Predict and prevent from misbehaving intruders in heterogeneous vehicular networks

Hichem Sedjelmaci, Sidi Mohammed Senouci, Tarek Bouali

Predict and Prevent From Misbehaving Intruders in Heterogeneous Vehicular Networks

Hichem Sedjelmaci, Sidi Mohammed Senouci
DRIVE EA1859, Univ. Bourgogne Franche Comté, F58000,
49 Rue Mademoiselle Bourgeois, 58000, Nevers, France
{Sid-Ahmed-Hichem.Sedjelmaci, Sidi-Mohammed.Senouci
}@u-bourgogne.fr

Tarek Bouali
AIT- Automotive, Infrastructure & Transport, Altran Technologies
2, rue Paul Dautier 78140 Vélizy-Villacoublay, France
tarek.bouali@altran.com

ABSTRACT
The great evolution of communication technologies and potential availability of network access mediums and service providers have led to the appearance of heterogeneous network concept. This paradigm refers to the seamless and ubiquitous interoperability between multi-coverage protocols with different access techniques. A heterogeneous vehicular network (HetVNet) is a heterogeneous network where a vehicle is a smart node equipped with various communication technologies such as Dedicated Short Range Communication (DSRC) and cellular network (3G/4G). The purpose of HetVNet is ensuring a wide area coverage to all vehicles in a large scale network, thus achieving the Always Best Connected (ABC) paradigm where the best continuous connectivity is offered to clients. In addition, HetVNet enables the acquisition and processing of a large amount of data from wide geographical areas via smart vehicles to offer various categories of services to drivers and passengers. There are many challenges in HetVNet and security is one of them since, in one hand, vehicles exchange vital data (about congestions, accidents, hazards, road-works, etc.) and in the other hand they form a specific network with particular characteristics (frequent fragmentation, dynamic topology, no centralized authority, etc.). Intrusion detection systems (IDS) act as a second wall of defense when cryptography is broken and already proved their effectiveness against both external and internal intruders. Therefore, in this research work we propose and implement an intrusion detection and prediction scheme able to detect and especially predict the future misbehavior of a malicious vehicle. The attack prediction technique proposed in this paper is based on a game theory to prevent the occurrence of malicious vehicles. Moreover, the proposed detection scheme detects the most dangerous attacks that target a HetVNet such as false alerts and Sybil attacks. This detection uses a rules-based technique to model a normal behavior of a vehicle. Simulations performed using NS-3 show that our scheme exhibits a high accuracy prediction, faster attack detection, and a low communication overhead compared to current detection frameworks.

Keywords: *HetVNet, Game model, Intrusion detection, Intrusion prediction, Accuracy prediction.*

I. INTRODUCTION

The unprecedented growth of sensing devices and communication technologies has led to the increase of the number of connected vehicles. According to recent statistics, in 2020, a significant number of smart vehicles will be deployed where a variety of Intelligent Transportation System (ITS) applications will be provided such as traffic efficiency and infotainment [1]. To benefit from these services and a continuous Internet connectivity, these smart vehicles are featured with a variety of heterogeneous communication technologies such as Dedicated Short Range Communication (DSRC) and cellular network (3G/4G) [2]. The vehicular network, composed of such smart vehicles and also known as Heterogeneous Vehicular Network (HetVNet), supports well the requirements of the different ITS applications since by combining these communication technologies, a wide area coverage and a good quality of service (QoS) is achieved and ensured, respectively [3]. Hence, in HetVNet, the vehicle is a smart node equipped with a computation unit, a set of sensors, and different communication mediums to exchange data with either other vehicles or the infrastructure [3].

The success of heterogeneous vehicular networks depends mainly on the underlying communications system, and particularly the information security since the vehicles exchange, in one hand, vital data (about congestion, accident, hazard, road-works, etc.) and

in the other hand form a specific network with particular characteristics (frequent fragmentation, dynamic topology, no centralized authority, etc.). Intrusion detection system (IDS) is a security mechanism that has the ability to detect a malicious behavior that targets the network and raises an alarm when the intruder is detected [4]. It acts as second wall of defense when cryptography is broken and already proved its effectiveness against both external and internal intruders. Such system aims to detect cyber-attacks with a high accuracy, such as Denial of Service (DoS) and false alert's dissemination attacks. Recently IDS was used in both Vehicular Ad Hoc Networks (VANET) and HetVNet to detect and eject any threats that target such networks [5][6]-[9][10][11]. The intrusion detection frameworks proposed in [5][6]-[9] take a final decision (i.e. categorize the vehicle as normal or attacker) based only on the current behavior of a target vehicle. However, the behavior of a malicious node could switch in the future to a normal mode, and keeps this mode throughout its lifetime. In this case, it is interesting to not eject it directly especially when the network is sparse.

In this paper we propose an efficient attack detection and prediction scheme that aims to detect and especially predict the future misbehavior of a vehicle. Our scheme relies on game theory concept to predict the misbehavior of an attacker. The attack-defense problem is formulated as a game between two players: the Attacker (i.e. misbehavior vehicle) and the Services Centre (SC). Based on *Nash Equilibrium* (*NE*) concept, we predict the future behavior of monitored vehicles. Moreover, our intrusion detection scheme has the ability to detect the most dangerous attacks that target the HetVNet; we cite for instance False alert's dissemination and Sybil attacks. The proposed scheme is based on a rules-based detection technique to model vehicles' normal behavior and hence identify any misbehavior that occurs. According to the simulation results, it outperforms other intrusion detection schemes in terms of accuracy prediction, detection time and communication overhead. These results are achieved even when the number of vehicles and malicious vehicles are high.

This paper is organized as follows: In Section 2, we describe the current intrusion detection frameworks for HetVNet and VANET. Section 3 describes both the network architecture and the attack models that target such HetVNet network by providing the detection techniques to detect them. Section 4 describes our misbehavior's prediction approach based on *games theory* and Section 5 presents NS3 simulation results and analyzes them. Finally, a conclusion and discussion on future works are presented in Section 6.

II. RELATED WORK

The IDS technique is very effective in protecting the network against malicious nodes [4]. However, the current IDS frameworks conceived for HetVNet and/or VANET [5][6]-[9][10][11] take a final decision (i.e. the vehicle is a normal node or attacker) based only on the current behavior of a target vehicle. In [8], the authors propose a scalable reputation and trust-based framework that assigns to each monitored node a reputation value that depends on the performed action. In their research, they focus on detecting a false warning message generated by an attacker. Furthermore, according to a reputation value, the monitored node is categorized into one of these classes: *not trust*, *+/- trust* and *trust*. In their simulation, the authors prove that their framework is accurate to detect malicious vehicles. However, they don't make an extensive set of simulations to make their contribution worthwhile, as they don't evaluate, for instance the false positive and overhead. In [9], the authors propose a stochastic learning solution for intrusion detection (SLAID) to identify the current attacks that occur in VANET. In this research, the attacker that disseminates false information is detected. According to their experimental result, their system exhibits a high detection rate. However, the main weakness of this system lies in the fact that it generates a high overhead since such heavy learning is embedded at every vehicle. In addition, this system is not applicable for real-time applications because the learning algorithm requires a certain time to model a normal pattern of a target node. In [7], the authors propose a data-centric detection system (DCMD) to identify the

cyber-attacks that disseminate the false message alert, e.g. Post-Crash Notification (PCN) alert. They propose a rule-based detection technique to model the normal behavior of a target vehicle. In case, when the action that a monitored vehicle performs does not match this modeled behavior, it will be suspected as a node that disseminates a false alert message. According to their simulation result, their system requires a low communication overhead to detect these cyber-attacks. However, they do not evaluate the security performance when such attack occurs, e.g. detection rate. In [12], the authors propose a security system to detect the intruder that generates a false Post Crash Notification alert. The vehicle near a crash area issues this notification later. As in [7], authors model the vehicle's expected behavior after the alert generation and compare it with the real action followed by the vehicle. According to their simulation results, their system exhibits a low false negative and false positive rates when the attacks occur. The major drawback of this detection scheme is the fact that the authors claimed that the position information sent in the alert is correct when the false alert is generated. However, this assumption is not correct in some cases since the intruder could provide false information in order to not be identified.

In [5][13], the authors design a secure cluster-based vehicular networks (IDFV) scheme that aim to build safe clusters based on the trust level of monitored vehicle, i.e. the vehicle with the highest trust level play the role of cluster-head. According to their simulation results, the cyber-attacks such as denial-of-service (DoS) are detected with a high accuracy. However, the major weakness of IDFV is the high-generated communication overhead, specifically when the number of misbehavior vehicles is high.

To the best of our knowledge, the Intrusion Prevention and Detection System (IPDS) [14] is the only publicly available work to deal with the misbehavior's prediction in HetVNet. IPDS is based on Kalman filter to predict the future behavior of vehicles. This mechanism organizes the network into 1-hop clusters where the trustworthiness vehicle is chosen to be a Cluster Head (CH) and monitors its neighbors and predicts their behaviors. To increase the prediction accuracy, authors have chosen to designate some specific vehicles in every cluster called recommenders to collect trust levels about their neighbors and send them to the CH. The IPDS exhibits a high prediction rate and low communication overhead. However, the major weakness of this system is its high generated false positives rate.

In this paper, we develop an accurate intrusion prediction and detection scheme that handles the weaknesses of the intrusion prevention and detection schemes proposed in the current literature. The objective of this work is to propose a new security mechanism based on game theory to promptly detect and particularly predict the future misbehavior of attackers with high prediction rate and low number of false positive.

III. Network Architecture and Intrusion Detection Technique

In this section, we present the HetVNet architecture with a focus on the application scenario that we attempt to secure. Afterwards, we give an overview of the different attack models with their corresponding detection policies.

A. Network architecture and general security assumptions

As shown in Fig 1 an HetVNet architecture includes mainly three components[3][15]: The *vehicle* with its on-board unit (OBU) equipped with heterogeneous communication interfaces like DSRC and 3G/4G interfaces, the *Infrastructure* (Road Side Unit - RSU or eNodeB) and the *Cloud* with its Services Centre (SC). The communication in a HetVNet is either between vehicles (V2V) or with the infrastructure (V2I). Transport Layer Security (TLS) protocol is used by RSU and eNodeB to communicate with SC through the cloud as shown in Fig 1. TLS has the ability to ensure data confidentiality and node authentication [16]. The SC offers a couple of services to the vehicles through I2V and V2V communications [17]. These services are various and range from road safety to other useful services for drivers/passengers. Most of the safety-oriented HetVNet applications rely mainly on alert

messages dissemination to inform vehicles when an event (e.g. road accident) is detected. Among alert messages, we can cite for instance Post Crash Notification (PCN) and Emergency Electronic Brake lights (EEBL) [7]. In this research work, we use a dissemination protocol proposed in [2] to broadcast an alert when an event occurs. In this protocol, the vehicle that receives a packet, retransmits it at most once [18] to the next forwarder selected as the farthest node from the sender [19][20]. Vehicles obtain next forwarder's information through an embedded GPS device and through periodic exchange of neighbors' beacons [20].

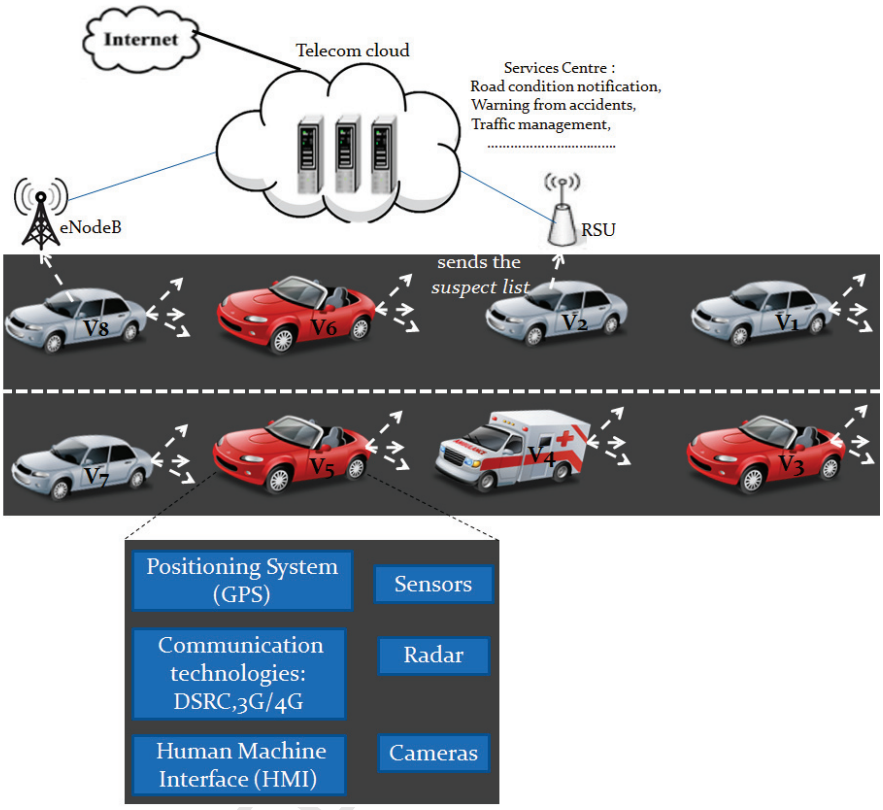


Fig. 1. The targeted HetVNet architecture.

In this HetVNet, security is one of the main issue specifically for safety-oriented applications and a reliable security mechanism becomes mandatory. Therefore, in this paper, we develop an efficient intrusion detection and prediction scheme that aims to identify and predict a future misbehavior of an attacker. To identify a misbehaving vehicle, an *Intrusion detection agent (IDA)* is activated at each vehicle to monitor its neighbors. When a node is suspected to carry out an attack, the IDA sends a message (i.e. *suspect list*) either to RSU or eNodeB depending on the context, i.e. depending on user preferences, service requirements, and the network manager responsible of handover decision [2]. Afterward, the selected infrastructure (i.e. RSU or eNodeB) forwards the *suspect list* to the SC through cloud for further analysis (see section IV).

Let's mention that the intrusion detection system has not acquired the ability to ensure the communication privacy [21]. Therefore, we opted to use Elliptic Curve Cryptography (ECC) provided by the current VANET standard [22] to provide communication privacy and ensure source authentication [23][24]. In our scheme, each vehicle is equipped with private and public keys. The elliptic curve digital signature algorithm (ECDSA) is adopted to authenticate the vehicle identity. Each vehicle

that wants to communicate with a neighbor or with an infrastructure, signs a message using its private key to generate an ECDSA signature as illustrated in Fig 2. In addition, the elliptic curve integrated encryption scheme (ECIES) is applied to encrypt the message and hence ensure data confidentiality. The vehicle encrypts a message with a public key of its neighbor that wants to communicate with; and the neighbor decrypts the message using its private key. Furthermore, for confidentiality of subsequent communications between the vehicles or between the vehicle and infrastructure, a session key $SK_{idi-idj}$ is generated by the two parties, as illustrated in Fig 2. This session key is generated by using an *elliptic curve diffie–hellman* (ECDH).

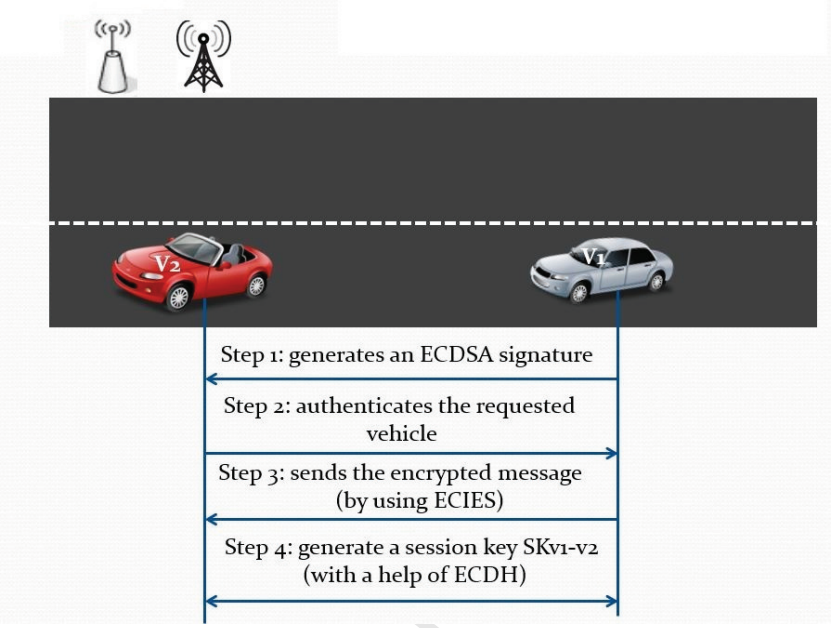


Fig. 2. The main steps to ensure the source authentication and data confidentiality

In safety-oriented HetVNet applications, alert messages are generated to ensure the safety of persons, vehicles and infrastructure. However, the attacker could broadcast a false alert in order to cause a critical disaster (e.g. road accident). Therefore, in this paper our aim is to prevent the occurrence of such misbehavior by monitoring the vehicles' behavior before, during and after the alert. We focus here in post-crash notification (PCN) alert where a vehicle involved in an accident broadcasts a message to vehicles around until the accident is cleared [7]. To detect a misbehaving vehicle, a mutual monitoring concept is applied. This latter means that each vehicle monitors the behavior of its neighbors since all vehicles within a network could be malicious and could launch an attack. Each vehicle has the ability to play an IDA agent role. However, only an optimal number of vehicles activate their IDA agents. In fact, when a high number of IDAs activate their monitoring process, the overhead highly increases and as a consequence the network performance decreases. Therefore, the activation strategy proposed in our recent work [21] is used. Here, at the beginning all vehicles activate their IDA agents. Afterward, when a suspected vehicle is detected only the closest vehicle to this suspected node still monitors it during a predefined period (defined as a *monitoring period* Δt) and the other IDSs switch to the idle mode (i.e. do not monitor). When this period has elapsed, the active IDS switches to idle model and another IDS node (the closest one) activates its monitoring within the same period. This process is continued until the malicious vehicles is ejected from the network.

To identify the attackers that disseminate false alerts, a set of rules is proposed to model a normal vehicle behavior as explained in the following:

The IDA agent relies on a *promiscuous mode* to monitor the vehicle that disseminates an alert about an event (e.g. accident or road conditions). According to [7], when a monitored vehicle disseminates a PCN alert, its lane and speed should change and decrease, respectively. Therefore, the IDS agent will monitor the used lane and the speed of a target vehicle before, during and after the dissemination of the alert. As shown in Fig 3, the vehicle *v* disseminates regularly to its neighbors a Cooperative Awareness Message (CAM) that includes its position (x_{cam_v}, y_{cam_v}), time when CAM message was disseminated (t_{cam}) and speed ($v_{\text{speed\_cam}}$). As cited above when an event is detected (e.g. accident), a PCN alert is broadcasted by *v*. This alert contains the current position of vehicle *v* (x_{alert_v}, y_{alert_v}), time when the alert was generated (t_{alert}) and speed ($v_{\text{speed\_alert}}$). The IDA agent v_{IDA}, that receives these messages (i.e. CAM and alert) from the monitored vehicle *v*, computes the vehicle's *v* speed ($s_{cam-alert}$) between the time when it receives the CAM message and the time when it receives the subsequent alert message, and computes the vehicle's *v* speed ($s_{alert-cam'}$) between the time when it receives the alert message and the time when it receives the subsequent CAM message.

The vehicle *v* is considered as a normal node when it changes the lane and the equation (1) holds. Otherwise, it will be suspected as an attacker that disseminates a false PCN alert.

$$v \text{ is normal if } \begin{cases} s_{alert-cam'} < s_{cam-alert} \\ \text{and} \\ v_{\text{speed\_cam}'} < v_{\text{speed\_alert}} \end{cases} \quad (1)$$

We note that the attacker could provide a false position defined as a *Sybil* attack and sends a false speed (e.g. $v_{\text{speed\_alert}}$ and $v_{\text{speed\_cam}}$) defined as *integrity target* attack. Therefore, to identify these attacks the detection policy proposed in our recent work [21] is applied. To detect Sybil attack, the position verification method proposed in [21] is used. This method is based on *Signal*

Strength Intensity (SSI) and *Round Trip Time (RTT)*. Furthermore, to detect the attack that targets the packets integrity, the messages that are interchanged between target vehicles are monitored and hence the message alteration is verified.

When the IDA agent detects that a monitored vehicle exhibits a malicious behavior, it stores in the *suspect list* the following information: IDA's identity, identity of misbehaving vehicle, attack type and detection time. This list will be sent to the infrastructure (i.e. RSU or eNodeB) as shown in Fig 3. Afterward, the infrastructure forwards the *suspect list* to the SC through cloud.

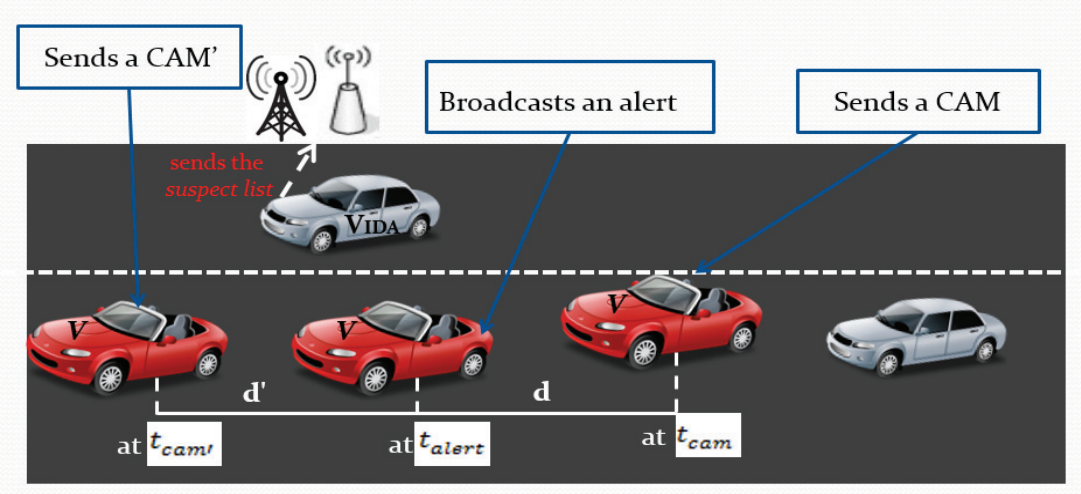


Fig. 3 Detection's process

The SC computes the *attack probability (AP)* related to each monitored vehicle *v* during a *monitoring period* Δt as shown in equation (2). We note that, a set of Δt's values were used and we chose the one that allows us a high accuracy prediction rate and less detection time, see Table V.

$$AP(\Delta t) = \frac{\sum_{i=1}^{k} R_i * rate\_detection}{s} \quad (2)$$

$$\text{and } 0 \leq AP \leq 1$$

where, $rate\_detection$ (equal to k) is the number of IDA agents that suspect a monitored vehicle v as a misbehavior node, $R_i \in [0,1]$ is the efficiency of detection and s is the number of v 's neighbors during Δt.

Based on game theory approach, the SC determines the future misbehavior of a malicious vehicle and categorizes it into the appropriate list according to the action it performs. The misbehavior's prediction approach is explained in the following section.

IV. PROPOSED MISBEHAVIOR'S PREDICTION SOLUTION GAME

In this research work, we choose a game theory approach for misbehavior's prediction and according to a future misbehavior of a suspected vehicle, the SC categorizes this vehicle in one of the following lists: Green, Yellow, Red and Black. In our model, we consider two players, the SC and the vehicles. In the following, we first provide the payoff game between these two players.

Afterwards, based on *Nash Equilibrium (NE)* concept, we show how to predict the misbehavior of monitored vehicles in future stages. Finally, the monitored vehicles' categorization process is explained.

A. Security Game

We consider two main players, which are the SC and the suspected vehicle (detected by IDS as intruder). The players carry out a set of actions to maximize their payoffs. We note that, in game theory concept, the players are rational and want to maximize their own payoff [25]. The SC player carries out one of these actions: *prevent* or *wait*. We note that in *prevent* action, the SC categorizes the suspected vehicle in one of the following lists: Yellow, Red and Black (see subsection IV.C). Furthermore, the vehicle player carries out one of these actions: *attack* or *wait*.

In this game, the time is divided into a set of stages and at each stage there are a series of game interactions between the vehicle and the SC. Different strategies between them are defined and based on *Nash equilibrium* the future misbehavior of a malicious vehicle is determined. In this study, we present two states: (i) *Transitory state*: the attacker oscillates between a well and badly behaving node and (ii) *Permanent state*: the attacker behaves persistently bad, i.e. does not switch to a well behaved node, which represents the worst case. Table I illustrates the payoff matrix of our security game.

Table I. Matrix game: payoff

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

Some notations are defined in Table II;

Table II. Game theory notations

p	Probability that the SC carries out a prevent action
q	Probability that the vehicle carries out an attack action
(1-p)	Probability that the SC carries out a wait action.
(1-q)	Probabilities that the vehicle carries out a wait action.
$false\ detection_{i,j}$	Number of malicious vehicles v_j that SC_i does not suspect, i.e. false negative rate.
$false\ positive_{i,j}$	Number of normal vehicles v_j that are suspected by SC_i as attacker, i.e. false positive rate.
$attacks\ detection_{i,j}$	Number of attackers v_j that CA_i suspects.
Cost	Overhead rate that SC requires for preventing the attacker to occur, i.e. classify the target vehicle into a suitable list.

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,

By observing, the SC computes the belief function $Ht_{k+1}(\Omega_i|v_i)$ based on the behavior of a monitored vehicle by using the following equation [26]:

$$Ht_{k+1}(\Omega_i|a_i) = \frac{Ht_k(\Omega_i)\, Pt_k(v_i|\Omega_i)}{\sum_{\Omega_i \in \theta} Ht_k(\Omega_i) Pt_k(v_i|\Omega_i)} \qquad (3)$$

where, $Ht_k(\Omega_i)$ >0 and $Pt_k(v_i|\Omega_i)$ is the probability that an attacker v_i observed at this stage of game given the type Ω_i (normal or malicious behavior), which is equal either to q or 1-q depending on the attacker's behavior (i.e. malicious or normal). *K={1...n}*, where *n* is the maximum number of stages that should be defined to predict with a high accuracy rate the future misbehavior of a malicious vehicle. See Table III on how to determine *n*.

In the following, we describe the set of strategies between the monitored vehicles and SC. Afterward, based on these strategies, we determine the optimal solution for which the malicious vehicle and SC do not change their actions in the future stage. This optimal solution defined as *NE*, which is a worst case since the malicious vehicle remains in a permanent sate :

- Strategy combination (*Prevent*, *Attack*): In this strategy, the malicious vehicle plays an *attack* action and the SC *detects and categorizes* this attacker into a selected list. In this case, the SC player's payoff that is equal to X_{11} depends on detection rate that SC exhibits, the number of attackers that SC does not detect and the cost to *detect and categorize* v_j in an appropriate list. The vehicle player's payoff is equal to Y_{11} which depends on the rate of misdetection by SC and detection rate that SC exhibits,
- Strategy combination (*Prevent*, *Wait*): In this strategy, the SC detects a monitored vehicle v_j as an attacker while it does not exhibit any attack. Therefore, SC player's payoff, which is equal to X_{12}, decreases. In addition, the cost caused by *detection and categorization* process also decreases SC player's payoff. The vehicle player's payoff is equal to Y_{12}, which increases when the SC wrongly accuses the normal vehicle as an attacker,
- Strategy combination (*Wait*, *Attack*): In this strategy the malicious vehicle attacks and the SC switches to a *wait* action. In this case, when a vehicle v_j performs an attack, vehicle player's payoff increases, which is equal to Y_{21}. In other side, the SC player's payoff decreases when a vehicle v_j carries out an *attack*, which is equal to X_{21},
- Strategy combination (*Wait*, *Wait*): In this strategy, both SC and the monitored vehicle don't perform a *Prevent* and *attacks* actions, respectively. Therefore, the payoff of both players is equal to zero.

B. Misbehavior's prediction solution

NE is a concept used in a game theory to study the interaction between the players and define a stability between them [25]. In this section, we determine the *NE* solution in which both SC and malicious vehicle do not change their actions. This solution is defined as a permanent state of an attacker which is a worst case since it does not switch to a normal behavior.

Theorem 1 *There is at least one NE solution {SC player (prevent, p*), vehicle player $(attack, q*)$} in which the SC carries out a prevention action and the misbehaving vehicle behaves persistently bad (i.e. dost not switch to a normal behavior) when the probabilities $p < p^*$ and $q > q^*$, respectively.*

Proof

The SC expected payoff function U_{SC} is defined as follow:

$$U_{SC} = [X_{11} * q * p + X_{12} * p * (1-q) + X_{21} * q * (1-p) + X_{22} * (1-q) * (1-p)] * Ht(\mu_i = malicious\ behavior) + [X_{12} * p + X_{22} * (1-p)] * (1 - Ht(\mu_i = malicious\ behavior)).$$

$$= \Big[\Big(\big(attacks\ detection_{i,j}\big) - \big(Cost + false\ detection_{i,j}\big)\Big) * q * p - \big(false\ positive_{i,j} + Cost\big) * (1-q) * p - false\ detection_{i,j} * q * (1-p)\Big] * Ht(\mu_i = malicious\ behavior) - [\ false\ positive_{i,j} + Cost) * p * (1 - Ht(\mu_i = malicious\ behavior)] \quad (4)$$

The purpose of SC is to maximize its payoff by choosing an appropriate value of q* to prevent the malicious vehicle to persist to attack in the future stage. This solution ensures an equilibrium, which is defined as follow:

$$U_{SC}(p^*, q^*) > U_{SC}(p, q^*)$$

The SC determines the optimal probability q* by calculating the first derivative of U_{SC} with respect to p* and setting it to zero, which is equal to the following equation:

$$q > q^*, \text{ where } q^* = \frac{false\ positive_{i,j} + cost}{Ht * (false\ positive_{i,j} + attacks\ detection_{i,j})} \quad (5)$$

and $0 < q^* \leq 1$,

On the other hand, the malicious vehicle *v* expected payoff function U_v is defined as follow:

$$U_v = Y_{11} * p * q + Y_{12} * p * (1-q) + Y_{21} * q * (1-p) + Y_{22} * (1-p) * (1-q)$$
$$= (false\ detection_{i,j} - attacks\ detection_{i,j}) * p * q + false\ positive_{i,j} * p * (1-q) + false\ detection_{i,j} * q * (1-p)$$

The purpose of malicious vehicle is to maximize its payoff by choosing an appropriate value of p* to attack a maximum number of legitimate vehicles without being detected. This solution ensures an equilibrium, which is defined as follow:

$$U_v(p^*, q^*) > U_v(p^*, q)$$

The attacker determines the optimal probability p* that leads a malicious vehicle to persist an attack by calculating the first derivative of U_v with respect to q* to zero. Thus, we have

$$p < p^*, \text{ where } p^* = \frac{false\ detection_{i,j} + false\ positive_{i,j}}{attacks\ detection_{i,j} + false\ positive_{i,j}}, \quad (6)$$

and $0 < p^* \leq 1$

As a result, we conclude that when the attack's probability of a malicious vehicle is above q^* and the prevention's probability of SC is lower than p^*, both players do not change their actions. Therefore, an equilibrium is reached defined as *NE* solution. In this

case, this malicious vehicle behaves persistently bad (i.e. does not switch to a normal behavior) and hence it will be stored in a *Black list* as shown in Table IV.

As explained in subsection IV.A, Ht depends on the number of stages *n* that SC should respect. As shown in Table III, we vary *n* and the number of vehicles, and then compute the accuracy prediction rate (see section V about this metric). According to our simulation results illustrated in this table, n depends mainly on the number of vehicles within a network since in a scaling mode (in our case 300 vehicles) n should be increased to get a high accuracy prediction. This is due to the fact that the belief of SC toward the monitored vehicle, depends on the number of interactions of this target vehicle with other vehicles during certain stages.

Table III. Number of stages vs. intrusion prediction stages

Number of vehicles	Number of stages (n)	Accuracy prediction rate
100	15	100
200	20	98
350	23	94.5

The SC computes at each stage a belief function Ht, see equation 3, and when the equilibrium is reached i.e. $p < p^*$and $q > q^*$, the suspected vehicle is detected as a node that persists to attack, i.e. does not switch to a normal behavior.

B. Vehicles' classification

The behavior of a vehicle could oscillate between a legitimate and malicious behavior during its lifetime. Thereby, it is not wise to eject the monitored vehicle directly when it launches a malicious anomaly [7]. Therefore, to reduce the false positive and false negative, the SC classifies the monitored vehicle into the appropriate list as shown in Table IV.

Table IV. Monitored vehicle's classification

List	Behavior	Threshold
Green	The vehicle exhibits a normal behavior during its passage through the network	$AP = 0$
Yellow	The behavior of a vehicle varies between a well and badly behaved node. However, in the future stages the switching rate to a normal node is more than to a misbehavior node.	$q'^* \leq AP < q''^*$
Red	The behavior of a vehicle varies between a well and badly behaved node. However, in the future stages the switching rate to a normal node is less than to a misbehavior node.	$AP > q''^*$
Black	The behavior of a vehicle varies between a well and badly behaved node. However, in the future stages it does not switch to normal behavior i.e. *Permanent state (worst case)***.**	Here, *AP* converges to 1. In other words, $AP > q^*$ (*Nash equilibrium)*

Here, $q^* > q''^* > q'^*$. q^* is computed by using the formula of *NE,* see equation 5. The probabilities q'^* and q''^* that achieve a high level of security is analyzed in our experiment, see section II.B.

It's noted that, the suspected vehicles that are in a *Yellow* and *Red lists* are limited on their participation on the network. The vehicles in *Yellow list* do not have the right to disseminate the alert messages (i.e. PCN) and the vehicles in *Red list* do not have the right to play an IDA agent role and dissemination of alert messages. However, when they persist to launch their IDA agents and broadcast these alerts messages, their AP will be increased. Furthermore, the vehicles that are stored in a *Black list* will be ejected from the network, in other words these misbehavior vehicles do not have the cryptography keys to communication with other vehicles).

The SC informs the legitimate vehicles about the identities of the malicious vehicles (i.e. stored in Green, Yellow, Red and Black lists). To decrease the communication overhead, the SC filters these lists and forwards a fraction of it to the RSU or eNodeB that has a probability to pass within its radio range. This fraction of malicious vehicles is selected according to a mobility-perdition mechanism [27].

V. PERFORMANCE EVALUATION

The proposed intrusion detection and prediction scheme was implemented in NS3 simulator [28]. In this section, we first study the optimal probabilities thresholds q'^* and q''^* that satisfy the security requirement, i.e. accuracy prediction. After that, we compare the performances of our scheme with current prevention and detection frameworks proposed for HetVNet and VANET, namely: IDFV [5], DCMD [7], SLAID [9] and IPDS [14] frameworks. Here, we evaluate the accuracy prediction rate (i.e. prediction rate and number of false positive). Furthermore, the required time that these schemes exhibit to detect the attackers and the generated communication overhead are also evaluated. These metrics are defined as follow:

- **Accuracy Prediction Rate (APR)**, which is equal to prediction rate (PR) – false positive rate (FPR). Where PR is the rate of attacks' prediction. The number of legitimate nodes that are classified into the inappropriate lists (i.e. Yellow, Red or Black) is defined as FPR,
- **Detection Time (DT)**, which is the required time to identify the misbehaving vehicles [5].

$$DT = \sum_{i=1}^{s} \frac{D_i - T_i}{\text{Sampling frequency} * s} \quad (7)$$

  Where D_i is the detection time of the attacker, T_i is the time when the attack started and *s* is the number of attackers. This metric is important, specifically in real-time applications since it allows evaluating the performances of our intrusion prediction scheme in terms of fast attack detection,
- **Communication Overhead,** measures the number of bytes that vehicles generate to achieve a high security level.

A. Mobility model & simulation parameters

In our simulation, we use a Manhattan Grid area of size 3000×3000m² generated by the *Simulation of Urban Mobility* (SUMO) simulator [29]. This latter generates also a mobility trace that was used as an input to NS-3. The number of attackers varies from 10% to 40% of overall vehicles. In our simulation, we inject three types of malicious vehicles stored in Yellow, Red and Black lists, respectively. The main simulation parameters are summarized in Table V. These parameters were chosen to be as closely realistic as possible.

Table V. Simulation parameters

Simulation area	$3000 \times 3000 m^2$
Simulation time	250 seconds
802.11p maximum range	400 meters
Number of vehicles	From 50 to 300
Velocity	80 to 150 km/h, step 20
Monitoring period (Δt)	4 seconds
Propagation model	Two ray ground
Mobility generator	SUMO
Maximum number of attackers	40% of overall vehicles

B. Results and discussion

In this subsection, we summarize the main results of our approach. First of all, we determine the optimal probabilities *q'** and *q''** that achieve a high level of security, i.e. high accuracy prediction rate. Afterward, we compare the performance of our scheme with current intrusion detection and prevention frameworks in term of accuracy prediction rate, detection time and communication overhead.

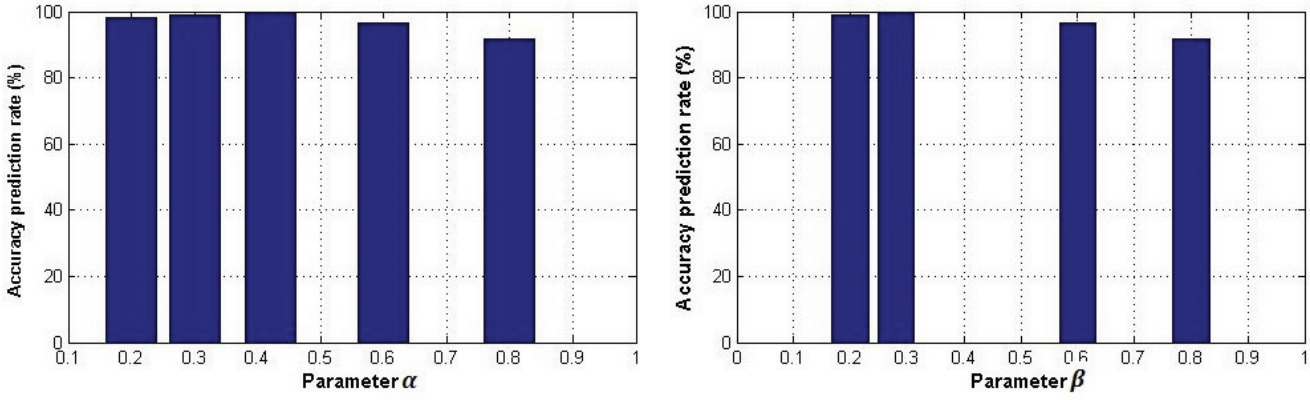
*1) Optimal values of q'** and *q''**

In this subsection, we study the optimal values of q'* (probability that classifies malicious vehicles into a *Yellow list*) and *q''** (probability that classifies malicious vehicles into a *Red list*) that allow us to achieve a dilemma between a high prediction rate and low number of false positive. The optimal values of these probabilities are modeled as follow:

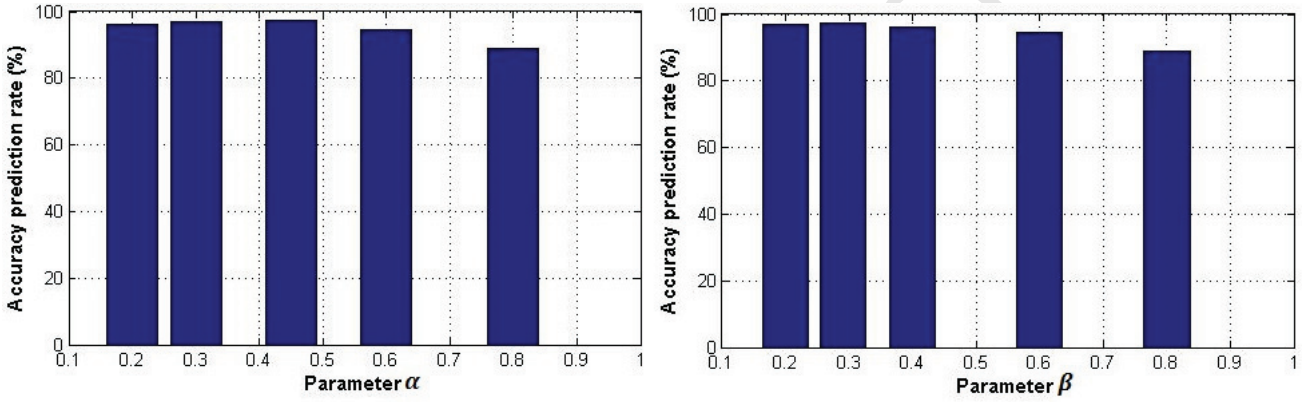
$$\begin{aligned} q'^* &= q^* - \alpha \\ q''^* &= q^* - \beta \end{aligned} \quad (8)$$

As shown in Fig.4, we varied α and β values and computed afterward the accuracy prediction rate (APR). Here, the number of malicious vehicles vary from 10%, 20% to 40% of overall vehicles, and the number of vehicles is fixed to 250 nodes. The optimal probabilities thresholds *q'** and *q''** that allow a high APR are selected. In the following, we summarize our main results:

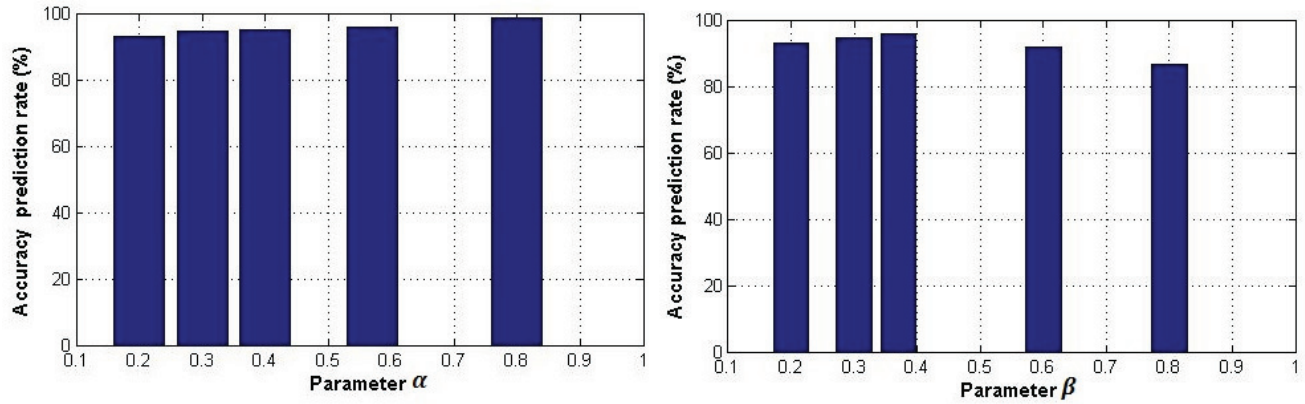
Fig.4 highlights the accuracy prediction rate when α and β values increase. It's noted that q* is determined by using *NE* solution, see equation 5. According to Fig.4, we found that the optimal values of α and β that make a tradeoff between detection (prediction) and false positive rates depend mainly on the number of attackers that occur in the network. In fact, when the number of malicious vehicles is equal to 10%, 20% and 40% of overall vehicles, the optimal values of α and β that allow a high APR (close to 97%) are equal to (0.42, 0.28), (0.45, 0.29) and (0.57, 0.36), respectively. Furthermore, when the number of attackers increases, the APR decreases. This is due to the fact that the number of trusted vehicles and IDS agents are reduced.



(a)



(b)



(c)

Fig.4 Optimal probability thresholds with a number of attackers equal to (a) 10%, (b) 20% and (c) 40 % of overall vehicles.

In the following, the proposed prediction scheme is compared to some recent detection and prevention frameworks by computing accuracy prediction rate, detection time and communication overhead. In this study, we investigate the effect of scaling mode, i.e. varying the number of nodes from 50 to 300 nodes. It's noted that, the number of attackers is set to 40% of overall vehicles, where the values of parameters α and β are equal to 0.57 and 0.36, respectively.

2) Performance comparison

In this subsection, we compare the performance of the proposed scheme with IDFV, DCMD, SLAID and IPDS in terms of accuracy prediction, detection time and communication overhead required to achieve a high level of security. Here, the number of vehicles varies from 50 to 300 nodes. As cited above, the optimal probabilities thresholds used are (α (q'*) = 0,57 and β (q''*) =0,36). Hereafter, we summarize the most important results:

a) Attack prediction and False positive. As shwon in Fig. 5(a), when the number of vehicles increases our scheme exhibits a high attack prediction and generates a low false positive compared to the current detection and prevention schemes IDFV, DCMD, SLAID and IPDS. We show also that IDFV, DCMD and SLAID have not the capability to predict the future misbehavior of a malicious vehicle since their prediction rates and false positive rates decrease and increase, respectively. Furthermore, IPDS generates a high false positive rate due to the noise and incorrect observations. As a result, we can claim that by using *Nash equilibrium* concept, our intrusion detection and prediction scheme can predict the future misbehavior of an attacker, even when the number of vehicles and attackers increase. This result is achieved thanks to the *Nash Equilibrium* concept that models the behavior of vehicles in future stages based on early ones, which lead to an increase on the detection rate and the decrease on the false positive rate. This is unlike IDFV, DCMD and SLAID frameworks, where there is no intrusion prediction technique.

b) Detection time. Fig.5 (b) presents the detection time of each intrusion detection (and prevention) framework. As shown, when the number of nodes is high, the required time to identify a malicious vehicle and to categorize it in the appropriate list for each framework increases. However, according to Fig.5 (b), we can easily observe that our proposal and IDFV require a shorter time compared to DCMD and SLAID, specifically when the number of vehicles is important. Hence, we can claim that our intrusion prediction scheme could be used in delay-sensitive applications [5]. This improvement is attributed to the following reasons: *(i) Optimal number of IDA agents.* We activate an optimal number of intrusion detection agents that have the ability to monitor and report any misbehavior to the RSU or eNodeB in a short time. *(ii) Lightweight intrusion detection and prediction.* At vehicles level, we use a certain detection rules to identify a misbehavior, unlike SLAID that applies an anomaly detection based on a learning algorithm, which requires a considerable amount of time to model an abnormal behavior as proved in [4][30]. Moreover, to reduce the detection time, our misbehavior's prediction based on game theory is embedded in a powerful node, the SC.

c) Communication overhead. Fig.5 (c) illustrates the communication overhead required to achieve a high security level. We found out that our scheme, DCMD and IPDS generate a low overhead (between 4.5 and 15 KBytes) compared to IDFV and SLAID. This result is achieved even in a scaling mode and when the number of attackers is high. This improvement is due to the fact that our scheme relies on a policy that minimizes the amount of information disseminated by the SC to the vehicles through RSU and eNodeB.

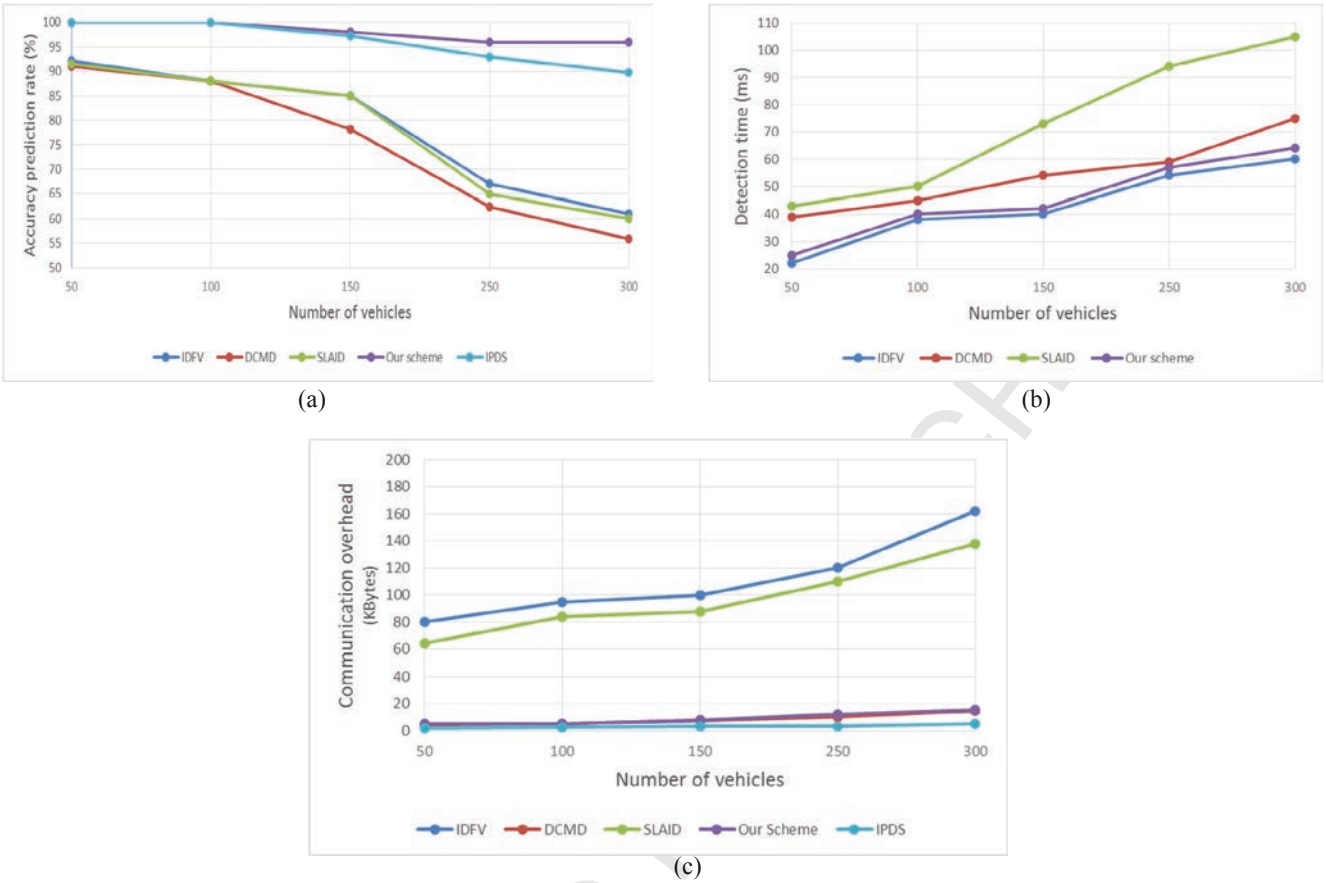


Fig.5. Performance comparison: (a) Accuracy prediction detection, (b) Detection time and (c) Communication overhead.

VI. CONCLUSION

Security in HetVNet is a challenging issue, due to the vital exchanged information [31]. In this paper, we propose and design a new attacks detection and prediction scheme for HetVNet. Our scheme relies on a *Nash equilibrium* concept to detect and specifically predict the future misbehavior of an attacker. The aim in this work is to prevent the occurrence of the most dangerous attacks that target HetVNet. Therefore, detection rules are proposed to model the normal behavior of the vehicles. We have analyzed the performances and demonstrated the efficiency of our proposed scheme using NS-3, and showed that it outperforms other detection and prevention frameworks proposed in the current literature in terms of security requirements and overhead since it exhibits a high accuracy prediction rate, low detection time and a low communication overhead. This result is achieved even in a worst case (the number of vehicles equal to 300).

ACKNOWDELGMENT

This research work is funded by the European Union project CarCoDe [32]. It's an enhanced and extended version of the paper presented at IEEE Globecom 2014 [33].

REFERENCES

[1] H. Moustafa, G. Pau, F. Bai, Y. Zhang, "Internet of Vehicles (IoV)", *IEEE Internet of Things Journal,* Vol 1, Issue 6, 2014, pp.522-524.

[2] T. Bouali, SM. Senouci "A Fuzzy Logic-Based Communication Medium Selection for QoS Preservation in Vehicular Networks", *IEEE ICC'2016*, Kuala Lumpur, Maaysia, 23-27 May 2016.

[3] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges and Solutions", IEEE Communications Surveys & Tutorials*,* Vol 17, Issue 4, 2015, pp 2377 – 2396.

[4] H. Sedjelmaci, S.M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks", *Security and Communication Networks*, Vol. 6, Issue 10, 2013, pp. 1211–1224.

[5] H. Sedjelmaci, and SM. Senouci, "A New Intrusion Detection Framework for Vehicular Networks", *IEEE ICC*, Sydney, Australia, 10-14 June 2014.

[6]T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith. "A Distributed Advanced Analytical Trust Model for VANETs", *IEEE GLOBECOM*, California, USA, 2012, pp. 201-206.

[7]S. Ruj, M.A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs", *IEEE Vehicular Technology Conference (VTC Fall),* San Francisco, USA, 2011, pp. 1-5.

[8] F. Marmol, G. Perez, TRIP: a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, *Journal of Network and Computer Applications*, 35(3), 2011, pp.934-941.

[9]S. Misra1, P. V. Krishna, and K. I. Abraham,"A stochastic learning automata-based solution for intrusion detection in vehicular ad hoc networks", *Security and Communication Networks*, Vol. 4, Issue 6, 2011, pp. 666–677.

[10] K.Zaidi, M. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, "Host Based Intrusion Detection for VANETs: A statistical approach to Rogue Node Detection*", IEEE Transactions on Vehicular Technology*, 2015.

[11] K.Zaidi, M. Milojevic, V. Rakocevic, M. Rajarajan, "Data Centric Rogue Node Detection in VANETs", *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, Pekin, 2013, pp. 398 – 405.

[12] M. Ghos, A.Varghese, A.A. Kherani, and A. Gupta,, "Distributed misbehavior detection in VANETs", *IEEE Wireless Communications and Networking Conference,* Budapest, Hungary, 2009, pp. 1-6.

[13] H. Sedjelmaci, and S.M. Senouci, "An accurate and efficient collaborative Intrusion detection framework to secure vehicular networks ", *Computer & Electrical Engineering*, Vol 43, 2015, pp. 33-47.

[14] T. Bouali, S.M. Senouci, and H. Sedjelmaci, "A distributed detection and prevention scheme from malicious nodes in vehicular networks", *International Journal of Communication Systems, Wiley,*2016.

[15] L. Fuqiang, and S. Lianhai, "Heterogeneous vehicular communication architecture and key technologies*",* ZTE Communications, Issue 4, 2010, pp 39-44.

[16] Z.Md. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato: "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis", *IEEE/ACM Trans*. Netw. Vol. 18, Issue 4, 2010, pp. 1234-1247.

[17] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. ShenAn, "Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks*", IEEE INFOCOM proceeding*, Phoenix, USA, 2008, pp.816-824.

[18] S. Mehar, G. Rémy, and SM. Senouci, "Dissemination protocol for heterogeneous cooperative vehicular networks", *IEEE Wireless Days*, Dublin, Ireland, 2012.

[19] G. Yu , G.J. Heijenk. "Abiding geocast for warning message dissemination in vehicular ad-hoc networks", In *Proceedings of the IEEE Vehicular Networks and Applications Workshop (Vehi-Mobi)*, Beijing, China, 2008.

[20] M. Rondinone, J. Gozalvez,"Contention-based forwarding with multi-hop connectivity awareness in vehicular ad-hoc networks", *Computer network*, Vol. 57, Issue 8, 2013, pp. 1821-1837.

[21] H. Sedjelmaci, SM. Senouci, M. A. Abu-Rgheff, "An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks", *IEEE Internet of Things Journal*, Vol1, Issue 6, 2014, pp. 570-577.

[22]IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, *IEEE Std.1609.2-2013*, April, 2013.

[23] K. Mershad, and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks", *IEEE Transactions on Vehicular Technology*, Vol. 62, No. 2, 2013, pp. 536 - 551.

[24] J.J. Huang, L-Y. Yeh, and H-Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks", *IEEE Transactions on Vehicular Technology,* Vol. 60, No. 1, 2011, pp.248-262.

[25] A. Agah, K. Basu, and S.K. Das, Preventing DoS attack in sensor networks: a game theoretic approach, *IEEE International Conference on Communications (ICC),* 2005.

[26] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, P. Bhattacharya, "A moderate to robust game theoretical model for intrusion detection in MANETs*, IEEE International Conference on Wireless & Mobile Computing, Networking & Communication,* Avignon, France , 2008, pp 608-612.

[27] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in Service-Oriented Vehicular Networks", *IEEE Wireless Communications* (2009), Vol. 16, No. 4, pp. 16-22.

[28] Network Simulator (NS-3). Available on http://www.nsnam.org.

[29] Simulation of Urban Mobility (Sumo). Available on http://sumo-sim.org/.

[30] T.H. Hai, E.N. Huh, and M. Jo, "A lightweight intrusion detection framework for wireless sensor networks", *Wireless Communications and Mobile Computing* 2010; Vol 10, No.4:559–572.

[31] A. Mabrouka, A. Kobbane, E. Sabir, J.B. Othman, M. ElKoutbi, "Meeting Always-Best-Connected paradigm in heterogeneous vehicular networks: Agraph theory and a signaling game analysis", *Vehicular Communications*, 2016.

[32] ITEA 2 CarCoDe project (2013-2015), http://www.itea2-carcode.org/

[33] H. Sedjelmaci, T. Bouali, SM. Senouci, "Detection and Prevention From Misbehaving Intruders in Vehicular Networks", *IEEE GLOBECOM*, Austin, USA, 8-12 December, 2014.