Lightweight Intrusion Detection Scheme for Wireless Sensor Networks

Yassine MALEH, *Member, IAENG,* and Abdellah Ezzati

***Abstract*— Wireless sensor networks are increasingly used in a wide range of potential applications, including security and surveillance, control, actuation and maintenance of complex systems and fine-grain monitoring of indoor and outdoor environments. The nature of wireless sensor networks makes them very vulnerable to attack. The mobile nodes are randomly distributed, there are no physical obstacles for the adversary, therefore, they can be easily captured, and attacks can come from all directions and target any node. Consequently, security of wireless sensor networks (WSN) is the most challenging for this type of network. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. In this paper, we propose a lightweight intrusion detection system for sensor networks. Our intrusion detection model exploits advantage of support vector machine (SVM) and signature model to detect malicious behaviors and provide a global lightweight IDS in cluster based topology. The proposed model can detect and prevent most of routing attacks.**

***Index Terms*— Wireless Sensor Network, Hybrid Intrusion Detection System, Support Vector Machine (SVM), Signatures, False alarm, Detection rate, Energy consumption**

I. Introduction

Wireless Sensor Network (WSN) is a distributed network of sensor nodes, used to monitor and collect data. There are many application areas based on sensor networks, including weather data (temperature, pressure), tele-medicine, emergency situations (fires, catastrophe and other), military operations (location of moving targets, the territorial propagation of chemical weapon) and more others files of applications [1].

The different characteristics of wireless sensor networks (energy limited, low-power computing, use of radio waves, etc...) expose them to many security threats [2]. We can classify attacks in this type of network in two main categories: Active and Passive. In passive attacks, attackers are typically camouflaged, i.e. hidden, and tap the communication lines to collect data. In active attacks, malicious acts are carried out not only against data confidentiality but also against data integrity. Several papers have presented the security attacks in WSN [3][4][5][6][7][8]. To deal with these attacks protection systems exists. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing attacks.

Moreover, intrusion detection techniques must be designed to detect and prevent the execution of the most dangerous attacks. In addition, these techniques must be lightweight to suit the limited resources of WSN. Energy consumption is a very important factor in this type of network. Therefore, many researchers worked on this issue by proposing a network architecture based on clustering approach. This architecture consists of the construction of one or more (cluster) nodes in each of them a cluster head is elected, it is responsible for collecting data sent by the members of his group, aggregation and subsequently transmitting data to the base station. This architecture is designed to minimize the power consumption of the nodes, and consequently the extension of network lifetime.

Hence, the idea that we propose is to integrate intrusion detection mechanisms in this type of topology. Our proposed hybrid model exploits the advantages of anomaly based approach and signature rules to provide a global IDS. The paper is structured as follows. In the next section, we present in related work. Section 3 describes the proposed model and the defense methods against network attacks. In the Section 4, we present mathematical analysis and performance evaluations of our scheme. Finally, the paper ends with a conclusion and future works.

II. Related Work

There are a few works that aim to combine between anomaly-based model and detection technique based on signatures (hybrid model) to benefit from the advantages of both detection policies and try to detect a significant number of attacks. We find in the literature some hybrid intrusion detection systems. In this section, we analyze and discus some proposed IDSs for WSN.

Besson et al. [9] apply two collaborative approaches (data sharing and making collaborative decisions). In each cluster the IDSs are implemented in a subset of nodes, these agents are designed to propagate the intrusion data between them. When the IDS agent triggers an alarm regarding the presence of an attack on the network, a voting mechanism is performed between the IDS nodes in the same cluster and the cluster-head, who exchange his vote with other cluster heads in the network. The advantage of this scheme is the high level of accuracy in intrusion detection by the application of collaborative approaches. However, this approach generates high communication load due to the

Manuscript received January 29, 2015; revised May 24, 2015. This work was supported in part by LAVETE Laboratory at the Faculty of Science and Technology in Settat, Morocco.

Yassine Maleh is IT Project Manager at the National Port Agency in Morocco. He is currently towards his PhD degree in Networks Security at Hassan 1st University Settat, Morocco. (Phone: 212-608-867568; e-mail: y.maleh@uhp.ac.ma).

Prof. Abdellah Ezzati is an associate professor at Hassan 1st University in Morocco and he is the Head of Bachelor of Computer Science at the Faculty of Sciences and Technology, Hassan 1st University, Settat, Morocco (e-mail: abdezzati@gmail.com).

large number of packets sent and received by each cooperating node.

Abduvaliyev et al. [10] proposed a hybrid intrusion detection system based on anomaly and misuse detection techniques in a cluster wireless sensor topology. The results showed that the proposed scheme allows a high detection rate with low level of energy consumption. However, this scheme does not detect most network attacks.

Soumya et al. [11] proposed an intrusion detection mechanism based on ant colonies system. Their basic idea is to identify the affected path of intrusion in the sensor network by investigating the pheromone concentration. However, they do not specify the detail solution on the routing attacks.

Wu et al. [12] proposed a secure aggregation tree to detect and prevent cheating in WSNs, in which the detection of cheating is based on topological constraints in a constructed aggregation tree.

Krontiris et al.[13] Introduced a lightweight intrusion detections scheme for detecting selective forwarding and black hole attacks in WSN. In this scheme, the nodes monitor their neighbors and collaborate to decide if there is a possible malicious node or an intrusion has taken place.

In recent work [14], Sedjelmaci et al. implemented a lightweight Framework for securing wireless sensor networks, combines the advantages of both cryptography and IDS technology to detect the most dangerous network attacks, and provide a trust environment based on clusters. The results show that the scheme performs well in terms of detection rate, but generates high overhead and energy consumption.

To conclude, there is a need to develop a global and lightweight intrusion detection scheme that emphasizes on the strengths of existing models and overcome the limitations. Our contribution in this paper is to propose a novel IDS model that addresses the issue of detection generality by incorporating anomaly based technique and specifications based model in a cluster wireless sensor topology.

III. COMPARATIVE ANALYSIS OF SOME POPULAR IDSS

Due to architectural differences between wired and wireless networks, their IDSs cannot be used interchangeably. There are specific techniques for WSN. Table 1 presents a comparative analysis of some popular intrusion detection schemes in literature. In the next section, the proposed IDS model is introduced.

TABLE I. COMPARISON OF SOME POPULAR IDS MODELS FOR WSN

IDS Proposed	Network architecture	Detection technique	Energy consumption	Strenght and Features
Da Silva *et al.*[15]	Distributed	Rule based approach	Low	Scalable, robust and fast intrusion detection.
Roman *et al. [16]*	Distributed	Spontaneous watchdogs	Low	Relies on the broadcast nature of sensor communications and takes advantage of the high density of sensors being deployed in the field.
Strikos [17]	Hierarchical	Rule based	Low	Combined already existing approaches, in order to achieve a more complete solution. Can detect both existing and new attacks.
Krontiris *et al. [13]*	Distributed and Cooperative	Specification based	Medium	Proposed solution works only when there is one attacker.
Doumit and Agrawal [18]	Hierarchical	Game theory along with Markov decision process	High	Consider resource parameters (energy and reliability)
Agah *et al. [19] [20]*	Hierarchical	Statistical anomaly based approach (parametric), hidden Markov model	Medium	Only one of the clusters of the network is monitored at a time. This leaves the rest of the network un-protected.
Rajasegarar *et al.* [21]	Distributed	Anomaly based approach, support vector machine	High	Minimizes communication overhead while performing in network anomaly detection.
Tran Hoang Hai et al [22]	Distributed	Hybrid model	Low	Proposed lightweight techniques that can prevent most of routing attacks on sensor networks.

IV. Our Proposed Model

As shown in Fig. 1, the example of hierarchical WSNs consists of four clusters and a base station .We propose a cluster-based architecture that divides the array of sensors into a plurality of groups, each of them includes a cluster-head (CH). In this architecture, every node belongs to only one of the clusters which are distributed geographically across the whole network. Cluster head is used to reduce energy consumption, amount of data in the entire network and to increase network lifetime. This is achieved by designating one known as the leader of the group (cluster-head) that forwards packets (data aggregated) to the base station (BS) instead of all nodes send their collected data to a remote location (base station). We suppose that the WSN are configured and organized following cluster based protocols in hierarchical routing topology.

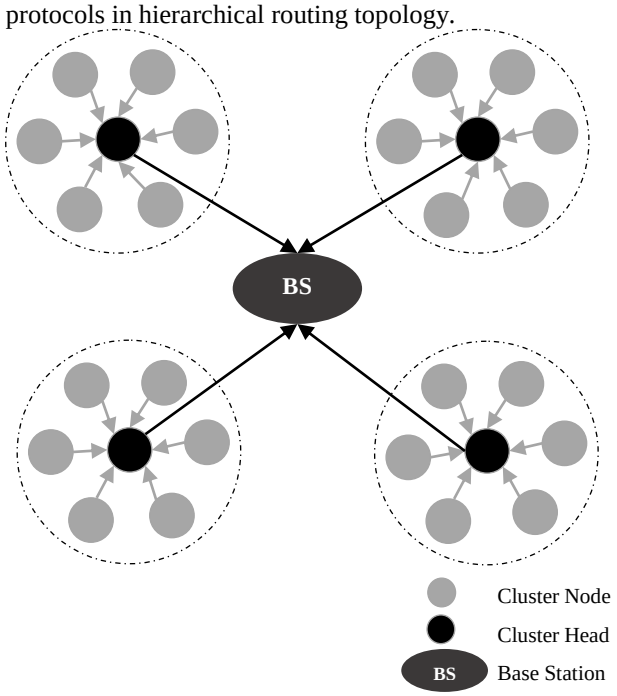

Fig. 1. Hierarchical Architecture

The proposed scheme uses anomaly detection based on SVM technique and a set of attacks represented by fixed signature rules, they are designed to validate the malicious behavior of a target identified by the technique of anomaly detection. Each sensor node has an intrusion module called local IDS agent uses pre-defined rules. Global agent executed on cluster head used both rules based model and support vector machine algorithm. CH is elected dynamically according to his energy. The BS announces the process of CH election, the the CHs calculate residual energy by equation $Vi(t) = [Initial – Ei(t)] / r$, Where Initial is the initial energy, Ei(t) is the residual energy and r is the current round of CH selection [23]. BS calculates the average value and average deviation, according to obtained values. CH announces the CH election procedure for nodes. Old CH broadcasts a message about the withdrawal of authority. New CH sends alert messages to the sensor nodes. CH is responsible for authentication of other members of the cluster, and the base station (BS) is responsible for CH authentication. The anomaly detection based on fixed rules, and support vector machine algorithm are used to filter a large number of packet records.

In the end, the decision making model combines the outputs of anomaly detection based on rules and SVM algorithm. It determines whether an intrusion has occurred, and classifies the type of attacks. The output of the decision-making model is then reported to the administrator for supervision. Fig.2 shows intrusion detection architecture for WSNs.

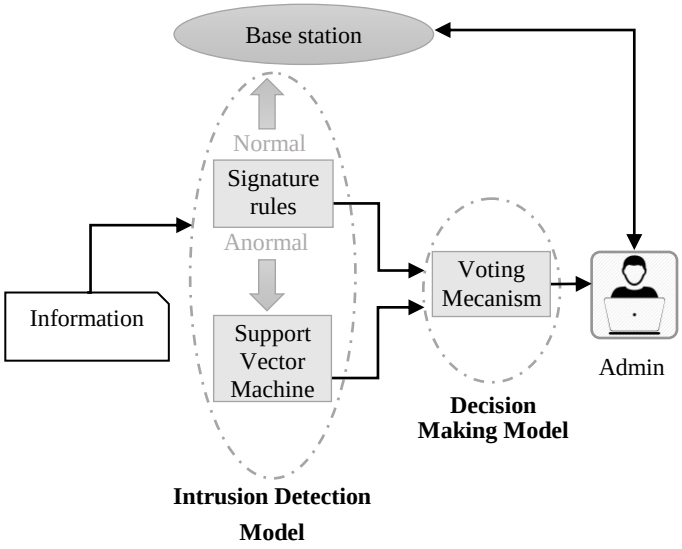

Fig. 2. Proposed Intrusion Detection Model

A. Strategy location of IDS agent

Intrusion detection and response systems should be both distributed and cooperative for the needs of sensor networks. In our scheme, IDS agent is located in every sensor node. Each sensor node has an intrusion module called local IDS agent. The cluster head execute a global IDS agent. Because of limited battery life and resources, each agent is only active when needed. Local agent module is responsible to monitor the information sent and received by the sensor, and forward it to the cluster head. Global agent is responsible for making decision. Because the broadcast nature of wireless network, every node can receive all the packets going through its radio range. Fig .3 below describes the strategy location of IDS.

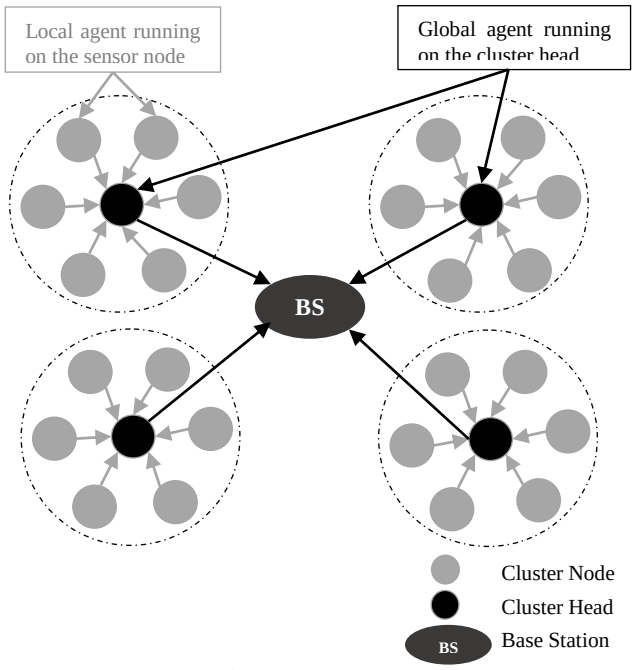

Fig. 3. Strategy location of IDS

B. Phase 1: Anomaly detection using SVM

Support vector machines (SVMs) are a class of machine learning algorithms, due originally to Vapnik [24], which is a sorter design method based on the small sample study, and also suitable to the classification of small sample data [25][26]. Therefore, the SVM method is suited to classify the high-dimension data in IDS. During the training phase, which takes place offline at a system with abundant resources, data are collected from the physical, medium access control (MAC) and network layers. Then, the collected training data are pre-processed using a data reduction process, which aims to reduce their size in order to be processed by SVM.

The solid points and the hollow points, which showed in Fig .4, express the two classes training sample respectively. Hy is the class line which divides the two classes without mistake, Hy1 and Hy2 are the line that pass through the points which are the nearest to the class line in each class's samples and parallel to the class line. The distance between Hy1 and Hy2 is called the separating margin of the two classes. We want the optimal class line not only can separate the two classes correctly which ensure the experience risk minimization, but also can have the maximum separating margin of the two classes which ensure the real risk minimization. For the high dimension, the optimal class line is the optimal classify hyperplane.

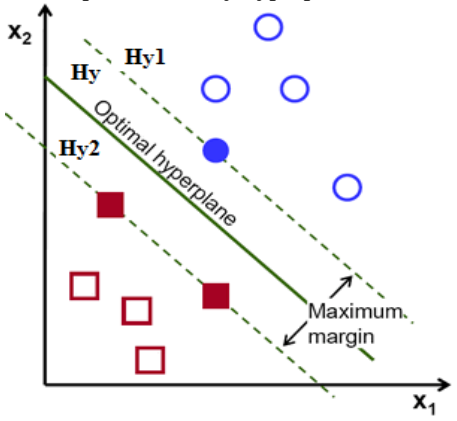

Fig. 4. Classification hyperplane

Classification hyperplane of training data which may be divided by linear classification plane or not via mapping the training data vector to higher dimensional space with some function and transferring the problem to an linear classification problem in that space . After the mapping procedure, SVM finds out a linear separating hyperplane with the maximum margin in the space. In [24] [27], Vapnik et al. described the problem as finding a solution of convex optimization problem, following formulae give you a glance. Given the training datasets:

$$(xi, yi), i = 1, \ldots, n, \text{where } xi \in Rd, yi \in \{-1, 1\},$$

In our case {1} is normal, and {-1} is abnormal. We want to find the hyperplane that have a maximum margin:

$$w.x = b \quad (1)$$

Where $\boldsymbol{w}$ is a normal vector and the parameter $\boldsymbol{b}$ is offset. In order to find the optimal hyperplane, we must solve the following convex optimization problem:

$$\begin{cases} \min\{\dfrac{\|w\|^2}{2} + c\sum_{i=1}^{n}\varepsilon_i\} \\ y_i(w \cdot x_i + b) \geq 1 - \varepsilon_i, \varepsilon_i \geq 0, 1 \leq i \leq n \end{cases} \quad (2)$$

ε_i Slack variables allow some classification errors during the learning process. The regularization constant $\boldsymbol{C > 0}$ quantifies the tradeoff between the number of misclassification and the margin maximization.

$\sum_{i=0}^{n} \varepsilon_i$ relax the constraints on the learning vectors, and $\boldsymbol{C}$ is a constant that controls the tradeoff between number of misclassifications and the margin maximization.

The Eq. (1) can be deal by using the Lagrange multiplier [28]:

$$\begin{cases} maximize\ L(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{i=1}^{n} \alpha_i \alpha_j y_i y_j\, k(x_i, x_j) \\ subject\ to \sum_{i=1}^{n} x_i y_i = 0, and\ 0 \leq \alpha_i \leq C\ for\ all\ 1 \leq i \leq n \end{cases} \quad (3)$$

Here $\boldsymbol{k(x_j, x_j)}$ is the kernel function and $\propto_i$ are the Lagrange multipliers. According to the condition of Kuhn-Tucker (KKT), the s that corresponding to > 0 are called support vectors (SVs). Once the solution to Eq. (2) is found, we can get [28]:

$$w = \sum_{i=1}^{n} \alpha_i x_i y_i \quad (4)$$

Thus, the decision function can be written as:

$$f(x, a, b) = \{\pm 1\} = sgn(\sum_{i=1}^{n} y_i \alpha_i\, k(x, x_i) + b) \quad (5)$$

The SVM method provides very good results with less training time compared to neural networks. Another advantage of SVM is the lowest expected probability of generalization errors [29] [30].

C. Phase 2: Intrusion Detection Model

This module uses a discovery protocol based on the specifications to detect malicious nodes and prevent network disruptions by these nodes. The purpose of this protocol is to classify the behavior of a target as normal or abnormal based on a set of rules. In our case there's four rules for each attack. Followed rules detection for different attacks:

- Rule for hello flood attack: The rule for detecting the Hello flood attack is the received signal strength (ISSR) at the IDS agent, it is greater than a certain threshold (δissrh).

```
1. {
2. if (ISSR > δissrhf)
3.   Then {
4.     Create (alert);
5.     Send(alert, node_ID, ISSR);}
6. Else receive(packetp)}
```

Fig. 5. Rules for hello flood attack

- Rule for selective forwarding attack: The rule for detecting the attack Selective forwarding is defined by the number of packets dropped (PDR) and a node that is above a certain threshold δ_{sf}).

```
1. {
2. if(PDR > δsf)
3. Then {
4.     Create (alert);
5.     Send(alert, node_ID, ISSR); }
6. Else receive(packetp) }
```

Fig. 6. Rules for selective forwarding attack

- Rule for black Hole attack: The rule for detecting the attack Black hole is defined by the number of PDR (greater than seuil δ_{issrbh}) and excess of the signal power (above the threshold δ_{issrbh}).

```
1. {
2. if(PDR > δbh && ISSR>δissrbh )
3. Then {
4.     Create (alert);
5.     Send(alert, node_ID, PDR, ISSR);}
6. Else receive(packetp)}
```

Fig. 7. Rule for black Hole attack

- Rule for Wormholes attack: the rule for detecting the attack excess wormholes is the signal power (above the threshold $\delta_{issrhwh}$) and none of the neighboring nodes malicious node makes the retransmission of packets received from this opponent (PDR threshold the threshold δ_{wh}).

```
1. {
2. if (ISSR > δissrwh && (PDR > δwh)
3. Then {
4.    Create (alert);
5.  Send(alert, node_ID,ISSR); }
6. Else receive(packetp) }
```

Fig. 8. Rule for Wormholes attack

- Global IDS agent: Once the receipt of alerts from the IDS agents, Cluster head takes the decision from its malicious nodes database, creates and propagates the rule.

```
\\Global detection on Cluster head
1. Repeat
2.    If Looking(alert, malicious node's
   database)
3.  then {
4.     Drop (packetp);
5.           Create(rule);
6.           Propagate(rule);
7.   } }
```

Fig. 9. Rule for Global detection

D. Phase 3: Decision making model

If more than half of IDS nodes says the suspected target is malicious, CH ejects node and calculates the appropriate rule of this new intrusion detected. CH sends a message to all IDSs, so they proceed to update their table of signatures. Finally, the CH will be excluded from the network and a new CH will be elected. Note that for each cluster, this threshold is equal to N/2 where N is the number of IDS agents in each cluster. Fig.10 below illustrates Structure of the proposed intrusion detection model.

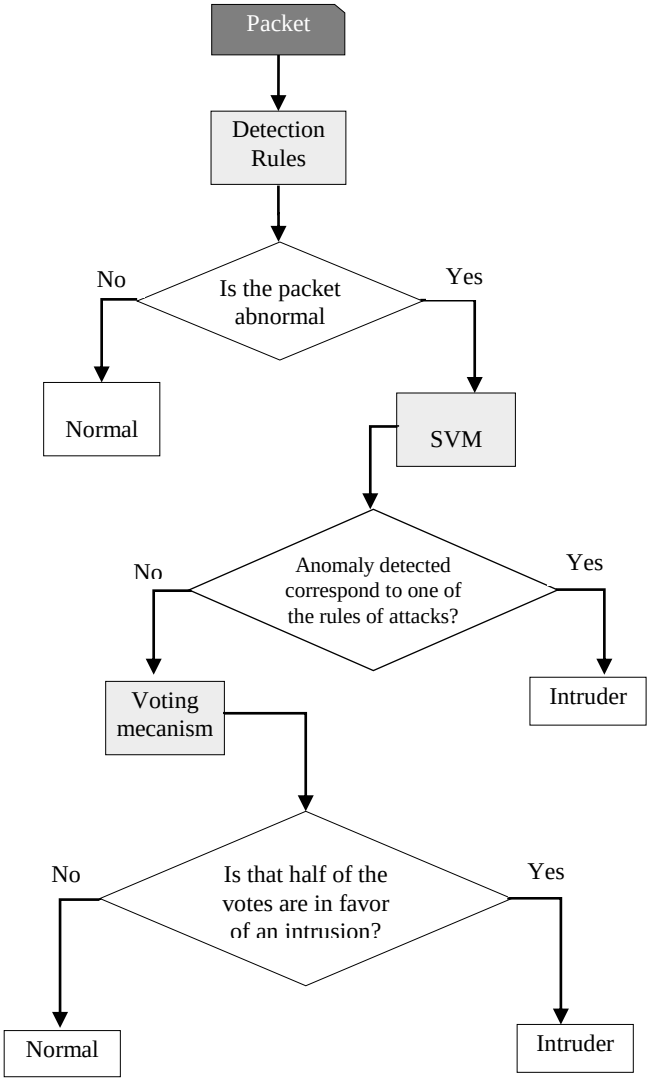

Fig. 10. Structure of the proposed intrusion detection model

V. Performances Analysis and Discussion

This section presents performance analysis of our proposed intrusion detection model.

A. Mathematical Evaluation

In this section, we analyse and evaluate the proposed detection capability, to determine the performance of our approach. The probability of detection an attack, P_D, depends on three factors: number of monitoring nodes in a cluster, the probability of a missed detection of a monitor nods (i.e. cluster head), and our malicious counter threshold *T*. We defined *M* as the number of monitor nodes and P_c as the probability of a collision occurring in a transmission link:

$$P_D = \sum_{I=T}^{M} \binom{M}{T} (1 - P_C)^T P_C^{M-T} \quad (6)$$

We defined P_F is the probability of false accusation against a legitimate node. The probability of false positive is expressed by following equation:

$$P_f = (1 - P_c)^2 P_c + P_c^2 (1 - P_c) \quad (7)$$

According to equation (7), the probability of false detection is expressed through following equation:

$$P_{FD} = \sum_{i=T}^{M} \binom{M}{T} (1 - P_F)^T P_F^{M-T} \quad (8)$$

As shown in Fig. 11, the proposed scheme is effective when the number member nodes are increased. In addition, the probability of a missed detection affects the efficiency of our scheme. However, the proposed model performs better in term of detection rate, exceeding over 95%.

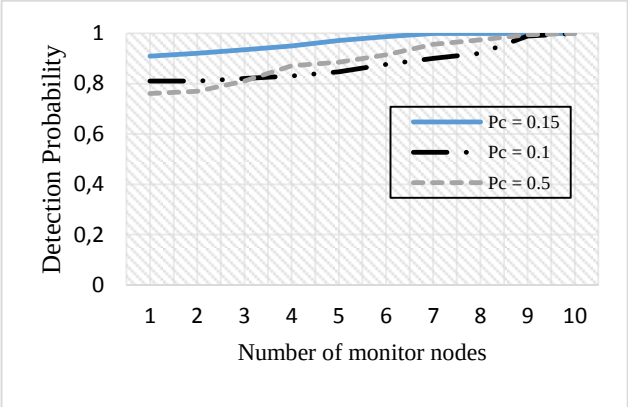

Fig. 11. Detection probability

The probability of false positive detection is shown in Fig.12. It indicates that the increasing number of nodes results in an increase in the probability of a collision.

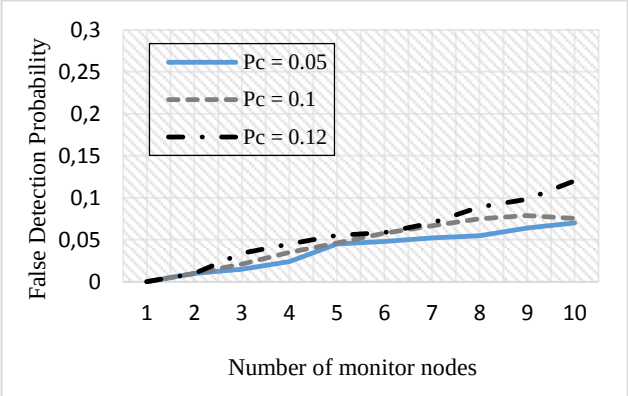

Fig. 12. False detection probability

B. *Performance Evaluation*

In our experiment, we used the simulator TOSSIM [31], which is a discrete event simulator for sensors with the TinyOS operating system. The simulated network consists of 100 nodes randomly distributed in a field of 100×100m2. The network consists of 6 clusters, over all the nodes are static. We use mica2 CC1000-based stack and an interference model for radio simulations. The simulation parameters for detection modules are given in Table II.

TABLE II. SIMULATION PARAMETERS

Attribut	Value
Simulation time	624 seconds
Simulation area	100 * 100m
Number of nodes	100
Radio model	Lossy
Number of clusters	6
Number of IDS agent per cluster	1-10
Routing protocol	HEED modifier
MAC	TDMA
Radio range	10m
Initiale energy	4 Joules
δ_{issrhf}	-45 (dBm)
δ_{sf}	65%
δ_{bh}, δ_{issrbh}	95%, -46 (dBm)
δ_{wh}, δ_{issrwh}	-45 (dBm), 98%

Assuming that there is no attack at the beginning of the simulation, we varied the number of nodes per cluster IDS 1 to 10 for evaluating the performance of our IDS model. To evaluate the effectiveness of the proposed model, a set of metrics has been adopted to determine the most efficient intrusion detection model.

- Detection Rate: Represents the percentage of attacks detected on the total number of attacks.
- False positive rate (false alarms): This is the ratio between the number classified as an anomaly on the total number of normal connections.
- Energy consumption: Measuring the energy consumed by each IDS agent.

For each attack the simulation was repeated more than 10 times. Figures below present a performance comparison of some existing intrusion detection models for WSN in TOSSIM Simulator. In our simulation, four attacks are used to evaluate the performance of the proposed intrusion detection system. Our model achieves high detection rates and low false positive rate under all attacks, as shown in fig. 13.

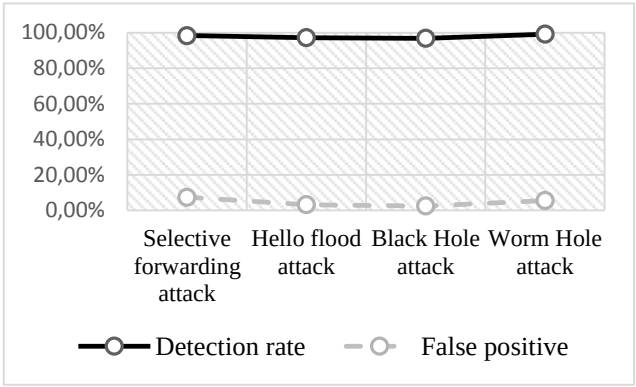

Fig. 13. Detection and false positive rate under four attacks

We can observe in Fig.14, that our model requires less energy to detect attacks. This improvement was achieved through two main reasons: the first is that we use a cluster-based topology. The second reason is that each IDS agent relies on a policy that minimizes packet transmission. In conclusion, we can say that our approach improves network lifetime.

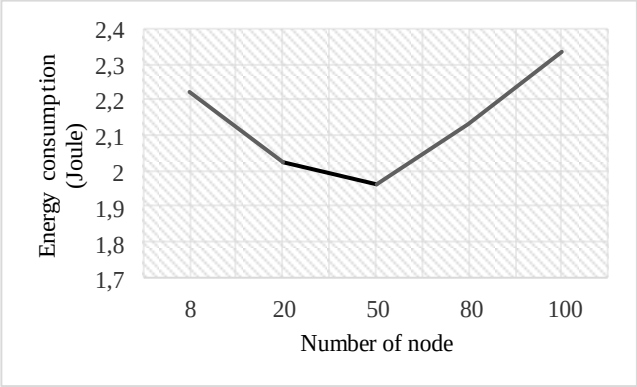

Fig. 14. Energy Consumption

To determine the effectiveness of our approach, we compared our model with others hybrids models proposed by authors Bin et al. [32], Khanum et al. [33], Yuan et al. [34] and Hai et al. [22], analyzing in particular the detection rate and false alarms and generated by IDS agents.

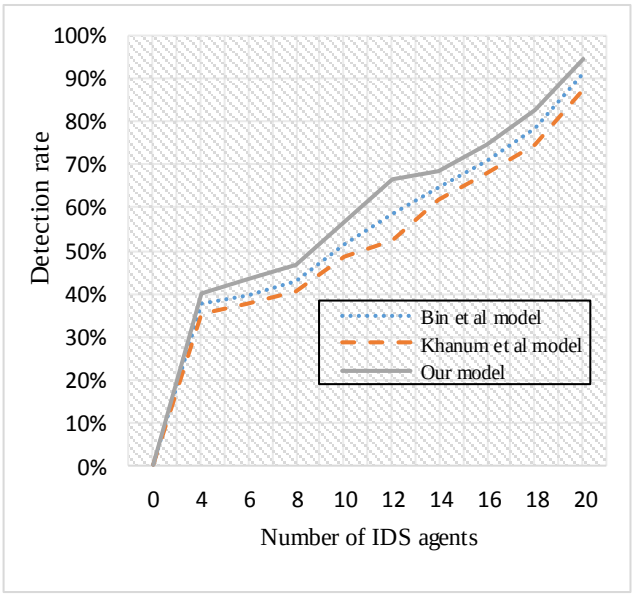

Fig. 15. Detection rate

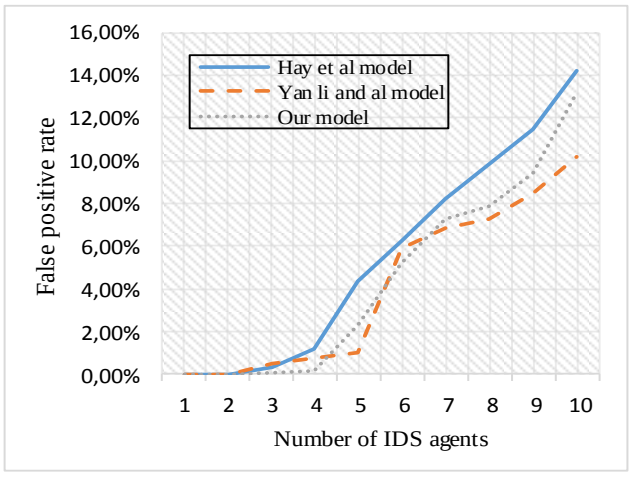

Fig. 16. False positive rate

From Fig. 15 and Fig. 16, the proposed hybrid model has a better efficiency in terms of detecting attacks and false positive rates compared to other models.

VI. CONCLUSION AND FUTURE WORK

This article proposed a hybrid intrusion detection approach for WSN, based on the two existing models such as anomaly based and signature based. Indeed, the combination of these two techniques to offer an intrusion detection system with a high detection rate. Our detection approach is integrated in a cluster based topology, to reduce communication costs, which leads to improving the lifetime of the network.

For our future work, more research on this topic needs to be undertaken with combination of cryptography algorithm and our intrusion detection to achieve a high level of security. We expect the result to be available soon in the future.

REFERENCES

[1] F. Alassery, K. M. Ahmed Walid, M. Sarraf and V. Lawrence, "A Low Computational Complexity Statistical Discrimination Algorithm for Collision Detection in Wireless Sensor Networks", *IAENG International Journal of Computer Science*, Vol. 41, No. 3, pp. 204-211, 2014.

[2] Y. Maleh, A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor network", *International Journal of Wireless & Mobile Networks*, Vol. 5, No. 6, pp. 79-90, December 2013.

[3] M. Patel, A. Aggrwal, "Security attacks in wireless sensor networks: A survey", *International Conference on Intelligent Systems and Signal Processing*, March 2013.

[4] Q. Sarhana, "Security Attacks and Countermeasures for Wireless Sensor Networks: Survey", *International Journal of Current Engineering and Technology*, Vol. 3, No. 2, pp 628-635, June 2013.

[5] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *the first IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.

[6] J. Lopez, R. Roman and C. Alcarez, "Analysis of security threats requirements, technologies and standards in wireless sensor networks", *Springer Lecture Notes in Computer Science*, Vol. 5705, pp. 289-338, 2009.

[7] W. Wang, S. Zhang, G. Duan, H. Song, « Security in wireless sensor networks", *Wireless Network Security Springer Book*, 2013.

[8] A. Araujo, J. Blesa, E. Romero, D. Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", *EURASIP Journal on Wireless Communications and Networking*, February 2012.

[9] L. Besson, P. Leleu, "A distributed intrusion detection system for ad-hoc wireless sensor networks", *The 16th IEEE International Conference on Systems, Signals and Image Processing*, Vol. 1, pp. 1-3, June 2009.

[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*, Vol.2, pp. 25-29, August 2010.

[11] Soumya, C. Grosan, A. Abraham, P. K. Mahanti, "Intrusion Detection on Sensor Networks Using Emotional Ants", *The 5th International Conference on Intelligent Systems Design and Applications*, Vol. 1, pp 344-349, September 2005.

[12] K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure Data Aggregation without Persistent Cryptographic Operations in Wireless Sensor Networks", *Elsevier Ad hoc Networks Journal*, Vol. 15, No. 1, pp. 100-111, January 2007.

[13] I. Krontiris, Z. Benenson, T. Giannetsos, F. Freiling, T. Dimitriou, "Cooperative Intrusion Detection in Wireless Sensor Networks", *Lecture Notes in Computer Science*, Vol. 5432, pp. 263-278, February 2009.

[14] H. Sedjelmaci, S.M Senouci, "A Lightweight Hybrid Security Framework for Wireless Sensor Networks", *IEEE International Conference on Communications (ICC)*, Vol. 1, pp. 3636-3641, June 2014.

[15] A. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks", *international workshop on Quality of service & security in wireless and mobile networks*, Vol. 1, pp. 16-23, October 2005.
[16] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," *the 3rd IEEE Consumer Communications and Networking Conference*, Vol .1, pp. 640-644, January 2006.
[17] A.A. Strikos, "A full approach for intrusion detection in wireless sensor networks", *School of Information and Communication Technology*, March 2007.
[18] S.S. Doumit and D.P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks", *in IEEE Military Communications Conference*, Vol. 1, pp. 609-614, October 2003.
[19] A. Agah, S.K. Das, K. Basu and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach", *3rd IEEE International Symposium on Network Computing and Applications*, Vol.1, pp. 343-346, August 2004.
[20] A. Agah and S.K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach", *International Journal of Network Security*, Vol.5, No.2, pp.145-153, September 2007
[21] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", *The 7th IEEE International Conference on Communications*, Vol. 1, pp. 3864-3869, June 2007.
[22] T. Hoang Hai, F. Khan, E Huh , "Hybrid Intrusion Detection System for Wireless Sensor Networks", *Lecture Notes in Computer Science*, Vol. 4706, pp. 383-396, August 2007.
[23] A. MeenaKowshalya, A. Sukanya, "Clustering algorithms for heterogeneous wireless sensor networks - a brief survey", *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, Vol.2, No.3, pp. 57-69, September 2011.
[24] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A Training Algorithm for Optimal Margin Classifiers", *The 5th Annual ACM Workshop on Computational Learning Theory*, Vol. 1, pp. 144-152, July 1992.
[25] I. Nurtanio, E. R. Astuti, I. K. Purnama, M. Hariadi, "Classifying Cyst and Tumor Lesion Using Support Vector Machine Based on Dental Panoramic Images Texture Features," *IAENG International Journal of Computer Science*, Vol. 40, No. 1, pp. 29-37, 2013.
[26] J. M. Yang, Z. Y. Liu, Z. Y. Qu, "Clustering of Words Based on Relative Contribution for Text Categorization", *IAENG International Journal of Computer Science*, Vol. 40, No. 3, pp. 207-219, 2013.
[27] Vapnik, "V.N.: Statistical study theory essential", *Qinghua University publishing press*, 1995.
[28] C. Cortes and V. Vapnik, "Support-vector network", *Machine Learning 20*, 1995.
[29] B. Scholkopf, and A. J. Smola, "Learning with Kernels", *the MIT Press*, December 2001.
[30] A. H. Sung, and S. Mukkamala, "Identifying Important Features for Intrusion Detection using Support Vector Machines and Neural Networks", *IEEE Symposium on Applications and the Internet*, Vol. 1, pp. 209-216, January 2003.
[31] Simulating TinyOS networks,http://www.cs.berkeley.edu/pal/research/tossim.html, 2003
[32] W. H. Bin, Y. Zheng, W. C. Dong, "Intrusion detection for wireless sensor networks based on multi-agent and refined clustering", *International IEEE Conference on Communications and Mobile Computing*, China, pp. 450-454, 2009
[33] S. Khanum, M. Usman, K. Hussain. "Energy-efficient intrusion detection system for wireless sensor network based on MUSK architecture", *Lecture Notes in Computer Science*, Vol.5938, pp. 212-217, 2009.
[34] L. Yuan, L.E Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response", IEEE Southeastcon, Vol. 1, pp. 37-42, April 2008.

Maleh Yassine is from Morocco. He received his Master degree (2012) in Network and IT Security from Faculty of Science and Technology Settat, Morocco, and his Bachelor in Networks and IT Systems (2009) from Hassan 1st University Morocco. He is IT Project Manager at the National Port Agency in Morocco. He is currently towards his PhD degree in Networks Security at University Hassan 1st Settat, Morocco. His research interests include Wireless Sensor Networks, Virtual Laboratory, and Networks Security.

Prof. Abdellah Ezzati is a research Scientist in Faculty of Science and Technology in Morocco. He obtained his PHD in 1997 in Faculty of science in Rabat and member of the Computer commission in the same Faculty. Now is an associate professor in Hassan 1st University in Morocco and he is the Head of Bachelor of Computer Science. He participate to several project as the project Palmes, which elaborate a Moroccan Education Certification. His research spans various aspects of technology and engineering, Networks, and software development.