicular network security in recent years.

However, traditional academic research in this field has largely focused on static models of attacks and defenses, without considering the dynamic nature of real-world cyber threats. In particular, the intensity of attacks can vary over time, and attackers and defenders are constantly adjusting their strategies in an ongoing battle for control.

To address these challenges, there is a need for a dynamic defense system that can adapt to changing attack patterns and defend against intelligent attackers under various attack situations. In this report, we propose a different approach for defending against multiple types of attacks and threats on a VANET. Our model takes into account the limitations of resources, as well as the security value of the assets on the network. By considering different intensities of attacks, the relative cost to launch them, and the learning process of the defender, we provide suitable responses for the defender.

We model the interactions between attackers and defenders as a cyber-warfare game, as this has been shown to be a highly efficient mathematical method for analyzing and modeling scenarios with conflicting objectives. This approach allows us to design a dynamic defense system that can adjust its strategies to achieve the best defense performance against intelligent attackers and under various attack situations. Through simulations and experiments, we aim to demonstrate the effectiveness of our proposed defense mechanism in improving the security of VANETs.

## II. Related Work

The field of network cybersecurity under a game theoretic framework has seen a significant amount of research in recent years. Many studies have been conducted in the areas of privacy, intrusion detection, and trust management. In the area of privacy, research has focused on using game theory to analyze the interactions between entities in a network, with an emphasis on location privacy [3], [4]. In the area of intrusion detection, studies have examined the use of game theory to model the interactions between attackers and defenders [5], [6]. In the area of trust management, research has looked at using game theory to model trust relationships between entities in a network [7], [8].

Department of Physics and Astronomy "Galileo Galilei", University of Padova

[†]luca.agosti@studenti.unipd.it

[‡]aidin.attar@studenti.unipd.it

[⋆]alberto.coppi@studenti.unipd.it

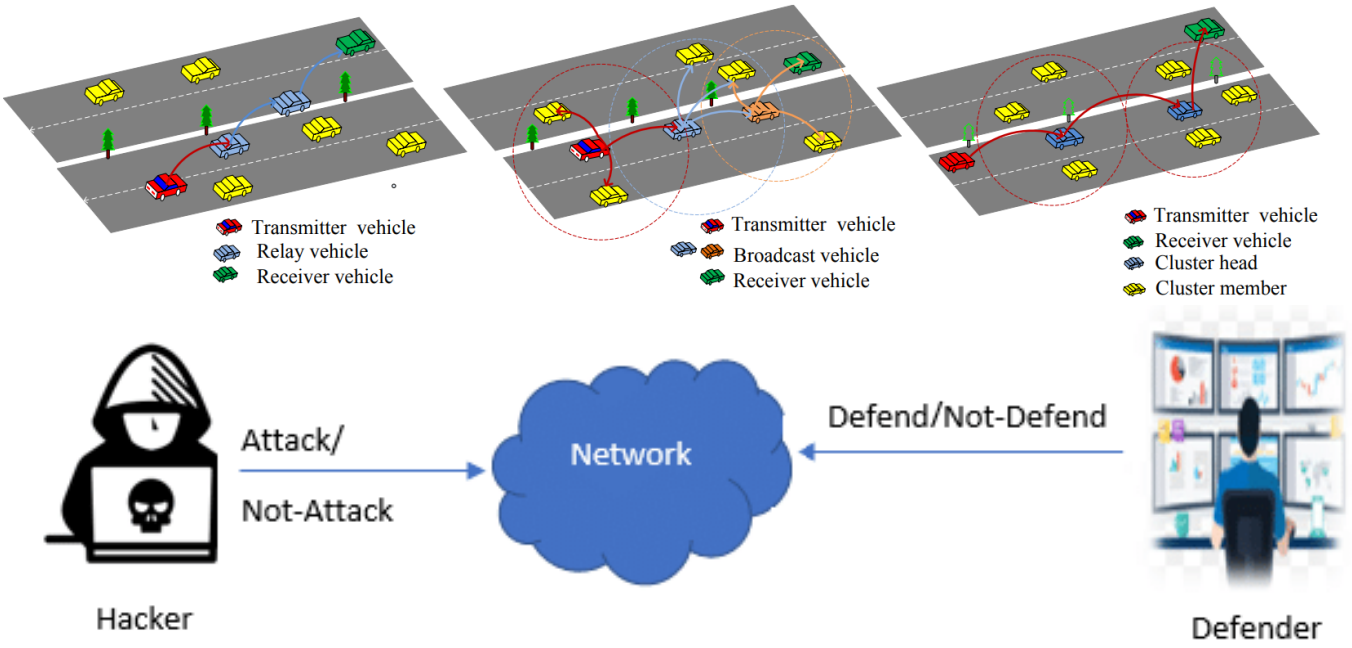


Fig. 1: (a) Schematic representations of a VANET system [1]; (b) Schematic representation of the interaction between attacker and defender in a cyber secury context [2].

One notable example of a game theoretic approach to intrusion detection is the work by Liu et al. in [9]. They proposed a Bayesian game approach for intrusion detection in wireless ad-hoc networks, which utilizes the concept of Nash equilibrium in both static and dynamic scenarios. This approach allows for the analysis of the interactions between pairs of attacking and defending nodes, providing insight into the behavior of the network under different attack scenarios.

Overall, the use of game theory in network cybersecurity has been widely studied and has been shown to be a powerful tool for analyzing the interactions between entities in a network. In this report, we build upon this existing research by applying game theory to the field of vehicular network security, specifically focusing on the use of game theory to analyze the security of VANETs.

## III. Non-Cooperative Attack-Defense Repeated Game

In this section, we discuss how an attacker-defender security game is formulated as a repeated non-cooperative game. A non-cooperative game is a game in which players are not bound to cooperate with each other and each player's objective is to maximize their own utility. In the context of an attacker-defender security game, this means that the attacker's goal is to successfully attack the network while the defender's goal is to protect the network from attacks.

To model this game, we consider the strategies of both the attacker and defender. The attacker's strategies are the different methods they can use to attack the network and their corresponding costs. The defender's strategies are the different methods they can use to protect the network and their corresponding costs. Both the attacker and defender have different levels of strategies, depending on the cost that they are willing to pay and the intensity of the attack or defense that is required.

The attacker aims to choose the strategy that maximizes their chances of being successful while minimizing the resources they have to spend. In contrast, the defender aims to choose the strategy that maximizes their chances of protecting the network without overspending resources on defense. Therefore, the attacker and defender are in a competition with each other, each trying to outsmart the other.

In this repeated game, both attacker and defender can learn from past actions and adjust their strategies accordingly. This allows for a dynamic and adaptive game where the strategies of both players evolve over time. By formulating the attacker-defender security game as a repeated non-cooperative game, we can gain insight into the behavior of the network under different attack scenarios and determine the optimal strategies for both the attacker and defender.

### A. Non-cooperative Game model

In this sub-section, we introduce a two-player non-cooperative repeated game model to analyze the interactions between an attacker and a defender in a vehicular network. The game is represented by $G =< N, S, U >$, where $N = D, A$ represents the two players, where player A represents the malicious attacker and player D represents the defender. The strategy space, $S = a_r, d_r | r \in 0, 1, 2$, represents the set

of actions that are available for each player for each game and their utilities are given by $U$.

As previously mentioned, the attacker and the defender can use one of three levels of strategies during the game. For the attacker, level zero means that they decide not to attack, denoted by $a_0 = No - Attack$, level one is a low intensity of attack, denoted by $a_1 = Attack - 1$, and level two is a high intensity of attack, denoted by $a_2 = Attack - 2$. From the attacker's perspective, compared to the strategy Attack-1, the strategy Attack-2 is more effective in generating a successful attack, but takes more resources or costs more for the attacker to implement.

Similarly, for the defender, level zero means that they decide not to implement any defense, denoted by $d_0 = No - Defend$, level one is a low intensity of defense, denoted by $d_1 = Defend - 1$, and level two is a high intensity of defense, denoted by $d_2 = Defend - 2$. The defender's objective is to minimize the damage caused by the attacker while minimizing the resources used for defense.

Both players choose their strategies simultaneously and independently, assuming common knowledge about the game. The game is repeated multiple times, and the behavior of the two strategies profiles is studied. The purpose of the game is to determine the optimal strategies for both the attacker and defender in different scenarios. It is important to note that this game model allows for a dynamic and adaptive game where the strategies of both players evolve over time.

### B. Game Assumptions

This section of the paper aims to provide a detailed explanation of the assumptions made in our game-theoretic model of vehicular network security. We will explain the key points of the game assumptions and how they are used to simplify the analysis and understanding of the behavior of the players in the game. The assumptions we have made will be clearly outlined and their implications for the game model will be discussed. The purpose of this section is to provide a comprehensive understanding of the assumptions made in the game model, which will help the reader to better understand the results and conclusions of our study.

*1) Repeated game:* In our study, we have made the assumption that the game being played is a repeated game. This means that the game is played multiple times and both players have the ability to adjust their strategies based on the outcome of previous rounds. However, it is important to note that we have assumed that each player only considers the current game round and does not take into account the future rounds. This is known as a myopic assumption. This assumption is made for the purpose of simplifying the analysis and understanding the behavior of the players in the current round without the added complexity of considering future rounds. However, it is worth noting that in reality, players may take into account future rounds when making their decisions and this assumption may not hold true.

*2) Probability of success for the attacker:* An important assumption made for the simulations in this study is the probability of success for the attacker. To model the learning process of the defender, we have made the interaction between the attacker and defender stochastic by using a probability of success that decreases as an exponential function with the learning rate and the number of iterations as variables. Specifically, the unnormalized probability of a successful attack is represented by the exponential function

$$p = \frac{e^{-L \cdot t}}{2^{n-2}}, \tag{1}$$

where $L$ is the learning rate, $t$ is the index of the iteration and $n$ is the number of strategies for each player. To determine the success of an attack, a random number is generated and compared to the probability modulated by a matrix that contains multipliers based on the strategies played by the two players. The comparison simply checks if the extracted sample is less than the modulated probability. If the modulated probability is greater than the generated sample, the attack is considered successful. This stochastic model allows for the simulation of the evolution of the defense mechanism over time, capturing the dynamic and adaptive behavior of both the attacker and defender.

## IV. Models

In this section, we present the detailed models used for the payoffs, costs, and probabilities in our simulations. These models form the foundation of our game-theoretic approach for analyzing the cybersecurity of VANETs, and they play a crucial role in determining the behavior of the attacker and defender in the game. We begin by providing an overview of the assumptions made in our models, followed by a detailed description of how we modeled the payoffs, costs, and probabilities of the different strategies. We also provide a mathematical formulation of our models to facilitate the understanding of our approach. The purpose of this section is to provide a clear understanding of the underlying mechanisms that drive the behavior of the players in our game-theoretic model, and how they contribute to the overall security of the VANETs.

### A. Model 1

In the first model, we assumed that the payoffs for the attacker and the defender were constant, while the costs of the strategies were modeled as exponential functions that increased with the strength of the strategy itself. Additionally, we used a probability multiplicator matrix to model the likelihood of a successful attack depending on the strategies chosen by the attacker and the defender.
In table 1, 2 and 3 we present the parameters used for this simulation.

TABLE 1: Utilities for defender and attacker in case of successful attack (left) and unsuccessful attack (right).

| | N | W | S |
|---|---|---|---|
| N | -30, 30 | -30, 30 | -30, 30 |
| W | -30, 30 | -30, 30 | -30, 30 |
| S | -30, 30 | -30, 30 | -30, 30 |

| | N | W | S |
|---|---|---|---|
| N | 0, 0 | 0, 0 | 0, 0 |
| W | 0, 0 | 0, 0 | 0, 0 |
| S | 0, 0 | 0, 0 | 0, 0 |

TABLE 2: Costs for defender and attacker, according to the exponential growth $k(2^n - 1)$ with $n = [0, 1, 2]$ and $k = 5$.

| N | W | S |
|---|---|---|
| 0 | 5 | 15 |

TABLE 3: Probability multiplicator coefficients of success of attack

| | N | W | S |
|---|---|---|---|
| N | 0 | $\infty$ | $\infty$ |
| W | 0 | 1 | 2 |
| S | 0 | .5 | 1 |

### B. Model 2

In the second model, we assumed that the utilities for the attacker and the defender were modeled as exponential functions that increased with the difference between the strategies chosen by the attacker and the defender.
In table 4, 5 and 6 we present the parameters used for this simulation.

TABLE 4: Utilities for defender and attacker in case of successful attack (left) and unsuccessful attack (right), based on a growing exponential $k \cdot 2^{m-n}$ with $m, n = [0, 1, 2]$ and $k = 5$.

| | N | W | S |
|---|---|---|---|
| N | 0, 0 | -60, 120 | -120, 120 |
| W | 0, 0 | -30, 30 | -60, 60 |
| S | 0, 0 | -15, 15 | -30, 30 |

| | N | W | S |
|---|---|---|---|
| N | 0, 0 | 0, 0 | 0, 0 |
| W | 0, 0 | 0, 0 | 0, 0 |
| S | 0, 0 | 0, 0 | 0, 0 |

TABLE 5: Costs for defender and attacker, according to the exponential growth $k(2^n - 1)$ with $n = [0, 1, 2]$ and $k = 5$.

| N | W | S |
|---|---|---|
| 0 | 5 | 15 |

TABLE 6: Probability multiplicator coefficients of success of attack

| | N | W | S |
|---|---|---|---|
| N | 0 | $\infty$ | $\infty$ |
| W | 0 | 1 | 2 |
| S | 0 | .5 | 1 |

### C. Model 3

In the third model, we assumed that the payoffs for the attacker and the defender were constant, while the costs of the strategies were modeled as exponential functions that increased with the strength of the strategy.
The difference with Model 1 is that we add an even more intense strategy. In table 7, 8 and 9 we present the parameters used for this simulation.

TABLE 7: Utilities for defender and attacker in case of successful attack (top) and unsuccessful attack (bottom).

| | N | W | S | V |
|---|---|---|---|---|
| N | -30, 30 | -30, 30 | -30, 30 | -30, 30 |
| W | -30, 30 | -30, 30 | -30, 30 | -30, 30 |
| S | -30, 30 | -30, 30 | -30, 30 | -30, 30 |
| V | -30, 30 | -30, 30 | -30, 30 | -30, 30 |

| | N | W | S | V |
|---|---|---|---|---|
| N | 0, 0 | 0, 0 | 0, 0 | 0, 0 |
| W | 0, 0 | 0, 0 | 0, 0 | 0, 0 |
| S | 0, 0 | 0, 0 | 0, 0 | 0, 0 |
| V | 0, 0 | 0, 0 | 0, 0 | 0, 0 |

TABLE 8: Costs for defender and attacker, according to the exponential growth $k(2^n - 1)$ with $n = [0, 1, 2, 3]$ and $k = 5$.

| N | W | S | V |
|---|---|---|---|
| 0 | 5 | 15 | 35 |

TABLE 9: Probability multiplicator coefficients of success of attack

| | N | W | S | V |
|---|---|---|---|---|
| N | 0 | $\infty$ | $\infty$ | $\infty$ |
| W | 0 | 1 | 2 | 4 |
| S | 0 | .5 | 1 | 2 |
| V | 0 | .25 | .5 | 1 |

## V. Results

In this paper, we proposed a game-theoretic approach to analyze the cybersecurity of VANETs by modeling the strategic decision-making of vehicles and attackers in the VANET as a non-cooperative game. Through simulations and experiments, we have shown that our proposed models and solutions can effectively improve the security of VANETs.

In the Results section, we will first present the results of our theoretical analysis, where we show that game theory can be used to analyze the effectiveness of different security mechanisms. We will then present the results of our simulations, where we validate our approach and demonstrate the effectiveness of our proposed solutions in improving the security of VANETs. Finally, we will discuss the implications of our results for future research and practical applications.

### A. Theoretical Results

A theoretical approach was used to solve the game in the case of *Model 1*, described in IV-A. All the numerical results proposed in the following are obtained setting the model parameters to $\{k_1 = 30, k_2 = 5, L = 0.05\}$, so that the theoretical results can be compared with the simulation.

As a first step we put the game in extensive form: Figure 2 shows the resulting tree.

Then we try to study this model using a Bayesian approach, hence the players' payoffs are weighted with the associated probability. Thus we obtain the following normal form representation of the game, as shown in Table 10.

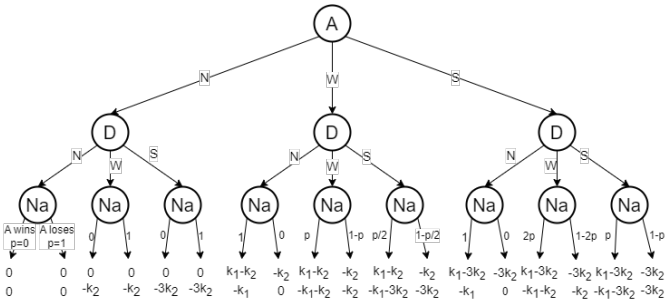


Fig. 2: Extensive form representation of Model 1 game: *A* is the attacker, *D* the defender and *Na* is nature; $k_1$ is the constant utility, $k_2$ is the constant in the costs expression, and p is the probability.

TABLE 10: Expected utilities for attacker (top) and defender (bottom).

| | N | W | S |
|---|---|---|---|
| N | 0 | $k_1 - k_2$ | $k_1 - 3k_2$ |
| W | 0 | $pk_1 - k_2$ | $2pk_1 - 3k_2$ |
| S | 0 | $\frac{p}{2}k_1 - k_2$ | $pk_1 - 3k_2$ |

| | N | W | S |
|---|---|---|---|
| N | 0 | $-k_1$ | $-k_1$ |
| W | $-k_2$ | $-pk_1 - k_2$ | $-2pk_1 - k_2$ |
| S | $-3k_2$ | $-\frac{p}{2}k_1$ | $-pk_1 - 3k_2$ |

*1) Domination analysis:* Initially, the domination of a particular strategy over another is studied, both for player 1 (D) and player 2 (A).
Let's start with player A. We see that, for $t \leq 8$, strategy *N* is dominated by *W*. On the other hand, for $t > 8$, *S* is dominated by *W*.
For player D we obtain the same result for $t > 8$: strategy *S* is dominated by *W*.

*2) Mixed strategies:* Here we focus on the problem in the case $t > 8$: strategy *S* does not belong to the support of both players, thus the problem is much simpler and can be studied using mixed strategies. In order to find the evolution of mixed strategies of player D as a function of the game iteration we impose the following:

$$\begin{aligned} u_A(N,\ [p_D(t),\ 1-p_D(t)]) &= u_A(W,\ [p_D(t),\ 1-p_D(t)]) \\ u_A(S,\ [p_D(t),\ 1-p_D(t)]) &< u_A(N,\ [p_D(t),\ 1-p_D(t)]) \end{aligned} \tag{2}$$

Solving the equations, we can find a mathematical expression for $p_D(t)$, thus obtaining a theoretical expectation of the evolution of the game for player D. The result is shown in Figure 3.

We can apply the same approach to player A, using player D's expected payoffs. The first condition of Eq. 2 can be solved, while the second one leads to a false statement. For this reason we couldn't predict the mixed strategies evolution of player A.

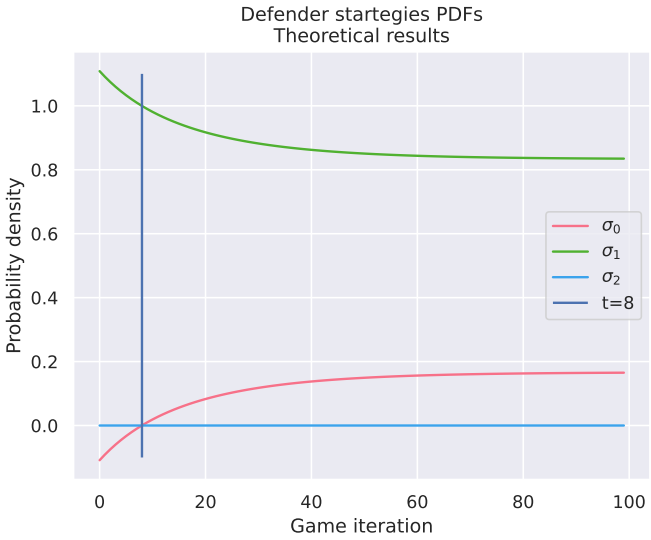


Fig. 3: Evolution of the PDF of player D's strategies. As $t$ gets bigger they resemble the results obtained in the corresponding simulation. Note that this result holds for $t > 8$

### *B. Simulation Results*

In this section, we present the key findings of our simulations, which were designed to investigate the effectiveness of different security mechanisms in VANETs under different attack scenarios. We implemented these simulations using `Python` and the `NashPy`, in particular the latter was used only to find the equilibria of the single games, all the code can be found at [10]. We conducted three simulations, each with different assumptions about the payoffs, costs, and utilities of the strategies available to the attacker and the defender.

Overall, these simulations suggest that a game-theoretic approach can be an effective tool for analyzing the cybersecurity of VANETs. While the defender becomes able to protect the network in all of our simulations, the attacker was able to cause more damage when using a strong attack strategy, highlighting the importance of considering dynamic attack intensity in the design of security mechanisms for VANETs. Additionally, the simulation results support the idea that the defender can improve its defense performance by learning from the attacker's strategies over time and that the attacker stop attacking when the defender becomes too strong.

To further validate the effectiveness of this approach, we also performed a statistical analysis of the simulation results. Our statistical analysis showed that the defender's strategy of increasing the intensity of defense as the attack intensity increases was effective in protecting the network. Furthermore, we observed that the defender's ability to adapt its strategies based on the attacker's behavior was crucial in achieving a high level of network security.

We also presented the results in the form of probability density functions (PDFs) for each strategy, which showed the distribution of the strategies chosen by the players in the population of 2000 agents that we simulated. These

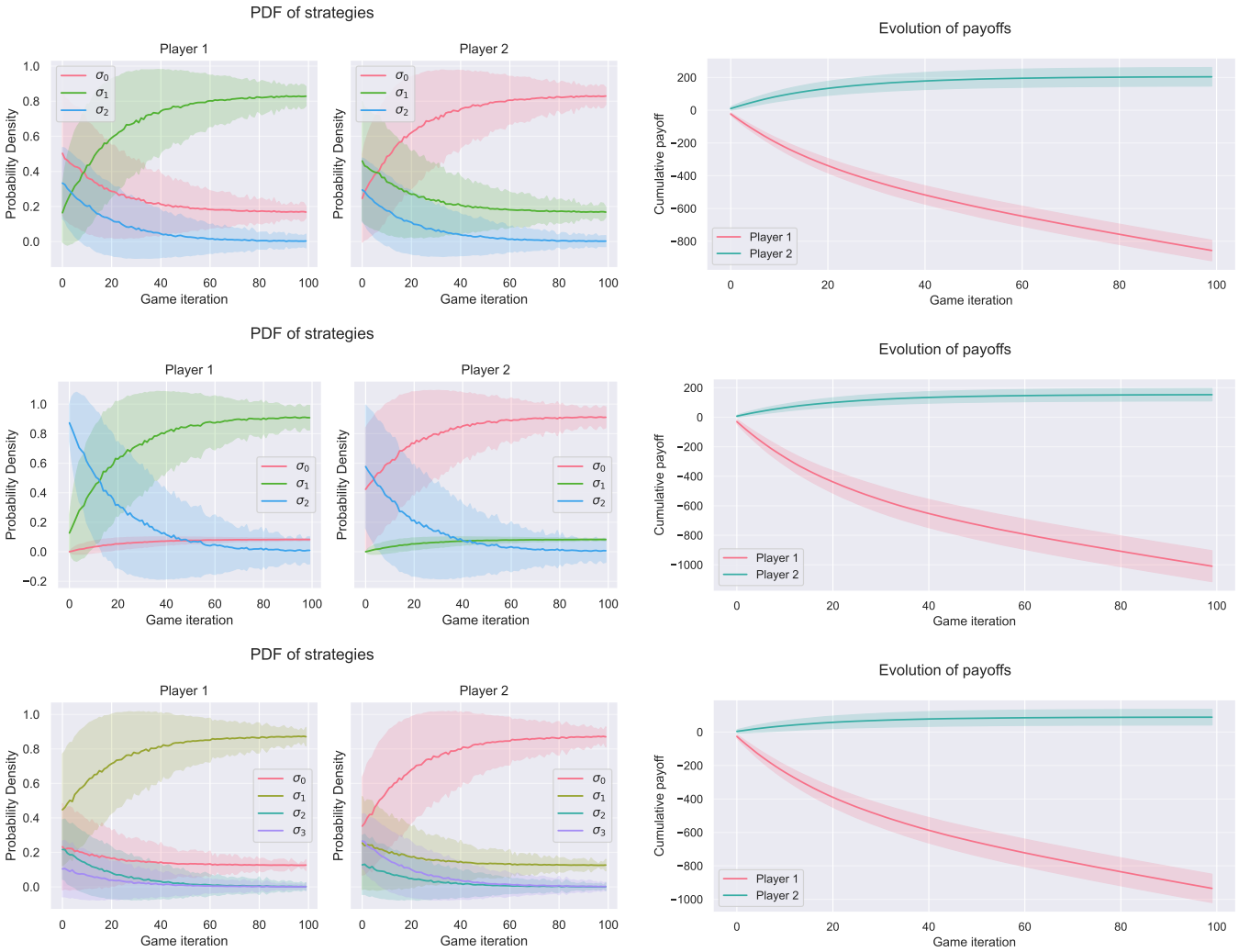


Fig. 4: (left) Probability distribution functions for the Model 1 (top), 2 (center), 3 (bottom); (right) Payoff functions for the case for the Model 1 (top), 2 (center), 3 (bottom); (right). In both the cases Player 1 is the defender and Player 2 is the attacker, strategies are numbered from the weaker (no game) to the stronger.

results demonstrate the effectiveness of our proposed model in representing the behavior of the players in the game.

Now, we present the results of our simulations in relation to the models used for the payoffs, costs, and probabilities. We begin by discussing the results of *Model 1*, shown in Figure 4 (top left). They indicate that the defender initially employs a strong strategy, while the attacker employs a weak strategy. This is due to the fact that the probability of success is at its maximum and our configuration gives a strong strategy dominated by the weak one for the attacker. As the probability of success decreases, the attacker rapidly stops playing, and the defender starts defending with a weak strategy. Figure 4 (top right) illustrates the evolution of payoffs for the two players, with the upward and downward trend being determined by the definitions of the utilities. It is observed that while the defender can at most limit its loss, the attacker cannot lose, net of costs.

For *Model 2*, the results, as shown in Figure 4(center left), indicate that both the defender and the attacker initially employ a strong strategy, as the probability of success is at its maximum. As the probability of success decreases, the attacker rapidly stops playing, and the defender starts defending with a weak strategy.

Finally, in *Model 3*, we consider a fourth strategy. The results, as shown in Figure 4(bottom left), indicate that both the defender and the attacker start with the strategy they are going to play in the end: weak for the defender and no game for the attacker. Overall, these results provide a clear understanding of the underlying mechanisms that drive the behavior of the players in our game-theoretic model, and allow us to better understand the trade-offs between the different strategies available to the attacker and the defender. They also highlight the importance of considering the evolution of costs and utilities over time when analyzing the security

of VANETs. Additionally, the results from the third model demonstrate the potential impact of including more strategies in the analysis, and the need for further research in this area.

## VI. Concluding Remarks

In conclusion, our game-theoretic approach to analyze the cybersecurity of VANETs has demonstrated its effectiveness in understanding the behavior of attackers and defenders in different attack scenarios. The results of our simulations provide a clear understanding of the underlying mechanisms that drive the players in the game. The theoretical approach we chose gave us only a glimpse of the evolution of the game. The bayesian approach seems not to be powerful enough to solve the game in a coherent and complete way, thus further investigations are needed.

The results of our simulations support the idea that the defender can improve its defense performance by learning from the attacker's strategies over time, and that increasing the intensity of defense as the attack intensity increases is an effective strategy for protecting the network.

Future research directions include considering the impact of more players in the game, as well as more accurately modeling the VANET by considering the collaboration of multiple players against hackers. Additionally, incorporating machine learning techniques to allow the defender to learn and adapt in real-time based on the actions of the attacker, could further improve the security of VANETs. Overall, our work provides a useful tool for understanding the security challenges of VANETs and for developing effective defense mechanisms against cyber-attacks.

## References


[1] Z. Sun, Y. Liu, J. Wang, C. Anil, and D. Cao, "Game theoretic approaches in vehicular networks: A survey," 2020.

[2] P. Aggarwal and V. Dutt, "Role of information about opponent's actions and intrusion-detection alerts on cyber-decisions in cybersecurity games," *Cyber Security: A Peer-Reviewed Journal*, p. In press, 02 2020.

[3] B. Ying and A. Nayak, "Location privacy-protection based on p-destination in mobile social networks: A game theory analysis," in *2017 IEEE Conference on Dependable and Secure Computing*, pp. 243–250, IEEE, 2017.

[4] J. Wang, N. He, F. Mei, D. Tian, and Y. Ge, "Optimization and non-cooperative game of anonymity updating in vehicular networks," *Ad Hoc Networks*, vol. 88, pp. 81–97, 2019.

[5] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Computers & Electrical Engineering*, vol. 43, pp. 33–47, 2015.

[6] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for vanet," *Future Generation Computer Systems*, vol. 82, pp. 12–28, 2018.

[7] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for vehicular ad hoc networks (vanets)," *Computer Networks*, vol. 121, pp. 152–172, 2017.

[8] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Networks*, vol. 90, p. 101740, 2019.

[9] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proceeding from the 2006 workshop on Game theory for communications and networks*, pp. 4–es, 2006.

[10] L. Agosti, A. Attar, and A. Coppi, "Modeling cyber attack and defense strategies in vehicular networks using game theory." https://github.com/aidinattar/VehicularNetworks_GT, 01 2023.