Signaling Game-based Approach to Improve Security in Vehicular Networks

Abdelfettah Mabrouk, Abdellatif Kobbane and Mohammed EL Koutbi
MIS/SIME Lab, ENSIAS, Mohammed V University of Rabat, Rabat, Morocco

Keywords: Vehicular Ad-hoc Networks, Signaling Game, Intrusion Detection Game.

Abstract: Secure communication between vehicle nodes is significant in Vehicular Ad Hoc Networks (VANETs). To guarantee public safety on the roads, vehicular networks need an appropriate security mechanism to protect them from various malicious attacks. In this paper we present an intrusion detection system available to detect internal malicious nodes. When an accident appear on the road, the vehicles must have information about this, but the existence of malicious nodes, the information will be deleted from the network. Because of this, we have adopted a mathematical model based on coalition and signaling game theory to design an Intrusion Detection Game (IDG) modeling the interaction between malicious nodes and the Coalition Head that equipped with Intrusion Detection System (CH-IDS) agent and seek its Bayesian Nash Equilibrium (BNE) for the optimal detection strategy.

1 INTRODUCTION

One special type of Mobile Ad hoc Networks (MANETs) is the network among moving vehicles, which is known as Vehicular Ad hoc Network (VANET). In such network, vehicles communicate with each other on the road or with equipment placed along the roads. This type of network is currently receiving increased attention from manufacturers and researchers to improve safety on the roads or proposed aid to drivers. VANETs differ MANETs in several ways: the high node mobility, large-scale networks, geographical constraints of topology, highly dynamic topology, the high stress of real-time, sporadic network connectivity, slow deployment, unreliable communication channels, etc.

Securing communications in wireless networks as in wired networks requires the implementation of mechanisms to achieve a number of general security objectives. These objectives include:

1. Authentication: allows network members to ensure the proper identity of the members with whom they communicate.
2. Non-repudiation: ensures that no issuer can not deny being the source of a message. This objective is essential in electronic transactions and all sensitive communications.
3. Confidentiality: guarantees that only authorized nodes that can access the data which transmitted across the network. These data may concern the application layer or the lower layers.
4. Integrity: ensures that the data exchanged are not subject to voluntary or accidental alteration. So it allows recipients to detect data tampering by unauthorized entities and reject the packages.
5. Availability: assure the entities authorized to access network resources with an adequate quality of services.

The mobility of nodes makes the topology of VANETs unstable. It is not easy for vehicle to know correctly the neighborhood. Attackers can thus forge and disseminate false topology information to build roads that pass through them and realize attacks designed to cause accidents or congestion of roads. By this means, an ad hoc non-secure routing protocol can be easily attacked. In addition, the mobility of attackers can also make them more difficult to detect or locate. The nature of radio transmission in the air, allowing a hacker to listen passively all messages exchanged in the emission zone, operating in “promiscuous mode” and using software that allows capturing transmitted packets (sniffer). The opponent will have access to the network and can easily intercept the data transmitted, without the issuer has knowledge of the intrusion. The intruder, being potentially invisible, can jam the radio channel to block the transmissions, in-

Mabrouk, A., Kobbane, A. and EL Koutbi, M.
Signaling Game-based Approach to Improve Security in Vehicular Networks.
DOI: 10.5220/0006784004950500
In *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018)*, pages 495-500
ISBN: 978-989-758-293-6

jected massive packets to exhaust the resources of nodes, save, edit, and then re-transmit packets as if they had been sent by a user legitimate. In ad-hoc networks there are some very sophisticated attacks, such as the wormhole attack, can only be committed by compromised nodes and are hard to avoid. The use of cryptography does not solve the problem of these nodes compromised by a simple authentication because these nodes are legitimate participants in the routing process prior to being controlled by the attacker, so we have to especially considering other solutions to this problem like detection approaches.

An Intrusion Detection System (IDS) is a mechanism that monitors a network or systems to identify abnormal or suspicious activities. It allows having information of failed or successful intrusions attempts. Solutions are proposed by IDS for detecting internal attacks. In order to minimize the impact of malicious vehicles, VANETs demand the IDS that is capable of detecting attacks that have broken down the network. In order to ensure their normal operation, VANETs will be able to respond and isolate the intruders using the IDS system. But before the IDS can be applied to the VANETs practically, there is a primary issue that has to be solved is how to select the profitable and optimal detection strategy.

Game theory is a mathematical tool that studies situations of conflict and cooperation between several involved players. It has been widely applied in the field of network security, preventing DoS attack (Mohi et al., 2009), and intrusion detection (Reddy, 2009). When a game in a system with incomplete information has many stages, the signaling game in which the posterior probability can be updated dynamically is always considered to model the system. Briefly, the signaling game is a dynamic game that studies the situation of incomplete information and involving two players: the first one (called the *Sender*) is informed and the second one (called the *Receiver*) is not. The strategy set of the *Sender* consists of actions contingent on its type while the strategy set of the *Receiver* consists of actions contingent on the *Sender*'s actions. Generally, in a signaling game, the *Sender* has a private information while the *Receiver* has a common information.

The intrusion detection in VANETs can be modeled as a signaling game. Generally, a classic IDS for guaranteeing VANET security is composed of the monitor and decision modules. The monitor module aims to check the VANET events while the decision module aims to decide whether an event is normal or not. This dynamic situation is an interaction between malicious vehicle nodes and the IDS that is designed and implemented to make VANETs secure. Signaling game is considered as a tool that is very profitable to depict the characteristic of interactive situations above. This approach can achieve the consequence of selecting the *Defend* strategy optimally, which will improve IDS' real positive outcomes.

In this paper, our work focused on the signaling game approach to study and analyze the interactions between a malicious vehicle node and a CH-IDS agent in VANETs. We set up the distributed-centralized network model, in which each vehicle has been equipped with an IDS agent. Not all IDS agents, but only the IDS agent in coalition head (CH-IDS) will launch to to reduce channel contention and packet collisions.

The rest of this paper is organized as follows. Section II presents related work based on the IDS' solutions in VANETs. The Intrusion Detection Game model, the stage Intrusion Detection Game, its pure and mixed strategy BNE are introduced in Section III. Finally, Section IV concludes this work.

2 RELATED WORK

The security issues on VANETs have become one of the primary concerns. Because of the high nodes mobility, the shared wireless medium and the absence of centralized security services in VANET, it is inherently very vulnerable to attacks than wired network. Cryptographic solutions, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have limited prevention and are not efficient in general, and they are designed for a set of previously known attacks. They are unlikely to avoid most recent malicious attacks. For this reason, there is a need of another technique to "detect and notify" these newer attacks, i.e. "intrusion detection". This section aims to present a current techniques of Intrusion Detection System (IDS) aware wireless networks. In (Pattnaik and Pattanayak, 2014), the authors have focused on some characteristics of VANETs with possible types of attacks based on intrusion detection. Also they have discussed the most suitable IDS technique like watchdog with their effect in VANETs. The application of VANETs is a rising technology which can provide the future directions of research in vehicular environment. In (Sen, 2010), the authors have proposed a cluster-based semi-centralized approach that integrates a local intrusion detection in a node or in a cluster. In the network architecture proposed in this work, the nodes are grouped into clusters which are monitored by cluster head while the inter-cluster communication takes place through gateways by using mobile agents

and every node maintains a database of known attack for signature based detection. In (Ghosh et al., 2009), a security system is proposed to detect the intruder that generates a false Post Crash Notification alert. While the vehicle that near a crash area issues this notification later. In (Zhang and Lee, 2000), the authors have proposed a cooperative distributed architecture where each node is responsible for detecting signs of intrusion locally using IDS agent. While the IDS agent is responsible for data collection and detection of malicious nodes, the neighbors IDS agents cooperate with each other for global intrusion detection. The model of the IDS agent is composed of six modules, then one among them called local data collection module, is responsible to collect real-time data. From data collected, the local module detection engine can decide if the system is attacked or not, and it can initiate a response if an attack is detected with specific evidence. This response can be executed by the local module response (local alert) or by the global module response (global alert). When an abnormality is detected with weak evidence, the cooperative detection engine module is executed and requests the cooperation of the other network nodes through another secured communication module called secure communication. In (Misra et al., 2011), a stochastic learning solution for intrusion detection (SLAID) is proposed 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 (Ruj et al., 2011), a data-centric detection system (DCMD) is proposed to identify the cyber-attacks that disseminate the false message alert, e.g. Post-Crash Notification (PCN) alert. The authors proposed in this work 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. The simulation results show that their system requires a low communication overhead to detect these cyber-attacks. However, the security performance is not evaluated when such attack occurs, e.g. detection rate. In (Sedjelmaci et al., 2016), an intrusion detection and prediction scheme has proposed to detect and especially predict the future misbehavior of a malicious vehicle. The attack prediction technique proposed in this work is based on a game theory to prevent the occurrence of malicious vehicles. Moreover, the detection scheme detects the most dangerous attacks that target a VANET such as false alerts and Sybil attacks.

Our work is distinguishable in terms of game type and equilibrium. We model the interactions between a vehicle and a CH-IDS agent with signaling game. In addition, we seek the pure and mixed strategy BNE for the stage game. These equilibriums determine when and how the CH-IDS agent takes a Defend action. Finally, we get different equilibrium equations as a result. Besides, our work is focused on the signaling game to decide the optimal strategy of intrusion detection in VANETs. In addition, we think that our network model is profitable to make the IDS agent reside in every vehicle, but only the IDS agent in coalition head (CH) performs intrusion detection based on the signaling game.

3 SYSTEM MODEL

3.1 Network Model

The use of techniques such as cryptography does not offer the ability to detect new attacks or even defend the network against internal nodes compromise. However, this type of system is used as first line of defense while the second line of defense is occupied by Intrusion Detection Systems commonly known by its acronym IDS. An IDS operates in three phases: a data collection phase followed by an analysis phase and finally a response phase to prevent or minimize the impact on the system. Generally, IDS is implanted in certain special nodes called monitors or monitoring nodes.

IDS can be classified as detection techniques as follow:

- Fault detection system: the system detects any behavior that deviates the preset normal behavior and triggers a response.
- Signature-based system: the system has a database of some attacks which are compared with the data collected. An attack is detected if the collected data coincide with an already registered malicious behavior.
- System based on specifications: the system defines a set of conditions that a protocol must meet. An attack is detected in the case where the program or protocol does not meet the established requirements of the operation.

IDS can also be classified according to the architecture into three categories :

- Purely distributed : the IDS checks the abnormal behavior of neighboring nodes locally.
- Purely centralized : the IDS is installed in the base station, which requires an additional routing protocol that collects data from nodes to analyze the behavior of each node.
- Distributed-centralized: the IDS is only installed in special nodes that play two roles at the same time, performing activities like normal nodes and checking for intrusion detection.

Our network model adopt the distributed-centralized approach in which IDS agents are deployed in each vehicle instead of installing it in the monitors' vehicles only. At the same time, coalition is used to organize our network into a connected hierarchy. By using coalitional game, vehicles are organized into coalitions. Each coalition has a coordinator, called the Coalition Head (CH), and a number of member vehicles. Coalition results form a two-tier hierarchy in which CHs represent the higher tier while member vehicles represent the lower tier. In this hierarchy, member vehicles send their data to the responsible CH while this latter aggregates the data and sends them to the Base Station (BS).

The vehicular network depicted in Fig. 1 consist of N vehicles and M gateways. The vehicles can form coalitions and the gateways can cooperate the transmission of the vehicles when they are in the same coalition. Let $V = \{1,2...,N\}$ and $G = \{1,2...,M\}$ represent the set of gateways (coalition head), respectively. We assume that :

1. All vehicles are equipped with GPS receivers.
2. Each vehicle uses GPS capabilities to obtain its current location and speed.
3. Vehicles' coalition are formed dynamically according to our previous work presented in (Mabrouk et al., 2015).

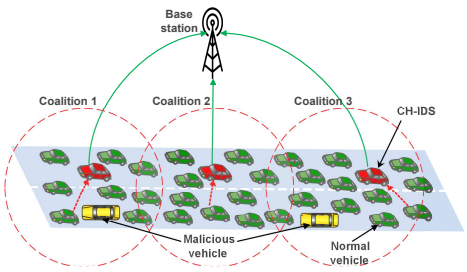

Figure 1: Network Model.

3.2 Stage Intrusion Detection Game

According to the characteristics of VANETs and IDS, we choose some parameters for our Intrusion Detection Game. When the malicious vehicle makes attacks to waste the VANETs resources, the network will be disrupted and gradually crashed during the communication between two vehicles which can cause unexpected events. This process gives malicious vehicle a payoff from their attacks; at the same time, they pay a cost of consumption due to their attacks. Therefore, for a malicious vehicle, we introduce g_A and c_A to denote attack gain and cost respectively. A member vehicle is available to communicate when it selects the action *Cooperate*, the packet then can be forwarded successfully. The normal member vehicle will benefit from this good network while the malicious vehicle will also get payoff for its disguise. In order to simplify, we suppose that both the normal and malicious nodes pay the same cost as well as get the same payoff. Therefore, for a member vehicle, we introduce c_C and g_C to denote cooperation cost and gain respectively. The CH-IDS agent gets the gain g_D, when it selects the *Defend* strategy, for having successfully detected the malicious member vehicle node. At the same time, it should pay for the cost, c_D, for energy consumption. Obviously, in the CH-IDS agent like any general IDS, there exist the detection rate and the false alarm rate denoted by α and β respectively. The false alarm means that the CH-IDS agent detects a member vehicle in normal communication in error, which will lead to a loss l_F.

Hence, we consider in our stage Intrusion Detection Game (IDG) two players: member vehicle as a *Sender S* denoted by θ_S, and CH-IDS agent as a *Receiver R* dented by θ_R. Member vehicle S may be *Normal* or *Malicious*, and its type is private information to CH-IDS agent R. At each time slot, the players choose their actions from their actions spaces. Because it wants to disguise itself, a malicious member vehicle S may attack or cooperate. When member vehicle S is *Normal*, it always cooperates. The CH-IDS agent should not always be the action *Defend*, sometimes it should be *Idle*. That is, the action of CH-IDS may be *Defend* or *Idle*. Table 1 presents different utilities of the Intrusion Detection Game (IDG).

Except IDS' *Idle*, all other actions in Table 1 incur costs. For the action profile (*Attack*, *Defend*), i.e. when a malicious vehicle chooses the *Attack* action and the CH-IDS agentchooses the *Defend* action, the utility of θ_S is the gain of being not detected minus the loss of being detected minus the attack cost while the utility of θ_R is the gain of detecting successfully minus the loss of not detecting minus the detection

Table 1: Utilities of intrusion detection game.

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

cost. In case of the action profile (*Attack*, *Idle*), the utility of θ_S is the attack gain minus the attack cost while the utility of θ_R is the loss of being attacked. For the action profile (*Cooperate*, *Defend*), the utility of θ_S is the cooperation gain minus the cooperation cost while the utility of θ_R is the loss of false alarm minus the defend cost. Thus, the static Intrusion Detection Game (IDG) is defined as follows.

The stage Intrusion Detection Game (IDG) is defined by 5-tuple (N, Θ, A, P, U) where:

- $N = \{$member vehicle S, CH-IDS agent $R\}$ is a set of 2 players;
- $\Theta = \Theta_S \times \Theta_R$, where Θ_S is the set of type space (malicious or normal) of the player S and Θ_R is the set of type space of the player R;
- $A = A_S \times A_R$, where A_S and A_R are the set of actions available to the player S (*Attack* or *Cooperate*) and the set of actions available to the player R (*Defend* or *Idle*) respectively;
- $P : \Theta \mapsto [0,1]$ is a probability distribution over types, $P = (p, 1-p)$ where p denotes the probability that a vehicle can be malicious node and $1-p$ denotes the probability that a vehicle can be normal node;
- $U = (u_S, u_R)$, where u_S is the utility function for the player S and u_R is the utility function for the player R, the values of u_S and u_R are illustrated in Table 1.

3.3 Equilibriums of Stage Intrusion Detection Game

As a game based on signaling game theory, the stage Intrusion Detection Game can attain Bayesian Nash equilibrium (BNE), but the CH-IDS agent R does not know the type of the member vehicle node S. A virtual player (*Nature*) is introduced at the beginning of the signaling game, and will act firstly to decide the type of player S.

Theorem 1. *In the stage Intrusion Detection Game, there is a pure-strategy BNE when*

$$p < (\beta \cdot l_F + c_D)/(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F) \quad (1)$$

Proof. 1) When a vehicle node S selects the pure-strategy (*Attack*, *Cooperate*) which means that vehicle S always plays *Attack* if it is malicious and *Cooperate* if it is normal. Then, according to Table 1, the expected utilities of *Defend* and *Idle* for the CH-IDS agent R are:

$$u_R(Defend) = p \cdot (\alpha \cdot g_D - (1-\alpha)\cdot g_A - c_D) + (1-p)\cdot(-\beta - l_F - c_D) \quad (2)$$

and

$$u_R(Idle) = -p \cdot g_A + (1-p)\cdot 0 = -p \cdot g_A \quad (3)$$

If $u_R(Defend) \geq u_R(Idle)$, we get

$$p \geq (\beta \cdot l_F + c_D)/(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F) \quad (4)$$

then the dominant strategy for the CH-IDS agent R is *Defend*. However, if CH-IDS agent R plays *Defend*, is reasonable that *Attack* will not be the dominant strategy for member vehicle node S because:

$$(1-\alpha)\cdot g_A - \alpha \cdot g_D - c_A < g_C - c_C \quad (5)$$

Therefore, (*Attack* for malicious vehicle, *Cooperate* for normal vehicle, *Defend* for CH-IDS agent) is not a pure strategy BNE.
If $u_R(Defend) < u_R(Idle)$, we get

$$p < (\beta \cdot l_F + c_D)/(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F) \quad (6)$$

then the dominant strategy for CH-IDS agent R is *Idle*. Correspondingly, *Attack* will be the dominant strategy for member vehicle node S because:

$$g_A - c_A > (1-\alpha)\cdot g_A - \alpha \cdot g_D - c_A \quad (7)$$

Therefore, (*Attack* for malicious vehicle S, *Cooperate* for normal vehicle S, *Idle* for CH-IDS agent R) is a pure-strategy BNE. 2) When vehicle S selects the pure-strategy (*Cooperate* for malicious vehicle, *Cooperate* for normal vehicle) which means it always plays the action *Cooperate* regardless of its type. For CH-IDS agent R, the best response to *Cooperate* of vehicle S is *Idle*; and for malicious vehicle, the best response to *Idle* of CH-IDS agent R is *Attack*. This is contradictive to the pure-strategy (*Cooperate* for malicious vehicle, *Cooperate* for normal vehicle), therefore, {*Cooperate*, *Cooperate*, *Idle*} is not a pure-strategy BNE.

In summary, when

$$p < (\beta \cdot l_F + c_D)/(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F) \quad (8)$$

there is a pure-strategy BNE {*Attack*, *Cooperate*, *Idle*} which means the malicious vehicle always plays *Attack* and the normal vehicle always plays *Cooperate* while the CH-IDS agent R always plays *Idle*. Although this pure-strategy BNE is not practical because CH-IDS agent R must take action *Idle*. That is, the malicious member vehicle nodes will not be caught forever. Therefore, for detecting malicious vehicle

nodes, it is essential to find a mixed-strategy BNE.

Theorem 2. *In the stage Intrusion Detection Game, there is a mixed-strategy BNE when*

$$p \geq (\beta \cdot l_F + c_D)/(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F) \quad (9)$$

Proof. Let $\sigma_S = (\rho, 1-\rho)$ and $\sigma_R = (\delta, 1-\delta)$ are the mixed strategy for the malicious vehicle S and the mixed strategy for the CH-IDS agent R, respectively. Then, according to Table 1, the expected utilities for the vehicle S and the the CH-IDS agent R are:

$$\begin{aligned} u_S(\rho,\delta) &= p\cdot\rho\cdot\delta\cdot((1-\alpha)\cdot g_A - \alpha\cdot g_D - c_A) \\ &+ p\cdot\rho\cdot(1-\delta)\cdot(g_A - c_A) + p\cdot(1-\rho)\cdot\delta\cdot(g_C - c_C) \\ &+ p\cdot(1-\rho)\cdot(1-\delta)\cdot(g_C - c_C) + (1-p)\cdot\delta\cdot(g_C - c_C) \\ &+ (1-p)\cdot(1-\delta)\cdot(g_C - c_C) \end{aligned} \quad (10)$$

and

$$\begin{aligned} u_R(\rho,\delta) &= p\cdot\rho\cdot\delta\cdot(\alpha\cdot g_D - (1-\alpha)\cdot g_A - c_D) \\ &+ p\cdot\rho\cdot(1-\delta)\cdot(-g_A) + p\cdot(1-\rho)\cdot\delta\cdot(-\beta\cdot l_F - c_D) \\ &+ p\cdot(1-\rho)\cdot(1-\delta)\cdot 0 + (1-p)\cdot\delta\cdot(-\beta\cdot l_F - c_D) \\ &+ (1-p)\cdot(1-\delta)\cdot 0 \end{aligned} \quad (11)$$

then, from $\partial_\rho(u_S(\rho,\delta)) = 0$ and $\partial_\delta(u_R(\rho,\delta)) = 0$ we get,

$$\rho^* = (\beta \cdot l_F + c_D)/(p\cdot(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F)) \quad (12)$$

and

$$\delta^* = (p\cdot g_A - p\cdot c_A - g_C + c_C)/(p\cdot(\alpha\cdot g_A + \alpha\cdot g_D)) \quad (13)$$

Since $\rho^* \leq 1$ because it is a probability, we have:

$$p \geq (\beta \cdot l_F + c_D)/(\alpha \cdot g_D + \alpha \cdot g_A + \beta \cdot l_F) \quad (14)$$

In summary, there is a mixed strategy BNE (*Attack*, *Cooperate*, *Defend*) when (14) is achieved, which means the malicious vehicle plays *Attack* with probability ρ^* and the normal vehicle always plays *Cooperate* while the CH-IDS agent R plays *Defend* with probability δ^*.

4 CONCLUSION

Because of its frequently changing network topology and deployed applications, the intrusion detection in VANETs is considered as a challenging task. Every individual wants to stay safer and secured on the road during driving. For this reason, we have proposed an Intrusion Detection Game based on the signaling game. This game simulating the interactions between vehicles and IDS agent indicates the characteristic of different stage of attack and defend. The stage Intrusion Detection Game has revealed the essence of VANETs at every individual slot time. At the same time, its pure-strategy BNE and mixed-strategy BNE have made the IDS agent choose *Idle* or *Defend* action, not always *Defend*. So, the CH-IDS agent can choose its optimal strategy for defending the malicious vehicle's *Attack* actively.

ACKNOWLEDGEMENTS

We appreciate and would like to thank the anonymous referees for their constructive comments and suggestions which will improve the presentation of this work supported by Mobile Intelligent System (MIS) Research Group, Laboratory of Mobile and Embedded Information System, ENSIAS, Mohammed V University of Rabat, Morocco

REFERENCES

Ghosh, M., Varghese, A., Kherani, A. A., and Gupta, A. (2009). Distributed misbehavior detection in vanets. In *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, pages 1–6. IEEE.

Mabrouk, A., Kobbane, A., Sabir, E., and Koutbi, M. E. (2015). Coalitional game theory for cooperative transmission in vanet: Internet access via fixed and mobile gateways. In *International Conference on Networked Systems*, pages 490–495. Springer.

Misra, S., Krishna, P. V., and Abraham, K. I. (2011). A stochastic learning automata-based solution for intrusion detection in vehicular ad hoc networks. *Security and Communication Networks*, 4(6):666–677.

Mohi, M., Movaghar, A., and Zadeh, P. M. (2009). A bayesian game approach for preventing dos attacks in wireless sensor networks. In *Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on*, volume 3, pages 507–511. IEEE.

Pattnaik, O. and Pattanayak, B. K. (2014). Security in vehicular ad hoc network based on intrusion detection system. *American Journal of Applied Sciences*, 11(2):337.

Reddy, Y. B. (2009). A game theory approach to detect malicious nodes in wireless sensor networks. In *Sensor Technologies and Applications, 2009. SENSORCOMM'09. Third International Conference on*, pages 462–468. IEEE.

Ruj, S., Cavenaghi, M. A., Huang, Z., Nayak, A., and Stojmenovic, I. (2011). On data-centric misbehavior detection in vanets. In *Vehicular technology conference (VTC Fall), 2011 IEEE*, pages 1–5. IEEE.

Sedjelmaci, H., Senouci, S. M., and Bouali, T. (2016). Predict and prevent from misbehaving intruders in heterogeneous vehicular networks. *Vehicular Communications*.

Sen, J. (2010). An intrusion detection architecture for clustered wireless ad hoc networks. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on*, pages 202–207. IEEE.

Zhang, Y. and Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 275–283. ACM.