Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks

Hichem Sedjelmaci, Sidi Mohammed Senouci

Efficient and Lightweight Intrusion Detection Based on Nodes' Behaviors in Wireless Sensor Networks

Hichem Sedjelmaci and Sidi Mohammed Senouci
University of Bourgogne, DRIVE Lab
49 Rue Mademoiselle Bourgeois, 58000, Nevers, France
{ Sid-Ahmed-Hichem.Sedjelmaci , Sidi-Mohammed.Senouci}@u-bourgogne.fr

***Abstract*— In this paper, we design and implement an Efficient and Lightweight Intrusion Detection (ELID) framework based on a new detection technique. This later relies on the fact that nodes that are located within the same cluster have almost a similar behavior. This fact is demonstrated by both simulation and experimental studies. According to the obtained results, ELID exhibits a high detection rate, low false positive rate, low energy consumption and requires less time to detect the following attacks: Selective forwarding, Black hole, Sinkhole, Wormhole and Denial of Service (DoS).**

Keywords— Wireless Sensor Network; Intrusion detection; Nodes' behaviors; Lightweight; Efficiency

I. INTRODUCTION

Wireless sensor networks (WSNs) are applied in both civilian and military application. These networks represent an attractive target for the attackers due to their characteristics such as restriction on energy and their deployment in a hostile environment. Thereby, an effective security mechanism against different kinds of threats is primordial for WSNs. Cryptographic technique has been used to ensure the authentication and data integrity. It is very useful to prevent an external attacker to penetrate a network. However, such technique has not the ability to detect the insider attack. On other side, Intrusion Detection System (IDS) is very useful to protect the network against internal and external attacks. Detection techniques applied by the IDS agent can be classified into three main approaches [1][2][3]: (i) Misuse detection relying on comparing the behavior of a node against a set of predefined attacks. This technique detects only known attacks, and new attacks require new rules to be constructed [4]. (ii) The anomaly detection builds a model of normal profiles and attempts to track deviations from normal behavior that may be subject to a possible intrusions. Such technique has the ability to detect novel attacks. However, the main disadvantage of such technique is the high false positive rate that can be generated [4]. (iii) Specification-based detection that aims to combine the advantages of anomaly and misuse detections [2]. However the weakness of this detection technique is the necessity of a continuous rules' update to build the normal behavior.

In this research work, we design and implement a new detection technique that fixes all the issues occurred by the previous ones. The concept of detection relies on the fact that nodes that are located within the same cluster should have almost similar behaviors. A node is considered as malicious if its behavior significantly differs from the behaviors of its neighbors. This statement is demonstrated in our simulation and experiment when the maximum size of a cluster is two hops. Based on this result, we developed an Efficient and Lightweight Intrusion Detection (ELID) framework that relies on this concept to detect the most dangerous attacks that attempts to damage the network. To the best of our knowledge, none of the existing detection frameworks have proposed a detection policy based on the nodes' behaviors within the same cluster.

The remainder of this paper is organized as follows: In Section 2, we give some related work about intrusion detection in wireless networks based on neighbors' behaviors. In Section 3, we highlight some simulation and experiment results corresponding to the nodes' behaviors distribution, afterward we explain our detection policies based on nodes' behaviors to identify the most dangerous attacks. Section 4 gives more details about ELID framework and Section 5 provides simulation and experimental results. Simulations were carried out using TOSSIM simulator [5] and experiments using a platform composed of a set of MICAZ motes. Finally, we conclude the paper and give some future perspectives that we envisage to carry out in Section 6.

II. RELATED WORK

Intrusion detection technique is most reliable technique since it has the ability to detect internal and external attacks with a high accuracy, unlike cryptography technique which assures only the not penetration of an external attack to the network. As stated above, there are three detection approaches applied by the IDS agent: misuse detection, anomaly detection, and specification-based detection. Each one of them has its own advantages and weaknesses. Recently, a new efficient and lightweight detection approach proposed by the authors in [6][7] outperforms the previous ones in terms of attacks detection and energy consumption. This approach is based on neighbors behavior to detect the malicious node and explores the fact that nodes in close proximity tend to have a similar behaviors.

In [6], the authors proposes an intrusion detection schema for wireless sensor networks in order to detect selective forwarding, jamming and hello flood attacks. In their schema, the IDS agent collects and computes a set of features from their neighbors such as received signal strength, packet dropping rate, packet sending rate and packet receiving rate. These features are then transmitted to the detection module that uses a set of rules, i.e. the node with the highest signal strength is suspected to be hello flood attack, the node with the number of packet sending or packet dropping is very important compared

to its neighbors is defined as jamming or selective forwarding, respectively. According to simulation results, all attacks cited above are detected with a high accuracy. However, the major weakness of their schema is that the energy consumption of their approach is not evaluated.

In [7], the authors aim to group sensors in the same cluster according to the sensed data, i.e. all sensors that have the same sensed data are grouped in the same cluster. In addition, they propose a detection policy based on the fact that nodes located close to each other have almost the same value of monitoring attributes such as sensed data, packet sending rate, packet dropping rate, packet mismatch rate, packet receiving rate and received signal strength. According to experimental results, the authors claim that by using the sensed data as main attribute the attack that aim to alter the information is detected with a high accuracy. However, the other attributes are unused which leads to make the network vulnerable to other attacks such as black hole.

Our proposed detection framework is based on node's behaviors to detect a set of dangerous attacks against WSN. In the following, we describe a new detection approach based on the normal distribution concept and detection rules related to each attack. Afterward, we provide a design of ELID framework and its working.

III. Intrusion Detection Technique Based on Nodes' Behaviors

In this section, we demonstrate according to our simulation and experiments results that when the number of hops at each cluster does not exceed two hops, nodes that are located within a same cluster their behaviors (Received Signal Strength Intensity - RSSI, Packets Forwarding Ratio - PFR and Packets Sending Ratio - PSR) follow a normal distribution. According to this interesting result, we propose new detection policies to detect the most dangerous routing attacks, which are: Selective forwarding, Black hole, Sinkhole, Wormhole and Denial of Service (DoS).

We organize this section into two subsections: In the first one, we highlight some simulation and experiment results corresponding to the nodes' behaviors distribution. We note that, simulations are carried out under TOSSIM simulator [5] and real experiments are performed using 10 MICAZ sensors. In the second subsection, we describe the characteristics of some routing attacks with explaining a set of detection policies based on normal distribution related to each one of them.

A. Node's behaviors based on normal distribution

In a normal distribution concept data are correctly distributed if they vary within an interval [mean- 3*STD, mean+ 3*STD] [8], where STD is a standard deviation. In both simulation and experimental studies, we varied the number of hops at each cluster from 1 to n hops and study the variation of the following behaviors: RSSI, PFR and PSR. We note that, to get accurate results no attacks occurred in the network. According to our simulation and experimental results, we found that when the number of hops is equal at most two hops RSSI, PFR and PSR related to each node located within the same cluster follow a normal distribution i.e. each behavior of normal node lies within three standard deviations of the mean as illustrated in Fig. 1.

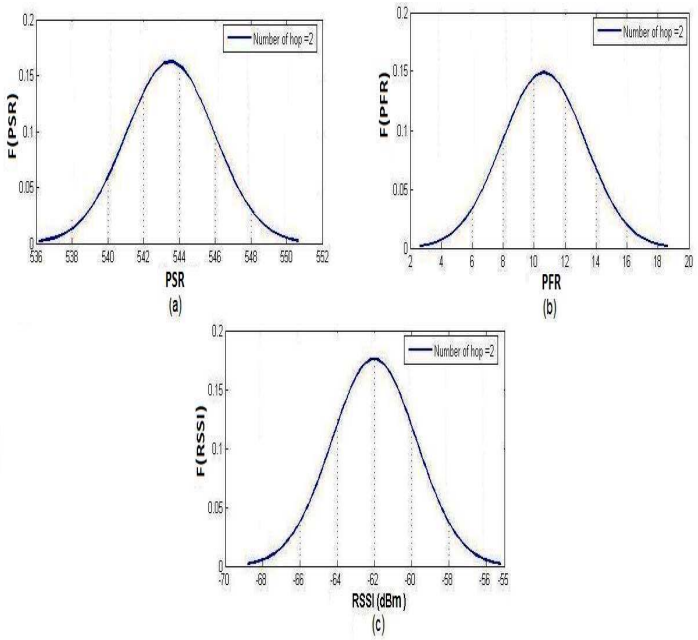

Fig. 1. The normal distribution of the behaviors: simulations and experiments results under two-hops cluster configuration

According to these results, we provide new detection policies to identify malicious nodes with a high accuracy. Our detection policies explore the fact that the nodes that are located within the same cluster, their behaviors (cited above) should follow a normal distribution. Thereby, to determine a malicious node that has a behavior different compared to other nodes located within the same cluster, we compute the Euclidean distance [6].

The IDS agent monitors the behaviors of its neighbor's nodes by computing the RSSI, PFR and PSR related to each one of them. Afterward, to determine if a node s_i exhibits an attack or not, the IDS computes the Euclidean distance related to each behavior from $f_m(s_i)$ to the center of the set $f_m(s_i)$, …, $f_m(s_n)$, which is defined as $ED(f_m(s_i))$ (see equation 2). Here i= {1,…n}, where n is the number of nodes that are monitored by the IDS, m is a selected behavior and the center of this set is determined by computing the arithmetic mean (AM) of its elements. In addition, we note that the monitoring behaviors of node s_i observed by IDS are modeled by the following function: $f(s_i) = f_1(s_i), f_2(s_i), f_3(s_i)$, where $f_1(s_i) = RSSI$, $f_2(s_i) = PFR$ and $f_m(s_i) = PSR$, and m={1,…3}. In case when $ED(f_m(s_i))$ is greater than a certain threshold δ, the node s_i is considered as an attacker. We note that, each attack has it corresponding threshold δ, in subsection V.A we carry out a set of simulation to determine an optimal threshold related to each attack.

$$AM(f_m(s)) = \sum_{i=1}^{n} \frac{f_m(s_i)}{n} \quad (1)$$

$$ED(f_m(s_i)) = f_m(s_i) - AM(f_m(s)) \quad (2)$$

B. Routing attacks and their corresponding detection policies

In our research work, we attempt to detect and prevent the most dangerous routing attacks that have a high severity damage in the network such as: Selective forwarding, Black hole, Sinkhole, Wormhole and Denial of Service (DoS) attacks.

To detect these attacks, we apply detection policies based on the concept that within a cluster, all nodes that are located within the same cluster should have almost the same behaviors.

Selective forwarding and Black hole attacks. The Selective forwarding is performed by an attacker that refuses to forward certain packets and simply drops them [*6*]. However, the Black hole drops all the received messages. The node that carries out one of these attacks, its Packets Forwarding Ratio (PFR) will be lower compared to a legitimate node. Therefore, we can conclude that all nodes that are located within the same cluster their PFR must follow a normal distribution. The rule of Selective forwarding and Black hole attacks detection is illustrated in Fig. 2 (a).

Sinkhole and Wormhole attacks. The common feature between the two attacks is that the attacker will use a high power transmission to convince a legitimate node that is at one hop away from the sink or cluster-head [9][4]. As a result, the Received Signal Strength Intensity (RSSI) of each node located within the same cluster should follow a normal distribution. The rule of Sinkhole and Wormhole attacks detection is illustrated in Fig. 2 (b).

Denial of Service (DoS) attack. The intruder aims to exhaust an energy resource of a legitimate node by sending a considerable number of unwanted traffic [10]. Therefore, in case when no one of DoS attacks are occurred in the network, the Packets Sending Ratio (PSR) of each node located within the same cluster follows a normal distribution. The rule of DoS attack detection is illustrated in Fig. 2 (c).

```
// Rules for Selective forwarding and Black hole attacks
if PFRs of nodes s_i don't follow a normal distribution within a cluster K
  if ED(PFR(s_i)) > δ_sf
    // node s_i performs a Selective forwarding attack
    Send Distress message(node_id, attack type);
  else
  if ED(PFR(s_i)) > δ_bh
  // node s_i performs a Black hole attack
  Send Distress message(node_id, attack type);
                    (a)
// Rules for Sinkhole and Wormhole attacks
if RSSIs of nodes s_i don't follow a normal distribution within a cluster K
  if ED(RSSI(s_i)) > δ_sh
    // node s_i performs a Sink hole attack
    Send Distress message(node_id, attack type);
  else
  if ED(RSSI(s_i)) > δ_wo
  // node s_i performs a Wormhole attack
  Send Distress message(node_id, attack type);
                    (b)
// Rules for Dos
if PSRs of nodes s_i don't follow a normal distribution within a cluster K
  if ED(PSR(s_i)) > δ_dos
    // node s_i performs a Dos attack
    Send Distress message(node_id, attack type);
                    (c)
```

Fig. 2. Detection rules for (a) Selective and blackhole attacks, (b) Sinkhole and Wormholes attacks, and (c) DoS attack

IV. ELID FRAMEWORK AND ITS WORKING

Our aim in this research work is to propose an efficient detection framework that is reliable in terms of attacks detection and lightweight in terms of computation and communication processes i.e. exhibits low energy consumption.

Our detection approach is based on the concept that all nodes that are located within the same cluster should have similar behaviors. The following features defined in the previous sections represent these behaviors: NPD, NPS, RSSI. In our research work, we used a cluster-based topology since it leads to extend the network lifetime compared to a flat topology. In this research, we used HEED protocol [11] for the cluster formation and CH election. In order to satisfy the requirement that within the same cluster all nodes should have the same behaviors, we fix the number of hops at each cluster equal to maximum two hops. We note that, in our application sensors are randomly distributed on a grid-like area and are continuously sensing the environment to send reports to the CH, which aggregates and forwards them to a base station. In this section, we detail the mains components of ELID framework.

A. Intrusion detection and reaction agents

In our schema we propose two kinds of agents for the intrusion detection and decision purpose, which are running at two level: Intrusion Detection Agent (IDA) and Decision Making Agent (DMA). The former applies a behavior-based detection to identify malicious nodes, which is activated at a cluster members level. The later aims to check whether a suspected node detected by IDA is malicious or not and mitigates the number of false positives that occurred when the IDA suspects the normal node as an attacker. This agent is activated at each CH.

1) *Intrusion Detection Agent (IDA).* The activation strategy of IDS agents is an important issue, since increasing the number of agents in the network leads to a high computation and communication overhead and hence a decrease of the network lifetime. Therefore, the proposed strategy should consider nodes' energy constraint. Our solution activates an IDA to monitor each two links in a promiscuous mode as illustrated in Fig. 3. This strategy allows getting an overview on all packets that circulate in the network by a low number of detection agents. In addition, when energy consumption of IDA is important, the process of a new IDA selection is launched as explained below. As a result, this strategy leads to detect all malicious nodes with a low overhead. The IDA is equipped with the following modules as illustrated in Fig. 4.

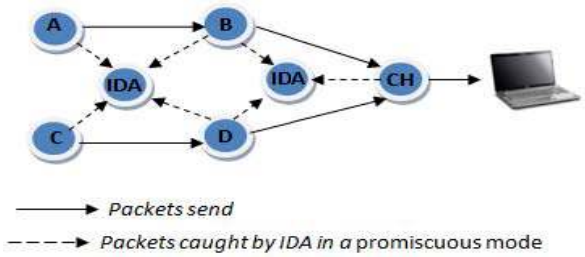

Fig. 3. Activation strategy of IDA

a) Data collection module. Each IDA collects the packets within its radio range, stores the *id* of monitored nodes and computes the following behaviors related to each node: RSSI, PFR and PSR.

b) *Intrusion detecion module*. This module applies the detection policy based on the fact that at each cluster, the following behaviors: RSSI, PFR and PSR should follow the normal distributions (as proved in our simulation and experimental results, see subsection III.A). The IDA monitors the nodes that are located within its radio range by computing the Euclidean distance of their behaviors (see subsection III.B for attacks detection rules). Furthermore, an attacker could attack the cluster-head since it contains a relevant information. In order to avoid this issue, an IDA monitors the behavior of the CH.

c) *Reaction module*. When IDA detects a node as an attacker it forwards a *Distress _ message* to its corresponding CH for further confirmation. This message includes: the id of suspected node and attack type. Furthermore, when a CH exhibits an attack, the IDA broadcasts a *CH_ Distress message* (containing the *id* of suspected CH and attack type). In case when more than half of CH's IDA neighbors claim that a CH is malicious, the process of new CH election is launched, which is based on three parameters: (i) IDA's vote: selection of the nodes that are identified as less malicious by IDAs, (ii) Node proximity: select the nodes that are on the neighborhood of the older CH, and (iii) energy consumption: the node that exhibits a high residual energy is designed as a new CH.

d) *IDA election module*. If the IDA has been detected by DMA (located at CH) as malicious node (see subsection IV.A.2) or has consumed more than 60% of the overall energy, it will be designated as ordinary node and a new IDA will be elected. We note that, this maximum energy, i.e. 60%, is determined by carrying out several simulation, which is an optimal one as it satisfy our requirement, i.e. high detection rate and an increase on the network lifetime. The election of new IDA relies on two mains parameters: (i) IDA's node proximity: the nodes that are located in the same radio range of the older IDA are selected, (ii) energy consumption: the node that exhibits a high residual energy among these selected nodes is elected. The election of a new IDA must assure the condition that at each two links, there is one agent that monitors the behaviors of its neighbors.

2) Decision Making Agent (DMA). At each CH the DMA is activated. This agent is equipped with two main modules as illustrated in Fig. 4 and detailed in the following

*a) Data collection module***.** This module receives a *Distress_message* from its IDA members and forwards it to a Decision-making module in order to take a final decision, i.e. whether the malicious node claimed by the IDA agent is an attacker or not and also check the reliability of message provided by this agent. Such message contains the *id* of suspected node and attack type.

b) Decision-making module. When a CH receives a *Distress_message,* it stores the *id* of the suspected node in a blacklist database. In case when more than half of IDAs within a same cluster claim that a suspected node is malicious, it will be ejected from the cluster. In other hand, the IDAs that provide a false detection i.e. claim that a normal node is malicious, they are stored in a black list and a malicious counter related to each one of them is increased. When this counter exceeds the threshold T_{IDA}, defined as a number of IDAs per cluster over two, the IDA will be designed as ordinary node, in other words not being able to play the detection agent role and a new one will be elected as explained above.

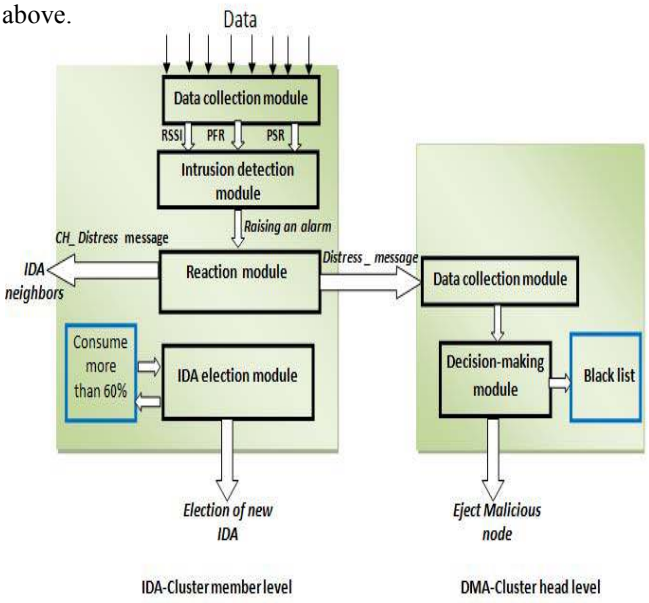

Fig. 4. Architecture of detection agents

V. SIMULATION AND EXPERIMENTAL RESULTS

In our study, we use TOSSIM simulator [10], a simulator of TINYOS sensor nodes to evaluate the performances of ELID framework. In the simulation phase, we study the variation of the thresholds related to the Euclidean distance and their impact on the detection and false positives rates. All simulation parameters are summarized in Table 1.

TABLE1. SIMULATION PARAMETERS

Simulation time	680 seconds
Simulation area	80*80m^2
Number of nodes	200
Number of clusters	8
Radio model	Lossy radio model
Routing	HEED protocol
Radio range	15m
Sensor initial energy	5 Joules

We then embed our detection framework into real MICAZ sensor nodes and study the required time of an intrusion detection agents to detect the attacks (defined as Average Efficiency), detection and false positives rates. In addition, we evaluate the energy consumed during the execution of our application. All these metrics are defined hereafter:

Detection Rate (DR): Measures the rate of correctly identified attacks over the total number of attacks,

False Positives Rate (FPR): Computed as the ratio between the number of normal node that are incorrectly classified as an attacker and the total number of normal node,

Energy consumed (EC): Defined as the total amount of energy consumed by all nodes over the total number of nodes in the networks,

Efficiency (E): Determines the required time for an intrusion detection agent to detect the occurrence of one attacker [12]. It is computed as follow:

$$\frac{ED - ET}{Sampling frequency}$$

Where ED is the detection time of the attacker and ET is the start time of an attack. To determine the required time for an intrusion detection agents to detect all attacks in the network, we compute the Average Efficiency (AE), which is defined as follows:

$$AE = \frac{\sum_{i=1}^{n} E_i}{n}$$

Where n is the number of attackers.

A. Simulation results

In the simulation phase, we insert the attacks cited above separately and vary the number of malicious nodes from 0 to 45% of overall nodes. Afterward, we varied the Euclidean threshold δ related to each attack detection and compute the detection and false positive rates. Therefore, the optimal threshold corresponds to a high detection and low false positive rates when the attacks occur. We note that to identify these optimal thresholds, we carry out a set of 50 simulations in order to determine the accuracy thresholds that allow us to detect these attacks with a high detection and low false positives rates. These thresholds are specific for configuration where the number of hops in a cluster is not more than two. Table 2 summarizes all the optimal Euclidean thresholds of RSSI, PFR and PSR.

TABLE2. THE OPTIMAL EUCLIDEAN THRESHOLDS

Thresholds	Definition	Values
δ_{sf}	Euclidian distance's threshold of PFR Under Selective forwarding	9.2
δ_{bh}	Euclidean distance's threshold of PFR under Black hole	52.4
δ_{sh}	Euclidean distance's threshold of RSSI under Sinkhole	9 dBm
δ_{hf}	Euclidean distance's threshold of RSSI under Wormhole	7.25dBm
δ_{dos}	Euclidean distance's threshold of PSR under DoS	35

B. Experimental Results

When the optimal thresholds related to the Euclidean distance of each behavior are founded, we use these thresholds in the detection policies (see Fig. 2) and embed our detection framework in a testbed composed of 10 Micaz. In this section, we study detection rate, false positives rate, energy consumption, and the average efficiency. When the clusters are formed, we inject separately different attacks: Selective forwarding, Black hole, Sinkhole, wormholes and DoS. Afterward, we investigate the effect of each attack in the network in isolation by varying the number of attackers from 1 to 3.

Selective forwarding and Black hole attacks. According to Fig. 6, we show that that the detection and false positives rates are equal to 100 % and 0%, respectively and these rates remain constant even when the number of attackers is important. In addition, as shown in Fig. 5 (a), ELID requires less time to detect these attacks. The required time of the detection framework to detect all Selective forwarding is close to 3 seconds. For Black hole attacks, it is equal to 2 seconds.

Sinkhole and Wormholes. When the Sinkhole or Wormhole attacks occur, the average efficiency of ELID is equal and close to 2 seconds, respectively as shown in Fig. 5 (b). Furthermore, the detection of these attacks is achieved with a high accuracy (i.e. Detection Rate=100% and False Positive Rate =0%) as illustrated in Fig. 6.

DoS. As mentioned above, our aim is to detect a specific kind of DoS attack , that attempts to exhaust the resource of a legitimate node by sending a considerable number of unwanted packets. As shown in Fig. 6, when the DoS attack occur, ELID exhibits a high accuracy detection. In addition, the average efficiency under DoS attacks is close to 2 second (see Fig. 5 (a)). As a result, our detection framework has the ability to detect a DoS attack with a high accuracy and a less times.

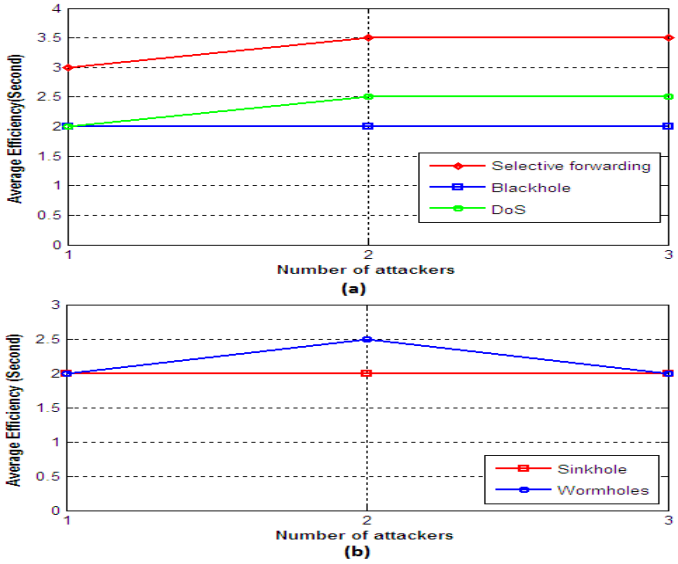

Fig. 5. Experimental detection performances: (a) Average Efficiency under Selective forwarding, Black hole and DoS attacks, (b) Average Efficiency under Sinkhole and Wormhole attacks.

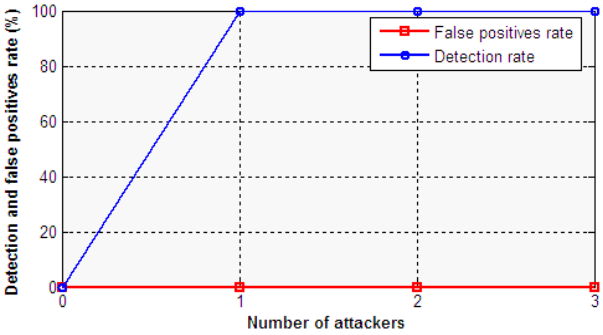

Fig. 6. Experimental detection performances: Detection and False positive rates for each attack

According to these experimental results, we prove the efficiency of our detection framework in terms of attacks detection and required time to identify them. In the following, we evaluate the energy consumption of our detection framework to detect these attacks

Energy consumption. In this section, we study the energy consumption caused by our detection framework and compare it with EIDF framework proposed by the authors in [12] and eHIDS framework proposed by the authors in [2]. In order to measure the energy consumed at each node, we use the approach that uses a shunt resistor [13]. In this approach, two voltages are measured: the first is over a MICAZ, which is constant and equal to 2.7V. The second is over the resistance, which is varying over time. In this section, we compute the energy consumption when each attack occurs separately. Afterward, the average of these energies is computed. As shown in Fig.7, our detection framework exhibits a low energy consumption compared to the frameworks proposed by the authors in [2] and [12]. In addition, we found that, the energy consumed by all nodes remains constant even when the number of nodes increases. These results are achieved since our intrusion detection agents (IDA and DMA) generate a low computation and communication overhead to detect theses attacks.

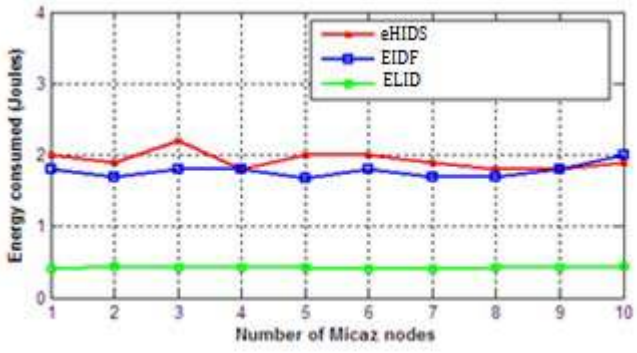

Fig. .7 Energy consumption

V. CONCLUSION

In this paper, we propose an efficient and lightweight approach to detect the attackers based on the nodes' behaviors. In particular, our research shows that the nodes belonging to the same cluster have almost a similar behaviors. Furthermore, we have extended our approach and applied this concept to detect more dangerous attacks against WSNs such as: Selective forwarding, Black hole, Sinkhole, Wormhole and DoS attacks. The process of intrusion detection is carried out at the cluster-members (IDA) and the cluster-head (DMA) to eliminate any security threat that may disrupt the network. These agents collaborate with each other's to detect malicious nodes with a high accuracy. According to our simulation and experiment results, we found that when the optimal thresholds related to the Euclidean distance are selected, ELID framework spends a short time to detect these attacks while achieving a lower false positive rate and full detection rate. These results are achieved with very low energy consumption.

In the near future, our aim is to extending our approach to identify other malicious attacks. In addition, we will carry out simulation and experimental studies within a mobile WSN.

REFERENCES

[1] M. Ketel ," Applying the mobile agent paradigm to distributed intrusion detection in wireless sensor networks", The 40th Southeastern Symposium on System Theory, IEEE, New Orleans, USA, 2008.

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

[3] I. Krontiris, T. Dimitriou, F.C Freiling, "Towards intrusion detection in wireless sensor networks", The 13th European Wireless Conference, Paris, France, 2007.

[4] T.H Hai,E.N Huh, M. Jo, "A lightweight intrusion detection framework for wireless sensor networks", Wireless Communications and Mobile Computing, 10(4), 2010, pp. 559-572.

[5] Simulating tinyOS networks. Available at http:// www.cs.berkeley.edu/ pal/research/tossim.html; 2003.

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

[7] G. Li, J. He, Y. Fu, "A Group-Based Intrusion Detection Scheme in Wireless Sensor Networks", The 3rd International Conference on Grid and Pervasive Computing, IEEE, 2008.

[8] C. Wang, K. Viswanathan, L. Choudur ,V. Talwar, W. Satterfield, K. Schwan, "Statistical techniques for online anomaly detection in data centers", The 12th International Symposium on Integrated Network Management, IEEE, Dublin, Ireland, 2011.

[9] W. R. P. J´unior, T. H. P. Figueiredo, H. C. Wong, A. A. F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks", 18th International Proceedings on Parallel and Distributed Processing Symposium, IEEE, 2004

[10] S. Rajasegarar, C. Leckie, M. Palaniswami. In: Beyah R, McNair J, Corbett C, editors, "Detecting Data Anomalies in Wireless Sensor Networks" Security in Ad-hoc and Sensor Networks, World Scientific Publishing, pp. 231-260, 2009.

[11] O. Younis , S. Fahmy, "HEED: a hybrid energy efficient distributed clustering approach for ad hoc sensor networks", IEEE Transactions on Mobile Computing 3(4)(2004) 366–379.

[12] H. Sedjelmaci, S.M. Senouci, M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks", Security and Communication Networks 2013.

[13] A. Stetsko, M. Stehlik, V. Matyas, "Calibrating and comparing simulators for wireless sensor networks", The 8th International Conference on Mobile Ad hoc and Sensor Systems, IEEE, Valencia, Spain, 2011.