Munster Technological University
SWORD - South West Open Research Deposit

Publications Riomh

2021-03-03

Cyber Security Framework for Vehicular Network based on a Hierarchical Game

Hichem Sedjelmaci
IRT SystemX, Palaiseau, France

Imane Horiya Brahmi
Atomic Energy Comission (CEA), Grenoble, France

Nirwan Ansari
Electrical and Computer Engineering, Newark College of Engineering, New Jersey Institute of Technology, Newark, NJ, USA

Mubashir Husain Rehmani
Department of Computer Science, Munster Technological University, Bishopstown Campus, Cork, Ireland, mubashir.rehmani@cit.ie

Follow this and additional works at: https://sword.cit.ie/riomhart

 Part of the Computer Sciences Commons

Recommended Citation

H. Sedjelmaci, I. H. Brahmi, N. Ansari and M. H. Rehmani, "Cyber Security Framework for Vehicular Network Based on a Hierarchical Game," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 1, pp. 429-440, 1 Jan.-March 2021, doi: 10.1109/TETC.2018.2890476.

This Article is brought to you for free and open access by the Riomh at SWORD - South West Open Research Deposit. It has been accepted for inclusion in Publications by an authorized administrator of SWORD - South West Open Research Deposit. For more information, please contact sword@cit.ie.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

Cyber Security Framework for Vehicular Network based on a Hierarchical Game

Hichem Sedjelmaci, *Member, IEEE,* Imane Horiya Brahmi, *Member, IEEE,* Nirwan Ansari, *Fellow, IEEE,* and Mubashir Husain Rehmani, *Senior Member, IEEE*

Abstract—The growth of electronic devices in connected vehicles and their connections to the untrusted network, present unprecedented exposure to attacks. Therefore, a reliable and efficient cyber security framework is mandatory to protect vehicular networks against the cyber attackers. Thereby, we propose a cyber defense framework based on a hierarchical cooperative game to secure legitimate vehicles from attacks. In the proposed hierarchical game, there are two kinds of players, the head agent and secondary agents that cooperate between each other to detect, predict and react efficiently against suspected attacks. The Intrusion Detection System (IDS), Intrusion Prediction System (IPS), and Intrusion Reaction System (IRS) represent the secondary players, where their strategies are to carry out the detection, prediction and reaction actions, respectively. The Intrusion Decision Agent (IDA) is the head player and is responsible for making decisions in launching the strategies of IDS, IPS and IRS players. The secondary and head agents are to collaborate in order to decrease the false positive and false negative rates, while minimizing the processing delay and overhead. Numerical results show that, our cyber defense game requires low communications overhead and low delay to achieve low false positive and false negative rates as compared to the current intrusion detection and prediction frameworks.

Index Terms—VANET, Hierarchical game model, Cyber security framework, Delay, Overhead.

1 Introduction

Vehicular ad hoc network (VANET) is an important component of the Intelligent Transportation System (ITS), due to their important role in making the road safer and the traveling experience more pleasant. In VANET, the car is considered as a smart mobile node equipped with diverse communication technologies such as 802.11p and cellular networks such as 3G/4G to communicate efficiently with its neighboring cars and the external network, e.g. Internet [1]. Recently, vehicular networks have become the subject of a variety of cyber threats, which can be classified as attacks that target the integrity, availability, and confidentiality of a vehicle [2], [3]. The threats that target the integrity aim to inject fake data, and force the infected vehicles to broadcast false information and drop all the packets that circulate through their radio range. The main purposes of availability attacks such as Denial of Service (DoS) attacks is to exhaust the bandwidth, jam the wireless communications, and disturb network operations [4]. The passive attack or the cyber threat that targets confidentiality, probes the most attractive node (e.g., cluster head) and the most sensitive data by launching its promiscuous mode, i.e., overhearing all the traffic that circulates through its radio range. Afterward, the attacker switches from a passive mode to an active mode in order to launch a cyber-attack, e.g., dropping packets and spreading false information. Launching these attacks against the vehicle nodes is considered harder as compared to the traditional IT network, because of the critical organs of a vehicle that could be infected by a malicious software are massively interconnected black box systems. Furthermore, several research scientists in industry and academia have shown that the vehicle node could be hacked by an external hacker, by launching an attack from a remote device and executing locally a malicious software in the infected vehicle's hardware [5], [6]. Therefore, a reliable and efficient cyber security framework is mandatory to deter external and internal attacks.

The current cyber security framework developed for VANET is either based on Intrusion Detection System (IDS) or Intrusion Prediction System (IPS) [3], [5] [7], [8], [9], [10], [11], [12], [13]. The authors in [12], [13], [14] proposed a new security framework for vehicular networks, where the IDS and IPS are launched simultaneously to detect the current and future misbehavior of attackers. According to their simulation results, they proved that when the number of vehicles is lower than 300 nodes, their framework exhibits a high detection with a low overhead. However, the security framework requires a high communications overhead to detect and predict accurately the misbehaviors when there are more than 300 nodes. This communication overhead could affect the V2X (vehicle to vehicle and vehicle to infrastructure) communications; therefore, the safety of passengers and cars could be threatened [15]. Moreover, the decision delay for an IDS and IPS agents to react against cyber attacks could degrade the performances of the proposed security framework and affect the V2X communications. When the decision delay is low, the security framework will not have enough time to detect and predict the current and future misbehaviors of cyber-attacks. On the other hand, when this delay is high, the security framework exhibits a high overhead. To overcome these issues and detect almost all attacks that infect the legitimate vehicles, we propose a Cyber Defense Game (CDG) for VANET.

CDG aims to minimize the delay and communication over-

- *H. Sedjelmaci is with IRT SystemX, 8 avenue de la Vauve 91120 Palaiseau, France.*
  E-mail: hichem.sedjelmaci@irt-systemx.fr
- *I.H. Brahmi is with Atomic Energy Comission (CEA), Grenoble, France.*
  E-mail:hi.brahmi@gmail.com
- *N. Ansari is with Electrical and Computer Engineering, Newark College of Engineering, New Jersey Institute of Technology, New Jersey, USA.*
  E-mail: Nirwan.Ansari@njit.edu
- *M.H. Rehmani is with Waterford Institute of Technology, Ireland.*
  E-mail: mshrehmani@gmail.com

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

head, while reducing the false positive and false negative rates. The CDG framework is based on multiple security agents: IDS, IPS and Intrusion Reaction System (IRS) to detect, predict, and react promptly against attacks. The IRS agent triggers different reactions, which depend on the type of the attack before a critical damage occurs (e.g., vehicles crash). Our security framework relies on a hierarchical cooperative game to activate optimally these security agents, i.e., finding a tradeoff between the network metrics (overhead and delay) and security metrics (false positive and false negative) in the activation of IDS, IPS and IRS. In the hierarchical cooperative game, there are two types of players, the secondary agents, which are the IDS, IPS and IRS, and the head agent, which is the Intrusion Decision Agent (IDA). The role of IDA is to launch the secondary agents while maintaining a tradeoff between the network and security metrics. To the best of our knowledge, this is the first cyber security framework that takes into account of the delay and overhead as the main parameters for influencing the decision-making taken by the head agent IDA. The decision provided by IDA is to request the secondary agents to launch the detection, prediction and/or reaction strategies. The optimal solution is attained when the secondary players launch the strategies that the head player requests. To validate the proposed CDG, we have conducted numerous simulation scenarios using NS-3 (Network Simulator 3). The achieved performances are promising in the sense that our security framework achieves low false positive and low negative rates as compared to the existing intrusion detection and prediction frameworks for VANETs. These results are achieved for a large-scale vehicular network, where CDG exhibits a low overhead and low delay.

The rest of this paper is structured as follows: in Section 2, we highlight the most notable research papers that have motivated our work and in Section 3, we present the cyber defense architecture for the vehicular network. In Section 4, we describe our hierarchical security game by detailing the security mathematical model and the corresponding proofs. In Section 5, we assess CDG and present/discuss the obtained simulation results. Finally, we present our conclusions and highlight some future works in Section 6.

2 RELATED WORK

IDS is classified into two classes: (i) Network IDS (N-IDS) monitors the flux of data originated from the antenna of the vehicle and focuses on the detection of remotely instigated external attacks [16], which target the critical organs of the vehicle (e.g., decision pilot, radar, and camera). (ii) Host IDS (H-IDS) analyzes the behavior of hardware upon which the IDS is activated and focuses on the detection of the malicious code that runs locally in the hardware. Both N-IDS and H-IDS have the capability to detect only the current misbehavior of the attacker or the current execution of malicious software that runs within the infected vehicle [17]. Furthermore, to detect the future misbehavior of an attacker, the IPS agent is used to monitor and track the future malicious patterns of attackers.

Several previous works have addressed the issue of intrusion detection and prevention in vehicular networks [3], [5] [7], [8], [9], [10], [11], [12], [13]. The authors in these works proposed detection and prediction frameworks to detect and predict respectively the current and future misbehavior of intruders. Their frameworks are based on a distributed, centralized or hybrid IDS (IPS) to protect the vehicular networks against the attacker or a group of attackers. The authors in [3], [7] proposed collaborative intrusion detection frameworks, where the IDS agent is activated at each vehicle to monitor locally and globally the behavior of the legitimate vehicle and the behaviors of the suspected vehicle's neighbors, respectively. They focused on the protection of VANET against DoS attacks, such as black hole and selective forwarding threats and false alert generation attacks. According to their simulation results, an important number of internal attacks are detected with a low false positive rate. However, when collaborative cyber-attacks are launched simultaneously, the detection rate decreases exponentially, especially when the number of attacks increases. Yu et *al*. [8] aimed to protect the vehicular networks against the most lethal threat, Sybil attack. In their research results, they found that the signal strength is the main feature required to detect this attack. They developed a signature-based detection technique to monitor the malicious signal that the Sybil node generates. In the simulation results, they proved that, almost all Sybil nodes are detected. However, their solution requires a certain delay to detect the attack since the IDS must parse all the signatures before making a decision. In [5], a host-based IDS solution is developed to protect the VANET against false data injection and Sybil attacks. To detect these attacks, the IDS uses a statistical technique to model a normal pattern of the legitimate vehicle and hence the behavior of a vehicle that deviates from this normal pattern is categorized as an infected node. In the simulation results, the authors proved that almost all attacks are detected. However, their solution requires a certain decision delay to react against the detected attack as each host IDS waits for the decision of the other IDS neighbors to make its own decision, e.g., stores the infected vehicle in the blacklist. In [9], a new intrusion detection framework, named Rule-Enforced Security Technique (REST-Net) is developed to secure the vehicular networks against the attacks that alter the beacons messages and/or send fake messages. Their IDS solution is based on a plausibility checks approach to verify if the broadcasted messages are fake or not. This approach is based on a couple of dynamic rules, where each rule could contain a set of security thresholds. The threshold is updated over time, and depends on the attack that is detected by the IDS. The authors aimed to detect two types of attacks: the constrained threat and the unbounded threat. The first threat alters the beacon message and forces the legitimate vehicles to clear the road, while the second threat alters the identities of privileged cars (e.g., firefighter truck). In the simulation results, REST-Net exhibits high true negative and true positive rates. However, REST-Net generates a high false positive rate especially when the true positive increases. In [10], an anomaly detection technique based on a neural network is developed to enhance the security in a vehicular network. The anomaly detection is used by the network IDS to detect the malicious packets, for instance, the packet that is sent remotely by the attacker or a modified packet. The proposed network IDS relies on the unsupervised training algorithm in order to increase the detection accuracy, i.e., improve the true positive and the true negative rates. Their security solution is embedded in a Controller Area Network (CAN) bus and the obtained results are promising in the sense that their approach achieves a high level of security when attackers launch their attacks against the CAN. The major drawback of this solution is the high overhead and a high reaction delay since the IDS is based on a heavy algorithm for its detection and reaction process. As in [10], Boudguiga et *al*. [11] aimed to enhance the security of the CAN by proposing a lightweight IDS. They proposed to embed at each microcontroller an IDS agent to monitor the CAN and hence identify the infected frames. The

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

detection rules defined in this research work have the ability to detect Denial of Service (DoS) attacks. DoS attacks that target the CAN aim to prevent the electronic control units to access the CAN bus. According to their security analysis, they proved that their lightweight IDS could detect accurately this kind of DoS attacks. However, they did not analyze the performances of their solution within the simulators dedicated for VANET or in a real environment.

Recently in [12], [13], the authors developed new security frameworks to predict the future misbehavior of attackers and hence prevent their occurrences. To the best of our knowledge, these works were the first that propose an IPS solution for vehicular networks. Specifically, Bouali et *al*. [12] proposed a distributed intrusion prediction systems for VANET. The main goal of their system is to predict network attacks such as DoS and false alert attacks, and hence prevent their occurrence. In the simulation results, it is apparent that their system exhibits a high prediction rate and low false positive rates, when these network attacks occur. Sedjelmaci et *al*. [13] developed an intrusion prediction framework based on a game theory to secure the legitimate vehicles against the malicious devices that aim to launch future lethal attacks and hence create chaos the within network. In their approach, they modeled the interaction between the attackers and IPS as a non-cooperative game, where the IPS is activated in a centralized node, i.e., service center. The centralized IPS framework is embedded in NS3 (Network Simulator 3) [18], where the obtained performances are promising in the sense that the framework is able to predict with a high accuracy the future misbehavior of attacks as compared to the contemporary intrusion detection frameworks. In both attack prediction frameworks proposed in [12], [13], distributed IDS solutions are also developed to detect the current attack that occurs within a network. In their simulation results, they showed that both frameworks generate a low overhead in the detection and prediction process. Furthermore, after further simulations, it is apparent that, when the number of vehicles is over 350, the overhead and decision delay increase exponentially because of the simultaneous activation of the IPS and IDS, and the increase of audit messages (which contain the features and identities of infected vehicles) exchanged between vehicles. In Table 1, we compare the different approaches discussed above in the scaling mode (i.e., over 350 nodes), based on the following criteria:

- Attack prediction
- Attack detection
- Communication overhead
- Decision delay

Table 1: Comparison between IDS and IPS frameworks for VANET

Security frameworks	Attack prediction	Attack detection	Communication overhead	Decision delay
[3]	No	Yes	Low	Medium
[7]	No	Yes	Medium	Medium
[8]	No	Yes	Low	High
[5]	No	Yes	Low	High
[9]	No	Yes	/	/
[10]	No	Yes	High	High
[11]	No	Yes	Low	Low
[12]	Yes	Yes	High	High
[13]	Yes	Yes	High	High

In this research work, we circumvent the drawbacks mentioned above and propose a novel cyber defense framework for a large-scale vehicular network that aims to launch respectively the detection, prediction and reaction process only when an attack occurs or is expected to occur, while taking into account the decision delay and the communication overhead.

3 SECURITY ARCHITECTURE

CDG is activated at vehicle nodes and equipped with the following multi-agent systems, IDS, IPS, IRS and IDA, as shown in Figure 1. These security agents are defined as follows:

- H-IDS monitors locally the behavior of a vehicle, where it is activated and hence deters an internal intruder (e.g. executes locally a malicious software) from launching an attack. N-IDS is used to protect the vehicular network against an external intruder from discovering a security breach within 802.11 p or/ and 3G/4G networks and launching lethal attacks, such as Sybil or false data injection attacks. Both systems, N-IDS, and H-IDS, rely on a specification based detection technique [19], [20], [21] to detect the intruders. This statistical technique builds a normal pattern of a target vehicle by using a set of security rules. Hence, the vehicle is detected as an infected node when its behavior deviates from this normal pattern. N-IDS and H-IDS activated within a vehicle can collaborate with other IDSs that are within the same neighborhood in order to update the security rules and hence decrease the false positive and false negative rates. Both IDSs are equipped with the following modules: (i) Data monitoring module: H-IDS monitors the process and software that are executed within a monitored vehicle and N-IDS collects the network packets coming from 802.11 p and 3G/4G networks. (ii) Detection module: the IDSs rely on a couple of security rules related to each attack pattern to detect the intrusions. (iii) Rule update module: to increase the detection rate and decrease the false positive rate, each IDS collaborates with its neighborhood node by exchanging the security rules and hence updates their backlist databases. Readers are referred to [5], [7], [10] for more detail on how to detect the internal and external intruders by H-IDS and N-IDS.
- A distributed IPS solution is used to predict the future misbehaviors of intruders before a critical damage occurs. In this solution, each IPS (activated at the vehicle) collaborate with its neighbors IPSs to predict accurately the attacks. The most promising prediction techniques that have been applied in the traditional network include neural network, support vector machine, Markov chain, Kalman filter and game theory. A machine learning based on game theory could be a propitious learning technique to predict accurately the attacks while taking into account the resource constraints [22], [23], [24] of a target network. A centralized prediction framework based on game theory [13], [14] has recently been proposed to protect the VANET against the most lethal threats that could occur in the near future. As mentioned in the related work, such framework is not suitable for a large-scale network as it incurs a large overhead and high decision delay. To overcome these issues, a distributed prediction game is a potential solution for such large-scale network. The prediction game could be modeled as $L_i(Q'_1, S'_1)$ and $L'_j(Q'_2, S'_2)$ [25], where Q'_1 and Q'_2 are respectively the

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

gains of IPS (activated at vehicle i) and $attacker_j$, and S'_1 and S'_2 are respectively the sets of strategies that IPS_i and $attacker_j$ possess. The goal of IPS is to determine the future stable state defined as a Nash equilibrium, in which $attacker_j$ will launch an attack against vehicle i. Readers are referred to [12], [13] for more details on how to predict the misbehavior of vehicles by using game theory and Kalman filtering.

- IRS triggers a set of actions when the IDS or/and IPS detects and predicts an attack, respectively. These actions depend on the severity level of the detected (predicted) attacks. If a group of hackers launches several attacks simultaneously, the reaction time against each attack depends on the nature of the threat. For instance, when a lethal threat such as broadcasting a false warning is launched by an adversary, IRS should respond immediately to avoid traffic collision. The actions that the IRS triggers can be summarized as follows: (i) IRS broadcasts a blacklist with a list of infected vehicles to neighboring vehicles, thus preventing the vehicles (nodes) from communicating with these infected vehicles (nodes). (ii) IRS changes the pseudonym of a vehicle (where IRS is activated in the vehicle) and requests the legitimate vehicles located within its neighborhood to change their pseudonyms, thus [26] preventing the attacker from tracking the target vehicle. (iii) IRS updates the cryptography keys periodically to ensure the communication privacy and prevents the attackers from altering the data exchanged between vehicles.
- IDA plays the role of a head agent and its main function is to activate the secondary agents: IDS, IPS and IRS, while taking into account of the delay and overhead constraints. The head agent aims to maximize its payoff and improves the reward of each secondary agent by computing the best response of each one of them. In this work, we assume that the IDS, IPS, IRS and IDA agents are honest and not selfish, and all the information that IDA receives from other agents are correct. In fact, this assumption should hold since the proposed hierarchical game cannot resolve the non-cooperative game in which each agent tries to infect negatively the payoff of other agents, e.g., an IDS agent provides a false detection (i.e., claims the honest vehicle as malicious) to IDA.

Once misbehaviors are identified by the head agent IDA, IDA will request the IDS, IPS and IRS to execute the detection prediction and reaction process, respectively; then, the IDS, IPS and IRS will respond by deciding whether to follow the request in activating the requested processes.

4 HIERARCHICAL SECURITY GAME

The hierarchical cooperative game is composed of two interrelated cooperative games [27] [28] [29] to determine a tradeoff between the network and security metrics. In the upper-level, the head agent IDA determines the optimal strategies (i.e., whether to launch the detection, prediction and reaction actions) that could be undertaken by the secondary agents. These optimal strategies depend on the costs imposed on the secondary agents to achieve their expected rewards. In the lower-level, the secondary agents play their best strategies by taking into account of the strategies envisaged by the head agent. The rewards and costs of the IDS, IPS, IRS and IDA are defined in Subsection 4.1, and q_1, q_2 and q_3 are the probabilities of the secondary agents in launching their detection, prediction and reaction strategies, while p_1, p_2 and p_3 are the probabilities of the head agent to request the IDS, IPS and IRS to launch their optimal strategies. In the proposed game, there is cooperation between players in order to increase the total payoff function of the game, i.e., increasing the rewards and minimizing the costs [30], [31]. This is unlike the non-cooperative game, where each player aims to increase its own payoff and decreases the payoff of its opponents.

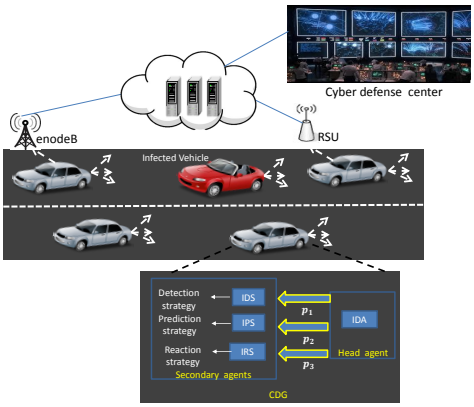


Figure 1: Cyber defense architecture for a vehicular network: optimal activation of IDS, IPS and IRS agents by the head agent, IDA.

In this section, first of all, we determine the payoffs of the secondary and head agents. Afterward, we determine the optimal strategies of the players in which a tradeoff between the rewards and costs are maintained. At last, we define the consensus game between our CDG and the attacker.

4.1 Payoff functions

The payoff functions of the secondary players depend on the required costs to obtain the optimal rewards. The rewards of the secondary agents include the detection and prediction accuracies of cyber-attacks, and the reaction rate against these threats (e.g., broadcasting a list of suspected vehicles). The costs are the communication overheads and decision delays that the secondary agents generate and are required respectively, to achieve the optimal rewards. The payoff functions of the secondary agents (u_{IDS}, u_{IPS} and u_{IRS}) can be modeled as described in Equations (1), (2) and (3).

$$u_{IDS}(D'_{IDS}, O'_{IDS}) = \max_{O'_{IDS}, D'_{IDS}} \sum_{ij} \left(\frac{u^1_{IDS} \times u^2_{IDS}}{D'_{IDS} + O'_{IDS}}\right), \quad (1)$$

$$\text{s.t.} \quad \sum_{i=0}^{T} D'_{IDS_i} \leq D_{IDS_{max}}, \quad \sum_{j=0}^{T} O'_{IDS_j} \leq O_{IDS_{max}}, \quad D'_{IDS_i} \times O'_{IDS_j} \geq 0.$$

where

- $u^1_{IDS} = x - e^{D'_{IDS_i}}$
- $u^2_{IDS} = x - e^{O'_{IDS_j}}$

$x \in [0, 1]$ is the attack detection rate by the IDS, O_{IDS} is the communication overhead incurred by the IDS to detect the

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

attack, D_{IDS} is the processing delay incurred by IDS to detect attack. $D' \in [0,1]$ and $O' \in [0,1]$ are the normalized values. For instance, the normalized value of D_{IDS} is computed as follows:

$$D'_{IDS} = \frac{D_{IDS_i} - D_{IDS_{min}}}{D_{IDS_{max}} - D_{IDS_{min}}},$$

where $D_{IDS_{min}}$ and $D_{IDS_{max}}$ are the minimum and maximum of all obtained delays during attack detection, and D'_{IDS} is the ith normalized delay. Each time period is indexed by $0 \leq i, j \leq T$ where T is the total number of periods

The communication overhead and delay are the two main parameters taken into account in developing a security mechanism for a vehicular network. When the values of these parameters increase, they could impact the safety of the vehicles. For example, an important overhead due to detection framework communications may impact the reception of V2X safety critical messages. Meanwhile, an important reaction delay may lead to catastrophic situations when attacks on critical components of a vehicle are not detected and prevented quickly. Therefore, the exponential functions are used to represent the generated overhead and the required delay for attack detection, in which the value of payoff u_{IDS} decreases rapidly when the values of these parameters increase.

$$u_{IPS}(D'_{IPS}, O'_{IPS}) = \max_{O'_{IPS}, D'_{IPS}} \sum_{ij} \left(\frac{u^1_{IPS} \times u^2_{IPS}}{D'_{IPS} + O'_{IPS}}\right), \quad (2)$$

$$\text{s.t.} \quad \sum_{i=0}^{T} D'_{IPS_i} \leq D_{IPS_{max}},$$
$$\sum_{j=0}^{T} O'_{IPS_j} \leq O_{IPS_{max}},$$
$$D'_{IPS_i} \times O'_{IPS_j} \geq 0.$$

where

- $u^1_{IPS} = y - e^{D'_{IPS_i}}$
- $u^2_{IPS} = y - e^{O'_{IPS_j}}$

$y \in [0,1]$ is the attack prediction rate by the IPS, O_{IPS} is the communication overhead incurred by the IPS to predict the attacks and D_{IPS} is the processing delay incurred for the prediction process. Here, as described in Section 3, the process of the attack prediction is done in a distributed manner, where the IPS relies on its local information and those of its neighbors to predict the future misbehavior of an attacker. $D'_{IPS} \in [0,1]$ and $O'_{IPS} \in [0,1]$ are respectively the normalized values of the overhead and delay.

$$u_{IRS}(D'_{IRS}, O'_{IRS}) = \max_{O'_{IRS}, D'_{IRS}} \sum_{ij} \left(\frac{u^1_{IRS} \times u^2_{IRS}}{D'_{IRS} + O'_{IRS}}\right), \quad (3)$$

$$\text{s.t.} \quad \sum_{i=0}^{T} D'_{IRS_i} \leq D_{IRS_{max}},$$
$$\sum_{j=0}^{T} O'_{IRS_j} \leq O_{IRS_{max}},$$
$$D'_{IRS_i} \times O'_{IRS_j} \geq 0.$$

where:

- $u^1_{IRS} = e^z - D'_{IRS_i}$
- $u^2_{IRS} = e^z - O'_{IRS_j}$

$z \in [0,1]$ is the reaction rate. As explained in Section 3, the reaction could be, for instance, preventing the legitimate vehicles from communicating with the infected vehicles or launching a new key updating process. O_{IRS} and D_{IRS} are respectively the communication overhead and the processing delay incurred by the IRS agent to react to attackers. $D'_{IRS} \in [0,1]$ and $O'_{IRS} \in [0,1]$ are the normalized values.

Note that the reaction action is mandatory in vehicular networks since the cyber-attacks that target the vehicles could be lethal, for example, hacking the braking system to disable the vehicle brakes. Therefore, the exponential function is used for computing z.

The IDA's cost depends on the overhead and delay incurred by the head agent to launch optimally the strategies of IDS, IPS and IRS agents. The false decision rate increases when the IDA requests the secondary agents to trigger their strategies to secure the vehicle or its neighborhood when there is no attack. The communication overhead and processing delay are the costs incurred by the IDA to implement the detection, prediction and/or reaction strategies. The payoff function of IDA is computed as

$$u_{IDA} = \frac{(O'_{Total} - e^f).(D'_{Total} - e^f)}{\sum_{j=0}^{T} O'_{IDA_j} + \sum_{i=0}^{T} D'_{IDA_i}}, \quad (4)$$

where:

- $O'_{Total} = \sum_{j=0}^{T} O'_{IDS_j} + \sum_{j=0}^{T} O'_{IPS_j} + \sum_{j=0}^{T} O'_{IRS_j}$
- $D'_{Total} = \sum_{i=0}^{T} D'_{IDS_i} + \sum_{i=0}^{T} D'_{IPS_i} + \sum_{i=0}^{T} D'_{IRS_i}$

$f \in [0,1]$ is the false decision rate. As the false decision provided by IDA could impact the security performance of CDG, we represent f by an exponential function. The costs caused by the head IDA are normalized, $D'_{IDA} \in [0,1]$ and $O'_{IDA} \in [0,1]$.

Figure 2 and Table 2 illustrate the extensive representation of our hierarchical security game and the correspondent strategic representation of head-secondary payoff matrix. In the proposed game, the IDA acts first by setting the requested probabilities p_1, p_2, and p_3. The secondary players then act by setting the probabilities q_1, q_2 and q_3 of executing their detection, prediction and reaction process, respectively, after having observed p_1, p_2, and p_3.

Table 2: Payoff matrix of a hierarchical security game

		Secondary agents		
		Detection (q_1)	Prediction (q_2)	Reaction (q_3)
Head agent	Detection (p_1)	(u^*_{IDA}, u^*_{IDS})	(u_{IDA}, u_{IPS})	(u_{IDA}, u_{IRS})
	Prediction (p_2)	(u_{IDA}, u_{IDS})	(u^*_{IDA}, u^*_{IPS})	(u_{IDA}, u_{IRS})
	Reaction (p_3)	(u_{IDA}, u_{IDS})	(u_{IDA}, u_{IPS})	(u^*_{IDA}, u^*_{IRS})

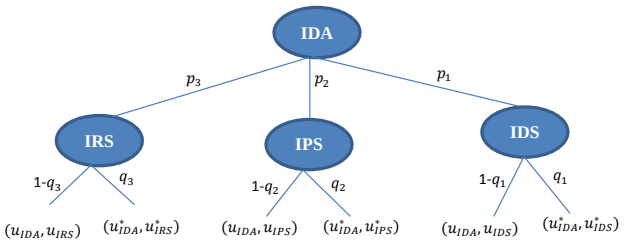


Figure 2: Extensive-form representation of a hierarchical security game

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

4.2 Hierarchical security game solution

In the proposed hierarchical cooperative game, the head player IDA computes the optimal delays and overheads incurred by the secondary players IDS, IPS and IRS to achieve high detection, prediction and reaction rates. According to these optimal costs, the secondary players decide whether to activate (or not) the strategies requested by the head player. Therefore, the equilibrium is attained when the secondary players launch the strategies that the head player requests.

Lemma 1. Equations (5), (6), (7) and (8) are respectively the best response (φ) of the IDS, IPS, IRS and IDA agents, where x^{φ} is the number of attacks that are detected with a high accuracy, y^{φ} is the number of attacks that are predicted with a high accuracy, z^{φ} is the number of reactions against attackers, $f^{'\varphi}$is the number of correct decisions made by IDA toward the IDS, IPS and IRS, and $f^{'} = 1 - f$.

$$x^{\varphi} = \frac{e^{\sum_{i=0}^{T} D'_{IDS_i}} + e^{\sum_{j=0}^{T} O'_{IDS_j}}}{2}. \tag{5}$$

$$y^{\varphi} = \frac{e^{\sum_{i=0}^{T} D'_{IPS_i}} + e^{\sum_{j=0}^{T} O'_{IPS_j}}}{2}. \tag{6}$$

$$z^{\varphi} = \ln\left(\frac{\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}}{2}\right). \tag{7}$$

$$f^{'\varphi} = \ln\left(\frac{2e}{O'_{Total} + D'_{Total}}\right). \tag{8}$$

Proof 1. The best responses (φ_s) of the secondary agents, IDS, IPS and IRS, and the head IDA are determined by computing respectively the first derivative of u_{IDS}, u_{IPS}, u_{IRS} and u_{IDA}. The first derivative of u_{IDS} with respect to x is

$$\frac{\partial u_{IDS}}{\partial x} = \frac{2x - (e^{\sum_{i=0}^{T} D'_{IDS_i}} + e^{\sum_{j=0}^{T} O'_{IDS_j}})}{(\sum_{i=0}^{T} D'_{IDS_i} + \sum_{j=0}^{T} O'_{IDS_j})}.$$

By fixing $\frac{\partial u_{IDS}}{\partial x} = 0$, we get $x = \frac{e^{\sum_{i=0}^{T} D'_{IDS_i}} + e^{\sum_{j=0}^{T} O'_{IDS_j}}}{2}$.
The first derivative of u_{IPS} with respect to y is

$$\frac{\partial u_{IPS}}{\partial y} = \frac{2y - (e^{\sum_{i=0}^{T} D'_{IPS_i}} + e^{\sum_{j=0}^{T} O'_{IPS_j}})}{(\sum_{i=0}^{T} D'_{IPS_i} + \sum_{j=0}^{T} O'_{IPS_j})}.$$

By fixing $\frac{\partial u_{IPS}}{\partial y} = 0$, we get $y = \frac{e^{\sum_{i=0}^{T} D'_{IPS_i}} + e^{\sum_{j=0}^{T} O'_{IPS_j}}}{2}$.
The first derivative of u_{IRS} with respect to z is

$$\frac{\partial u_{IRS}}{\partial z} = \frac{2e^{2z} - (\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}).e^{z}}{\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}}.$$

By fixing $\frac{\partial u_{IRS}}{\partial z} = 0$, we get $z = \ln\left(\frac{\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}}{2}\right)$.
The first derivative of u_{IDA} with respect to f' is

$$\frac{\partial u_{IDA}}{\partial f'} = \frac{e^{1-2f'}.(e^{f'}.(O'_{Total} + D'_{Total}) - 2e)}{\sum_{j=0}^{T} O'_{IDA_j} + \sum_{i=0}^{T} D'_{IDA_i}}.$$

By fixing $\frac{\partial u_{IDA}}{\partial f'} = 0$, we get: $e^{f'}.(O'_{Total} + D'_{Total}) - 2e = 0$ as $e^{1-2f'}$ is strictly positive. Thus,

$f' = \ln\left(\frac{2e}{O'_{Total} + D'_{Total}}\right)$
The second derivatives of u_{IDS}, u_{IPS}, u_{IRS} and u_{IDA} are

$$\frac{\partial^2 u_{IDS}}{\partial^2 x} = \frac{2}{(\sum_{i=0}^{T} D'_{IDS_i} + \sum_{j=0}^{T} O'_{IDS_j})}. \tag{9}$$

$$\frac{\partial^2 u_{IPS}}{\partial^2 y} = \frac{2}{(\sum_{i=0}^{T} D'_{IPS_i} + \sum_{j=0}^{T} O'_{IPS_j})}. \tag{10}$$

$$\frac{\partial^2 u_{IRS}}{\partial^2 z} = \frac{e^{z}.(4e^{z} - \sum_{i=0}^{T} D'_{IRS_i} - \sum_{j=0}^{T} O'_{IRS_j})}{\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}}. \tag{11}$$

$$\frac{\partial^2 u_{IDA}}{\partial^2 f'} = \frac{e^{1-2f'}.(4e - e^{f'}.(O'_{Total} + D'_{Total}))}{\sum_{j=0}^{T} O'_{IDA_j} + \sum_{i=0}^{T} D'_{IDA_i}}. \tag{12}$$

From Equations (9) and (10), we notice that $\frac{\partial^2 u_{IDS}}{\partial^2 x}$ and $\frac{\partial^2 u_{IPS}}{\partial^2 y}$ are positives. Therefore, the payoffs u_{IDS} and u_{IPS} are strongly convex [32], with strong convexity equal to $\frac{2}{(\sum_{j=0}^{T} O'_{IDS_j} + \sum_{i=0}^{T} D'_{IDS_i})}$ and $\frac{2}{(\sum_{j=0}^{T} O'_{IPS_j} + \sum_{i=0}^{T} D'_{IPS_i})}$, respectively. Since u_{IDS} and u_{IPS} are convex functions, Equations (5) and (6) are proved. From Equation (11), we notice that u_{IRS} is a convex function only when $(4e^{z} - \sum_{i=0}^{T} D'_{IRS_i} - \sum_{j=0}^{T} O'_{IRS_j}) \geq 0$ since e^{z} and $(\sum_{j=0}^{T} O'_{IRS_j} + \sum_{i=0}^{T} D'_{IRS_i})$ are positives. Therefore, Equation (7) is the best response of the IRS only when Equation (13) holds.

$$z \geq \ln\left(\frac{\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}}{4}\right). \tag{13}$$

From Equation (12), u_{IDA} is a convex function only when $4e - e^{f'}.(O'_{Total} + D'_{Total}) \geq 0$
Hence, Equation (8) is the best response of the head agent IDA only when the Equation (14) holds.

$$f' \leq \ln\left(\frac{4e}{O'_{Total} + D'_{Total}}\right). \tag{14}$$

□

***Theorem** 1:*
The cooperative secondary players are incentivized not to unilaterally deviate from the equilibrium state. The equilibrium point o_E is equal to (x_E, y_E , z_E).

Proof 2.
According to Shapley Theorem [33], x^{φ}, y^{φ} and z^{φ} represent the optimal equilibrium in a hierarchical cooperative game since the payoffs functions u_{IDS}, u_{IpS} and u_{IRS} are convex. Equations (5), (6) and (7) can be modeled by a set of linear equations as follow

$$\begin{cases} x^{\varphi} + 0.y^{\varphi} + 0.z^{\varphi} = \frac{e^{\sum_{i=0}^{T} D'_{IDS_i}} + e^{\sum_{j=0}^{T} O'_{IDS_j}}}{2}, \\ 0.x^{\varphi} + y^{\varphi} + 0.z^{\varphi} = \frac{e^{\sum_{i=0}^{T} D'_{IPS_i}} + e^{\sum_{j=0}^{T} O'_{IPS_j}}}{2}, \\ 0.x^{\varphi} + 0.y^{\varphi} + z^{\varphi} = \ln\left(\frac{\sum_{i=0}^{T} D'_{IRS_i} + \sum_{j=0}^{T} O'_{IRS_j}}{2}\right). \end{cases} \tag{15}$$

The determinant of these linear equations is computed as follows: According to [34], the equilibrium could be solved

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

by using the Cramer rule. The point (x_E, y_E, z_E) is computed as follows:

$$x_E = \frac{\det(M_x)}{det(M)}, y_E = \frac{\det(M_y)}{det(M)}, z_E = \frac{\det(M_z)}{det(M)}.$$

$\det(M)$ is the determinant of the linear equations, which is equal to 1, where $\det(M_x)$, $\det(M_y)$ and $\det(M_z)$ are the determinants of matrices M_x, M_y and M_z, which are computed as follows:

$$\det(M_x) = \begin{vmatrix} \alpha & 0 & 0 \\ \beta & 1 & 0 \\ \gamma & 0 & 1 \end{vmatrix}$$

$$\det(M_y) = \begin{vmatrix} 1 & \alpha & 0 \\ 0 & \beta & 0 \\ 0 & \gamma & 1 \end{vmatrix}$$

$$\det(M_z) = \begin{vmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & \gamma \end{vmatrix}$$

Therefore, (x_E, y_E, z_E) corresponds to the optimal equilibrium point since $x_E = \alpha$, $y_E = \beta$ and $z_E = \gamma$, where $\alpha = x^{\varphi}$, $\beta = y^{\varphi}$, and $\gamma = z^{\varphi}$.
The equilibrium point $o_E^*(x_E^*, y_E^*, z_E^*) = (\alpha^*, \beta^*, \gamma^*)$. α, β and γ are normalized as follows:
$\alpha^* = \frac{\alpha_j - \alpha_{min}}{\alpha_{max} - \alpha_{min}}$, $\beta^* = \frac{\beta_j - \beta min}{\beta max - \beta min}$, $\gamma^* = \frac{\gamma_j - \gamma min}{\gamma max - \gamma min}$ where (α_{min}, βmin, γmin) and (α_{max}, βmax, γmax) are respectively the minimum and maximum values obtained during the detection, prediction and reaction process. (α_j, β_j, γ_j) are the jth normalized values. Here, α^*, β^* and $\gamma^* \in [0, 1]$.
□

The secondary agents trigger their detection, prediction and reaction strategies, only when the equilibrium is reached, i.e., $q_1 \geq \alpha^*$, $q_2 \geq \beta^*$, and $q_3 \geq \gamma^*$. The proposed game is repeated until the equilibrium is reached, i.e., the secondary players launch the strategies that the head player requests. This type of game is defined as a finitely repeated game [35] [36]. It is apparent that the security performance of CDG depends mainly on the costs (i.e., delays and overheads) that the secondary agents are required to achieve a high level of security. Note that in this security game, we assume that the head player IDA has the knowledge of the probabilities q_1, q_2, and q_3 since IDA is located within the same vehicle, where the pseudocode of the detection, prediction and reaction processes by CDG is running. The pseudocode is illustrated by Algorithm 1.
Our game is represented in the extensive form (as shown in Figure 2), in which the game's payoff function is stored as a multidimensional table (as shown in Table 2) with one entry for each player's payoff under each pure strategy. Therefore, the size of the linear feasibility program of our equilibrium solution o_E is polynomial in the size of the extensive form representation of the game. Note that there exist polynomial-time algorithms for solving linear feasibility programs, e.g., the ellipsoid method.

Algorithm 1 Cyber security process of CDG

Begin:
Repeat:
The normalized Delays (D'_{IDS_i}, D'_{IPS_i}, D'_{IRS_i}) and overheads (O'_{IDS_j}, O'_{IPS_j}, O'_{IRS_j})are computed by the secondary players
if $q_1 \geq \alpha^*$ **then**
  IDA requests its IDS agent to launch the detection process
else
  IDA does not send any request to IDS,
  if $(D_{IDS_i} \geq D_{IDS_{max}}) \| (O_{IDS_j} \geq O_{IDS_{max}})$ **then**
    IDA stops the detection process of IDS until $(D_{IDS_i} < D_{IDS_{max}})$ & &$(O_{IDS_j} < O_{IDS_{max}})$,
  end if
end if
if $q_2 \geq \beta^*$ **then**
  IDA requests its IPS agent to launch the prediction process,
else
  IDA does not send any request to IPS
  if $(D_{IPS_i} \geq D_{IPS_{max}}) \| (O_{IPS_j} \geq O_{IPS_{max}})$ **then**
    IDA stops the detection process of IPS until $(D_{IPS_i} < D_{IPS_{max}})$ & &$(O_{IPS_j} < O_{IPS_{max}})$,
  end if
end if
if $q_3 \geq \gamma^*$ **then**
  IDA requests its IRS agent to launch the reaction process
else
  IDA does not send any request to IRS
  if $(D_{IRS_i} \geq D_{IRS_{max}}) \| (O_{IRS_j} \geq O_{IRS_{max}})$ **then**
    IDA stops the reaction process of IRS until $(D_{IRS_i} < D_{IRS_{max}})$ & &$(O_{IRS_j} < O_{IRS_{max}})$,
  end if
end if
Until: the end of hierarchical security game

4.3 Consensus game between CDG and attacker

Let ϕ_1 be the probability that an attacker launches an attack against vehicle i, and ϕ_2 be the probability of CDG to activate its IDS or IPS to protect vehicle i. Let $S(\phi_1, \phi_2)$ be the probability of successful prevention of an attack by CDG. S can be expressed as shown in Equation (16). In this game, the players, attacker, and CDG, possess a set of pure strategies $\omega_{Attacker} = \{\omega_i^1 | i = 1, ..., s\}$ and $\omega_{CDG} = \{\omega_j^2 | j = 1, ..., s'\}$, where s and s' are respectively the number of pure strategies that the attacker and the CDG can use.

$$S(\phi_1, \phi_2) = \frac{\phi_2}{\phi_2 + \phi_1}. \quad (16)$$

It is apparent from Equation (16) S is increasing in ϕ_2 from 0 to 1 as ϕ_2 equal to 0 and it tend to a maximum value (ϕ_{max}), respectively. S is decreasing in ϕ_1 from 1 to 0 when ϕ_1 is equal to 0 and it tends to a maximum value (ϕ'_{max}), respectively. Let G_{CDG} and $G_{Attacker}$ be the expected utility of CDG to protect vehicle i and the expected utility of attacker, respectively:

$$G_{Attacker} = R'.(1 - S(\phi_1, \phi_2)) - C'.\phi_1.$$

$$G_{CDG} = R.S(\phi_1, \phi_2) - C.\phi_2.$$

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

where R is the CDG's reward to detect/predict successfully an attack and R' is the attacker's reward for a successful attack. C and C' are respectively the costs incurred by CDG and the attacker to protect and attack vehicle i.

***Theorem** 2:* The game between the players CDG and attacker converges to a unique NE point (ϕ_1^*, ϕ_2^*), $\phi_1^* = C^{''}.R^{''}.\frac{R^{'}}{C'.(1+C^{''}.R^{''})^2}$ and $\phi_2^* = \frac{R^{'}}{C'.(1+C^{''}.R^{''})^2}$ where $C^{''} = \frac{C}{C'}$ and $R^{''} = \frac{R'}{R}$

Proof 3. We have

$$\frac{dG_{CDG}}{d\phi_2} = \frac{R.\phi_1}{(\phi_2+\phi_1)^2} - C. \tag{17}$$

$$\frac{dG_{Attacker}}{d\phi_1} = \frac{R'.\phi_2}{(\phi_2+\phi_1)^2} - C'. \tag{18}$$

To find the equilibrium, we set Equations (17) and (18) equals to 0, and hence we get

$$C = \frac{R\phi_1}{(\phi_2+\phi_1)^2}. \tag{19}$$

$$C' = \frac{R'.\phi_2}{(\phi_2+\phi_1)^2}. \tag{20}$$

Dividing Equation (19) by (20), we get

$$\phi_1 = C^{''}.R^{''}.\phi_2.$$

Substituting ϕ_1 into (20) yields

$$\phi_2 = \frac{R'}{C'.(1+C''.R'')^2}. \tag{21}$$

$$\phi_1 = C^{''}.R^{''}\frac{R'}{C'.(1+C''.R'')^2}. \tag{22}$$

In the following, we aim to prove that Equation (21) converges to NE of the CDG, ϕ_2^*, and Equation (22) converges to NE of the attacker, ϕ_1^*.

According to [37] [38], the couple (ϕ_1, ϕ_2) converges to the NE point, (ϕ_1^*, ϕ_2^*), if and only if there exists a couple of pure strategies (ω_1^1, ω_s^1) and $(\omega_1^2, \omega_{s'}^2)$, such that the couple $(\phi_1(\omega_1^1), \phi_2(\omega_1^2)) = (0,0)$ and

$$G_{Attacker_i}(\omega_s^1, \phi_{2_j}^*) > G_{Attacker_i}(\omega_1^1, \phi_{2_j}^*).$$
$$G_{CDG_j}(\omega_{s'}^2, \phi_{1_i}^*) > G_{CDG_j}(\omega_1^2, \phi_{1_i}^*).$$

where $G_{Attacker_i}(\omega_s^1, \phi_{2_j}^*)$ is the utility of the attacker when it carries out strategy ω_s^1 with respect to the CDG's strategy, ω_j^2. $G_{CDG_j}(\omega_{s'}^2, \phi_{1_i}^*)$ is the utility of CDG when it carries out strategy $\omega_{s'}^2$ with respect to the attacker's strategy, ω_i^1.

δ and δ' are two positive values such that, $G_{Attacker_i}(\omega_s^1, \phi_{2_j}) - G_{Attacker_i}(\omega_1^1, \phi_{2_j}) \geq \delta > 0$, $G_{CDG_j}(\omega_{s'}^2, \phi_{1_i}) - G_{CDG_j}(\omega_1^2, \phi_{1_i}) \geq \delta' > 0$ $G_{Attacker_i}(\omega_s^1, \phi_{2_j})$ and $G_{CDG_j}(\omega_{s'}^2, \phi_{1_i})$ can be written as:

$$G_{Attacker_i}(\omega_i^1, \phi_{2_j}) = R'.(1 - \sum_{i=1}^{s} S(\phi_{1_i}, \phi_{2_j})) - C^{'}.\sum_{i=1}^{s}\phi_{1_i}. \tag{23}$$

$$G_{CDG_j}(\omega_j^2, \phi_{1_i}) = R.\sum_{j=1}^{s'} S(\phi_{1_i}, \phi_{2_j}) - C.\sum_{j=1}^{s'}\phi_{2_j}. \tag{24}$$

From Equations (23) and (24), we get

$$\begin{aligned} G_{Attacker_i}(\phi_{2_1}) + \delta &= R'.(1 - \sum_{i=1}^{s} S(\phi_{1i}, \phi_{2_1})) - C'.\sum_{i=1}^{s}\phi_{1i} \\ &\leq R'.(1 - \sum_{i=1}^{s} S(\phi_{1_i}, \phi_{2_{s'}})) - C^{'}.\sum_{i=1}^{s}\phi_{1_i} \\ &= G_{Attacker_i}(\phi_{2_{s'}}). \end{aligned} \tag{25}$$

$$\begin{aligned} G_{CDG_j}(\phi_{1_1}) + \delta' &= R.\sum_{j=1}^{s'} S(\phi_{1_1}, \phi_{2_j}) - C.\sum_{j=1}^{s'}\phi_{2_j} \\ &\leq R.\sum_{j=1}^{s'} S(\phi_{1_s}, \phi_{2_j}) - C.\sum_{j=1}^{s'}\phi_{2_j} \\ &= G_{CDG_j}(\phi_{1_s}). \end{aligned} \tag{26}$$

According to Equations (25) and (26), we claim that the attacker and CDG choose respectively the strategies ω_s^1 and $\omega_{s'}^2$, after sth and s'th iterations. Hence, we get the couple $(\phi_1(\omega_1^1), \phi_2(\omega_1^2)) = (0,0)$. Thus, CDG and the attacker reach consensus at the NE point.

$$(\phi_1^*, \phi_2^*) = (C^{''}.R^{''}.\frac{R'}{C'.(1+C''.R'')^2}, \frac{R'}{C'.(1+C''.R'')^2}) =$$
$$(\arg_{\phi_1} max_{G_{Attacker}}(\phi_1, \phi_2^*), \arg_{\phi_2} maxG_{CDG}(\phi_1^*, \phi_2)).$$

□

5 PERFORMANCE EVALUATION

The proposed cyber defense architecture CDG, based on a hierarchical cooperative security game is evaluated by using a network simulator (NS3) [18]. In this section, we first study the coverage of the equilibrium point o_E (x_E, y_E, z_E). Here, we aim to determine the optimal values of delays, and overheads (D'_{IDS_i}, O'_{IDS_j}), (D'_{IPS_i}, O'_{IPS_j}), and (D'_{IRS_i}, O'_{IRS_j}) to reach this equilibrium point. Afterward, we evaluate the performance of CDG with current cyber detection and prediction framework, developed for vehicular networks [5], [12], [13]. Specifically, we compute the following metrics: false positive rate, false negative rate, delay and communication overhead. These metrics are defined as follows:

- *False positive*, CDG classifies the vehicles that are not attacked by the attackers as infected vehicles.
- *False negative*, CDG classifies the infected vehicles as honest nodes.
- *Delay* is the required time for CDG to predict and detect accurately the infected vehicles.
- *Overhead* is the number of bytes that the IDS and IPS agents exchanges between their neighbors to detect, predict and react efficiently against cyber-attacks.

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

5.1 Simulation setup

In our simulation, we vary the number of vehicles from 300 to 700 nodes. The mobility model of vehicles follows a probabilistic pattern, which is generated by the Simulation of Urban Mobility (SUMO) simulator [39]. In this probabilistic model, the vehicle follows a well-defined path and chooses a speed from the set [min speed, max speed]. The number of attackers varies from 10% to 30% of the overall vehicles. In our simulation, we inject the most lethal attacks that could target the vehicular network, such as black hole, false data injection and false dissemination attacks. Black hole attack drops all the messages that the infected vehicle receive, false data injection attack alters the gathered data from a sensor of a vehicle and injects wrong information, and false dissemination attack broadcasts a false alert to lure the legitimate vehicle that an accident has occurred in order to cause a traffic jam. The use case that we attempt to secure is a safety-oriented application, which may help a driver mitigate dangerous situations (e.g., car crash) by monitoring the road and listening to the safety messages exchanged between vehicles. The network is partitioned into a number of clusters, each with a cluster head (CH) that manages the information sent from its cluster members. In case of a crash, vehicles close to the area of the crash can broadcast alert messages to their CH, which in turn forwards the aggregated message to its neighboring CHs. This aggregated alert message crosses from one CH to another until it reaches the destination (e.g., road side unit). As explained in Subsection 3, the IDS relies on a specification based detection technique to detect these attacks. Furthermore, to detect the future misbehavior of an attacker the IPS relies on a predictive game theory concept. Readers are referred to these recent works [5], [12], [13] regarding the detection and prediction of current and future attacks. The main simulation parameters are summarized in Table 3.

Table 3: Summary of Simulation Parameters

Simulation area	20000*20000 m^2
Simulation time	400 seconds
Number of vehicles	From 300 to 700
Number of attackers	From 10 % to 30 % of overall vehicles
Range	400 m
Routing protocol	Cluster-based protocol [40]
A mobility model generator	Simulation of urban mobility, SUMO [39]
Speed	From 50 to 90 km/h
Detection technique	Specification based detection [19]
Prediction technique	Predictive Game [14]

The most important results are summarized below.

5.2 Simulation results

5.2.1 Optimal detection, prediction and reaction systems, and Optimal equilibrium point O_E^*

As shown in Table 4, the probabilities to detect and predict the attackers with high accuracy and react promptly before critical damages occur depend mainly on the overheads, delays and (n, k, s). Here, n is the number of detected attacks by IDS, k is the number of predicted attacks by IPS and s is the number of reactions that IRS launches against the cyber-attacks. In this game, it is apparent that the secondary agents, IDS, IPS and IRS, aim to increase their rewards by detecting, predicting and reacting against a maximum number of attackers, while taking into account of the communication overheads and delays. Hence, there exists a dilemma between a reliable detection, prediction and reaction; low overheads and delays should both be ensured by the IDS, IPS and IRS. The head agent, IDA activates the IDS, IPS and IRS only when x, y and z reach x_E^*, y_E^*, z_E^*, respectively. In the hierarchical cooperative game, we fix n, s, and k and determine the optimal values of (D'_{IDS_i}, O'_{IDS_j}), (D'_{IPS_i}, O'_{IPS_j}), and (D'_{IRS_i}, O'_{IRS_j}) that allow us to reach the equilibrium point, x_E^*, y_E^*, z_E^*.

From Table 4, we can see that the communication overheads rates ($O^{'}/\sum O'$) incurred by the secondary agents IPS and IDS to detect and predict the attacks are greater than their processing delays rates ($D^{'}/\sum D'$). This is due to the fact that, the IDS and IPS agents collaborate with other secondary agents by exchanging a list of attack signatures. Furthermore, the processing delay rate that the secondary agent IRS requires to react against the attacker is greater than the overhead rate since the IRSs do not collaborate and the decision making is done locally.

Table 4: Equilibrium point O_E^*

$(a) x_E^*$

$O'_{IDS_n}/\sum_{j=1}^{n} O'_{IDS_j}$	$D'_{IDS_n}/\sum_{i=1}^{n} D'_{IDS_i}$	n	x_E^*
0.034	0.018	20	0.42
0.041	0.023	30	0.49
0.047	0.025	40	0.52

$(b) y_E^*$

$O'_{IPS_k}/\sum_{j=1}^{k} O'_{IPS_j}$	$D'_{IPS_k}/\sum_{i=1}^{k} D'_{IPS_i}$	k	y_E^*
0.037	0.022	20	0.28
0.047	0.023	30	0.34
0.057	0.026	40	0.4

$(c) z_E^*$

$O'_{IRS_s}/\sum_{j=1}^{s} O'_{IRS_j}$	$D'_{IRS_s}/\sum_{i=1}^{s} D'_{IRS_i}$	s	z_E^*
0.02	0.039	20	0.45
0.022	0.048	30	0.49
0.025	0.055	40	0.56

5.2.2 False positive and negative rates

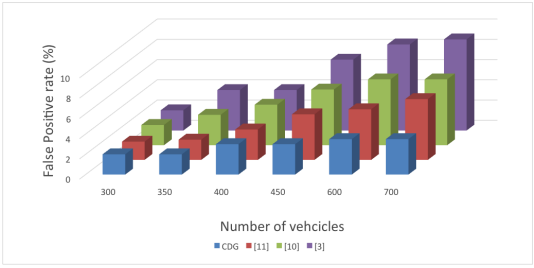
As shown in Figure 3, the number of false positives that is generated by the cyber defense game, CDG increases slowly compared to the current intrusion detection and prediction frameworks developed for vehicular networks [5], [12], [13]. Specifically, the host IDS proposed in [5], which is based on a statistical detection technique, which generates a high false positive rate when the number of attackers is over 400 nodes. From Figure 4, the number of false negatives of CDG, host IDS framework [5] and intrusion prediction frameworks [12], [13] increases, specifically, when the number of vehicles and attackers are above 400 nodes and equal to 30% of overall vehicles, respectively. This increase is much greater for the IDS framework [5] as compared to other security frameworks. These results are attributed to the fact that in [5], there is no attack prediction, the host IDS detects only the current cyber threats against the vehicle.

In the scaling mode, when the number of attackers is equal to 30% the overall nodes and number of vehicles is above 400 nodes, the false positive and negative rates of CDG increase slowly, which are lower than 4% and 5%, respectively, as shown in Figures 3(a) and 4(b). These results are attributed to the following:

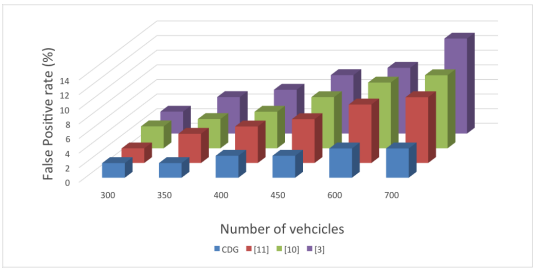
(i) *Distributed security game*: CDG is based on three secondary and one head agents that are activated within a vehicle and collaborate with other security agents (launched within other

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

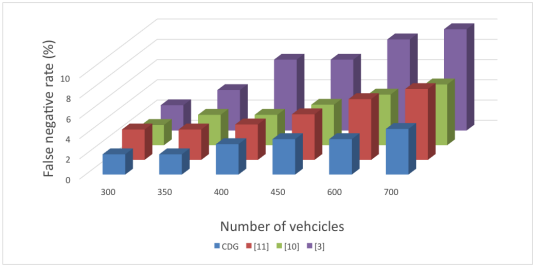


(a)

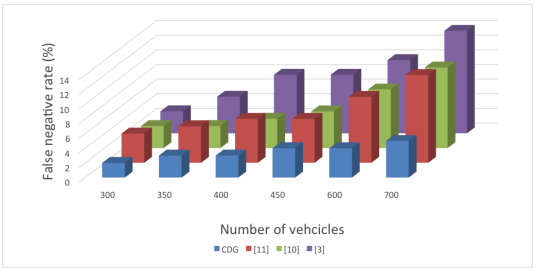


(b)

Figure 3: False positive rate: number of attackers equal to (a) 10 % of overall vehicles and (b) 30 % of overall vehicles.



(a)



(b)

Figure 4: False negative rate: number of attackers equals to (a) 10% of overall vehicles and (b) 30% of overall vehicles.

vehicles) to predict, detect and react efficiently against the malicious behaviors. Based on a hierarchical cooperative game, we can determine the optimal equilibrium O_E^* (x_E^*, y_E^*, z_E^*) that allows the CDG to identify accurately the infected vehicles and the cyber threats that launch attacks; hence, the false positive and negative rates are low and almost constants even in the scaling mode.

(ii) *Consensus game*: in this security game, there is a consensus between the attacker that targets the legitimate vehicle and CDG as demonstrated in Theorem 2. The CDG player knows the frequency of attacks launched by the cyber threat and hence it can detect and predict the current and future misbehaviors with high accuracy.

5.2.3 Overhead

Figures 5(a) and 5(b) illustrate the overheads generated by the intrusion detection and prediction frameworks [5], [12], [13] and a security game CDG, when the number of attackers is equal to 10% and 30% of overall vehicles, respectively. Figures 5(a) and 5(b) show that the communication overhead generated by each cyber security framework increases when the number of attackers and vehicles increases. This increase is much slower for CDG since the overheads in the detection and prediction frameworks [5], [12], [13] increase exponentially, in particular, when the number of vehicles and attacker is above 400 nodes and equals to 30% of the overall vehicles, respectively. Such results are attributed to the following reasons:

(i) *Hierarchical cooperative game*: in the proposed game, the head agent IDA determines what are the optimal overheads of the secondary agents IDS, IPS and IRS, while taking into account of the security performances of CDG (i.e., low false positive and negative rates). In fact, when the overheads are low, almost all attacks are not detected (predicted). On the other hand, when these overheads are high, the performance of V2X communications are degraded [15]. Therefore, the head and secondary agents aim to ensure a tradeoff between the low false positive and negative rates, and low overhead. These results are achieved even when the number of vehicles is equal to 700 nodes.

(ii) *Equilibrium overhead*: the goal of the attacker is to increase its payoff by decreasing the payoff of its opponent, CDG. The attackers aim to force the secondary agents to generate high communication overheads, while the goal of CDG is to detect and predict almost all attacks that target the legitimate vehicles while minimizing the communication overheads. As a result, we claim that, when the number of attackers and vehicles is high, the overhead generated by CDG remains low. Since almost all attackers that aim to exhaust the resources of vehicles (i.e., increase the overhead) are detected via the proposed security cooperative game.

5.2.4 Delay

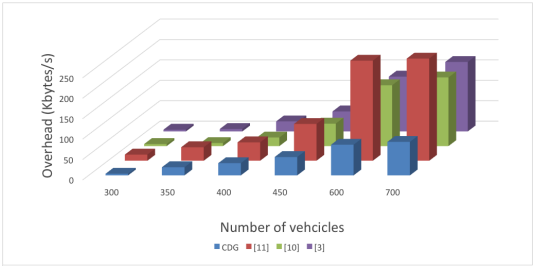
As shown in Figures 6(a) and 6(b), the required delay to detect and predict the attacks by CDG increases slowly, and it is smaller than 80 milliseconds (ms) when the number of both vehicles and attackers increases. This is unlike the other security frameworks, where the delays of the intrusion detection and prediction frameworks [5], [12], [13] are above 500 ms, 700 ms, and 400 ms, respectively, when the number of vehicles is equal to 700 nodes. These results are achieved due to the following reasons:

(i) *Hierarchical cooperative game*: in this security game, the required delays for CDG to predict and detect accurately the infected vehicles are considered as the main metric for influencing the final decision making provided by the head agent IDA to its secondary agents IDS, IPS and IRS, i.e., whether to activate the detection, prediction, and reaction strategies. The goal of CDG is to detect and predict almost all attacks that (will be) occur, while reacting promptly before a critical damage to the network is instigated.

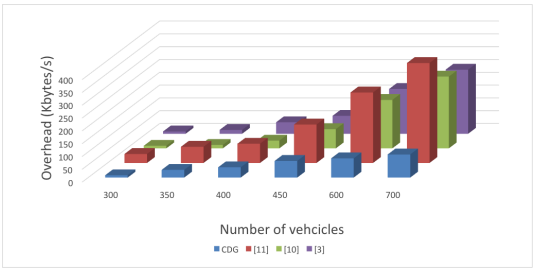
(ii) *Equilibrium delay*: as for the overhead, the CDG player aims to detect and predict promptly almost all attacks that (will) occur, while the attacker player forces the secondary agents

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

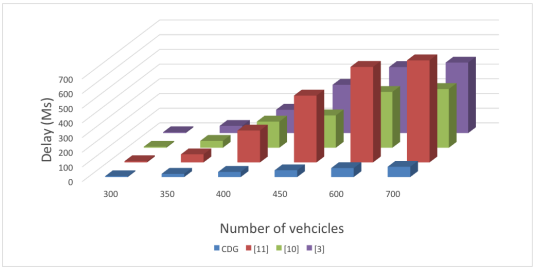


(a)

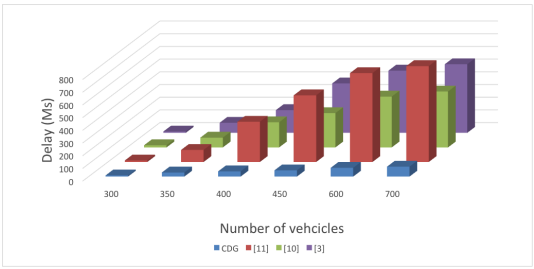


(b)

Figure 5: Overhead: number of attackers equals to (a) 10% of overall vehicles and (b) 30% of overall vehicles.



(a)



(b)

Figure 6: Delay: number of attackers equals to (a) 10% of overall vehicles and (b) 30% of overall vehicles.

IDS and IPS to generate high delays in order to launch an attack without being detected. Therefore, the goal of a head agent is to ensure a dilemma between low false positive and negative rates, while minimizing the required delays of the secondary agents.

6 CONCLUSION

Game theory plays an important part in the philosophy of defense, while the behavioral game is considered as a powerful tool to model the interactions between a cooperative and non-cooperative players. In this research work, we have proposed an efficient cyber security framework, where a tradeoff between the network and security metrics is achieved by using a hierarchical cooperative game. Furthermore, we have gained a new insight from a security cooperative game, where the head agent collaborates with the secondary agents to predict and detect with a high accuracy the lethal attacks, while taking into consideration of the overhead and delay. To the best of our knowledge, this is the first cyber defense framework that incorporates the overhead and delay as the main parameters for influencing the activation of IDS, IPS and IRS agents. Our simulation results show that CDG requires a rather small communication overhead and a short time to detect and predict the attacks with a low false positive and low false negative rate as compared to the contemporary intrusion detection and prediction frameworks [5], [12], [13]. CDG has also been shown to scale well for large vehicular networks, a more realistic scenario. Our future goal is to integrate other network metrics such as throughput and packet delivery ratio in the decision making process, and evaluate CDG in terms of detection and false positive rates.

7 ACKNOWLEDGEMENT

This work has been carried out in SystemX and it is part of the project Cybersecurity of Intelligent Transportation Systems (CTI) [41]. Is an enhanced and extended version of the paper that will be presented at IEEE CCNC, Las Vegas-USA, 2018 [42].

REFERENCES

[1] L. Peng, T. Miyazaki, K. Wang, S. Guo, and W. Zhuang, "Vehicle-assist resilient information and network system for disaster management," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 3, pp. 438 – 448, 2017.

[2] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Communications Magazine*, 2017.

[3] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in uav-aided networks: A bayesian game-theoretic methodology," *IEEE Trans. on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1143–1153, 2017.

[4] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad-hoc, and wireless sensor networks," *IEEE Wireless Communications Magazine*, vol. 14, no. 5, pp. 8–20, 2007.

[5] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for vanets: A statistical approach to rogue node detection," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, 2016.

[6] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *DEF CON*, 2015.

[7] T. Bouali, E.-H. Aglzim, and S.-M. Senouci, "A secure intersection-based routing protocol for data collection in urban vehicular networks," in *IEEE Global Communications Conference (GLOBECOM), Austin, TX, USA*, 2014, pp. 82–87.

[8] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting sybil attacks in vanets," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013.

[9] A. Tomandl, K.-P. Fuchs, and H. Federrath, "Rest-net: A dynamic rule-based ids for vanets," in *IEEE 7th IFIP Wireless and Mobile Networking Conference (WMNC), Vilamoura, Portugal*, 2014, pp. 1–8.

[10] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one*, vol. 11, no. 6, 2016.

[11] A. Boudguiga, W. Klaudel, A. Boulanger, and P. Chiron, "A simple intrusion detection method for controller area network," in *IEEE International Conference on Communications (ICC), Kuala, Lumpur malaysia*, 2016, pp. 1–7.

[12] 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*, vol. 29, no. 10, p. 1683–1704, 2016.

[13] H. Sedjelmaci, S. M. Senouci, and T. Bouali, "Predict and prevent from misbehaving intruders in heterogeneous vehicular networks," *Vehicular Communications*, vol. 10, pp. 74–83, 2017.

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.

This is the author's version of an article that has been published in this journal. Changes were made to this version by the publisher prior to publication.
The final version of record is available at http://dx.doi.org/10.1109/TETC.2018.2890476

[14] H. Sedjelmaci, T. Bouali, and S. M. Senouci, "Detection and prevention from misbehaving intruders in vehicular networks," in *IEEE Global Communications Conference (GLOBECOM), Austin, TX, USA*, 2014, pp. 39–44.
[15] J. Petit and Z. Mammeri, "Authentication and consensus overhead in vehicular ad hoc networks," *Telecommunication systems*, pp. 1–14, 2013.
[16] N. Tsikoudis, A. Papadogiannakis, and E. Markatos, "Leonids: A low-latency and energy-efficient network-level intrusion detection system," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 142 – 155, 2014.
[17] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks," *IEEE Trans. on Systems, Man, and Cybernetics: System*, 2017.
[18] "Network simulator (ns-3). available on http://www.nsnam.org."
[19] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-based anomaly detection: a new approach for detecting network intrusions," in *Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA*, 2002, pp. 265–274.
[20] R. Mitchell and R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16–30, 2015.
[21] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC), Pasadena, CA, USA*, 2011, pp. 184–193.
[22] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2273–2282, 2015.
[23] T. Alpcan and S. Buchegger, "Security games for vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 280–290, 2011.
[24] M. Hamdi and H. Abie, "Game-based adaptive security in the internet of things for ehealth," in *IEEE International Conference on Communications (ICC), Sydney, Australia*, 2014, pp. 920–925.
[25] T. Basar and Z. Georges, "Handbook of dynamic game theory," in *Springer International Publishing, Switzerland AG*, 2018.
[26] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks," in *IEEE Global Communications Conference (GLOBECOM), Washington DC, USA*, 2016, pp. 1–7.
[27] S. Kim, "Dynamic c-ran resource sharing scheme based on a hierarchical game approach," *EURASIP Journal on Wireless Communications and Networking*, vol. 3, pp. 1–12, 2016.
[28] D. Niyato, A. V. Vasilakos, and Z. Kun, "Resource and revenue sharing with coalition formation of cloud providers: Game theoretic approach," in *Proceedings of the 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing , Newport Beach, CA, USA*, 2011, pp. 215–224.
[29] K. Han, X. Cai, and H. Rong, "An evolutionary game theoretic approach for efficient virtual machine deployment in green cloud," in *IEEE International Conference on Computer Science and Mechanical Automation (CSMA), Hangzhou, China*, 2015, pp. 1–4.
[30] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Security games with unknown adversarial strategies," *IEEE transactions on cybernetics*, vol. 46, no. 10, pp. 2291–2299, 2016.
[31] N. Marchang, R. Datta, and S. K. Das, "A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1684–1695, 2017.
[32] T. Lara, N. Merentes, E. Rosales, and M. Valera, "Some characterizations of strongly convex functions in inner product spaces," 2014.
[33] L. S. Shapley, "Cores of convex games," in *Intern. J. Game Theory*, 1971, pp. 12–26.
[34] F. Shen, K. Hamidouche, E. Bastug, and M. Debbah, "A stackelberg game for incentive proactive caching mechanisms in wireless networks," in *IEEE Global Communications Conference (GLOBECOM), Washington DC, USA*, 2016, pp. 1–6.
[35] D. Kar, F. Fang, F. Delle Fave, N. Sintov, M. Tambe, and A. Lyet, "Comparing human behavior models in repeated stackelberg security games: An extended study," *Artificial Intelligence*, vol. 240, pp. 65 – 103, 2016.
[36] D. Kar, F. Fang, F. Delle Fave, N. Sintov, and M. Tambe, "A game of thrones: when human behavior models compete in repeated stackelberg security games," in *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems, Istanbul, Turkey*, 2015.
[37] T. Basar and G. Olsder, "Dynamic noncooperative game theory, philadelphia, pa, usa: Soc. ind," *Appl. Math*, 1998.
[38] W. Saad, A. Sanjab, Y. Wang, C. Kamhoua, and K. Kwiat, "Hardware trojan detection game: A prospect-theoretic approach," *IEEE Transactions on Vehicular Technology*, 2017.
[39] "Simulation of urban mobility (sumo). available on http://sumo-sim.org/."
[40] G. Remy, S.-M. Senouci, F. Jan, and Y. Gourhant, "Lte4v2x - collection, dissemination and multi-hop forwarding," in *IEEE International Conference on Communications (ICC), Ottawa, Canada*, 2012, pp. 1–6.
[41] "Cti project. http://www.irt-systemx.fr/project/cti/."
[42] H. Sedjelmaci, I. H. Brahmi, A. Boudguiga, and W. Klaudel, "A generic cyber defense scheme based on stackelberg game for vehicular network," in *IEEE International Conference on Consumer Communications and Networking Conference (CCNC), Las vegas, USA*, 2018, pp. 1–6.

Hichem Sedjelmaci (M'14) received the Ph.D. degree in telecommunication systems from University of Tlemcen, Algeria, in 2013. From 2013 to 2016, he was a postdoctoral researcher with the DRIVE Laboratory, University of Burgundy, Nevers, France. In 2017, he was a Research Engineer in cyber security at the Institute of Technological Research SystemX. In 2018, he joined Orange Labs as a Senior Research Engineer in cyber security and artificial intelligence. He published his work in major IEEE conferences and premium journals (IEEE TRANSACTIONS).

Imane Horiya Brahmi (M'16) received a B.S. degree from University of Tlemcen, Tlemcen, Algeria in 2008; an engineering degree (equivalent to a Master Diploma) from Télécom Sud-Paris Engineering School, Evry, France with a major in telecommunications and networking in 2012 and a Ph.D. degree in Computer Science from University College Dublin, Dublin, Ireland in 2016. She worked as postdoctoral researcher at University College Cork, Ireland after her P.h.D. She is currently working as a research engineer at the Atomic Energy Commission (CEA), France.

Nirwan Ansari (S'78-M'83-SM'94-F'09) received the B.S.E.E. degree (summa cum laude, with a perfect grade point average) from New Jersey Institute of Technology (NJIT), Newark, NJ, USA; the M.S.E.E. degree from University of Michigan, Ann Arbor, MI, USA; and the Ph.D. degree from Purdue University, West Lafayette, IN, USA. He is a Distinguished Professor of electrical and computer engineering with NJIT. His current research interests include green communications and networking, cloud computing, various aspects of broadband networks, and multimedia communications.

Mubashir Husain Rehmani (M'14-SM'15) is a Post-Doctoral Researcher at Waterford Institute of Technology, Ireland. He received the Ph.D. degree from the University Pierre and Marie Curie, Paris, France in 2011. He currently serves as Area Editor for the IEEE Communications Surveys and Tutorials and was recognized as "Exemplary Editor of the IEEE Communications Surveys and Tutorials for the year 2015" by the IEEE Communications Society.

Copyright (c) 2019 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.