International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/221903 Volume 10, Issue 3, May – June (2023)

REVIEW ARTICLE

Game Theory Application for Misbehavior Detection and Prediction in VANET: Review and Challenges

Mohamed Nabil
LAROSERI laboratory, FS, Chouaib Doukkali University, El Jadida, Morocco.
nabilmed77@gmail.com

Abdelmajid Hajam
LAVETE laboratory, FST, Hassan 1st University, Settat, Morocco.
abdelmajidhajami@gmail.com

Omar Boutkhoum
LAROSERI laboratory, FS, Chouaib Doukkali University, El Jadida, Morocco.
o.boutkhoum.fs@gmail.com

Abdelkrim Haqiq
IR2M laboratory, FST, Hassan 1st University, Settat, Morocco.
abdelkrim.haqiq@uhp.ac.ma

Received: 30 April 2023 / Revised: 07 June 2023 / Accepted: 12 June 2023 / Published: 30 June 2023

Abstract – The particular features of vehicular ad hoc networks (VANETs) make them very vulnerable to attacks, especially when these latter become frequent and have intelligent behaviors. For these, the security of vehicular ad hoc networks is substantially important to protect them from the misbehavior of cyber-attacks. Game theory is one of the important tools that have been proposed to accurately model and analyze attack misbehavior. This paper presents a review of game theory-based intrusion detection, prediction, and reaction in VANETs for enriching the literature and helping design a new game theory-based framework. It gives state-of-the-art of game theory-based frameworks by showing their advantages and weaknesses against attacks. In addition, it determines their players and strategies, the proposed solutions and their descriptions, and the types of attacks envisaged. Then, it treats the challenges of designing an efficient framework for intrusion detection, prediction, and reaction against attacks.

Index Terms – Game Theory, Intrusion Detection, Intrusion Prediction, Intelligent Attacks, Game-based Frameworks, VANETs.

1. INTRODUCTION

The vehicular Ad-Hoc Network (VANET) is a technology using moving vehicles like nodes to create a moveable network. This network's vehicles can self-organize and distribute information without centralized management or server-controlled connectivity. In other words, each participating vehicle in VANET becomes a wireless server or client simultaneously, enabling vehicles to connect and exchange information, creating a wide-range network. In this network, when vehicles move out of the coverage area and out of the network, other vehicles can participate by linking the vehicles together and creating a motional network. VANET is a unique variety among mobile ad hoc networks used to supply inter-vehicle or inter-vehicle and infrastructure connectivity [1], [2].

VANET offers several safety and non-safety applications for vehicles, vehicle traffic, drivers, and passengers, ranging from road safety to infotainment. VANET is a key component of intelligent transportation systems; its peculiarities differ from other ad hoc networks. In VANET, wireless communication technologies play a fundamental role in inter-vehicle or inter-vehicle and infrastructure connectivity, in which the vehicles are outfitted with equipment for wireless conversation and positioning systems (such as IEEE 802.11p/WAVE and GPS devices) [3], [4], [5]. However, a large number of challenges must be taken into account to achieve the goal of VANET. Security against attacks is one important task among these challenges.

A significant number of researchers [6], [7], [8], [9], [10], [11], [12] have examined attacks in VANETs for determining efficient solutions. In VANETs, a malicious vehicle can be any type of attacker. It tries to make resources and services unavailable between vehicles by jamming the physical channel. In addition, it duplicates several vehicles by assigning them the same identifier and sending them bad

REVIEW ARTICLE

messages. This evil vehicle loads network bandwidth and increases transmission latency by sending spam over the network. The malicious vehicle listens and injects false information into a communication established between other vehicles. It declares to have the shortest way to obtain the packets then it deletes them or transfers them to an undesirable vehicle. It can generate false vehicle positions causing accidents [13]. It is difficult to control this type of vehicle and secure wireless communication, due to the weak security and centralized administration infrastructure. Thus, communication and exchange of data between vehicles are complex in the existence of evil activities. The trend of vehicle reliability and inappropriate behavior detection is an important task, which needs to be explored.

Several mathematical tools (Kalman filter, Markov chain, neural network, support vector machine, game theory, etc) are used to detect and predict bad activities executed by attackers [14]. Game theory is a powerful one of these tools that can be easily applied to detect and predict complex attacks with great accuracy [15]. The game theory is seen as a mathematical tool for studying the conflict between the defender (system) and the attacker (abnormal vehicle) aiming of determining the best decision for a protector to properly classify the potential target as malevolent. Game theory secures VANET networks against some deadly attacks. Some researchers have used game theory to develop frameworks against intrusion detection and prediction attacks. These frameworks are called Intrusion Detection Systems (IDS) and Intrusion Prediction Systems (IPS). The game-theoretic-based IDS framework enables the evaluation of the vehicle being controlled type and choice fit monitoring strategies. The IDS scheme based on game theory uses a dynamic snooping strategy in which vehicles with great naughtiness values are controlled more frequently than vehicles with weak viciousness values.

There are generally two types of IDS schemes relying on game theory. One is a non-cooperative game in which the players (attacker and the system) aim to maximize their own gains so that the attacker initiates malicious activity against the normal vehicles and the system uses its best strategy to protect the legitimate vehicles. The other type is a cooperative game to defend VANETs from both internal and external threats in which the vehicles cooperate with each other to detect malicious vehicles [16]. However, there is much to learn about the relationship between a node's reliability and the detection of misbehavior.

Game theory is an important tool for detecting and predicting complex attacks with high accuracy. Current game theory-based frameworks are still at the beginning of the route and do not satisfy the requirements of VANET. There is still much to learn about the detection of bad behavior. Moreover, to my knowledge, no review article is specifically devoted to the detection and prediction of intrusions based on game theory in VANETs. For reason, this paper provides a review of papers proposing game theory as a solution for attack detection and prediction in VANET networks. This review highlights simply and understandably different solutions, their types of strategies, and their players proposed in the literature. It studies, analyses, and shows the advantages of these solutions and their shortcomings. Moreover, it mentions the challenges that will help in the design of a new game theory-based framework adaptable to the requirements of VANETs.

The rest of the paper presents a background of game theory in the section 2. After, the application of game theory for the detection and prediction of attacks in the section 3. Then, discussion and challenge for an effective IDS framework in the section 4. Finally, a conclusion in the section 5.

2. GAME THEORY BACKGROUND

This section proposes a background about some elements of game theory used in the papers mentioned in this work.

To my best knowledge, researchers John von Neumann and Oskar Morgenstern originally developed game theory. In their book [17], they claimed that the mathematics expanded in the physical sciences was a bad pattern in economics. They noticed that economics is very much like a game, in which agents anticipate the actions of others, and that this demands a new type of mathematics, which they called game theory. Therefore, game theory is a set of analytical tools that make it easier for understanding situations of interaction between rational decision-makers (normal vehicles and malicious vehicles). In game theory, the outcome for each player depends on the actions of the other. If you are a player (normal vehicle) in such a game, when you choose your plan of action or your strategy, you must take into account the choices of the other (malicious vehicle). However, as you reflect on his choices, you need to recognize that he is thinking about yours and in turn trying to take your thinking into his thinking [18], [19].

The different interaction contexts can be classified according to three dimensions:

- The type of relationship between the agents (cooperative or non-cooperative)
- Progress over time (simultaneous or sequential)
- The information available to agents (perfect information against imperfect; complete against incomplete)

2.1. Form of the Game (Progress over Time).

A simultaneous game (strategic game) is the model of a situation whereabouts each player determines his action complete plan once and for all at the beginning of the game. Therefore, the choices of all agents are done at the same time. Thus, when realizing his choice, the player is not advised of

REVIEW ARTICLE

the choices of others. Whereas, a sequential game indicates the right plan for the game; each player regards his plan of action not solely at the beginning of the game but as well each time he has to take a decision during the course of the game.

2.2. Type of Information

The information is perfect if each player is entirely well-informed of the past movement of the other players. Whereas, information is imperfect when a player does not know some of the choices that were made before him by one or more other players.

A game is complete information if each player knows the structure of the game perfectly (his possibilities of action, the possibilities of action of the other players, the gains resulting from these actions, and the motivations of the other players). Whereas, incomplete information games are situations where one of the conditions does not hold (for example, a player does not know the payoffs of others).

2.3. Strategy of Player

A pure strategy of player i is an action plan that prescribes an action of this player for each time he is likely to play. A mixed strategy of player i is a measure of probabilities p_i defined on the set of pure strategies of player i.

2.4. Type of Game

A cooperative game is a game in which all players gain or waste conjointly. Rather than playing against each other, players game jointly to reach one or more common goals, out of any competition esprit (the cooperation of normal vehicles against internal and external threats).

A non-cooperative game corresponds to situations of interaction between agents free in their choices and pursuing their own independent objectives. These individuals do not communicate prior to the game and do not necessarily have the means to commit to pursuing a particular strategy.

A non-cooperative game can describe in normal form as follows:

- A set n of players: I={1, 2, 3, … , n}
- For each player iϵI, a set of strategies $S_i = \{s_i^1, s_i^2, \dots, s_i^k\}$ where k is the number of strategies disposable to player i, and $s_i \epsilon S_i$ is a particular strategy of player i.
- If each player chooses a strategy s_i among its available strategies, the profile of strategies (result) of the game can be set out by a vector, which contains the strategies chosen by players, as follows: $s = (s_1, s_2 \dots s_n)$.
- For each player i, the function of payoff (ui) represents the player i's preferences by giving him the value $u_i(s)$ for each game outcome. This function is defined as shown in equation (1):

$$u_i: S = XS_i \to \mathbb{R} \qquad (1)$$
$$s \equiv (s_1, s_2, \dots, s_n) \to u_i(s)$$

2.5. Equilibrium of Game

A profile $s_1^* = (s_1^* \dots s_n^*)$, where $s_i^* \in S_i$ and $i = 1 \dots n$, is a Nash equilibrium if no player has a benefit in unilaterally deflecting from its strategy s^*_i when the other players keep playing the profile S^*_{-i}, as shown in equation (2):

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \forall s_i \in S_i, \forall i = 1 \dots n. \qquad (2)$$

The Nash equilibrium in pure strategies of a static Bayesian game is a profile of strategies $s_1^* = (s_1^* \dots s_n^*)$ in which $s^*_i(t_i)$ maximizes the expected payoff of each player i for each of its types $t_i \epsilon T_i$ ($\forall i, \forall t_i \epsilon T_i$). Where T_i is the set of different possible types of player i, and $s_i(t_i)$ is the strategy of player i for each type t_i.

3. GAME THEORY APPLICATION FOR INTRUSION DETECTION AND PREDICTION

Some authors propose the cooperative game theory for detecting and predicting malicious vehicles in the global network by using a centralized center or between neighbors against attacks by exchanging trust information. Others develop frameworks using the non-cooperative game in which each vehicle is based on itself IDS to detect and predict attackers. Therefore, game-theoretic-based IDS frameworks can be divided into two families. One is based on a non-cooperative game and the other on a cooperative game.

3.1. Non-Cooperative Game for Intrusion Detection and Prediction

The authors [20] suggest a framework that performs the detection task of intrusion at three different levels. These latter are, from lowest to highest level, LIDS (Local Intrusion Detection System), CIDS (Cluster Intrusion Detection System), and GDS (Global Decision System) system. They use probabilistic monitoring strategies based on the game's Nash equilibrium to model the conflict between the malevolent vehicle and CIDS as a non-cooperative game with two players.

Table 1 Normal Form in Pure and Mixed Strategies between Malicious Vehicle and CH

			Malicious vehicle	
			p	1-p
			Attack	Wait
CH	q	Monitor	$(2\alpha - \gamma + 1, 1 + \delta - 2\alpha)$	$(-(\beta + \delta), \beta)$
	1-q	Not monitor	$(-(1 - \alpha), 1 - \alpha + \delta)$	(0,0)

REVIEW ARTICLE

This non-cooperative game is taken over by the CH (Cluster Head) for supervising the malevolent vehicles mentioned by vehicle agents. Each agent in this game has two pure strategies that are {Attack and Wait} for a malevolent vehicle, and {Monitor and Not Monitor} for the CH. Every player will choose the strategy that maximizes its global gain.

The different possible payoffs corresponding to each strategy profile are given in Table 1, where α, β, and γ stand for the rates of attack detection, false positives, and CH monitoring costs, respectively. δ is the cluster's average number of vehicles admitting and transmitting information about a malevolent vehicle.

For this non-cooperative game, as of Table 1, there is no NE in pure strategy. Hence, the authors come to a NE in mixed strategy. The likelihoods that the malevolent vehicle and CH will execute their respective pure strategies of "Monitor" and "Attack," respectively, are symbolized by p and q. As a result, the gain of the malevolent vehicle to game its pure strategy "Attack" is as shown in equation (3) when the CH plays its strategy "Monitor" with likelihood q:

$$U_A(\text{Attack}) = (1 + \delta - 2\alpha)q + (1 - \alpha + \delta)(1 - q). \quad (3)$$

The gain of the malevolent vehicle to play its pure strategy "Wait" is as shown in equation (4):

$$U_A(\text{Wait}) = \beta q. \quad (4)$$

The CH payoffs for using the pure strategies "not monitor" and "monitor" are as shown in equations (5) and (6), respectively, when the evil vehicle uses its mixed strategy "attack" with likelihood p:

$$U_D(\text{Not monitor}) = -(1 - \alpha)p. \quad (5)$$

And

$$U_D(\text{Monitor}) = (2\alpha - \gamma + 1)p - (\beta + \delta)(1 - p). \quad (6)$$

Nash equilibrium in mixed strategies is (q*, p*) where q* = (1-α-β)/(α+β) and $p^* = (\beta + \delta)/(2 + \alpha + \beta + \delta - \gamma)$ are the likelihoods of the CH and the evil vehicle to game their strategy Monitor and Attack, respectively. The attack and surveillance likelihoods of the evil vehicle and the CH are conversely pro rata to the rate of detection of the CH. Hence, a great value of α reduces the attack and surveillance likelihoods at the NE i.e., the suggested framework importantly decreases the IDS overhead in the VANET network. However, this framework is evaluated only for low speeds by considering the vehicles that are arrested at the traffic light and vehicles coming nearer the spot of the route junction. It is not evaluated for high speed at a different place in the city. In addition, this framework detects only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. It cannot detect the future misconduct of an attacker.

The authors [21] propose an intrusion detection model that relied on Bayesian game theory to detect the malicious behavior of vehicles in the UAV network. In order to optimize their profits, IDS and attackers strive to strike an equilibrium between a high detection rate and little overhead. The game is defined as follows:

- Players are $\{I_{IDS}, I_{attacker}\}$ IDS agent and attacker, respectively.
- SIDS = {launch intrusion detection (LID), not launch intrusion detection (NLID)} is the set of strategies of IDS.
- $S_{attaker}$ = {initiate a malicious behavior (IMB), not initiate a malicious behavior (NIMB)} is the set of strategies of the attacker.

Table 2 Strategic Form between IDS and Attacker

		Attacker	
		IBM	NIBM
IDS	LID	(D'*EDR, -D'*EDR OVERH)	(-FPDR - OVERH', FPDR)
	NLID	(- FNDR*D, FNDR*D- OVERH)	(-FPDR, FPDR)

The different possible payoffs corresponding to each strategy profile are given in Table 2, where FNDR is the probability that a node is considered normal, but performs malicious behavior. D is the harm caused by the attacker in executing malevolent behavior, and OVERH is the overhead caused by the attacker in executing malevolent behavior. D' is the damage caused to the IDS by the attacker's malevolent behavior. EDR is the detection rate expected by IDS when the detected node has a malevolent behavior. OVERH' is the overhead suffered by the IDS while executing the discovery process. FPDR presents the likelihood that a node is considered an evil node when executing normal behavior.

The authors determine the equilibrium between high detection of attackers by IDS and weak overhead using Bayesian Nash equilibrium. For achieving this equilibrium, authors calculate the expected payoff of IDS agents and attackers. This framework detects only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. It cannot detect the future misconduct of an attacker.

The authors [16] propose a Stackelberg investigative game model, which is a non-cooperative game and feature-security module to define and detect new distinctive attack features using Stackelberg's equilibrium concept. In the Stackelberg model, the authors consider that the intrusion detection system (IDS) [22] is a leading actor and that the attackers are the followers. Each of these players defines the best action which maximizes his gain, considering the better movement

REVIEW ARTICLE

performed by the other. The authors define the strategies and the gain functions of the players by analyzing the interaction between them.

The investigation model is defined as follows:

$\{D_i | i = 1 \dots n\}$ is the set of IDSs

$\{A_j | j = 1 \dots k\}$ is the set of attackers

q_j is the likelihood that A_j performs bad behavior, and $(1-q_j)$ is the likelihood that A_j does not perform bad behavior. p_i is the likelihood that D_i starts its security feature module to define the new type of attack, and $(1-p_i)$ is the probability that D_i is inactive.

$\varphi_{leader} = \{\varphi^1_1, \dots, \varphi^1_s\}$ is the set of leader strategies, where s is the total number of follower-launched feature-security modules to define new types of attacks.

$\varphi_{follower} = \{\varphi^2_1, \dots, \varphi^2_d\}$ is the set of follower strategies, where d is the number of types characterizing the bad behavior of the follower.

The expected gains of the leader (f_{leader}) and follower ($f_{follower}$) rely on the number of new types of attacks and the success rate of intrusion as shown in equations (7) and (8).

$$f_{leader} = q_j * (p_i / (q_j + q_i)) - C_{leader}) + (1 - q_j) * (1 - C_{leader}). \quad (7)$$

$$f_{follower} = q_i * (q_j / (q_j + q_i)) - C_{follower}) + (1 - q_i) * (1 - C_{follower}). \quad (8)$$

Where the C_{leader} and the $C_{follower}$ present the costs of protection and attack respectively.

Feature-security module is defined as follows:

The leader's objective is to detect a new assault feature, while the follower's objective is to launch a fatal attack without being noticed by the leader. In this case, each player plays the strategy (φ^{*i}) which maximizes his gain. Therefore, the optimal IDS and attacker strategies are determined by equations (9) and (10):

$$Y^{*1} = Bleader(\varphi^{*2}) = \arg\max_{pi} fleader(\varphi^1, \varphi^{*2}). \quad (9)$$

$$Y^{*2} = Bfollower(\varphi^{*1}) = \arg\max_{qj} ffollower(\varphi^{*1}, \varphi^2). \quad (10)$$

Stackelberg equilibrium will reach the profile (φ^{*1}, φ^{*2}) i.e. The follower launches a new deadly attack and the leader launches a feature-security module.

The weakness of this work is that not accurate in dense environments of vehicles, and how to distinguish features of attacks because the latter can be changed over time. In addition, this framework detects only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. It cannot detect the future misconduct of an attacker.

Authors [23] suggest a defense strategy for VANET Denial of Service (DOS) assaults by using non-cooperative game theory. The players are honest vehicles against attack vehicles; the honest player tries to reduce its loss and the attacker seeks to maximize its profit. The global cost of each player P_i in the game is computed as shown in equation (11).

$$TC(P_i) = \sum_{t=1}^{t=S} W_t(P_i) - \sum_{t=1}^{t=S} L_t(P_i). \quad (11)$$

Where TC(Pi), Wt(Pi), and Lt(Pi) are the overall cost, the gain at step s, and the losses at stage s of player P_i in the game, respectively. And, S presents the full number of stages in the game. This reaction game allows avoiding driving across attacked areas. For a truthful vehicle, an overcrowded area is not counseled to traverse and will possess an elevated loss value. Nevertheless, a vehicle bearing a jamming assault can assign to this area an elevated value of the payoff. The authors propose two games with perfect information, which are a zero-sum strategic game and an extensive-form game.

In the zero-sum game of strategy, the attacker's strategies are Attacker and Stop; the attacker can continue or arrest its malicious activity. While the truthful strategies are Continue and Change direction; either the honest vehicle can maintain moving in the present area, or it can switch its line for moving away from the attacker.

The different possible payoffs corresponding to each strategy profile are given in Table 3. The Nash equilibrium is reached when the attacker maintains to assail and the honest redirects its way. In the extensive-form game, the attacker strategies are Attacker and Stop; the attacker can either continue or arrest its malicious activity. While the truthful strategies are Continue, Change direction and stop; either the honest can maintain moving on the present area, or it can switch its way to moving away from the attacker.

Table 3 Payoff Matrix Between Honest and Attacker Vehicles

		Attacker vehicle	
		Attack	Stop
Honest vehicle	Continue	(-2, 2)	(2, -2)
	Change direction	(1, 1)	(-1, -1)

The gain of the honest vehicle is α_{ij} where the honest selects the strategy i and the attacker selects the strategy j. The payoff of an attacker is β_{ij} where the attacker selects the strategy j and the truthful selects the strategy i. Can you see the algorithms of [23] to know how to determine α_{ij} and β_{ij}.

As stated by simulation results, this framework assures a high packet delivery ratio while producing a weak overhead. However, the authors have not evaluated its framework in the level of accuracy; for example, the attack detection rate is not assessed as a metric of security. In addition, this framework detects only the current attacker misconduct or the current

REVIEW ARTICLE

malicious activities execution, which run in the infected vehicle. It cannot anticipate the future misconduct of attackers. The authors [24] suggest an effective attack detection and prediction framework, which uses game theory to identify and foresee attackers' future undesirable behavior. The problem of attack-defense is expressed as a game between misbehaving vehicle and the SC (Service Center) in heterogeneous VANETs. The prediction of the monitored vehicle's future behavior relies on the concept of Nash Equilibrium.

Table 4 Normal Form in Pure and Mixed Strategies between SC and a Suspected Vehicle

			Suspected vehicle	
			q	1-q
			Attack	Wait
SC	p	Prevent	(X_{11}, Y_{11})	(X_{12}, Y_{12})
	1-p	Wait	(X_{21}, Y_{21})	(X_{22}, Y_{22})

The SC player has two strategies that are "prevent" and "wait" and the vehicle player has also two strategies that are "attack" and "wait". The future misbehavior of an evil vehicle is determined based on Nash equilibrium.

The normal form of this game is defined in Table 4, where:

X_{11} = (attacks_detection$_{i,j}$) - (Cost + false_detection$_{i,j}$)

X_{12} = - (false_positive$_{i,j}$ + Cost)

X_{21} = -false_detection$_{i,j}$

X_{22} = 0

Y_{11} = false_detection$_{i,j}$ – attacks_detection$_{i,j}$

Y_{12} = false_positive$_{i,j}$

Y_{21} = false_detection$_{i,j}$

Y_{22} = 0

p is the likelihood that the SC plays the prevent action and hence (1 - p) is the likelihood that the SC plays the wait action. q is the likelihood that the vehicle plays attack action and hence (1- q) is the likelihood that the vehicle plays wait action.

Table 5 Non-Cooperative Game-based FRAMEWORKS for Intrusion Detection and Prediction (Player and strategy, Solution, Advantages, and Drawbacks

Framework	Function	Player and strategy	Solution	Solution description	Attack type	advantages	drawbacks
[20]	Intrusion detection	CH:{Monitor, Not Monitor} Malicious vehicle:{Attack, Wait}	NE in a mixed strategy	CH and the evil vehicle play their strategy Monitor and Attack, respectively.	Selective forwarding, black hole attacks, DoS attack, Wormhole attack, and Sybil attacks.	It importantly decreases the IDS overhead in the VANET network.	It is not evaluated for high speed at a different place in the city. It cannot detect the future misbehavior of attackers.
[21]	Intrusion detection	I_{IDS}:{LID, NLID} $I_{attacker}$:{IMB, NIMB}	BNE in a pure strategy	IDS is launched during an attacker's malicious behavior	DoS attacks, false alarms, and Sybil attacks	high detection rate and low overhead	It cannot detect the future misbehavior of attackers.

REVIEW ARTICLE

[16]	New intrusion definition and detection	$\{D_i \mid i = 1 \ldots n\}$ is the set of IDSs (leaders) $\{A_j \mid j = 1 \ldots k\}$ is the set of attackers (followers) $\varphi_{leader} = \{\varphi^1_1, \ldots, \varphi^1_s\}$ is the set of leader strategies $\varphi_{follower} = \{\varphi^2_1, \ldots, \varphi^2_d\}$ is the set of follower strategies.	Stackelberg investigative game in mixed strategy.	The follower launches a new deadly attack and the leader launches a feature-security module.	DoS attack that varies over time and changes its features.	It determines new distinguishing attack features and detects the zero-day lethal attack.	It is not evaluated for the overhead. It cannot detect the future misbehavior of attackers.
[23]	Intrusion detection and reaction	Honest vehicle:{ Continue, Change direction } Malicious vehicle:{Attack, stop}	Zero-sum strategic game and an extensive-form game in pure strategy.	The attacker maintains to assail and the honest changes its path.	DoS attacks	low overhead and high packet delivery ratio	It is not evaluated for attack detection rate. It cannot detect the future misbehavior of attackers.
[24]	Intrusion detection and prediction	SC:{prevent, wait} misbehaving vehicle:{Attack, Wait}	NE in a mixed strategy.	The misbehaving vehicle does not turn to its normal behavior and SC stores the suspect vehicle in the blacklist.		few overheads and a high detection rate in sparse to moderate numbers of vehicles	In a vehicle's dense environment, the framework needs great communication overhead for detecting and predicting misbehaviors.

$false\_detection_{i,j}$ is the number of evil vehicles of v_j that SC_i considers them as benign vehicles (false negative rate). $false\_positive_{i,j}$ is the number of normal vehicles v_j that are considered by SC_i as evil vehicles (false positive rate). $attacks\_detection_{i,j}$ is attackers number v_j which SC_i considers them evil vehicles. Cost is the rate of overhead that SC needs for prohibiting the attacker to happen.

The authors determine the Nash equilibrium in which SC and the evil vehicle do not change their strategies i.e. the attacker does not turn to its normal behavior and SC stores the suspect vehicle into the blacklist. To arrive at this balance, each player seeks to maximize his expected gain to determine the best strategy. The simulation results show that this framework presents a few overheads and a high detection rate in sparse to moderate numbers of vehicles. However, in the dense environment of vehicles, the framework needs great communication overhead for detecting and predicting misbehaviors. These works are summarized in Table 5.

3.2. Cooperative Game for Intrusion Detection

For investigating and evaluating the conflict between a malevolent vehicle and a Coalition Head agent outfitted with an Intrusion Detection System (CH-IDS) in VANETs, the authors [25] concentrated on the signaling game concept. They rely on a distributed centralized model of the network, in which an IDS agent has been embedded in each vehicle. However, only the IDS agent in the head of the coalition (CH-IDS) will monitor the network against attacks for decreasing channel contention and packet collisions. The authors try to find the Bayesian Nash Equilibrium (BNE) in pure and mixed strategies of this game. These BNEs define the manner and timing of the CH-IDS agent's defense strategy execution. Each coalition, which is made up of an amount of participating vehicles and a Coalition Head (CH), has a set of vehicles that make up its membership.

The authors include two participants in the stage Intrusion Detection Game (IDG), a membership vehicle as a sending (θS), and a CH-IDS agent as a recipient (θR). Member vehicles may be honest or evil, and their type is confidential information to CH-IDS agents. Strategies of malicious member vehicles are "attack" and "cooperate". Whereas the strategy of a normal member vehicle is always cooperating. Strategies of CH-IDS are "defend" and "idle".

REVIEW ARTICLE

Table 6 Strategic Form between Vehicle and CH-IDS

		CH-IDS	
		Defend	Idle
Malicious vehicle	Attack	$((1-\alpha)*g_A-\alpha*g_D-c_A, \alpha*g_D-(1-\alpha)*g_A-c_D)$	$(g_A-c_A, -g_A)$
	Cooperate	$(g_C-c_C, -\beta\cdot l_F-c_D)$	$(g_C-c_C, 0)$
Normal vehicle	Cooperate	$(g_C-c_C, -\beta*l_F-c_D)$	$(g_C-c_C, 0)$

Various possible gains of the IDG are displayed in Table 6, where g_A and c_A are attacking gain and cost respectively of malicious vehicles. c_C and g_C are cooperation costs and gain, respectively of member vehicles. g_D is the gain of the CH-IDS agent when it selects the defense strategy. α and β are the rate of detection and the rate of false alarm, respectively. The false alarm signifies that the CH-IDS agent mistakenly spotted a member vehicle while in normal contact, which will result in an l_F loss. Let p stand for the likelihood that a vehicle is malevolent, and then in IDG, there is a pure-strategy Bayesian Nash equilibrium when the equation (12) is met:

$$p < (\beta * l_F + c_D)/(\alpha * g_D + \alpha * g_A + \beta * l_F). \quad (12)$$

The pure profile of BNE is {*Attack, Cooperate, Idle*} which signifies the evil vehicle still executes Attack action and the normal vehicle still executes *cooperate* action while the CH-IDS agent still executes *Idle*. The authors show that this BNE is not handy because the CH-IDS agent plays always the strategy Idle. While the evil vehicle will not have attacked every time. Thus, to detect the malicious vehicle, authors find mixed-strategy Bayesian Nash equilibriums. There is a mixed-strategy BNE when the equation (13) is met:

$$p \geq (\beta * l_F + c_D)/(\alpha * g_D + \alpha * g_A + \beta * l_F). \quad (13)$$

The authors did not evaluate his scheme to determine its performance in terms of accuracy and network overhead. In addition, this framework detects only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. It cannot detect the future misconduct of an attacker.

Authors [26] set out a framework called Generic Cyber Defense Scheme (GCDS), which insures a little overhead for guaranteeing wide-ranging vehicular networks. This framework relies on agents of multi-security, which are IDS, IPS, and IRS, short for intrusion detection, intrusion prevention, and intrusion reaction systems, respectively. The role of IDS is the detection of threats and that of IPS is the prediction of menaces. Meantime, the role of the IRS is the reaction against menaces prior to the happening and then causing disasters. The IDS as a header player is responsible for the launching of IDS, IPS, and IRS players. This framework assures the network of vehicles versus evil vehicles while insuring a weak cost of overhead.

The decision of the GCDS procedure to launch its prediction, detection, or reaction system leads to some decision delay, which must be considered in plus to the overhead. Authors of this scheme express the defense problem of security as a Stackelberg game wherein IDA is the leading agent and IDS, IPS, and IRS are the follower players. IDA is accountable for launching the follower agents. It maximizes its payment and improves the payoff of its followers by determining the better reply strategies for them.

This Stackelberg game of security is performed between the IDA agent (the leading player) and its follower players. The leader player games earliest and proposes its optimum strategies to its follower agents. These optimum strategies are dependent primarily on the anticipated payoffs, which the leader and the followers players could present, and the engendered costs that the followers need for reaching their aims. The player strategies are $\{q_1, q_2, q_3\}$ and $\{p_1, p_2, p_3\}$, where q_1, q_2, and q_3 are respectively the likelihoods of IDS, IPS, and IRS for launching their strategies. While p_1, p_2, and p_3 are respectively likelihoods of IDA demanding the IDS, IPS, and IRS to carry out their optimum strategies. In this Stackelberg game, balance achieves when the follower agents launch their strategies wished by the leader.

The objective of this framework is to assure a compromise between an important detection rate and a weak overhead and a short delay. The results of the simulation are hopeful because their framework needs weak overhead and a short reaction delay for detecting a wide number of attacks. However, this scheme produces a great computational because the IDS agent is set in each vehicle.

Authors [27] propound a scheme relying on a hierarchical cooperative game for securing honest vehicles against offensives taking delay and overhead into account. This scheme is called Cyber Defense Game (CDG). In this framework, there are a pair of distinct kinds of agents: head agents (IDA) and secondary agents (IDS, IPS, and IRS). The role of the IDA agent is to define the best strategies that depend on the charges foisted on the secondary players to reach their hoped payoffs. The secondary agents are also launched by IDA while preserving a trade-off between network metrics (latency, control packets), and metrics for protection (false positives and false negatives). The secondary agents allow for detecting, predicting, and reacting quickly against attacks by playing their optimal strategies by considering into consideration the strategies played by the IDA agent. The strategies of all players are detection, prediction, and reaction actions. q_1, q_2, and q_3 are the likelihoods of the secondary players launching their strategies, while p_1, p_2, and p_3 are the likelihoods of the IDA requesting secondary players to play their optimum strategies. In this game, players cooperate with each other to improve the

REVIEW ARTICLE

game's global gain function (raising the payoff and lowering the costs).

Table 7 Normal Form in Pure and Mixed Strategies between Head and Secondary Players

			secondary players		
			q1	q2	q3
			detection	prediction	reaction
head player	p1	detection	(u_{IDA}, u_{IDS})	(u_{IDA}, u_{IPS})	(u_{IDA}, u_{IRS})
	p2	prediction	(u_{IDA}, u_{IDS})	(u_{IDA}, u_{IPS})	(u_{IDA}, u_{IRS})
	p3	reaction	(u_{IDA}, u_{IDS})	(u_{IDA}, u_{IPS})	(u_{IDA}, u_{IRS})

The gain matrix of this game is given in Table 7, where u_{IDA}, u_{IDS}, u_{IPS}, and u_{IRS} are the gain functions of the head player and the secondary players [27].

The IDA calculates the optimum costs (overheads and delays) suffered by secondary agents to reach the best response. Depending on these costs, the secondary agents choose whether to execute the head agent's recommended strategies. As a result, when the secondary agents play the IDA actor's strategies, equilibrium is attained. After determining CDG, authors determine the expected payoff of CDG (for protecting vehicle i) and the expected payoff of an attacker. Each player maximizes his payoff by playing his best strategy. The authors show that there is a unique Nash equilibrium between CDG and the attacker. However, when there are more attackers and vehicles, the performance of this framework degrades and becomes not accurate.

The work [28] concentrates on APTs detection. APTs are intelligent attackers that try to discover how the IDSs work and later supply the attack actions suitable to continue undetected [29] [30]. The authors of this work model the conflicts between manifold sorts of APTs and the TCM in the internet of vehicles. They designed a rehearsed Bayesian Stackelberg game to optimize protection movements below imperfect bits of knowledge about menaces sorts. Each strategy of TMC or APTs is a randomized combination of RSUs, which nourish IDSs with information for taking decisions. The strategies set of players is designated by $N = \{n, n \in \mathbb{N}^*, n \leq N\}$ wherein N presents the number of RSUs that spread on the transportation infrastructure. The attack types set is denoted by $Q = \{q, q \in \mathbb{N}^*, q \leq Q\}$, wherein Q is the number of attack types; and P^q is the likelihood of happening of attack sort in the opinion of the IDS. The action set of each attack type is $A = \{a_1,... a_j,..., a_A\}$, where A is the number of possible combinations of RSUs and a_j is an attack action that targets one or a set of RSUs at the same time. The probability distribution vector of mixed strategies of each attack type q is denoted by $y^q = (y^q_1,...,y^q_A)$, such that $y^q_j \geq 0$ $\forall a_j \in A$ and that the sum of y^q_j equals 1 $\forall a_j \in A$. The set of actions of the system defense implemented in IDS is represented by $D = \{d_1,..., d_i,..., d_D\}$, where D is the number of possible combinations of RSUs and d_i is a defense action that protects one or a set of RSUs simultaneously. The likelihood distribution vector of mixed defense strategies is represented by $x = (x_1... x_D)$, such that $x_i \geq 0 \; \forall d_i \in D$ and that the sum of x_i equals 1 $\forall d_i \in D$.

The normal form in pure and mixed strategies of TMC and an attacker type q are presented in Table 8, where U^q_{ij} and V^q_{ij} are the payoffs of TMC and APTs, respectively. These payoffs are defined in [28].

Each attacker q observes the mixed strategies vector played before by TMC (denoted by x); therefore, it determines its optimal action (that maximizes its gain) to x by solving the linear programming optimization problem as shown in equation (14):

$$\text{Maximize} \sum_{a_j \in A} \sum_{d_i \in D} V^q_{ij} x_i y^q_j \qquad (14)$$

Table 8 Normal Form in Pure and Mixed Strategies between Defense System and Attacker Type q

			Attacker type q				
			y^q_1	…	y^q_j	…	y^q_A
			a_1	…	a_j	…	a_A
Defense system	x_1	d_1	(U^q_{11},V^q_{11})	…	(U^q_{1j},V^q_{1j})	…	(U^q_{1A},V^q_{1A})
	…	…	...	…	…	…	…
	x_i	d_i	(U^q_{i1},V^q_{i1})	…	(U^q_{ij},V^q_{ij})	…	(U^q_{iA},V^q_{iA})
	…	…	…	…	…	…	…
	x_D	d_D	(U^q_{D1},V^q_{D1})	…	(U^q_{Dj},V^q_{Dj})	…	(U^q_{DA},V^q_{DA})

To determine the best strategy for TMC, the latter must maximize its payoff by solving the problem of equation (15) defined for multiple types of attack:

$$\text{Maximize} \sum_{d_i \in D} \sum_{q \in Q} \sum_{a_j \in A} P^q U^q_{ij} x_i y^q_j \qquad (15)$$

To solve these problems, authors have used the DOBSS method instead of the Harsanyi transformation [31] and Bayes-Nash equilibrium. However, when there are more attackers and vehicles, the performance of this framework degrades and becomes not accurate.

To expand the process of detection and protection of automated highway systems from large-scale and sophisticated attacks, authors [32] establish an inter-platoon CIDN by creating IDS hub coalitions. An IDS hub assesses the trust value of hubs of near platoons (that are in its coverage area) and joins into a coalition with other hubs if its overall payoff raises after joining. Authors use Bayesian coalitional game theory to create these coalitions between IDS

REVIEW ARTICLE

hubs using the trust value.

In this game, the players are malicious and benign hubs, $T = \{t_1, t_2, t_3, \ldots, t_n\}$ is a set of trust value type of a hub, $p = \{p_1, p_2, \ldots, p_n\}$ is the probability distribution vector of the trust value type ($P(t_i) = p_i$), and $g = \{g_1, g_2, \ldots, g_k\}$ is a vector of accumulating observations of trust value gathered during a period of time.

A hub's overall gain in its platoon is as shown in equation (16):

$$U_h = \sum_{i=1}^{n}(C_{ih} + S_{ih}) + A_h \quad (16)$$

Where C_{ih} and S_{ih} are the compatibility and satisfaction ratios between vehicle i and the hub, respectively. A hub u determines to accede a coalition with v after esteeming the trust value of v. The truthfulness of a hub v assessed by a hub u is as shown in equation (17):

$$\frac{1}{g_0^{uv}}\sum_{i=1}^{k} w_i g_i^{uv} \quad (17)$$

The gain of hub u in a coalition S with n collaborators can be defined as shown in equation (18):

$$U_u = U_u + \sum_{i=1}^{n}(p_{ui} + q_{ui}) \quad (18)$$

And, the global payoff of a coalition is as shown in equation (19):

$$U = \sum_{i=1}^{n}(U_u) \quad (19)$$

Equilibrium is obtained when each hub has no interest in changing its coalition. Therefore, this helps to improve the intrusion detection process.

This framework detects only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. It cannot pick up the future misconduct of an attacker.

The malicious node is identified per its neighbors by means of voting without a centrally managed station. For that, the authors [33] elaborate on a game of local voting (by modeling a static Bayesian game) in which the target node type can be malevolent or benevolent. They consider that benevolent nodes are uncertain about the malevolent node strategy in the network and they conceive incentives to promote nodes, which have yet to supervise the target node in the game. Each node (benevolent or malevolent) can participate in the voting game.

Table 9 Cooperative Game-based Frameworks for Intrusion Detection and Prediction

Framework	Function	Player and strategy	Solution	Solution description	Attack type	advantages	drawbacks
[25]	Intrusion detection	CH-IDS: {defend, idle} Malicious vehicle:{Attack, cooperate}	Signaling game: BNE in pure and mixed strategies.	The CH-IDS plays "Defend" with likelihood δ∗ and the normal vehicle every time plays cooperate whereas The evil vehicle plays "attack" with likelihood ρ∗.	Malicious vehicle deletes information from the network (DoS attacks).	It is not evaluated	It is not evaluated in terms of accuracy and network overhead. It cannot detect the future misbehavior of attackers.
[26]	Intrusion detection, prediction, and reaction.	leading agent (IDA):{p1, p2, p3}. Follower players are IDS, IPS, and IRS, and their strategies are q1, q2, and q3, respectively.	Stackelberg game in mixed strategies	Equilibrium is achieved when the follower players launch their strategies wished by the leader IDA.	DoS attacks	Important detection rate, weak overhead, and short reaction delay.	It produces a great computational because the IDS agent is installed in each vehicle

REVIEW ARTICLE

[27]	Intrusion detection, prediction, and reaction.	Leader agent (IDA):{ detection, prediction, reaction }. Secondary players are IDS, IPS, and IRS, and their strategies are detection, prediction, and reaction respectively.	Hierarchical cooperative game in mixed strategy.	Equilibrium will be attained when the secondary agents play the IDA actor's strategies.	Black hole, false data injection, and false dissemination attacks.	Weak overhead, and short-lived delay in detecting and predicting the attacks with high accuracy (low false positive and low false negative rate).	Not accurate when the number of vehicles and attackers increases.
[28]	Intrusion detection	APTs: $\{a_1,... a_j,..., a_A\}$ TCM: $\{d_1,..., d_i,..., d_D\}$	Bayesian Stackelberg game in a mixed strategy.	When the IDS monitors traffic data at a set of RSU_i the attackers are at the same time targeting this set of RSU_i.	APTs	It detects intelligent attacks (APTs).	It is not evaluated for the attack detection rate when the number of RSUs on the road and the number of RSU_i targeted increase at the same time.
[32]	Intrusion detection and protection	Players: malicious and benign hubs. $T = \{t_1, t_2, t_3, \ldots, t_n\}$ is a set of trust value types of a hub, $p = \{p_1, p_2, \ldots, p_n\}$ is the probability distribution vector of the trust value type.	Bayesian coalitional game in mixed strategy.	When each hub has no interest in changing its coalition.	Every type	high accuracy	It cannot pick up the future misconduct of an attacker.
[33]	Intrusion identification	Benign player: {vote, abstain} Target node: {attack, not attack}	BNE in a pure and mixed strategy.	malevolent node plays its strategy "attack" and a monitoring benign node plays its strategy "vote" in the game	Sybil attacks	Correct identification of the target node.	It is not evaluated for overhead in a dense environment. It cannot detect the future misconduct of an attacker.

The authors define this Bayesian game as follows:

- Set of players N = {target node, benign player}.
- Set of actions of benign player {vote, abstain}, and target node {attack, not attack}.
- Set of players' types, type of benign player Tb = {benign} and type of target node Tt = {malicious, benign}
- U = (u, v), where u is the payoff of the benign player, and v is the payoff of the target node.
- μ is a prior belief of a benign player for the target node being malicious, and the type of benign player is common knowledge.

The authors define the total gain of each player as the sum of the individual gain and that of the group, where the individual gain only accounts interactions between the target node and

REVIEW ARTICLE

benign player, whereas the gain of the group considers for the effect of a strategy of a player on all neighbors. They show that the game has a unique Bayesian Nash equilibrium in pure strategy, in which a malevolent node plays its strategy "attack" and a monitoring benign node plays its strategy "vote" in the game. This equilibrium only takes place under certain constraints. For determining a point of intersection of strategies of players (players are indifferent to the choice of strategy), and for more analysis of the game, authors determine a likelihood of attack q for a malicious target node and a likelihood of voting s for a monitoring benign node. Hence, a Bayesian Nash equilibrium in mixed-strategy is determined. However, this framework detects only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. It cannot detect the future misconduct of an attacker.

4. DISCUSSION AND CHALLENGE

Game theory is an important and rich field for the detection and prediction of malicious attacks in the VANET network. It is a promised tool for a very precise framework against intelligent threats. In [20], the framework importantly decreases the IDS overhead in the VANET network. However, it is not evaluated for high speed at a different place in the city, and cannot detect the future misbehavior of attackers. The scheme [21] has a high detection rate and low overhead. Nevertheless, it cannot detect the future misbehavior of attackers. In [16], the scheme determines new distinguishing attack features and detects the zero-day lethal attack. Even so, it is not evaluated for the overhead, and it cannot detect the future misbehavior of attackers. The scheme of [23] has a low overhead and high packet delivery ratio. Yet, it is not assessed for attack detection rate and cannot detect the future misbehavior of attackers. The framework [24] has a few overheads and a high detection rate in sparse to moderate numbers of vehicles. However, in a vehicle's dense environment, the framework needs great communication overhead for detecting and predicting misbehaviors. The work [25] is not evaluated in terms of accuracy and network overhead. It cannot detect the future misbehavior of attackers. In [26], the framework has an important detection rate, weak overhead, and short reaction delay. It produces a great computational because the IDS agent is installed in each vehicle. The scheme [27] has a weak overhead and short-lived delay in detecting and predicting the attacks with high. Yet, it is not accurate when there are more attackers and vehicles. The framework [28] detects intelligent attacks. However, it is not assessed for the attack detection rate when the number of RSUs on the road and the number of RSU_i targeted increase at the same time. The work [32] has high accuracy. Nevertheless, it cannot pick up the future misconduct of an attacker. The framework of [33] has a correct identification of the target node. Even so, it is not evaluated for overhead in a dense environment and cannot detect the future misconduct of an attacker. Consequently, these theory-based frameworks for intrusion detection and prediction are not efficient in dense environments of vehicles and are not assessed for high speed. Moreover, except [28], they do not take into account the metrics monitoring delay, reaction delay, and intelligent threats in their design. In addition, [20], [21], [16], [23] and [25] detect only the current attacker misconduct or the current malicious activities execution, which run in the infected vehicle. They cannot detect the future misconduct of an attacker.

Current intrusion detection frameworks for VANETs are still at the beginning of the route for establishing solid IDS for the abnormality detection and prediction process. There are still several challenges that should be taken into account for developing IDS, which meets the requirements proposed by applications in intelligent transportation systems. The most important of these challenges:

4.1. Overhead

The majority of frameworks suffer from high communication overhead in the dense environment of vehicles, especially in large cities. Consequently, these frameworks become inaccurate in detecting and predicting misconduct. Therefore, the quality of real-time applications may be affected and the security of vehicles and passengers may be menaced.

4.2. Monitoring delay

The decision delay of these frameworks to react against misbehavior could demean their performances and affects communications in VANETs. Because when the react decision delay of IDS and IPS is short, these frameworks will not have sufficient time for detecting and predicting the misbehaviors of attackers. In revenge, when this delay is high, these frameworks present a significant additional overhead.

4.3. Reaction delay

A long reaction delay of security frameworks against attackers (the security frameworks do not detect and prevent quickly the attacks on vital components of a vehicle) may conduct in disastrous situations.

4.4. Intelligent threats

Attackers begin to examine the intrusion detection systems deployed over a delay of time until they achieve sufficient recognition (gain useful knowledge of valuable assets and defense actions) to launch intelligent attacks with great effect on the network. Each framework must be aware of these types of attacks and must be designed to counter them.

4.5. Metrics of accuracy

How to determine the features of attackers and their level of accuracy in detecting and predicting attacks is a great challenge.

REVIEW ARTICLE

4.6. Relevance of information

Are information collected by vehicles relevant for detecting attacks? Missing or erroneous data remains a big problem for a real understanding of the attacks. Thus, a real dataset developed for intrusion detection in VANETs remains a major challenge.

5. CONCLUSION

This paper presents a review of game theory-based intrusion detection and prediction frameworks in VANETs. It mentions their proposed solutions, advantages, and weakness. Moreover, it gives some important challenges, which can be taken into account for designing new detection, prediction, and reaction systems against threats. In the future, we will propose a new intrusion detection, prediction, and reaction framework that takes into account these challenges by introducing machine-learning algorithms, for selecting the pertinent information against misbehavior.

REFERENCES

[1] S. Olariu et M. C. Weigle, Éd., Vehicular Networks: From Theory to Practice. New York: Chapman and Hall/CRC, 2009. doi: 10.1201/9781420085891.

[2] A. I. Ameur, A. Lakas, Y. M. Bachir, et O. S. Oubbati, " Peer-to-peer overlay techniques for vehicular ad hoc networks: Survey and challenges ", Veh. Commun., p. 100455, 2022.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, et H. Zedan, " A comprehensive survey on vehicular Ad Hoc network ", J. Netw. Comput. Appl., vol. 37, p. 380‑392, janv. 2014, doi: 10.1016/j.jnca.2013.02.036.

[4] A. Zekri et W. Jia, " Heterogeneous vehicular communications: A comprehensive study ", Ad Hoc Netw., vol. 75, p. 52‑79, 2018.

[5] M. L. Sichitiu et M. Kihl, " Inter-vehicle communication systems: a survey ", IEEE Commun. Surv. Tutor., vol. 10, nº 2, p. 88‑105, 2008.

[6] R. S. Raw, M. Kumar, et N. Singh, " Security challenges, issues and their solutions for VANET ", Int. J. Netw. Secur. Its Appl., vol. 5, nº 5, p. 95, 2013.

[7] G. Samara, W. A. H. Al-Salihy, et R. Sures, " Security Analysis of Vehicular Ad Hoc Nerworks (VANET) ", in 2010 Second International Conference on Network Applications, Protocols and Services, sept. 2010, p. 55‑60. doi: 10.1109/NETAPPS.2010.17.

[8] N. K. Chaubey, " Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study ", Int. J. Secur. Its Appl., vol. 10, nº 5, p. 261‑274, 2016.

[9] K. Lim et D. Manivannan, " An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks ", Veh. Commun., vol. 4, p. 30‑37, avr. 2016, doi: 10.1016/j.vehcom.2016.03.001.

[10] V. H. La et A. R. Cavalli, " Security attacks and solutions in vehicular ad hoc networks: a survey ", Int. J. AdHoc Netw. Syst. IJANS, vol. 4, nº 2, p. 1‑20, 2014.

[11] A. Y. Dak, S. Yahya, et M. Kassim, " A literature survey on security challenges in VANETs ", Int. J. Comput. Theory Eng., vol. 4, nº 6, p. 1007, 2012.

[12] M. Raya, A. Aziz, et J.-P. Hubaux, " Efficient secure aggregation in VANETs ", in Proceedings of the 3rd international workshop on Vehicular ad hoc networks, 2006, p. 67‑75.

[13] H. Hasrouny, A. E. Samhat, C. Bassil, et A. Laouiti, " VANet security challenges and solutions: A survey ", Veh. Commun., vol. 7, p. 7‑20, 2017.

[14] P. Sakarindr et N. Ansari, " Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks ", IEEE Wirel. Commun., vol. 14, nº 5, p. 8‑20, 2007.

[15] T. Alpcan et S. Buchegger, " Security Games for Vehicular Networks ", IEEE Trans. Mob. Comput., vol. 10, nº 2, p. 280‑290, févr. 2011, doi: 10.1109/TMC.2010.146.

[16] H. Sedjelmaci, M. Hadji, et N. Ansari, " Cyber security game for intelligent transportation systems ", IEEE Netw., vol. 33, nº 4, p. 216‑222, 2019.

[17] J. Von Neumann et O. Morgenstern, Theory of games and economic behavior, 2nd rev. ed. in Theory of games and economic behavior, 2nd rev. ed. Princeton, NJ, US: Princeton University Press, 1947, p. xviii, 641.

[18] J. W. Weibull, " Evolution, rationality and equilibrium in games ", Eur. Econ. Rev., vol. 42, nº 3‑5, p. 641‑649, 1998.

[19] J. W. Friedman, Game Theory with Applications to Economics. New York: Oxford University Press, 1986.

[20] B. Subba, S. Biswas, et S. Karmakar, " A game theory based multi layered intrusion detection framework for VANET ", Future Gener. Comput. Syst., vol. 82, p. 12‑28, mai 2018, doi: 10.1016/j.future.2017.12.008.

[21] J. Sun et al., " An intrusion detection based on Bayesian game theory for UAV network ", in 11th EAI International Conference on Mobile Multimedia Communications, 2018, p. 56‑67.

[22] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, et C. Chen, " Data-driven intelligent transportation systems: A survey ", IEEE Trans. Intell. Transp. Syst., vol. 12, nº 4, p. 1624‑1639, 2011.

[23] M. N. Mejri, N. Achir, et M. Hamdi, " A new security games based reaction algorithm against DOS attacks in VANETs ", in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2016, p. 837‑840.

[24] H. Sedjelmaci, S. M. Senouci, et T. Bouali, " Predict and prevent from misbehaving intruders in heterogeneous vehicular networks ", Veh. Commun., vol. 10, p. 74‑83, 2017.

[25] A. Mabrouk, A. Kobbane, et M. El Koutbi, " Signaling Game-based Approach to Improve Security in Vehicular Networks. ", in VEHITS, 2018, p. 495‑500.

[26] H. Sedjelmaci, I. H. Brahmi, A. Boudguiga, et W. Klaudel, " A generic cyber defense scheme based on stackelberg game for vehicular network ", in 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2018, p. 1‑6.

[27] H. Sedjelmaci, I. H. Brahmi, N. Ansari, et M. H. Rehmani, " Cyber security framework for vehicular network based on a hierarchical game ", IEEE Trans. Emerg. Top. Comput., vol. 9, nº 1, p. 429‑440, 2019.

[28] T. Halabi, O. A. Wahab, R. Al Mallah, et M. Zulkernine, " Protecting the Internet of vehicles against advanced persistent threats: a bayesian Stackelberg game ", IEEE Trans. Reliab., vol. 70, nº 3, p. 970‑985, 2021.

[29] I. Stellios, P. Kotzanikolaou, et M. Psarakis, " Advanced persistent threats and zero-day exploits in industrial Internet of Things ", Secur. Priv. Trends Ind. Internet Things, p. 47‑68, 2019.

[30] A. Alshamrani, S. Myneni, A. Chowdhary, et D. Huang, " A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities ", IEEE Commun. Surv. Tutor., vol. 21, nº 2, p. 1851‑1877, 2019.

[31] J. C. Harsanyi, " Games with Incomplete Information Played by "Bayesian" Players Part II. Bayesian Equilibrium Points ", Manag. Sci., vol. 14, nº 5, p. 320‑334, janv. 1968, doi: 10.1287/mnsc.14.5.320.

[32] A. Anwar, T. Halabi, et M. Zulkernine, " Scalable Collaborative Intrusion Detection in Autonomous Vehicular Networks: A hierarchical framework based on game theory ", Internet Things, vol. 20, p. 100631, 2022.

REVIEW ARTICLE

[33] A. Behfarnia et A. Eslami, " Misbehavior detection in ephemeral networks: A local voting game in presence of uncertainty ", IEEE Access, vol. 7, p. 184629‑184642, 2019.

Authors

Mohamed NABIL received the B.Sc. degree in Computer Sciences in 2001, a M.Sc. degree in engineering decision in 2008, and Ph.D. degree in computer science in 2019, from the Hassan 1st University, Faculty of Sciences and Techniques of Settat in Morocco. Assistant Professor at the Faculty of Sciences of El-jadida in Morocco- since 2019. His current research interests are: Vehicular Ad hoc Networks (Security and QoS), IOT, Natural Language Processing, and Game Theory.

Abdelmajid HAJAMI received Master degree in Networks, telecommunications and Multimedia, Mohamed V-Souissi University Rabat- Morocco. 2006. PhD in informatics and telecommunications, Mohamed V-Souissi University Rabat, Morocco, 2011. Ex Trainer in Regional Centre in teaching and training- from 1998 to 2011. Professor at the Faculty of Sciences and Technologies of Settat in Morocco- since 2011. Research interests: Wireless networks (Security and QoS), Radio Access Networks, Next Generation Networks , ILE: informatics Learning Environments and ELearning.

Omar Boutkhoum is an Associate Professor at computer Science department in the Faculty of Sciences of Chouaib Doukkali University, EL Jadida, Morocco. He received his PhD degree in Computer Science from the Faculty of Sciences and Techniques of Caddi Ayyad University, Marrakesh in 2017. His research interests are in the application of decision support systems and Blockchain technology to sustainable supply chain management.

Abdelkrim HAQIQ has a High Study Degree and a PhD, both in the field of modeling and performance evaluation of computer communication networks, from the University of Mohammed V, Agdal, Faculty of Sciences, Rabat, Morocco. Since September 1995 he has been working as a Professor at the department of Mathematics and Computer at the Faculty of Sciences and Techniques, Settat, Morocco. He is the Director of Computer, Networks, Mobility and Modeling laboratory. He is also the General Secretary of the electronic Next Generation Networks (e-NGN) Research Group, Moroccan section.

How to cite this article:

Mohamed Nabil, Abdelmajid Hajam, Omar Boutkhoum, Abdelkrim Haqiq, "Game Theory Application for Misbehavior Detection and Prediction in VANET: Review and Challenges", International Journal of Computer Networks and Applications (IJCNA), 10(3), PP: 469-482, 2023, DOI: 10.22247/ijcna/2023/221903.