A Lightweight Anomaly Detection Technique for Low-Resource IoT Devices: A Game-Theoretic Methodology

Hichem Sedjelimaci,, Sidi Mohammed Senouci, Mohamad Al Bahri

A Lightweight Anomaly Detection Technique for Low-Resource IoT Devices: A Game-Theoretic Methodology

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

***Abstract*— In the Internet of Things (IoT), resources' constrained tiny sensors and devices could be connected to unreliable and untrusted networks. Nevertheless, securing IoT technology is mandatory, due to the relevant data handled by these devices. Intrusion Detection System (IDS) is the most efficient technique to detect the attackers with a high accuracy when cryptography is broken. This is achieved by combining the advantages of anomaly and signature detection, which are high detection and low false positive rates, 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. However, the activation of anomaly detection for low-resource IoT devices could generate a high-energy consumption, specifically when this technique is activated all the time. Using game theory and with the help of *Nash equilibrium*, anomaly detection is activated only when a new attack's signature is expected to occur. This will make a balance between accuracy detection and energy consumption. Simulation results show that the proposed anomaly detection approach requires a low energy consumption to detect the attacks with high accuracy (i.e. high detection and low false positive rates).**

***Index Terms*— Anomaly detection, Low-resources devices, Game theory, Nash equilibrium.**

I. INTRODUCTION

The Internet of Things (IoT) has the ability to incorporate transparently a large number of heterogeneous devices such as, for instance cameras, wireless sensor network (WSN), smart meters, vehicles, etc, while providing open access to a variety of data generated by such devices to provide new services to citizens and companies [1]. Due to the services that IoT technology affords, it finds applications in many different domains such as medical aids, automotive, smart grid, and many others [2]. The relevant data exchanged between IoT devices are more vulnerable to attacks since they are often deployed in a hostile and insecure environment. Therefore, security solutions are mandatory to protect IoT devices from intruder attacks. In this paper, our aim is to secure low resources IoT devices such as smart meters and sensors against any malicious behaviors.

The Intrusion Detection System (IDS) is very effective to protect IoT devices against intruders since it has the capability to detect both internal and external attacks with a high accuracy [3]. In order to monitor and detect malicious devices, detection techniques can be classified into two main approaches [3][4][5]: *(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. Such technique aims to *reduce the false positive* and it 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 a supervised learning algorithms [6][7][8], 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.

According to several research works [9][5][10][11], the combination between anomaly and signature detection techniques (defined as hybrid intrusion detection system) incurs high detection and low false positive rates. However, the activation of an anomaly detection for low-resource IoT devices could generate a high energy consumption due to the computational cost leading to a rapid decrease of the network lifetime [6][8][12], specifically when this technique is activated all the time. Thereby, our aim in this paper is to make a dilemma between energy consumption and accuracy detection (i.e. high detection and low false positive rates) by activating the anomaly detection only when a new attack pattern (i.e. signature) is expected to occur. This dilemma is achieved, 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 device. With the help of *Nash Equilibriumi,* we determine

the equilibrium state that allows the IDS agent to activate its anomaly detection technique in order to detect new attack pattern.

This paper is organized as follows: In section II, we put highlight in context with the related work in this area. In Section III, we explain our anomaly detection technique based on game theory. Finally, we conclude our work and give directions for future works.

II. Related Work

IDS provides an effective protection to IoT networks against both external and internal intruders [3], and acts as second wall of defense when cryptography is broken. In recent research works [7][13][14], 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 performances.

In [3][5][9][15], the authors propose a hybrid intrusion detection framework for a heterogonous WSN, where 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 huge number of signatures are forwarded to sensor nodes, specifically when the number of attackers is higher in the network. In [10] both anomaly detection and signature-based detection techniques run at the same sensor node. According to their simulation results, their hybrid intrusion detection system generates a high detection rate with a low false positive rate. However, the 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 leading to a rapid decrease of the network lifetime.

The anomaly detection technique has the ability to detect almost all the attacks that occur in a network. However, a permanent activation (i.e. does not switch to idle time) of this technique for low-resource IoT devices could decrease rapidly their lifetimes. Thereby, in this paper we make a dilemma between constrained energy resources and accuracy detection by activating the anomaly detection only when a new attack's signature will be expected to occur.

III. Game-Theoretic Methodology for Optimal Activation of Anomaly Detection Technique for Low-Resource IoT Devices

Each IoT device activates an IDS agent to monitor its neighbor's devices. According to [16], 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 with a set of rules related to each attack pattern (i.e. signature) stored in the IoT device's database. The anomaly detection technique relies on a learning algorithm to carry out a training, classification and builds a rule related to each new detected attack pattern. Afterward, this rule is stored to be used by the signature detection technique. To save the energy, the anomaly detection technique is activated only when a new attack's signature will be expected to occur by a malicious device. Thereby to assure this dilemma, a security game approach for low-resource IoT devices is proposed.

In this section, first of all, we provide the payoff matrix of the game related to the IDS and attacker. Then, we define a set of strategies and payoffs that could occur and result between players, respectively. Finally, we determine, with the help of *Nash Equilibrium (NE),* 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, $P=\{p_1, p_{2,\dots,} p_n\}$, where each player represents either an IDS agent that runs at each IoT device or an attacker. Each player has a set of strategies. $S_t = \{sign_1, sign_{2,\dots,} sign_m\}$ is the probability that an IDS agent has detected m signatures at time t; and $S'_{t'} = \{ sign'_1, sign'_{2,\dots,} sign'_{m'} \}$ is the probability that the attacker launches m' signatures during a period of time t'.

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 given by equations (5) and (6), respectively. Based on this historical observation, the IDS can locally has knowledge of the frequencies of a signatures' occurrence; and with the help of *NE* it predicts when anomaly detection should be activated for rule building. The *NE* aims to make a dilemma between accuracy detection and energy consumption. Moreover, IDS agents located in the same neighborhood cooperate together in order to achieve the greatest 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 on the accuracy prediction.

$$Payoff1_{IDS} = \sum_{i=1}^{s} \frac{(Rep_{positive_i} - Cost_{IDS})}{s} \quad (1)$$

$$Payoff1_{attacker} = \sum_{i=1}^{s} \frac{-(Rep_{positive_i} + Cost_{attacker})}{s} \quad (2)$$

$$Payoff2_{IDS} = \sum_{i=1}^{k} \frac{-(Rep_{negative_i} + Cost_{IDS})}{k} \quad (3)$$

$$Payoff2_{attacker} = \sum_{i=1}^{k} \frac{Rep_{negative_i}}{k} \quad (4)$$

$$f_t = Payoff1_{IDS} + Payoff2_{IDS} \quad (5)$$

$$f'_{t\prime} = Payoff1_{attacker} + Payoff2_{attacker} \quad (6)$$

Here, $Rep_{positive}$ and $Rep_{negative}$ are respectively the positive and negative reputations, which are initialized at the beginning to zero and their values increase or decrease depending upon the actions done by the IDS and attacker, *s* is the number of correct signatures detection and *k* is the number of failure signatures detection, $Cost_{attacker}$ and $Cost_{IDS}$ 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 agent. It's noted that, $Payoff1_{IDS}$, $Payoff2_{IDS}$, $Payoff1_{attacker}$ and $Payoff2_{attacker}$ vary between 0 and 1.

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

TABLE I. PAYOFF MATRIX OF ANOMALY DETECTION GAME

Attacker	IDS			
	S_t	S_{t+1}	.....	S_{t+n}
$S'_t{}'$	$(f'_{t\prime}, f_t)$	$(f'_{t'}, f_{t+1})$	$(f'_{t\prime}, \ldots)$	(f'_t, f_{t+n})
$S'_{t\prime+1}$	$(f'_{t'+1}, f_t)$	$(f'_{t\prime+1}, f_{t+1})$	$(f'_{t'+1}, \ldots)$	$(f'_{t'+1}, f_{t+n})$
.....	$(\ldots, f_t)$	$(\ldots, f_{t+1})$	$(\ldots, \ldots)$	$(\ldots, f_{t+n})$
$S'_{t\prime+n}$	$(f'_{t\prime+n}, f_t)$	$(f'_{t\prime+n}, f_{t+1})$	$(f'_{t'+n}, \ldots)$	$(f'_{t'+n}, f_{t+n})$

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.

1) Static game between IDS and attacker

In a static game, once a player decides his/her strategy, he/she does not have a second chance to change it [17]. 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).

Theorem 1

Let $J(\rho^1, \rho^2)$ denotes the attacker and IDS's gains, where $\rho^1 \in \{S_t, S_{t+1}, \ldots, S_{t+n}\}$ and , $\rho^2 \in \{S'_{t\prime}, S'_{t\prime+1}, \cdots, S'_{t\prime+n}\}$, so that $J(S_{t+n}, S'_{t\prime+n}) = (f_{t+n}, f'_{t\prime+n})$.

A pair of strategies ($\rho^{1^*}$and ρ^{2^*}) is a *NE* point if the following inequality [18] is satisfied:

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

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

Proof 1

To find a *NE* point of the game, we calculate the average payoff of the game [18], which is expressed as:

$$J(S_{t+i}, S'_{t'+i}) = \sum_{i=0}^{n} S_{t+i} * S'_{t\prime+i} * (f'_{t'+i}, f_{t+i}) \quad (8)$$

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

$$\min_{S'_{t\prime+i}} \max_{S_{t+i}} J(S_{t+i}, S'_{t'+i}), \text{ where } i \geq 0$$

The *NE* of a mixed strategy is comprised of the strategies for both players, in the form of $(\rho^{1^*}, \rho^{2^*}) = (S_{t+i}{}^*, S'_{t'+i}{}^*)$, which satisfies the inequality (7). Hence, the mixed-strategy equilibrium is uniquely which is given by:

$$NE = \min_{S'_{t\prime+i}} \max_{S_{t+i}} J(S_{t+i}, S'_{t'+i}), \text{ where } i \geq 0 \quad (9)$$

The attacker will generate a new signature when he/she reaches the equilibrium, i.e. $\min_{S'_{t\prime+i}} J(S_{t+i}, S'_{t\prime+i})$, regardless the action taken by the IDS. Therefore, to assure a dilemma between accuracy detection and low energy consumption, the IDS activates its anomaly detection technique only when the equilibrium is reached, which is defined as $\max_{S_{t+i}} J(S_{t+i}, S'_{t'+i})$.

2) Dynamic game between IDS and attacker

In the *static game* model discussed above, no player has the chance to modify his/her strategy [17]. However, the *dynamic game* allows the IDS and attacker to adjust their strategies according to the observation 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 his (her) time serial payoffs over the entire game, i.e. $\sum_{t=1}^{h} J(\rho^1{}_t, \rho^2{}_t)$.

Theorem 2

The *NE* solution of the dynamic game satisfies recursively the following set of *h* pairs of inequalities for all $\rho^i{}_t$ with i =1, 2 and t=1,…, h:

$$\begin{cases} J(\rho^1_1,\dots,\rho^1_{h-1},\rho^{1*}_h;\ \rho^2_1,\dots,\rho^2_{h-1},\rho^2_h) \le \\ J(\rho^1_1,\dots,\rho^1_{h-1},\rho^{1*}_h;\ \rho^2_1,\dots,\rho^2_{h-1},\rho^{2*}_h) \\ \le J(\rho^1_1,\dots,\rho^1_{h-1},\rho^1_h;\ \rho^2_1,\dots,\rho^2_{h-1},\rho^{2*}_h) \\ J(\rho^1_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h;\ \rho^2_1,\dots,\rho^2_{h-1},\rho^{2*}_h) \le \\ J(\rho^1_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h;\ \rho^2_1,\dots,\rho^2{}_{*h-1},\rho^{2*}_h) \\ \le J(\rho^1_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h;\ \rho^{2*}_1,\dots,\rho^{2*}_{h-1},\rho^{2*}_h) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ J(\rho^{1*}_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h;\ \rho^2_1,\dots,\rho^{2*}_{h-1},\rho^{2*}_h) \le \\ J(\rho^{1*}_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h;\ \rho^{2*}_1,\dots,\rho^2{}_{*h-1},\rho^{2*}_h) \\ \le J(\rho^{1*}_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h;\ \rho^{2*}_1,\dots,\rho^{2*}_{h-1},\rho^{2*}_h) \end{cases} \quad (10)$$

Proof 2

The function of the value of outcomes in the whole game, $J(\rho^1_1,\dots,\rho^1_{h-1},\rho^1_h;\ \rho^2_1,\dots,\rho^2_{h-1},\rho^2_h)$ is independently addictive as proved in [18], i.e. the value of the dynamic game is added to the value of every single-*static-game* together for h time steps. It can be described as:

$$J(\rho^1_1,\dots,\rho^1_{h-1},\rho^1_h;\ \rho^2_1,\dots,\rho^2_{h-1},\rho^2_h) = J(\rho^1_1,\rho^2_1)+\cdots \\ +J(\rho^1_{h-1},\rho^2_{h-1})+J(\rho^1_h,\rho^2_h)$$

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

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

$$=$$

$$\begin{aligned} &J(\rho^1_1,\rho^2_1)+\cdots \\ &+J(\rho^1_{h-1},\rho^2_{h-1})+J(\rho^{1*}_h,\rho^2_h) \\ &\le J(\rho^1_1,\rho^2_1)+\cdots \\ &+J(\rho^1_{h-1},\rho^2_{h-1})+J(\rho^{1*}_h,\rho^{2*}_h) \\ &\le J(\rho^1_1,\rho^2_1)+\cdots \\ &+J(\rho^1_{h-1},\rho^2_{h-1})+J(\rho^1_h,\rho^{2*}_h) \end{aligned} \quad (12)$$

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

$$\begin{aligned} &J(\rho^{1*}_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h\ ;\ \rho^{2*}_1,\dots,\rho^{2*}_{h-1},\rho^2_h) \\ &\le J(\rho^{1*}_1,\dots,\rho^{1*}_{h-1},\rho^{1*}_h\ ;\ \rho^{2*}_1,\dots,\rho^{2*}_{h-1},\rho^{2*}_h) \\ &\le J(\rho^{1*}_1,\dots,\rho^{1*}_{h-1},\rho^1_h\ ;\ \rho^{2*}_1,\dots,\rho^{2*}_{h-1},\rho^{2*}_h) \end{aligned} \quad (13)$$

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

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

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.

IV. Performance Evaluation

Our approach was implemented in wireless sensor networks, well-known low-resource IoT devices. In the simulation, we use a TOSSIM simulator [19], a simulator of TinyOS sensor nodes.

As explained in the introduction, the hybrid intrusion detection system aims to combine between a signature-based detection and anomaly-detection techniques to get high detection and low false positive rates. In this section, we compare our lightweight hybrid intrusion detection system with current hybrid intrusion detection techniques [5][9][15]. In the latter and as explained in the related work, the anomaly detection technique runs on each sensor node and is activated at all 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) and energy consumption. These metrics are defined as follows:

- *Detection Rate (DR):* defined as the ratio between the number of correctly detected attackers and the total number of attackers,
- *False Positive Rate (FPR):* defined as the ratio between the number of normal sensor nodes incorrectly classified as attacker and the total number of normal sensor nodes.

These first two metrics allow us to evaluate the *accuracy detection (AD)***,** which is equal to (DR-FPR).

- *Energy Consumption (EC):* defined as the energy consumed by all sensors and computed as follows [6]:

$$E_{total} = \frac{\sum_{i=1}^{N} E_{node_i}}{N} \quad (15)$$

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

A. Simulation setup

The sensors are randomly deployed in a square area of (300×300) m^2. We vary the number of attackers from 10% to 40% of overall nodes. In the simulation, the attacker carries out the most dangerous attack, which is a Denial of Service (DoS) attack, where he/she aims to exhaust the network resources or disrupt its proper operation. The anomaly detection technique used by the IDS agents is a Back Propagation Network (BPN), which is the most typical and the most general model to use in a neural network [20]. The main simulation parameters are summarized in Table II. These parameters were chosen to be as most realistic as possible.

TABLE II. SIMULATION PARAMETERS

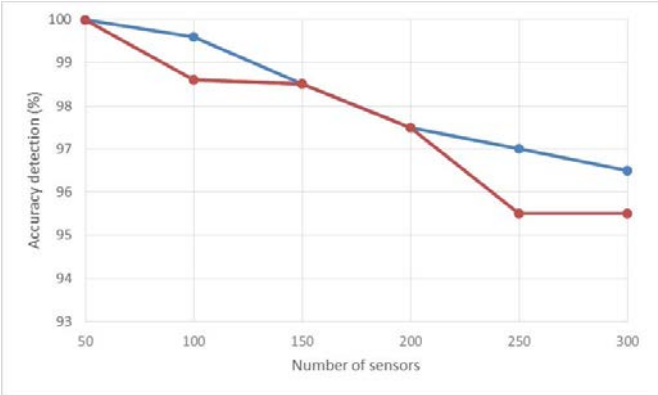
Simulation time	900 seconds
Simulation area	300*300 m^2
Number of sensors	From 50 to 300
Number of attackers	From 10 % to 40 % of overall nodes
Radio model	Lossy radio model
Radio range	15 meter
Sensor initial energy	9 Joule
Anomaly detection	BPN

B. Results analysis

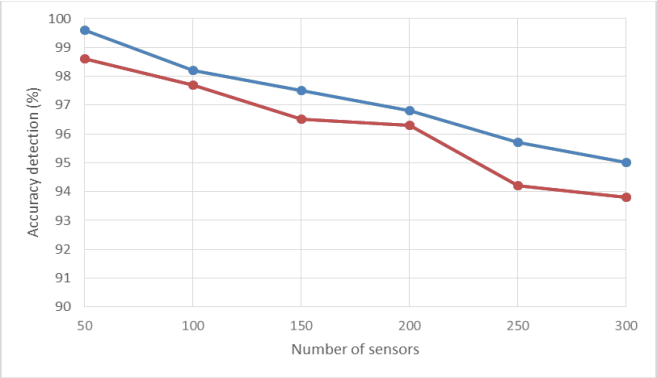
The main results are summerized bellow. In the simulation, we vary the number of sensors and attackers from 50 to 300 and from 10 % to 40 % of overall nodes, respectively. Here, we compute the accuracy detection and enenrgy consumption for both lightweight hybrid detection system and current hybrid detection systems [5][9][15], afterward we compare their performances. The accuracy detection and energy consumption metrics are computed for each hybrid detections system [5][9][15], and the average values of these metrics are used to be comapred with a lightweight hybrid detection system. It's noted that, we compute the average values because the accuracy detection and energy consumption for each system [5][9][15] are almost the same.

1) Accuracy detection

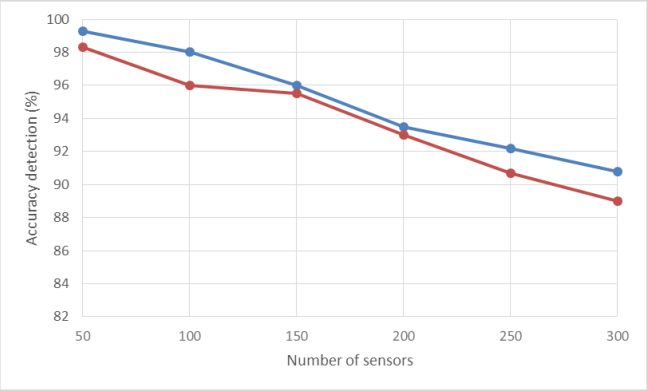
According to Fig 1 (a), (b) and (c), we show that when the number of sensor nodes and attackers increase, the accuracy detection of both hybrid detection systems exceeds 90%. Furhemore, we found out that the accuracy detection of our lightweight detection system is close to the current hybrid detection systems. This is achieved even in a scaling mode, i.e. when the number of sensors and attackers increase. The accuracy of attack detection that our approach exhibits is attributed to the game theory concept since with the help of *Nash equilibrium,* we can predict 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.



(a)



(b)



(c)

Fig1. Accuracy detection with a number of attackers equals to (a) 10% , (b) 30% and (c) 40% of overall nodes.

2) Energy consumption

A main constrained of a low resource IoT device is the energy consumption since when a heavy detection technique is embedded in such device, it decreases rapidly its lifetime. Thereby, energy is a very important point in the design and implementation of IoT applications. As shwon in Fig.2, we fix the number of attackers as 40% of overall nodes, afterward we vary the number of sensors and compute the energy consumption. It's 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 [5][9][15] since a high-energy consumption is generated specifically when the number of sensors increase. This spectacular result is attributed to the following reasons: (*i*) with a help of *Nash equilibrium,* the lightweight detection technique activates an anomaly detection only if needed leading to a decrease on a computation overhead generated by the NN learning algorithm. Therefore a low energy is required to build rules related to attackers' new signatures. (*ii*) In the current hybrid detection systems a huge 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 of communication overhead.

Fig 2. Energy consumption

V. Conclusion and Future Work

In this paper, we are dealing with security for low resources IoT-devices. We propose a lightweight anomaly detection technique based on game theory concept. With the help of *Nash equilibrium,* we predict the equilibrium state that allows the IDS agent to activate its anomaly detection technique to detect new attack's signature. We have analyzed the performance and demonstrated the viability of our proposed approach under WSN, using TOSSIM simulator. According to the simulation results, we prove that our lightweight anomaly detection approach requires a low energy consumption to achieve a high security level, i.e. high detection 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 activated at each node in a permanent fashion (i.e. does not switch to idle time). Our future direction is to embed our lightweight anomaly detection technique in large-scale IoT devices and will deal the accuracy detection, energy consumption and network delay.

Acknowledgement

This work has been funded by the European project ITEA FUSE-IT [21].

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] S. Raza, L. Wallgren, T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", *Ad Hoc Networks,* Vol 11, Issue8, 2013, pp. *2661-2674.*

[4] 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.

[5] 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, 2011, pp. 15234–15243.

[6] 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.

[7] 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.

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

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

[10] 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.

[11] 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.

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

[13] 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.

[14] S. Pan, T. Morris, and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems", *IEEE Transactions on Smart Grid*, 2015.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

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

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