This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

An Accurate Security Game for Low-Resource IoT Devices

Hichem Sedjelmaci[‡,⊗], Sidi Mohamed Senouci[‡], and Tarik Taleb[♯,†]
[‡] University of Bourgogne Franche Comté, Nevers, France
[♯] Aalto University, Espoo, Finland
[†] Sejong University, Seoul, Korea
[⊗] Institut de Recherche Technologique (IRT) SystemX, Paris Saclay
Emails: sid-ahmed-hichem.sedjelmaci@u-bourgogne.fr, sidi-mohammed.senouci@u-bourgogne.fr, tarik.taleb@aalto.fi

***Abstract*—The Internet of Things (IoT) technology incorporates a large number of heterogeneous devices connected to untrusted networks. Nevertheless, securing IoT devices is a fundamental issue due to the relevant information handled in IoT networks. The intrusion detection system (IDS) is the most commonly used technique to detect intruders and acts as a second wall of defense when cryptography is broken. This is achieved by combining the advantages of anomaly and signature detection techniques, which are characterized by high detection rates and low false positives, respectively. To achieve a high detection rate, the anomaly detection technique relies on a learning algorithm to model the normal behavior of a node, and when a new attack pattern (often known as signature) is detected, it will be modeled with a set of rules. This latter is used by the signature detection technique for attack confirmation. Activating the anomaly detection technique simultaneously at each low-resource IoT device and all the time could generate a high-energy consumption.**

Thereby, we propose a game theoretic technique to activate anomaly detection technique only when a new attack's signature is expected to occur; hence a balance between detection and false positive rates, and energy consumption is achieved. Even by combining between these two detection techniques, we observed that the number of false positives is still non null (almost equal to 5%). Thereby, to decrease further the false positive rate, a reputation model based on game theory is proposed. Simulation results show that this lightweight anomaly detection outperforms current anomaly detection techniques, since in scaling mode (i.e., when the number of IoT devices and attackers are high) it requires low energy consumption to detect the attacks with high detection and low false positive rates, almost 93% and 2%, respectively.

***Index Terms*—Anomaly detection technique, reputation model, IoT devices, game theory, and intrusion detection system.**

I. Introduction

INTERNET of Things (IoT) envisages a future in which a large number of digital and physical things or objects (e.g., cameras, wireless sensor network - WSN, smart meters, smartphone, and TV sets) can be connected; while providing open access to a variety of data generated by such devices to provide new services to citizens and companies [1]. IoT services span different domains, such as medical aids, automotive, smart grid, and many others [2]. The term internet of things refers to uniquely identifiable objects and their virtual representations in an "internet-like" structure. These objects can be anything from large buildings, industrial plants, planes, cars, machines, any kind of goods, specific parts of a larger system to human beings, animals and plants and even specific body parts of them. While IoT does not assume a specific communication technology, wireless communication technologies will play a major role, and in particular, WSNs will proliferate many applications and many industries. The small, rugged, inexpensive and low powered WSN sensors will bring the IoT to even the smallest objects installed in any kind of environment, at reasonable costs. Integration of these objects into IoT will be a major evolution of WSNs.

Security is one of the major challenging issues in IoT due to the wireless medium characteristics, the relevant information handled by IoT devices and the hostile environment where these devices are deployed. Intrusion Detection Systems (IDS) proved their effectiveness to secure networks against both internal and external attacks since they act as a second layer of defense when cryptography is broken [3]. In an IDS-based solution, we use special agents to monitor the behavior of a target device that raise an alarm when an intruder is detected [4],[5]. These detection policies could be categorized into two techniques [4]-[7]: *(i) Signature-based detection (or Misuse detection)*, which is based on detection of the attack type by comparing the behavior of the analyzed target to a set of predefined rules related to each attack signature [8],[9]. Such technique aims to *reduce the false positive* and requires a low computation overhead to model the normal behavior of a device. Nevertheless, the drawback of this technique is that it can only detect known attacks, described by a set of signatures. *(ii) Anomaly detection,* which uses supervised learning algorithms [10]-[13], such as data mining, support vector machine (SVM) and neural networks (NNs), to build the normal behavior. The advantage of such technique is its high detection rate since it has the ability to detect new attacks that have never occurred before. However, the main drawback is the high computation overhead required to model the normal behavior.

In recent works [7],[14]-[16], the combination of these two detection techniques, anomaly and signature, exhibited high detection and low false positive rates even under the worst case scenario (i.e., when the number of attackers is high). However, these hybrid techniques propose to activate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

the anomaly detection simultaneously and all the time at low-resource IoT devices; which could highly increase the overhead and as a consequence degrade the network performance [10],[12],[17]. Thereby, our aim in this research work is to propose a lightweight anomaly detection technique by assuring a tradeoff between a high level of security (i.e., high detection and low false positive rates) and a low energy consumption. This optimal tradeoff is achieved by activating the anomaly detection only when a new attack pattern (i.e. signature) is expected to occur. The activation of anomaly detection technique is done, thanks to a proposed security game model, where we modeled the security strategy as a *game formulation* between the intruder attack and the IDS agent embedded at IoT devices. With the help of *Nash Equilibrium,* we determine the equilibrium state that allows the IDS agent to activate its anomaly detection technique in order to detect new attack patterns. To the best knowledge of the authors, this research work is the first to propose the activation of anomaly detection in low-resource IoT devices. In fact, most of hybrid intrusion detection techniques [7],[14]-[16] activate the anomaly detection simultaneously at low-resource IoT devices; which could highly increase the overhead and as a consequence degrade the network performance. Moreover, the false positive issue is a major challenge to address since classifying a legitimate IoT device as an attacker leads to a degradation of the IDS's performance. Thereby, to decrease further the false positive rate, a reputation model based on game theory is proposed. This model aims to rank the monitored IoT devices into *Legitimate*, *Suspect* and *Malicious nodes* according to their reputation scores. Figure 1 illustrates the two components of the IDS agent: the lightweight anomaly detection and the reputation model.

In this paper, we target IoT scenarios aiming to secure the low powered WSN, whereby the objects are defined as low powered devices with memory and energy constraints. The objects could be used in a smart home to return the information related to temperature levels and energy consumption. They connected to Internet through a gateway to transmit sensitive information to a remote center for further analysis.

This paper is organized as follows. Section II highlights some related work. It also introduces the network model that we intend securing. In Section III, we explain the process of anomaly detection's activation by using a game theory approach. Section IV explains our reputation model and Section V provides the simulation results. We conclude our work and give directions for future research work in Section V.

II. Background

In this section, we first summarize some relevant intrusion detection frameworks presented in the literature and discuss their main shortcomings. Afterwards, we present the network architecture that we intend securing.

A. Related work

IDS provides an effective protection to IoT networks against both external and internal intruders [4], and acts as a second

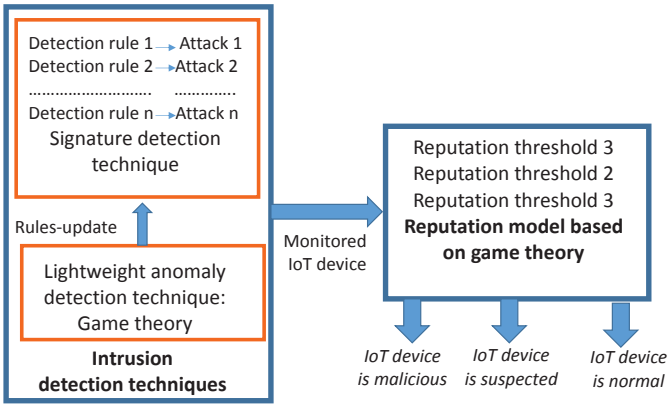


Figure 1. The main components of the envisioned IDS

wall of defense when cryptography is broken. In this subsection, we present some IDS examples, introduced for different networks (e.g., IoT, smart grid, wireless sensor networks - WSN, and vehicular networks - VANET), and discuss their shortcomings.

In [11],[18],[19], the authors use an anomaly detection technique to monitor the smart grid's IoT devices such as smart meters and identify any external or internal attack that targets the grid. According to their simulation results, the anomaly detection technique, which is based on a learning algorithm, exhibits a high detection rate (i.e. above 90%). However, embedding this heavy detection technique for low-resources IoT devices could incur a high computation overhead and subsequently degrades the smart grid performance.

In [4], the authors design and implement an intrusion detection system for low-resource IoT devices, named SVELTE. In SVELTE, rules are used to identify the most lethal attacks that target the routing protocol, e.g., spoofed or altered information, sinkhole, and selective-forwarding attacks. SVELTE is embedded in Contiki OS and according to the obtained simulation results, the detection system requires a low overhead to achieve a high detection rate. However, a high false positive is generated, specifically when the number of attacks increases.

In [7],[14],[20], the authors propose a hybrid intrusion detection framework for a heterogonous WSN, whereby a signature detection technique runs at each sensor node and anomaly detection technique runs at a powerful node, e.g. cluster-head or base station. The anomaly detection technique computes a rule related to each attack's signature that it detects and forwards this new rule to sensor nodes (located within its range). The sensor adds the rule into its database and compares the behavior of a monitored node with the stored rules (related to each signature). If a match occurs, the analyzed node is defined as an attacker. Such hybrid detection incurs a high communication overhead since a high number of signatures are forwarded to sensor nodes, specifically when the number of attackers is high in the network. In [15], both anomaly detection and signature-based detection techniques run at the same sensor node. According to the simulation results, the proposed hybrid intrusion detection system generates a high detection rate with a low false positive rate. However, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

major drawback of this work is that a heavy machine-learning algorithm is activated in permanent fashion at each sensor in order to build intrusion rules. Therefore, a high computation overhead could be generated resulting in a rapid decrease of the network lifetime.

Recently, new intrusion detection frameworks [21]-[23] are developed to secure VANETs against cyber-attacks. Specifically in [21], the authors design and implement an accurate and lightweight intrusion detection framework, called AECFV, in order to protect VANETs against the most dangerous attacks that could occur on such networks. Three kinds of IDS agents are proposed to secure the network. They are namely Local Intrusion Detection System (LIDS), Global Intrusion Detection System (GIDS) and Global Decision System (GDS). AECFV uses a hybrid detection technique (i.e. rules-based detection and anomaly detection based on support vector machine - SVM) to identify the attacks. According to the results of the conducted simulations, a hybrid detection technique allows a high detection and low false positive rates. However, AECFV generates a high overhead since the anomaly detection is activated all the time: it does not switch to idle mode. In [22], an efficient and lightweight intrusion detection mechanism, called ELIDV, is proposed to secure VANET. ELIDV relies on rules-based intrusion detection to identify three kinds of attacks: Denial of Service (DoS), integrity target, and false alert's generation. Simulation results show that ELIDV exhibits a high-level security in terms of highly accurate detection rate (detection rate more than 97 %), low false positive rate (close to 1%), and exhibits a low overhead compared to contemporary intrusion detection frameworks. However, when the number of attackers is high, the detection accuracy decreases exponentially.

Hence, the anomaly detection technique has the ability to detect almost all attacks that occur in a network. However, a permanent activation (i.e., no idle state) of this technique for low-resource IoT devices could decrease rapidly their lifetimes. Thereby, in this paper we make a tradeoff between constrained energy resources and detection accuracy by activating the anomaly detection only when a new attack's signature is expected to occur. Moreover, to decrease further the false positive rate a reputation model is proposed.

B. Network architecture

As shown in Figure 2, this paper addresses the security issues of mobile (and static) sensor nodes considered as the main components of IoT technology [24],[25]. Each IoT device (i.e. sensor) activates an IDS agent to monitor its neighboring devices. According to [26], the communication overhead may rapidly decrease the network lifetime compared to a computation overhead. Thereby, due to the communication overhead's issue, both anomaly and signature-based detection techniques should run in the same IDS agent. The signature-based detection technique compares the behavior of a target device against a set of rules related to each attack pattern (i.e. signature) stored in the IoT device's database.

In [6],[7],[10],[20],[22], the authors describe the signatures of cyber-attacks that target IoT devices and highlight some

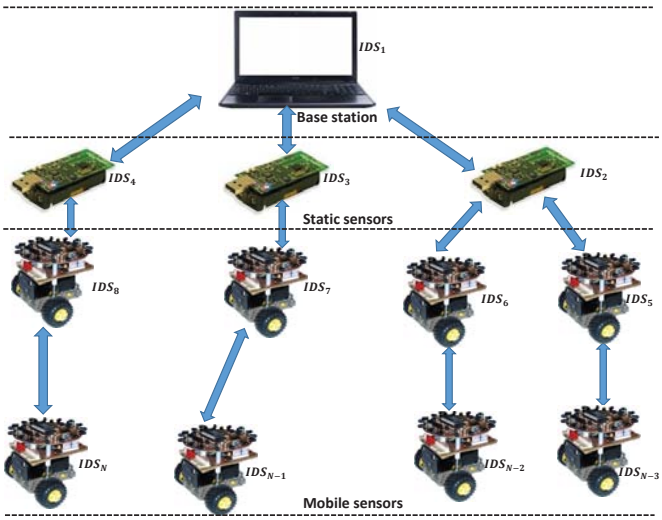


Figure 2. The main components of the envisioned IDS.

features and rules related to each attack signature in Table I. The anomaly detection technique relies on a learning algorithm to carry out a training and classification process, as shown in Algorithm 1. In the training process, the IDS agent monitors the features (e.g., PDR, SSI, TNR, MDR, PSR, and RTT) of the suspected IoT devices, and models a normal (and anomaly) behavior of a target device. In the classification process, the anomaly detection technique classifies the new features according to the anomaly and the normal patterns, determined during the training phase. In case a new attack pattern is detected, the IDS builds a rule related to each new detected attack pattern. Here, the threshold related to the new attack is updated as shown in Table 1. Afterward, this threshold is stored to be used by the signature detection technique. We refer the reader to [7][10][21] for more details about the anomaly detection based on machine learning algorithm. It shall be noted that in this research work, we use a threshold based scheme. However, other relevant schemes can be used, e.g., entropy-based signature detection [23].

To save energy, the anomaly detection technique is activated only when a new attack's signature is expected to occur by a malicious device. Thereby, a security game approach for low-resource IoT devices is proposed as explained in the next section.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

Algorithm 1 Anomaly detection process

1**: Begin** (at t=0)
2: IDS **Computes** the features of a suspected IoT device
3: **Models** the normal behavior of each $Feature_i$ and **Computes** their related threshold T_{i+1}
4: **If** ($Feature_i > T_{i+1}$) && ($T_{i+1} = T_i$)
5: *// The suspected IoT device is an attacker*
6: **Else If** ($Feature_i > T_{i+1}$) && ($T_{i+1} \neq T_i$)
7: The signature based detection should **Update** the rule (**Replace** T_i by T_{i+1})
8: **Else If** ($Feature_i < T_{i+1}$)
9: *// The suspected IoT device is a normal node*
10: **Repeat** until the attacker will be removed from the network

Table I
ATTACKS' SIGNATURES

Attacks	Features	Rules$_i$: attack detection depends on threshold T_i; where *n* is the number of suspected IoT devices
Hello flood and Sink hole	Packets Dropping Rate (PDR) and Signal Strength Intensity (SSI)	$PDR > T1_1 \ldots PDR > T1_n$ and $SSI > T2_1 \ldots SSI > T2_n$
Black hole	PDR	$PDR > T3_1 \ldots PDR > T3_n$
Jamming	Packets Send Rate (PSR) and SSI	$PSR > T4_1 \ldots PSR > T4_n$ and $SSI > T5_1 \ldots SSI > T5_n$
Resource exhaustion	Total Number of Requests (TNR)	$TNR > T6_1 \ldots TNR > T6_n$
Man-in-the-middle	Messages Modified Rate (MDR) and SSI	$MDR > T7_1 \ldots MDR > T7_n$ and $SSI > T8_1 \ldots SSI > T8_n$
Sybil	SSI and packet's Round Trip Time (RTT)	$SSI > T9_1 \ldots SSI > T9_n$ and $RTT > T10_1 \ldots RTT > T10_n$
Spoofed and altered information	MDR	$MDR > T11_1 \ldots MDR > T11_n$
Wormhole	PDR and SSI	$PDR > T12_1 \ldots PDR > T12_n$ and $SSI > T13_1 \ldots SSI > T13_n$
.....	.....	.....
Attack$_j$	Feature$_k$	Feature$_k$ $>T_i$

III. GAME-THEORETIC METHODOLOGY FOR OPTIMAL ACTIVATION OF ANOMALY DETECTION TECHNIQUE

In this section, we first derive the payoff matrix of the game related to the IDS and attacker; and define a set of strategies and payoffs that could occur between players, respectively. Afterward, with the help of *Nash Equilibrium (NE),* we determine the equilibrium state in which the IDS agent will activate its anomaly detection technique to train, classify and build a rule related to a new attack's signature.

A. Game description

In our approach, we consider a set of players, P=$\{p_1, \ p_{2,\ldots..}, \ p_n\}$, where each player represents either an IDS agent that runs at each IoT device or an attacker. Each player has a set of strategies, where strategy S_t = $\{sign_1, \ sign_{2,\ldots..}, sign_m\}$ represents m signatures detected by the IDS agent at time *t*; and strategy $S'_{t'}$ = $\{sign'_1, \ sign'_{2,\ldots..}, sign'_{m'}\}$ represents *m'* signatures launched by the attacker during a period of time *t'*. Let s_i denote the probability that the IDS has a strategy S_{t+i} and s'_j denote the probability that the attacker adopts the strategy $S'_{t'+j}$, where $\sum_{i=0}^{n} s_i$=1 and $\sum_{j=0}^{n} s'_j$=1. S and S' denote the probability distribution vectors S=$\{s_0,\ldots, s_n\}$ and S'=$\{s'_0,\ldots, s'_n\}$, respectively.

In this game, time is divided into regular intervals called time-slots. At the end of each time slot, the IDS player activates its anomaly detection technique to carry out training and classification processes; afterward it builds a rule related to each new attack's signature. Furthermore, when a new signature is detected, the IDS player's *payoff is* increased and the attacker player's *payoff* is decreased as shown in Equations 1 and 2, respectively. Otherwise, the IDS player's *payoff is* decreased and attacker player's *payoff* is increased as shown in Equations 3 and 4, respectively. The total *payoff* of IDS and attacker is equal to Equations 5 and 6, respectively. Based on this historic observation, the IDS can locally have knowledge of the frequencies of a signature's occurrence; and with the help of *NE* it predicts when anomaly detection should be activated for the definition of a rule. The *NE* aims at making a dilemma between accuracy detection and energy consumption. Moreover, IDS agents, located in the same neighborhood, cooperate together in order to achieve the highest possible total benefit. This means that IDSs exchange the list of signatures (with the signatures' detection time) to grow knowledge of the frequencies of attacks' occurrence and hence lead to an increase in the accuracy prediction.

$$Q_{IDS} = \sum_{i=1}^{s} \frac{(G_{positive_i} - Cost_{IDS})}{s} \tag{1}$$

$$Q_{attacker} = \sum_{i=1}^{s} \frac{-(G_{positive_i} + Cost_{attacker})}{s} \tag{2}$$

$$Q'_{IDS} = \sum_{i=1}^{k} \frac{-(G_{negative_i} + Cost_{IDS})}{k} \tag{3}$$

$$Q'_{attacker} = \sum_{i=1}^{k} \frac{G_{negative_i}}{k} \tag{4}$$

$$Q_t = Q_{IDS} + Q'_{IDS} \tag{5}$$

$$Q'_{t'} = Q_{attacker} + Q'_{attacker} \tag{6}$$

Here, $G_{positive}$ and $G_{negative}$ $\in$ [0,1] are respectively the positive and negative gains, which are set at the beginning to zero and their values increase or decrease depending on the actions carried out by the IDS and attacker. *s* is the number of correct signature detections and *k* is the number of failed signature detections. $Cost_{attacker}$ and $Cost_{IDS}$ $\in$ [0,1] are respectively the required cost's rate (i.e. overhead caused by the computing processing) to generate a new attack signature by an attacker and activation of anomaly detection by the IDS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

agent. Since the IDS agent monitors the behavior of attacker, we assume in this game that the IDS is aware of $Cost_{attacker}$ for an attacker. It shall be noted that Q_t and $Q'_{t'}$ vary between 0 and 1.

Our security game is a complete information game since the IDS agent knows the attacker player's *payoff* (located within its radio range).

Table II illustrates the payoff matrix of the game between IDS agent and attacker that targets IoT device.

Table II
TABLE II. PAYOFF MATRIX OF ANOMALY DETECTION GAME

Attacker	IDS			
	S_t	S_{t+1}	…..	S_{t+n}
$S'_{t'}$	$(Q'_{t'}, Q_t)$	$(Q'_{t'}, Q_{t+1})$	$(Q'_{t'}, \dots)$	$(Q'_{t'} \quad Q_{t+n})$
$S'_{t'+1}$	$(Q'_{t'+1}, Q_t)$	$(Q'_{t'+1}, Q_{t+1})$	$(Q'_{t'+1}, \dots)$	$(Q'_{t'+1}, Q_{t+n})$
……	$(\dots, Q_t)$	$(\dots, Q_{t+1})$	$(\dots, \dots)$	$(\dots, Q_{t+n})$
$S'_{t'+n}$	$(Q'_{t'+n}, Q_t)$	$(Q'_{t'+n}, Q_{t+1})$	$(Q'_{t'+n}, \dots)$	$(Q'_{t'+n}, Q_{t+n})$

B. IDS and attacker gaming

In this subsection, we introduce the *static* and *dynamic* game models to compute the *NE* that represents the best strategy of the IDS to launch its anomaly detection technique.

a) Static game between IDS and attacker: In a static game, once a player decides his strategy, he does not have a second chance to change it [27]. According to *Nash*, there is a mixed strategy *NE* in which both IDS and attacker do not change their actions. As a result, we use *NE* to predict the equilibrium state in which the attacker will generate a new signature regardless the action of IDS (i.e. launches an anomaly detection technique or not).

Lemma 1

Let $J(\rho^1, \rho^2)$ denote the attacker and IDS's gains, where $\rho^1 \in \{S_t, S_{t+1}, \dots, S_{t+n}\}$ and $\rho^2 \in \{S'_{t'}, S'_{t'+1}, \dots, S'_{t'+n}\}$, so that $J(S_{t+n}, S'_{t'+n}) = (Q_{t+n}, Q'_{t'+n})$. Here, n is the maximum number of strategies that IDS and attacker carry out.

A pair of strategies $(\rho^{1*}$and $\rho^{2*})$ is a *NE* point if the following inequality[29]is satisfied:

$$J(\rho^{1*}, \rho^2) \leq J(\rho^{1*}, \rho^{2*}) \leq J(\rho^1, \rho^{2*}) \tag{7}$$

There is at least one NE point $J(\rho^{1*}, \rho^{2*})$that satisfies Inequality 7.

Proof 1

The average payoffs of the attacker and the IDS are defined in Equations 8 and 9 respectively.

$$J(S_{t+i}) = \sum_{i=0}^{n} s_i * (Q_{t+i}) \tag{8}$$

$$J(S'_{t+i}) = \sum_{j=0}^{n} s'_j * (Q'_{t'+j}) \tag{9}$$

In this game, the IDS and attacker try to maximize and minimize $J(S_{t+i}, S'_{t+i})$, respectively. The equilibrium, achieved by the players in the mixed strategies, is defined as follows:

$$\min_{S'} \max_{S} J(Q_{t+i}, Q'_{t'+i}) = \begin{cases} \min_{S'} \sum_{j=0}^{n} S'_j * (Q'_{t'+j}) \\ , \\ \max_{S} \sum_{i=0}^{n} s_i * (Q_{t+i}) \end{cases}$$

The NE of a mixed strategy comprises the strategies of IDS and attacker, in the form of $(\rho^{1*}, s_i^*), (\rho^{2*}, s'^*_j)$ which satisfies Inequality 7. Hence, the mixed-strategy equilibrium is unique and it is given by:

$$NE = \begin{cases} \min_{S'} \sum_{j=0}^{n} s'_j * (Q'_{t'+j}) \\ , \\ \max_{S} \sum_{i=0}^{n} s_i * (Q_{t+i}) \end{cases} \tag{10}$$

The attacker will generate a new signature when he reaches the equilibrium, i.e. $\min_{S'} \sum_{j=0}^{n} s'_j * (Q'_{t'+j})$ regardless the action taken by the IDS. Therefore, to assure a tradeoff between accuracy detection and low energy consumption, the IDS activates its anomaly detection technique only when the equilibrium is reached, which is defined as $\max_{S} \sum_{i=0}^{n} s_i * (Q_{t+i})$.

b) Dynamic game between IDS and attacker: In the *static game* model discussed above, no player has the chance to modify his strategy [27]. However, the *dynamic game* allows the IDS and attacker to adjust their strategies according to the observations of both players' past choices.

Let us consider that the game lasts for *h* time steps in total. We compute the total payoff of a player by adding its time serial payoffs over the entire game, i.e.$\sum_{t=1}^{h} J(\rho^1{}_t, \rho^2{}_t)$.

Lemma 2

The *NE* solution of the dynamic game satisfies the following inequality for all ρ_t , where t=1…, h:

$$\begin{aligned} & J(\rho^{1*}{}_1, \dots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h ; \rho^2{}_1, \dots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h) \\ \leq\ & J(\rho^{1*}{}_1, \dots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h ; \rho^{2*}{}_1, \dots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h) \\ \leq\ & J(\rho^1{}_1, \dots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h ; \rho^{2*}{}_1, \dots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h) \end{aligned} \tag{11}$$

Proof 2

According to [28][29] the value of the dynamic game for h time steps can be described as:

$$\begin{aligned} J(\rho^1{}_1, \dots, \rho^1{}_{h-1}, \rho^1{}_h; \rho^2{}_1, \dots, \rho^2{}_{h-1}, \rho^2{}_h) = {} & J(\rho^1{}_1, \rho^2{}_1) \\ & + \dots + J(\rho^1{}_{h-1}, \rho^2{}_{h-1}) + J(\rho^1{}_h, \rho^2{}_h) \end{aligned} \tag{12}$$

Based on *Theorem1* introduced before, every *NE*-point solution at time h $J(\rho^{1*}{}_h, \rho^{2*}{}_h)$ satisfies the following inequalities:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

$$
\begin{aligned}
& J\ (\rho^1{}_1, \ldots, \rho^1{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^2{}_1, \ldots, \rho^2{}_{h-1}, \rho^2{}_h\ ) \\
\leq\ & J\ (\rho^1{}_1, \ldots, \rho^1{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^2{}_1, \ldots, \rho^2{}_{h-1}, \rho^{2*}{}_h\ ) \\
\leq\ & J\ (\rho^1{}_1, \ldots, \rho^1{}_{h-1}, \rho^1{}_h\ ;\ \rho^2{}_1, \ldots, \rho^2{}_{h-1}, \rho^{2*}{}_h\ ) \\
=\ & J\ (\rho^1{}_1, \rho^2{}_1\ ) + \ldots + J\ (\rho^1{}_{h-1}, \rho^2{}_{h-1}\ ) + J\ (\rho^{1*}{}_h, \rho^2{}_h\ ) \\
\leq\ & J\ (\rho^1{}_1, \rho^2{}_1\ ) + \ldots + J\ (\rho^1{}_{h-1}, \rho^2{}_{h-1}\ ) + J\ (\rho^{1*}{}_h, \rho^{2*}{}_h\ ) \\
\leq\ & J\ (\rho^1{}_1, \rho^2{}_1\ ) + \ldots + J\ (\rho^1{}_{h-1}, \rho^2{}_{h-1}\ ) + J\ (\rho^1{}_h, \rho^{2*}{}_h\ )
\end{aligned} \tag{13}
$$

Then, we subtract and add $J\ (\rho^1{}_1, \rho^2{}_1\ ) + \cdots + J\ (\rho^1{}_{h-1}, \rho^2{}_{h-1}\ )$ and $J\ (\rho^{1*}{}_1, \rho^{2*}{}_1\ ) + \cdots + J\ (\rho^{1*}{}_{h-1}, \rho^{2*}{}_{h-1}\ )$, respectively on both sides of the inequality sign. Hence, we obtain the following inequality:

$$
\begin{aligned}
& J\ (\rho^{1*}{}_1, \ldots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^{2*}{}_1, \ldots, \rho^{2*}{}_{h-1}, \rho^2{}_h\ ) \\
\leq\ & J\ (\rho^{1*}{}_1, \ldots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^{2*}{}_1, \ldots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h\ ) \\
\leq\ & J\ (\rho^{1*}{}_1, \ldots, \rho^{1*}{}_{h-1}, \rho^1{}_h\ ;\ \rho^{2*}{}_1, \ldots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h\ )
\end{aligned} \tag{14}
$$

Here, we can permute between 1 and *h*, hence we obtain:

$$
\begin{aligned}
& J\ (\rho^{1*}{}_1, \ldots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^2{}_1, \ldots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h\ ) \\
\leq\ & J\ (\rho^{1*}{}_1, \ldots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^{2*}{}_1, \ldots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h\ ) \\
\leq\ & J\ (\rho^1{}_1, \ldots, \rho^{1*}{}_{h-1}, \rho^{1*}{}_h\ ;\ \rho^{2*}{}_1, \ldots, \rho^{2*}{}_{h-1}, \rho^{2*}{}_h\ )
\end{aligned} \tag{15}
$$

As a result, we claim that the proposed security game assures a *NE* solution in a dynamic game by satisfying recursively a set of *h* pairs of inequalities.

The hybrid intrusion detection approach allows getting high detection and low false positive rates. However, the number of false positive is still not null, specifically when the number of attackers increases. Therefore, to address this issue a reputation model based on game theory is proposed and is detailed in the following section.

IV. Reputation Model

The false positive issue is a major challenge to address since ranking a legitimate node as an intruder makes the proposed security framework inefficient. Furthermore, it is not wise to eject the monitored node immediately when it is suspected to carry out a malicious anomaly since this misbehavior could be simply due to noise or an unreliable communication channel. Thereby, a reputation game is proposed to decrease the false positive rate by ranking the monitored target into *Legitimate*, *Suspect* and *Malicious node* according to its reputation score; which is defined as follows:

1) *Legitimate node* is an IoT node that exhibits a normal behavior throughout its network lifetime,
2) *Suspected node* is an IoT node that does not work correctly due to noise or to an unreliable communication channel; by exhibiting a misbehavior pattern, e.g. does not forward the packets from legitimate IoT devices. It is not interesting to rank immediately such node as an attacker and eject it. We propose to rank it as a *Suspected node,*
3) *Malicious node* behaves persistently bad, by launching lethal attacks. These attacks are DoS threats, where they aim at exhausting the network resources or disrupting its proper operation.

With the help of game theory, we determine the *reputation thresholds* that allow us to rank the monitored node as *Normal*, *Suspect* and a *Malicious node* according to their reputation scores and hence reduce the false positive rates. In the following, we explain how to compute the reputation thresholds for ranking the monitored targets into appropriate class, *Legitimate*, *Suspect* and *Malicious node.*

A. Security game

In the proposed security game, there are two players: The defender which is the IDS agent and the target node. Each one of them has a set of strategies to increase its reputation payoff. $\mathrm{J_{Defender}}$ and $\mathrm{J_{Target}}$ denote, respectively, the defender and the target node players in the following. The players $\mathrm{J_{Defender}}$ and $\mathrm{J_{Target}}$ have a set of strategies $\varphi_{\mathrm{defender}} = \{\varphi'^1{}_i \mid i = 1,2,3\}$ and $\varphi_{\mathrm{Target}} = \{\varphi'^2{}_j \mid j = 1,2,3\}$, respectively. $\varphi'^1{}_1$, $\varphi'^1{}_2$, $\varphi'^1{}_3$ are the strategies of $\mathrm{J_{Defender}}$ to rank the monitored target node as *Legitimate*, *Suspect* and *Malicious node,* respectively; and $\varphi'^2{}_1$, $\varphi'^2{}_2$, $\varphi'^2{}_3$ are the strategies of J_{Target} to be *Normal*, *Suspect* and *Malicious node,* respectively.

Let x_i be the probability that the $\mathrm{J_{Defender}}$ adopts $\varphi'^1{}_i$, and y_j be the probability that the attacker adopts $\varphi'^2{}_j$, where $\sum_{i=1}^{3} x_i = 1$ and $\sum_{j=1}^{3} y_j = 1$.

Tables III and IV illustrate the matrix game between players; R and R represent the *reputation payoff* of the $\mathrm{J_{Defender}}$ and $\mathrm{J_{Target}}$, respectively. To increase their utility function ($\mathrm{U_{Defender}}$ and $\mathrm{U_{Target}}$), each player performs an adequate strategy. Since the aim of this intrusion detection game is to determine the *reputation thresholds* of Suspect *node* and *Malicious node,* we assume that the defender and the target carry out only these couple of strategies ($\varphi'^1{}_1$, $\varphi'^1{}_2$) or ($\varphi'^1{}_1$, $\varphi'^1{}_3$) and ($\varphi'^2{}_1$, $\varphi'^2{}_2$) or ($\varphi'^2{}_1$, $\varphi'^2{}_3$), respectively.

Table III
FIRST REPUTATION PAYOFF

		y_1	y_2
	$\mathrm{J_{Target}}$ / $\mathrm{J_{Defender}}$	$\varphi'^2{}_1$	$\varphi'^2{}_2$
x_1	$\varphi'^1{}_1$	$(\mathrm{R}_{11}, \mathrm{R'}_{11})$	$(\mathrm{R}_{12}, \mathrm{R'}_{12})$
x_2	$\varphi'^1{}_2$	$(\mathrm{R}_{21}, \mathrm{R'}_{21})$	$(\mathrm{R}_{22}, \mathrm{R'}_{22})$

As shown in Table III, a set of *reputation payoffs* R *and* R' of the players $\mathrm{J_{Defender}}$ and $\mathrm{J_{Target}}$ could be defined according to the couple of strategies ($\varphi'^1{}_1$, $\varphi'^1{}_2$) and ($\varphi'^2{}_1$, $\varphi'^2{}_2$) that the players perform; which are:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

(a) In Eq. 16, the *reputation payoffs* of both players increase since the monitored target is a *Legitimate* node and the defender delivers a correct detection.

$$\begin{cases} R_{11} = \alpha_i H_{i,j}^t - Cost^t \\ R'_{11} = \alpha_i H_{i,j}^t \end{cases} \quad (16)$$

$H_{i,j}^t \in$ [0,1] represents the high reputation score given by defender_i to target_j at time t, $Cost^t \in$ [0,1] is the energy consumption generated by the defender to rank the target node as *Legitimate*, *Suspect* or *Malicious node* at time t and $\alpha_i \in$ [0,1] represents the weight factor.

(b) In Eq. 17, the *reputation payoffs* of the defender and target node decrease and increase, respectively since the defender provides a wrong detection; however the target is ranked as a *Legitimate* node.

$$\begin{cases} R_{12} = -(\beta_i M_{i,j}^t + Cost^t) \\ R'_{12} = \alpha_i H_{i,j}^t \end{cases} \quad (17)$$

$M_{i,j}^t$ represents the medium reputation score at time t; where $M_{i,j}^t$=1/2 $H_{i,j}^t$ and $\beta_i \in$ [0,1] represents the weight factor.

(c) In Eq. 18, the *reputation payoffs* of both players decrease since the defender provides a false detection and wrongly accuses the *Legitimate* node as *Suspect*.

$$\begin{cases} R_{21} = -(\beta_i M_{i,j}^t + Cost^t) \\ R'_{21} = -\beta_i M_{i,j}^t \end{cases} \quad (18)$$

(d) In Eq. 19, the *reputation payoff* of $\text{J}_{\text{Defender}}$ increases since it delivers a correct detection. On the other hand, the *reputation payoff* of J_{Target} decreases as it is detected as a *Suspect* node.

$$\begin{cases} R_{22} = \alpha_i H_{i,j}^t - Cost^t \\ R'_{22} = -\beta_i M_{i,j}^t \end{cases} \quad (19)$$

Table IV
SECOND REPUTATION PAYOFF

$J_{Defender}$ \ J_{Target}	y_1 $\varphi'^2{}_1$	y_3 $\varphi'^2{}_3$
x_1 $\varphi'^1{}_1$	(R_{31}, R'_{31})	(R_{32}, R'_{32})
x_3 $\varphi'^1{}_3$	(R_{41}, R'_{41})	(R_{42}, R'_{42})

A set of *reputation payoffs R* and *R'* can be defined according to couple of strategies ($\varphi'^1{}_1$,$\varphi'^1{}_3$) and ($\varphi'^2{}_1$,$\varphi'^2{}_3$) that $\text{J}_{\text{Defender}}$ and J_{Target} have adopted, i.e.

(a) The *reputation payoffs of* the players $\text{J}_{\text{Defender}}$ and J_{Target} increase since the defender ranks the *Legitimate* node as *Legitimate* and are respectively equal to R_{31} and R'_{31} as shown in Eq. 20.

$$\begin{cases} R_{31} = \alpha_i H_{i,j}^t - Cost^t \\ R'_{31} = \alpha_i H_{i,j}^t \end{cases} \quad (20)$$

(b) When J_{Target} is a *Malicious* node and $\text{J}_{\text{Defender}}$ ranks it as a *Legitimate* node, the *reputation payoffs* R'_{32} and R_{32} increases and decreases, respectively as shown in Eq. 21.

$$\begin{cases} R'_{32} = \alpha_i H_{i,j}^t \\ R_{32} = -(\gamma_i L_{i,j}^t + Cost^t) \end{cases} \quad (21)$$

$L_{i,j}^t \in$ [0,1] represents the low reputation score given by defender_i to target_j at time t and $\gamma_i \in$ [0,1] represents the weight factor, where α_i+β_i+ γ_i=1.

(c) When J_{Target} is a *Legitimate* node and $\text{J}_{\text{Defender}}$ ranks it as *Malicious* node, both *reputation payoffs* R'_{41} and R_{41} decrease as shown in Eq. 22.

$$\begin{cases} R'_{41} = -\gamma_i L_{i,j}^t \\ R_{41} = -(\gamma_i L_{i,j}^t + Cost^t) \end{cases} \quad (22)$$

(d) The *reputation payoffs of* the players J_{Target} and $\text{J}_{\text{Defender}}$ decrease and increase, respectively since the target is a *Malicious* node and defender ranks it as *Malicious* and are respectively equal to R'_{42} and R_{42} as shown in Eq. 23.

$$\begin{cases} R'_{42} = -\gamma_i L_{i,j}^t \\ R_{42} = \alpha_i H_{i,j}^t - Cost^t \end{cases} \quad (23)$$

It is desired that players J_{Target} and $\text{J}_{\text{Defender}}$ negotiate their interdependent strategies to reach to an optimized steady state solution in which a consensus between players is established and hence a stability of the games is established. In the following, the steady state solution, defined as a *Saddle-point equilibrium,* is determined.

B. Reputation thresholds

The stability in our game is the best strategy raised by J_{Target} regardless the strategy of $\text{J}_{\text{Defender}}$ and vise versa. In the following, we determine the utility function for each player, $\text{U}_{\text{Defender}}$ and U_{Target}. After that, we provide the *reputation thresholds* that allow us to rank the monitored node as *Normal*, *Suspect* and a *Malicious node.*

According to Tables III and IV, the utility functions of the players J_{Target} and $\text{J}_{\text{Defender}}$, which are respectively U_{Target} and $\text{U}_{\text{Defender}}$ depend on the strategy that players have adopted, i.e.,

$\text{U}_{\text{Target}}(\varphi_{\text{Target}} = \varphi'^2{}_1)$=$R'_{11}$. x_1+R'_{21}. x_2 or
R'_{31}. $x_1 + R'_{41}$. x_3
$\text{U}_{\text{Target}}(\varphi_{\text{Target}} = \varphi'^2{}_2) = R'_{12}$. $x_1 + R_{22}$. x_2
$\text{U}_{\text{Defender}}(\varphi_{\text{defender}}$=$\varphi'^1{}_1)$= R_{11}. y_1+R_{12}. y_2 or
R_{31}. $y_1 + R_{32}$. y_3
$\text{U}_{\text{Defender}}(\varphi_{\text{defender}} = \varphi'^1{}_2) =$ R_{21}. $y_1 + R_{22}$. y_2
$\text{U}_{\text{Target}}(\varphi_{\text{Target}} = \varphi'^2{}_3) = R'_{32}$. $x_1 + R'_{42}$. x_3
$\text{U}_{\text{Defender}}(\varphi_{\text{defender}} = \varphi'^1{}_3) =$ R_{41}. $y_1 + R_{42}$. y_3

Lemma3: J_{Target} is a *Suspect* node when $x_2 > x^*$ and J_{Target} ranks it as *Suspect* when $y_2 > y^*$; where (x^*, y^*) is defined as *a first Saddle-reputation equilibrium (O_{FR}) point.*

Proof 3: The target and defender adopt strategies $\varphi'^2{}_2$ and $\varphi'^1{}_2$, respectively when
$\text{U}_{\text{Target}}(\varphi_{\text{Target}} = \varphi'^2{}_2) > \text{U}_{\text{Target}}(\varphi_{\text{Target}} = \varphi'^2{}_1)$ and
$\text{U}_{\text{Defender}}(\varphi_{\text{defender}}$=$\varphi'^1{}_2) > \text{U}_{\text{Defender}}(\varphi_{\text{defender}}$=$\varphi'^1{}_1)$,i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

$$\begin{cases} R'_{12}.\ x_1 + R'_{22}.\ x_2 > R'_{11}.\ x_1 + R'_{21}.\ x_2 \\ , \\ R_{21}.\ y_1 + R_{22}.\ y_2 > R_{11}.\ y_1 + R_{12}.\ y_2 \end{cases} \quad (24)$$

It is noted that x_1+x_2 +$x_3 = 1$ and y_1+y_2 +$y_3 = 1$. Here, we assume that only a suspicious or normal behavior could be launched by $\mathrm{J_{Target}}$, which lead to x_1+x_2 >> x_3 and y_1+y_2 >> y_3. Hence we obtain, x_1= (1-x_2) and y_1= (1-y_2). As a result, we can deduce from Eq. 24 the following equation:

$$\begin{cases} x_2 > \frac{R'_{11} - R'_{12}}{R'_{22} + R'_{11} - R'_{12} - R'_{21}} \\ , \\ y_2 > \frac{R_{11} - R_{21}}{R_{22} + R_{11} - R_{21} - R_{12}} \end{cases} \quad (25)$$

Therefore, the IDS ranks the target IoT device as a *Suspected* node when O_{FR} point is reached which is equal to (x*, y*) = ($\frac{R'_{11} - R'_{12}}{R'_{22} + R'_{11} - R'_{12} - R'_{21}}$, $\frac{R_{11} - R_{21}}{R_{22} + R_{11} - R_{21} - R_{12}}$); where y* is a *reputation threshold* of a suspected node.

Lemma 4: $\mathrm{J_{Target}}$ is a *Malicious* node when x_3 >*x'** and $\mathrm{J_{Target}}$ ranks it as *Malicious* when y_3>*y'*;* where (*x'*, y'**) is defined as a *second Saddle-reputation equilibrium (O_{SR})* point.

Proof 4: The target and defender adopt strategies ${\varphi'^2}_3$ and ${\varphi'^1}_3$, respectively when $\mathrm{U_{Target}}(\varphi_{\mathrm{Target}} = {\varphi'^2}_3)$> $\mathrm{U_{Target}}(\varphi_{\mathrm{Target}} = {\varphi'^2}_1)$ and $\mathrm{U_{Defender}}(\varphi_{\mathrm{defender}}={\varphi'^1}_3)$>$\mathrm{U_{Defender}}(\varphi_{\mathrm{defender}}={\varphi'^1}_1)$,i.e.,

$$\begin{cases} R'_{32}.\ x_1 + R'_{42}.\ x_3 > R'_{31}.\ x_1 + R'_{41}.\ x_3 \\ , \\ R_{41}.\ y_1 + R_{42}.\ y_3 > R_{31}.\ y_1 + R_{32}.\ y_3 \end{cases} \quad (26)$$

Here, we assume that only a malicious or a normal behavior could be launched by $\mathrm{J_{Target}}$, which lead to x_1+x_3 >> x_2 and y_1+y_3 >> y_2. Hence, we obtain x_1= (1-x_3) and y_1= (1-y_3). As a result, we can deduce from Eq. 24 the following equation:

$$\begin{cases} x_3 > \frac{R'_{31} - R'_{32}}{R'_{42} + R'_{31} - R_{32} - R'_{41}} \\ , \\ y_3 > \frac{R_{31} - R_{41}}{R_{42} + R_{31} - R_{41} - R_{32}} \end{cases} \quad (27)$$

Therefore, the IDS ranks the target IoT device as a *Malicious* node when O_{SR} point is reached which is equal to (x'*, y'*) = ($\frac{R'_{31} - R'_{32}}{R'_{42} + R'_{31} - R_{32} - R'_{41}}$, $\frac{R_{31} - R_{41}}{R_{42} + R_{31} - R_{41} - R_{32}}$), where y'* is a *reputation threshold* of a malicious node.

y is the probability that IDS agents identify the target IoT device as *Suspected* or *Malicious* node, where y'*> y* and the condition to rank the monitored IoT device in an appropriate class is defined as follows:

$$\begin{cases} IoT\ device\ is\ a\ Malicous\ node\ when \\ y > y'^* = \frac{R_{31} - R_{41}}{R_{42} + R_{31} - R_{41} - R_{32}} \\ IoT\ device\ is\ a\ Suspected\ node\ when \\ y > y^* = \frac{R_{11} - R_{21}}{R_{22} + R_{11} - R_{21} - R_{12}} \\ IoT\ device\ is\ a\ Normal\ node\ when \\ y < y^* \end{cases}$$

V. Performance Evaluation

Our approach was implemented in wireless sensor networks, well-known for low-resource IoT devices. In the simulation, we use a TOSSIM simulator [30], a simulator of TinyOS sensor nodes. As explained in the introduction section, the hybrid intrusion detection scheme, combining the signature-based detection and anomaly-detection techniques, exhibits high detection and low false positive rates. In this section, we compare our lightweight hybrid intrusion detection system with current hybrid intrusion detection techniques [7],[14],[20]. In the latter and as explained in the related work section, the anomaly detection technique runs on each sensor node and is activated at all the time. This is unlike the lightweight technique, where the anomaly detection is activated (with the help of game theory) only when a new attack's signature is expected to occur. Here, we evaluate the accuracy detection (i.e., detection and false positive rates), energy consumption and efficiency. These metrics are defined as follows:

1) *Detection Rate (DR):* defined as the ratio of the number of correctly detected attackers to the total number of attackers,
2) *False Positive Rate (FPR):* defined as the ratio of the number of normal sensor nodes incorrectly classified as attackers to the total number of normal sensor nodes.
3) *Energy Consumption (EC):* defined as the total energy consumed by all sensors and computed as follows [10]:

$$E_{total} = \frac{\sum_{i=1}^{N} E_{node_i}}{N} \quad (28)$$

Where E_{total} is the total energy of the network and *N* is the number of sensor nodes.

1) *Efficiency (E),* defined as the time required to identify a malicious node.

$$E = \sum_{\mathrm{i}=1}^{n} \frac{\mathrm{R_i}}{n} \quad (29)$$

Where $\mathrm{R_i}$ is the time required for the IDS agent *i* to detect the occurrence of an attacker.

A. Simulation setup

In our network, the mobile and static sensors are randomly deployed over a square area of (300×300) m^2. Mobile sensor nodes follow a deterministic mobility model [31], whereby the mobile sensors follow well-defined paths and choose random speeds from within the interval [min speed, max speed]. We vary the number of attackers from 10% to 40% of overall nodes. We insert two categories of attackers: *(i) attackers with a transitory misbehavior* that oscillate between normal and malicious behaviors and *(ii) attackers with a permanent misbehavior* that persist to act as malicious node, i.e. does not switch on a normal behavior. In the simulation, the attacker carries out the most dangerous attack, which is a DoS attack, where he aims at exhausting the network resources or disrupting its proper operation. The anomaly detection technique used by the IDS agents is a Back Propagation Network (BPN), which is the most typical and most general model to use in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

a neural network [32]. The main simulation parameters are summarized in Table V. These parameters were chosen to be as most realistic as possible.

Table V
SIMULATION PARAMETERS

Simulation time	900 seconds
Simulation area	300*300 m2
Number of sensors	From 50 to 300
Number of attackers	From 10 % to 40 % of overall nodes
Radio model	Lossy radio model
Radio range	15 meter
Sensor initial energy	9 Joule
Anomaly detection	BPN
Mobility model	Deterministic mobility model

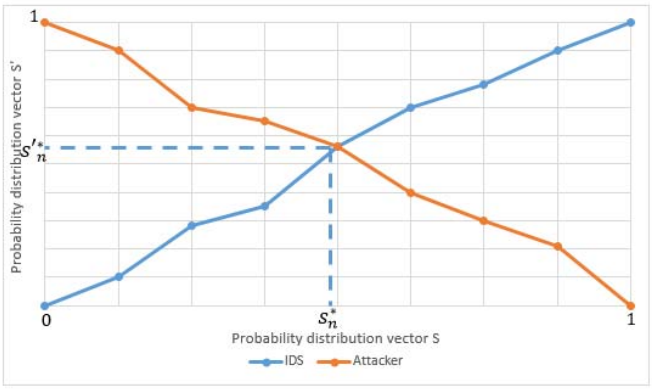


Figure 3. Probability distribution vectors (S and S'): NE point

B. Results analysis

The main results are summarized below. In our simulations, we first study the probability distribution vectors S=$\{s_0,\ldots, s_n\}$ and S'=$\{s'_0,\ldots, s'_n\}$ and determine the *NE* point where the attacker generates a new signature and the IDS launches an anomaly detection technique, respectively. Afterwards, we compute the accuracy detection, efficinecy and energy consumption for both lightweight hybrid detection system and current hybrid detection systems [7],[14],[20], and compare their performance. The accuracy detection and energy consumption metrics are computed for each hybrid detections system [7],[14],[20], and the average values of these metrics are compared against those of the lightweight hybrid detection system. We compute the average values because the accuracy detection and energy consumption for each system [7],[14],[20] are almost the same. The measurements are based on averaging the results obtained from 15 simulation runs by varying the number of sensors and attackers from 50 to 300 and from 10 % to 40 % of overall nodes, respectively.

a) Optimal Activation of Anomaly Detection: Optimal NE point : As shown in Figure 3, the probability that an IDS agent detects *(m+n)* signatures at time *(t+n),* i.e. s_n and the probability that the attacker launches *(m'+n)* signatures during a period of time *(t'+n),* i.e., s'_n increases and decreases, respectively. This is due to the fact that, as explained in proof 1, in this security game, the IDS and attacker try to maximize and minimize the value of $J(S_{t+i},\ S'_{t'+i})$ respectively, i.e.$\underset{S_{t+i}}{max} \sum_{i=0}^{n} S_{t+i} * (Q_{t+i})$ and$\underset{S'_{t'+i}}{min} \sum_{i=0}^{n} S'_{t'+i} * (Q'_{t'+i})$. The *NE* point (s^*_n,s^*_n) in which the attacker will generate a new signature regardless the action of IDS and vice versa is illustrated in Figure 3 and depends mainly on the values of $G_{positive}$, $G_{negative}$, $Cost_{IDS}$, $Cost_{attacker}$ and *n* as shown in Table VI.

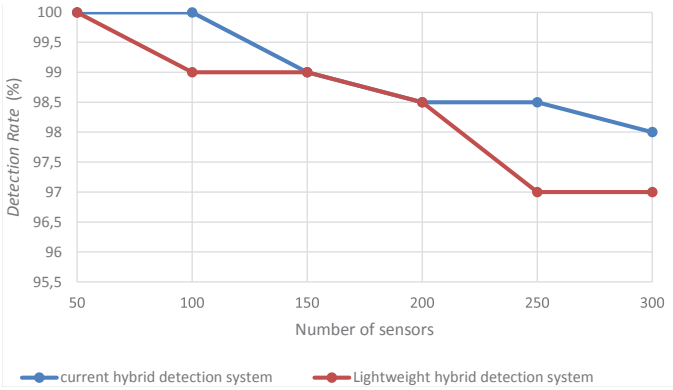
Table VI
NE POINTS

$G_{positive}$	$G_{negative}$	$Cost_{IDS}$	$Cost_{attacker}$	n	s^*_n	s'^*_n
0,08	0,2	0,2	0,3	20	0,43	0,24
0,1	0,3	0,3	0,4	25	0,50	0,31
0,18	0,4	0,5	0,65	30	0,55	0,35

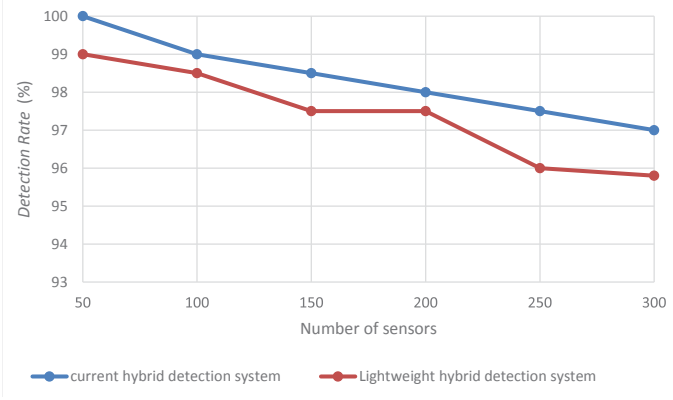
b) Detection & false positive rates: According to Figures 4 and 6, we observe that when the number of sensor nodes and attackers increase, the detection rate (and fasle postive rate) of both hybrid detection systems exceeds 92% (is lower than 3%). Furhemore, we found out that the detection and fasle postive rates of our lightweight detection system is close to the current hybrid detection systems [7],[14],[20]. This is achieved even when the number of sensors and attackers increase. High detection and low false positive rates achieved thanks to our detection system are attributed to the following reasons: (*i*) *Nash equilibrium*, as it allows to determine the state in which the attacker can launch a new signature with a goal to carry out an attack without being detected. In this case, the IDS agent activates its anomaly detection against the suspected nodes and ejects the malicious attacker before raising a lethal cyber-attack. *(ii) Reputation model*, as it aims to rank the monitored IoT devices in an appropriate class *Normal*, *Suspect* or *Malicious* according to their reputation scores and hence leads to a further decrease of the false postive rate. This is acheived by determining the optimal *Saddle-reputation equilibrium* points, O_{FR} *and* O_{SR}. According to Figure 5, it is apparent that without using the reputation model the false positive rate generated by our lightweight hybrid detection system increases quickly and reaches almost 5% when the numbers of attackers and sensors are high.

c) Efficiency: Figure 7 plots the efficiency of current hybrid detection systems [7],[14],[20] and our lightweight hybrid detection system. As shown in Figure 7, we set the number of sensors to 300 and vary afterward the number of attackers from 5% to 40% of overall nodes. When the number of attackers increases, the required time of IDS agents to detect all malicious nodes for each detection system increases. From Figure 7, we observe that our proposed lightweight hybrid detection system requires less time to detect the attacks contrary to the current hybrid detections systems. In our simulations, we observe that when the number of attakers increases, a considerable number of attackers can attack simultaneously the attractive link. Thereby, our approach aims to launch the anomaly detection technique in such link which leads the IDS agents to detect the attackers within a short time as illustrated in Figure 7. As a result, we claim that the lightweight hybrid

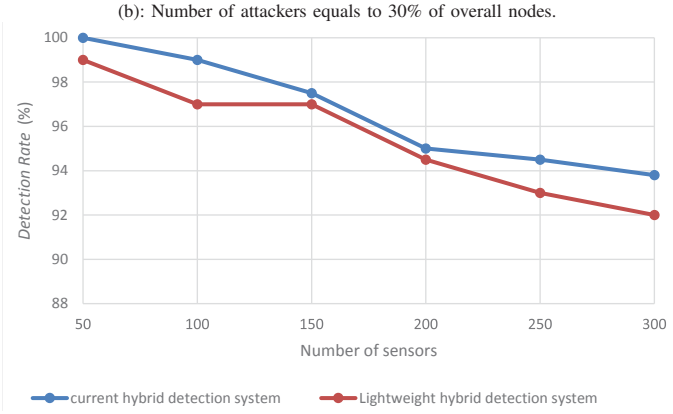
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology



(a): Number of attackers equals to 10% of overall nodes.



(b): Number of attackers equals to 30% of overall nodes.



(c): Number of attackers equals to 40% of overall nodes.

Figure 4. Detection rate of the current hybrid detection [7],[14],[20] and lightweight hybrid detection systems.

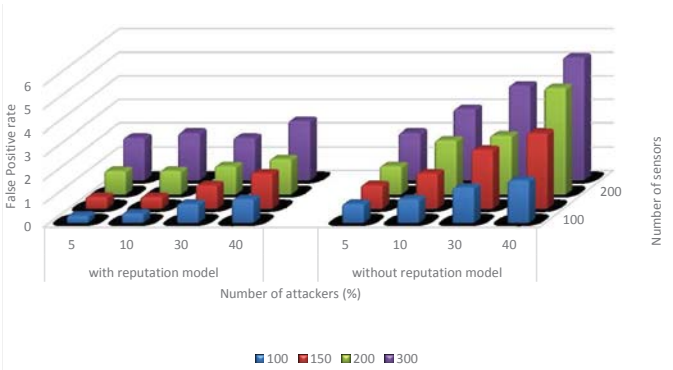
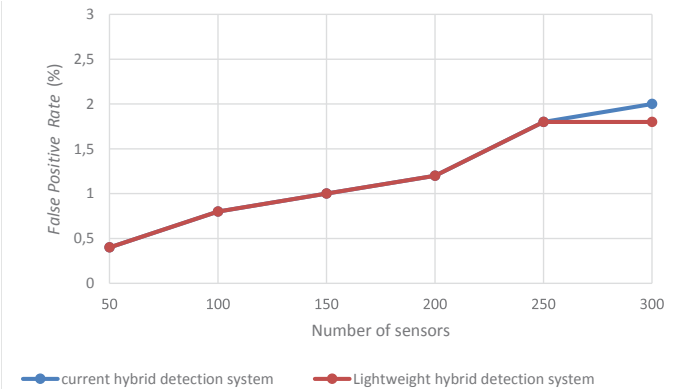
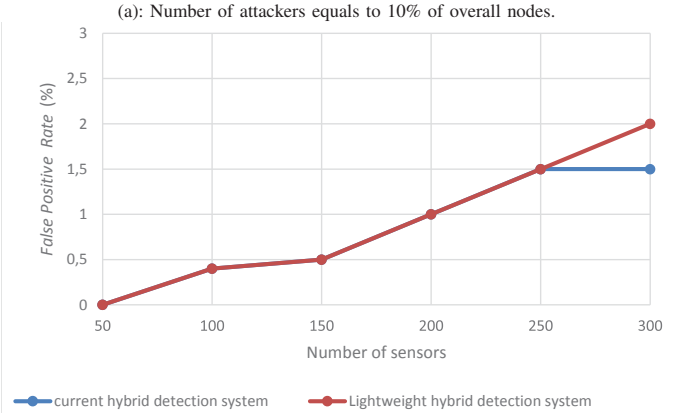


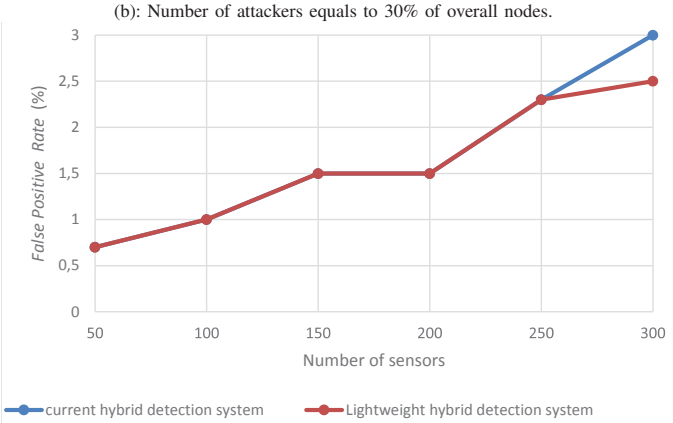
Figure 5. False positive rate generated by lightweight hybrid detection system: with and without reputation model.



(a): Number of attackers equals to 10% of overall nodes.



(b): Number of attackers equals to 30% of overall nodes.



(c): Number of attackers equals to 40% of overall nodes.

Figure 6. False positive rate of the current hybrid detection [7],[14],[20] and lightweight hybrid detection systems (with reputation model).

detection system requires a short time to detect the attackers.

d) Energy consumption : One of the main constraints of low-resource IoT devices is energy consumption since when a heavy detection technique is embedded in such device it decreases rapidly its lifetime. Thereby, energy is a highly important point in the design and implementation of IoT applications. As shown in Figure 8, we set the number of attackers to 40% of overall nodes, afterward we vary the number of sensors and compute the energy consumption. It becomes apparent that the lightweight detection technique requires a low energy consumption to achieve a high security level. This is unlike the current hybrid detection systems [7],[14],[20] since a high-energy consumption is generated

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2701551, IEEE Transactions on Vehicular Technology

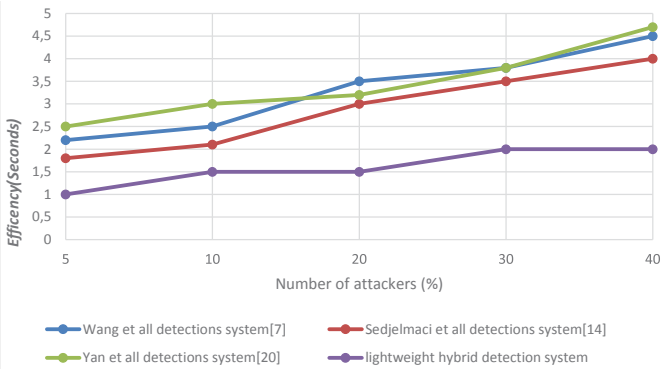


Figure 7. Efficiency

specifically when the number of sensors increases.

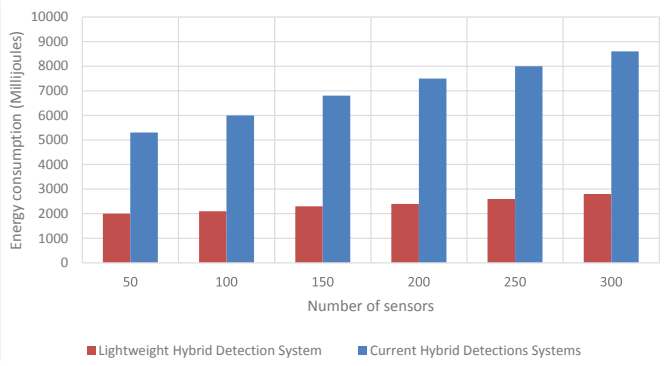


Figure 8. Energy consumption of the current hybrid detection [7],[14],[20] and lightweight hybrid detection systems

Proposition 1. $E_{total} >> E'_{total}$, where E_{total} and E'_{total} are the total energy consumed by all IoT devices in the hybrid intrusion detection scheme [7],[14] or [20] and our lightweight hybrid intrusion detection scheme, respectively.

Proof:

$E_{total}(M,d)=\sum_{i=1}^{N} \frac{(E_{TX_i}(M,d)+E_{RX_i}(M)+E_{Computation_i})}{N}$

and

$E'_{total}(M,d)=\sum_{i=1}^{N} \frac{(E'_{TX_i}(M,d)+E'_{RX_i}(M)+E'_{Computation_i})}{N}$,

where E_{TX_i} is an energy cost to transfer *M* bits messages to a distance d, E_{RX_i} is the energy cost to receive *M* bit messages, $E_{Computation_i}$ is the energy cost caused by the computation process and *N* is the number of IoT devices.

The condition $E_{total} >> E'_{total}$ is attributed to the following reasons: (*i*) With the help of *Nash equilibrium,* the lightweight detection technique activates an anomaly detection only if needed, leading to a decrease in the computation overhead generated by the NN learning algorithm. Owing to the fact that a low energy is required to build rules related to attackers' new signatures, we can easily claim that $E_{Computation_i} > E'_{Computation_i}$. (*ii*) In the current hybrid detection systems, a high number of intrusion messages (where the signature is stored) is exchanged within a network, specifically when the number of detected signatures is high, leading to an increase in communication overhead. Therefore, $(E_{TX_i}(M,d) + E_{RX_i}(M)) > (E'_{TX_i}(M,d) + E'_{RX_i}(M))$.

C. Security analysis

In this subsection, we analyze the security of the proposed approach against the false positive rate and a list of cyber-attacks.

(a) Security metrics

Proposition 2. $S >> S'$, where *S* and S' are the false positive rate generated by the hybrid intrusion detection technique [7],[14] or [20] and our lightweight hybrid intrusion detection system, respectively.

Proof: $S=\sum_{i=1}^{|Z|}\sum_{j=1}^{|K_i|} G(z_i,k_j) + \sum_{i=1}^{|Z|}\frac{O(z_i)}{K}$ and $S'=\sum_{i=1}^{|Z|}\sum_{j=1}^{|K_i|} G'(z_i,k_j) + \sum_{i=1}^{|Z|}\frac{O'(z_i)}{K}$, where $Z=\{z_1, \ldots..,z_n\}$ is the number of IoT devices in a network and $K=\{k_{i1}, \ldots..,k_{im}\}$is the number of IDS' neighbors. If an attacker does not launch an attack but the IDS categorizes it as malicious, $G(z_i,k_j)$=1. Otherwise $G(z_i,k_j)$=0. $O(z_i)$ is the number of IDS' neighbors that sent a wrong notification to IDS agent, i.e., claims that a well-behaved IoT device is a malicious node.

The condition $S >> S'$ is held for the following reasons: (*i*) in our lightweight hybrid detection system, $O(z_i)$ tends to zero since only a trusted number of IoT devices participate in the intrusion monitoring and decision process. This is unlike, the hybrid detection technique [7],[14] and [20], in which all nodes (trusted and no trusted nodes) activate simultaneously their IDS agents. (*ii*) Reputation model. It is not wise to eject the IoT device immediately when it is suspected to launch a malicious anomaly since this anomaly could be simply due to noise or an unreliable communication channel. To decrease further the false positive rate, our reputation game ranks the monitored IoT device into *Legitimate*, *Suspect* and *Malicious node* according to its reputation score; therefore $G(z_i,k_j) > G'(z_i,k_j)$.

(b) Cyber attack

We analyze our security game framework to prove that it is secured against attacks such as hello flood, sink hole, black hole, sybil, wormhole, spoofed and altered information and resource exhaustion attacks. Readers are referred to [10],[21],[33] for the taxonomy of these attacks.

Hello flood, sink hole and black hole attacks. These attacks generate a high Signal Strength Intensity (SSI) to lure the target devices that are close to the destination. Afterward, these attacks drop all packets received. Our IDS agent uses a signature based detection as shown in Table 1 to monitor the behaviors of neighboring IoT devices by analyzing the SSI and Packets Dropping Rate (PDR). To detect this kind of threats, each IDS agent monitors the SSI and PDR related to each neighboring node. In case, the values of SSI and PDR exceed certain predefined thresholds, T_{SSI} and T_{PDR} as explained in Table 1, the monitored node is qualified as an attacker. However these thresholds could vary over time and hence the false negative may increase. In order to address this issue, the proposed dynamic game launches the anomaly detection technique to update these thresholds and builds the rule related to each new attack's pattern.

Sybil attack. A Sybil node generates a set of fabricated identities in order to lure the legitimate IoT devices. According to [34], the main feature of this attack is the signal strength distribution. The IDS agent which is embedded at each IoT device analyzes the signal distribution of its neighbors by using its signature based detection technique as shown in Table 1. However, the normal patterns of signal distribution could vary over time. In this case, the anomaly based detection is activated by the proposed dynamic game in order to build new patterns to be used by the signature based detection technique. This is achieved when the equilibrium is reached as shown in Eq (10).

Resource exhaustion attack. This threat aims to exhaust the resources of legitimate IoT nodes, by requesting a considerable number of tasks. To detect this attack, the IDS monitors the, Total Number of Requests (TNR) by using the signature based detection technique, as shown in Table 1. To increase the detection rate, the anomaly detection is activated to detect the misbehavior patterns that are usually not detected by signature-based detection technique. Furthermore, this latter could generate a high number of false positives, specifically when the number of resource exhaustion attacks increases. Therefore, to decrease the false positive rate, a reputation model is developed that aims to rank the monitored IoT devices in an appropriate class, namely Normal, Suspect or Malicious, according to their reputation scores.

Wormhole, Spoofed and altered information attacks. These cyber threats are the most dangerous DoS attacks that could target IoT devices. To detect these threats, the IDS agent monitors the features PDR and Message Modification Rate (MMR) and launches the signature based detection as shown in Table 1. Therefore, in case the values of PDR and MMR exceed certain predefined thresholds (T_{SSI} and T_{PDR}), the monitored device could be qualified as wormhole, or altered information attacks. Our security game updates these thresholds by launching the anomaly based detection technique as shown in Eq (10). When these attacks occur, the anomaly detection technique could exhibit a certain number of false positives. To decrease the false positive rate, our reputation game is used to categorize the monitored device in an appropriate class.

VI. Conclusion and Future Work

Security for resource-constrained IoT devices is a challenging issue. In this paper, we proposed and designed a lightweight anomaly detection technique, where a tradeoff between detection accuracy, false positive rates, and energy consumption is achieved using the *Nash Equilibrium concept*. This latter determines the equilibrium state that allows the IDS agent to activate its anomaly detection technique to detect new attack's signature. Furthermore, even by combining between the anomaly and signature detection techniques, the number of false positives is still no null. Thereby, to decrease further the false positive rates a reputation model is proposed. We analyzed the performance and demonstrated the viability of our proposed approach in WSN using TOSSIM simulator. According to the simulation results, we proved that our lightweight anomaly detection approach required low energy consumption to achieve high detection accuracy and low false positive rates. This is unlike the current anomaly detection techniques that require a high energy to exhibit a high detection rate since these detection techniques are permanently activated at each node (i.e. nodes do not switch to idle time). As future research work, our goal, is to implement a part of our solution in order to secure a wireless sensor network composed of different low-power devices deployed in a smart building. These devices would collect different information (e.g., temperature, humidity, energy consumption, etc.) and send them to a remote center for further analysis through a gateway.

VII. Acknowledgements

This work has been funded by the European project ITEA FUSE-IT [35]. It is also partially supported by the ANASTACIA project, that has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N 731558 and from the Swiss State Secretariat for Education, Research and Innovation. The work is an enhanced and extended version of the paper presented at IEEE ICC KL, Malaysia, 2016 [36].

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things Journal*, Vol 1, No 1, 2014, pp. 22-32.

[2] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT urban scenarios," *IEEE Sensor Journal*,Vol 13, No 10, 2013, pp. 3558–3567.

[3] Z. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols through Traffic-Feature Analysis", *IEEE/ACM Transactions on Networking*, Vol 18, No 4, 2010, pp. 1234-1247.

[4] S. Raza, L. Wallgren, T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", *Ad Hoc Networks,* Vol 11*,* Issue 8, 2013, pp. *2661-2674.*

[5] H. W. Njogu, L. Jiawei, J. N. Kiere and D. Hanyurwimfua, "A comprehensive vulnerability based alert management approach for large networks," *Future Generation Computer Systems*, Vol 29, Issue 1, 2013, pp. 27-45.

[6] T.H. Hai, E.N. Huh, Jo M. "A lightweight intrusion detection framework for wireless sensor networks", *Wireless Communications and Mobile Computing*, Vol10, Issue 4, 2010, pp.559–572.

[7] S.S. Wang, K.Q.Yan, S.C.Wang, C.W.L, "An integrated intrusion detection system for cluster-based wireless sensor networks", *Expert Systems with Applications*, Vol 38, Issue 12, 2011, pp. 15234–15243.

[8] K. Simkhada, T. Taleb, Y. Waizumi, A. Jamalipour, and Y. Nemoto, "Combating against Internet Worms in Large-Scale Networks: An Autonomic Signature-based Solution", *Wiley InterScience Journal on Security and Communication Networks*, Vol 2, No 1, 2009, pp. 11-28.

[9] T. Taleb and Y. Hadjadj-Aoul, "QoS2: A Framework for Integrating Quality of Security with Quality of Service," *Wiley J. on Security & Communication Networks*, Vol 5, No 12, Dec. 2012. pp. 1462-1470.

[10] H. Sedjelmaci, SM. Senouci, M. Feham, "Efficient Intrusion Detection Framework in Cluster-Based Wireless Sensor Networks", *Security and Communication Networks*, Vol 6, Issue 10, 2013, pp. 1211–1224.

[11] M.A. Faisal, Z. Aung, J. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study", *IEEE Systems Journal*, Vol 9, Issue 1,2015, pp, 31-44.

[12] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks", *IEEE Wireless Communications*, Vol 15 , Issue 4 , 2008, pp.34-40.

[13] Á. Herrero, M. Navarro , E. Corchado, V. Julián, "RT-MOVICAB-IDS: Addressing real-time intrusion detection", *Future Generation Computer Systems*, Vol 29, Issue 1, 2013, pp. 250-261.

[14] H. Sedjelmaci, SM. Senouci, M. Feham, "Intrusion Detection Framework of Cluster-based Wireless Sensor Network", *IEEE ISCC*, Cappadocia, Turkey, 2012 pp. 893 -897 .

[15] A. Abduvaliyev, S. Lee, Y.K. Lee. "Energy efficient hybrid intrusion detection system for wireless sensor networks". IEEE International Conference on Electronics and Information Engineering, Kyoto, Japan, 2010, PP. 25–29.

[16] W. Lee, S. Stolfo, and K. Mok, "A data mining framework for building intrusion detection models," *in Proc. IEEE Symp. Sec. Privacy*, Oakland, CA, USA, 1999, pp. 120–132.

[17] L. Wallgren, S. Raza, and T.Voigt, "Routing attacks and countermeasures in the RPL-based internet of things", *International Journal of Distributed Sensor Networks,* 2013, pp.1-10.

[18] Y. Zhang , L.Wang, W.Sun, R. C. Green , M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids", *IEEE Transactions on Smart Grid*, Vol 2, Issue 4, 2011, pp. 796-807.

[19] S. Pan, T. Morris, and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems", *IEEE Transactions on Smart Grid*, Vol 6, Issue 6, 2015, pp. 3104 - 3113.

[20] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network", In Proc. 3rd IEEE International Conference on Computer Science and Information Technology, Chengdu, China, 2010, pp.114-118.

[21] H. Sedjelmaci, S M Senouci "An Accurate and Efficient Collaborative Intrusion Detection Framework to Secure Vehicular Networks", *Computers & Electrical Engineering,*, Vol 43, 2015, pp.33-47.

[22] H Sedjelmaci, S M Senouci, "An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks", *IEEE Internet of Things Journal,* Vol 1, Issue 4, 2014, pp. 570-577.

[23] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks", *IEEE Journal on Selected Areas in Communications*, Vol 25, No 8, 2007, pp. 1557-1568.

[24] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of Wireless Sensor Networks towards the Internet of Things: a Survey," i*n Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM '11)*, Split, Croatia 2011, pp. 1–6.

[25] M.T. Lazarescu, "Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications", *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*. Vol 3, Issue 1, 2013, pp.45–54.

[26] A. Stetsko , L. Folkman , V. Matay . "Neighbor-based intrusion detection for wireless sensor network", *IEEE 6th International Conference on Wireless and Mobile Communications*, Valencia, Spain, 2010, pp. 420–425.

[27] Q. Wu, S. Shiva, S. Roy, C. Ellis, V. Datla, "On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks", *Proceedings of the 2010 Spring Simulation Multiconference*, Orlando, Florida, USA, 2010.

[28] J. Ma, Y. Liu, L. Song, Z. Han, "Multi-act dynamic game strategy for jamming attack in electricity market," *IEEE Transactions on Smart Grid*, Vol 6, Issue5, 2015, pp. 2273 - 2282.

[29] T. Basar, G.J. Olsder, Dynamic noncooperative game theory, 2^{nd} Edition, *SIAM Series in Classics in Applied Mathematics*, Philadelphia, January 1999

[30] Simulating TinyOS networks. Available at: http://www.cs.berkeley.edu/pal/research/tossim.html

[31] T. Veerawadtanapong, W. San-Um, "A New Deterministic Node Mobility Model using Logistic Map for Mobile Ad Hoc Wireless Network", *5th International Conference on Knowledge and Smart Technology (KST),* Chonburi, Thailand, pp. 53 – 58, 2013.

[32] D.E. Philippe, "Neural network models: theory and projects", London ; New York : *Springer*, 1997.

[33] H. Sedjelmaci, S-M. Senouci, "A lightweight hybrid security framework for wireless sensor networks*", IEEE ICC*, Sydney, Australia , 10-14 June 2014.

[34] B. Yu, CZ. Xu, B. Xiao, "Detecting Sybil attacks in VANETs", *Journal of Parallel and Distributed Computing,*, Vol 73, Issue 6, 2013, pp. 746-756.

[35] Fuse-It project (2014-2017), http://www.itea2-fuse-it.com/.

[36] H. Sedjelmaci, S-M. Senouci, M. Al Bahri, "A Lightweight Anomaly Detection Technique for Low-Resource IoT Devices: A Game-Theoretic Methodology*", IEEE ICC*, Kuala Lumpur, Malaysia, 23-27 May 2016.

Hichem Sedjelmaci (M'14) received the Ph.D. degree in telecommunication systems from University of Tlemcen, Tlemcen, Algeria, in 2013. From 2013 to 2016, he was a PostDoc with the DRIVE Laboratory, University of Burgundy, Nevers, France. In 2017, he joined the Institut de recherche technologique SystemX, Paris saclay as Research Engineer in cyber security. He has been participating in several national and European-wide research projects such as ITEA CarCoDe (2013–2015) and ITEA FUSE-IT(2014–2017).He also participates in mounting research projects related to cybersecurity. Recently, he has been involved in mounting a European research project, i.e., cybersecurity in the airport areas (ITEA3-ALADIN project). He published his work in major IEEE conferences (ICC, GLOBECOM, WCNC,ISCC) and premium journals (IEEE TRANSACTIONS). His research interests include vehicular networks, wireless sensor networks, unmanned aerial vehicle, and security issues. Dr. Sedjelmaci is a member of the IEEE Communications Society.

Sidi-Mohammed Senouci (M'06) obtained his Ph.D. degree in October 2003 in the Computer Science at the University of Paris 6. From September 2010, he is full professor at ISAT, a major French post-graduate school located in Nevers, France, and component of the University of Bourgogne. His current research interests include Vehicular Communications, Ad hoc and Sensor Networks, TCP over Wireless, Wireless and Mesh Networks, Cooperative Networks, and Performance evaluation. He holds 7 international patents on these topics and published his work in major IEEE conferences and renowned journals. He was co-chair of AHSN Symposium in IEEE Globecom 2011 and co-chair of NGN Symposium in IEEE ICC'2012. He was vice-chair of SAC symposium in IEEE Globecom2010, co-chair of VCT Symposium in IEEE WCMC2010, and TPC co-chair of VehiCom2009 Workshop. He was the founding Chair of Ubiroads2007 workshop. He was the guest editor of a special issue of UBICC journal and was the special track co- chair in PIMRC'08 on ITS. He is founding co-editor of the IEEE ComSoc Ad Hoc and Sensor Network Technical Committee (AHSN TC) Newsletter. He has also been serving as TPC member of the following IFIP, ACM or IEEE conferences and workshops (ICC, GLOBECOM, PIMRC, GIIS, VTC, WiVeC, MWCN, IWWAN, Wireless Days, WITS, etc.). He is the Chair of IEEE ComSoc IIN Technical Committee, TCIIN (2014-2016). He is also a Member of IEEE and the Communications Society and Expert Senior of the French society SEE (Society of Electricity and Electronics).

Tarik Taleb (SM'10) received the B.E. degree (with distinction) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Professor with the School of Electrical Engineering, Aalto University, Espoo, Finland. Prior to his current academic position, he was a Senior Researcher and a 3GPP Standards Expert at NEC Europe Ltd. He was then leading the NEC Europe Laboratories Team working on RD projects on carrier cloud platforms. Before joining NEC and until March 2009, he was an Assistant Professor with the Graduate School of Information Sciences, Tohoku University, in a laboratory fully funded by KDDI. He has been also directly engaged in the development and standardization of the evolved packet system as a member of 3GPP's System Architecture working group. His research interests lie in the field of mobile core, mobile cloud networking, network function virtualization, software-defined networking, mobile multimedia streaming, and social media networking. Prof. Taleb is an IEEE ComSoc Distinguished Lecturer. He is serving as a Chair of the Wireless Communications Technical Committee. He is/was on the editorial board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEEWireless Communications Magazine, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE Communications Surveys Tutorials, and a number of Wiley journals. He has been a recipient of numerous awards, including the prestigious IEEE ComSoc Asia-Pacific Best Young Researcher award and the TELECOM System Technology Award from the Telecommunications Advancement Foundation. Some of his research studies have been also awarded best paper awards at prestigious conferences.