Implementation of a Hierarchical Hybrid Intrusion Detection Mechanism in Wireless Sensors Network

Lamyaa Moulad
Computer Science Dept.
ENSEM/EST Casablanca, Morocco

Hicham Belhadaoui
Computer Science Dept. EST
Casablanca, Morocco

Mounir Rifi
Computer Science Dept. EST
Casablanca, Morocco

***Abstract*—During the last years, Wireless Sensor Networks (WSNs) have attracted considerable attention within the scientific community. The applications based on Wireless Sensor Networks, whose areas include, agriculture, military, hospitality management, etc. are growing swiftly. Yet, they are vulnerable to various security threats, like Denial Of Service (DOS) attacks. Such issues can affect and absolutely degrade the performances and cause a dysfunction of the network and its components. However, key management, authentication and secure routing protocols aren't able to offer the required security for WSNs. In fact, all they can offer is a first line of defense especially against outside attacks. Therefore, the implementation of a second line of defense, which is the Intrusion Detection System (IDS), is deemed necessary as part of an integrated approach, to secure the network against malicious and abnormal behaviors of intruders, hence the goal of this paper. This allows improving security and protecting all resources related to a WSN. Recently, different detection methods have been proposed to develop an effective intrusion detection system for WSNs. In this regard, we proposed an integral mechanism which is an hybrid Intrusion Detection approach based on anomaly, detection using support vector machine (SVM), specifications based technique, signature and clustering algorithm to decrease the consumption of resources, by reducing the amount of information forwarded. So, our aim is to protect WSN, without disturbing networks performances through a good management of their resources, especially the energy.**

***Keywords*—Wireless Sensor Networks (WSNs); Intrusion Detection System (IDS); anomalies; specification-based detection; Denial Of Service (DOS) attacks; hybrid intrusion detection system; support vector machine(SVM); false alarm; detection rate**

I. Introduction

Sensors nodes are low power electronic devices that cooperate to form a network called wireless sensor network (WSN), often deployed in hostile areas, difficult to access, they are equipped with small batteries with limited energy, which makes very expensive and difficult to replace or charge these sensor's batteries [8].

Lately, the demand of wireless sensor networks (WSN) [1]-[3] have become a promising future to many new real applications, where data is communicated insecurely to critical destination, such as health monitoring, emergency, army, biometric application in airport, [8] etc. Thus, WSN are exposed to various malicious attacks which can generate an overconsumption of energy. Therefore, monitoring energy consumption is crucial topic to secure a WSN, which means that during the implementation, communication protocols dedicated to WSNs must consider the level of power consumption to provide optimal management [6] of this vital resource.

The goal of this work is to implement an integral security mechanism, a new hybrid intrusion detection system (HIDS) [28], [9] for WSN based on clustering algorithm, to reduce the volume of data forwarded through the network and decrease the exhaustion [7] of resources, especially energy. In general we have combined three main techniques: anomaly-based detection, to class data into normal and abnormal (binary classification), and detect abnormal behavior and anomalies. We have used, also, signature or misuse detection technique to detect known attack patterns, specifications based technique, and some other supporting techniques. Therefore, this combination, profit from the advantages of the cited detection techniques, and can absolutely offer a high detection rate and low false positive, to make a better decision in order to detect new kinds of intrusions.

The paper is organized as follows: In Section II, we provide background information about IDS [26] in WSNs and related works. Section III elaborates on the proposed scheme and architecture of our proposed Hybrid Intrusion Detection System. Section IV contains the simulation results with analysis of the proposed scheme are discussed. In Section V, we conclude our work with a further discussion of research directions.

A. Background of IDSs Security in WSNs

This paper examines one of the most important axes of Wireless Sensor Networks, which is security [21] and particularly Intrusion Detection Systems (IDS) [14]. As already stated, IDSs are defined as the second lines of defense; yet, key management and authentication represent just a first line of defense against just external attacks. Therefore, IDSs, allows detection and prevention from both internal and external [29] intrusions. Fig. 1 describes the process of IDSs.

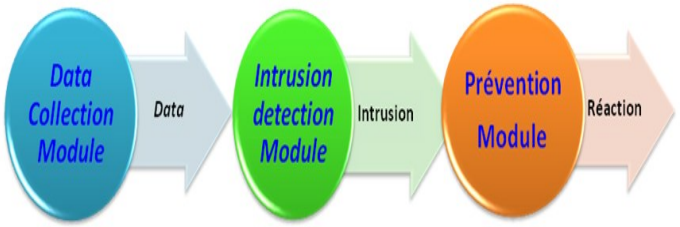

Fig. 1. Intrusion detection architecture.

Each IDS contains three modules:

1) Data Collection modules: Collect the information sent, received and forwarded by the sensors.

2) Intrusion detection module: It depends on the intrusion detection technique used (Signature, Anomaly or Specification-based detection), IDS agent sends an alarm message mentioning the suspect node, to all network.

3) Intrusion detection module: In case of abnormal behavior the IDs send an alarm to the rest of components, and remove the intruder.

IDSs [26], [20] are classified into three main techniques: signature based, anomaly based, and specification-based detection (Fig. 2).

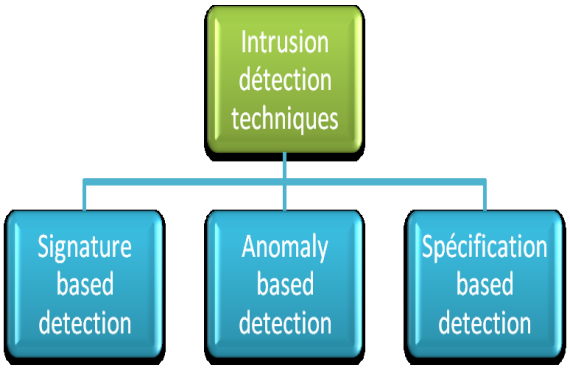

Fig. 2. Intrusion detection techniques [31].

Misuse detection (Signature): Misuse detection based IDS have a predefined collection of main rules that is formed of previously known security attacks, so the behavior of nodes is compared with well-known attack patterns already existing in database. Although, that this technique needs knowledge of attacks' patterns and can't detect new attacks [30], so we always have to update attack signatures database.

Anomaly detection: This technique works on the basis of threshold; it compares the behavior of observed nodes with normal behavior. This model first describes normal behaviors which are established by automated training (as SVM) and then flags as intrusions any activities varying from these behaviors. It is able to detect new intrusions, but, it has a major disadvantage of missing out on well-known attacks. The anomaly based model has a high detection rate, but it has also a high false positive rate.

Specification-based detection: This technique is based on deviations from normal behaviors defined by neither machine learning techniques and nor by training data. Yet, specifications are defined manually and monitor any action by applying the predefined specifications.

However, to improve the level of detection, we can use another solution called the hybrid Intrusion Detection model, which is a combination of detection techniques already mentioned. Therefore, this combination allows the system to benefit from theirs advantages. This mechanism can make a better decision, which might detect new kinds of intrusions with higher detection rate and lower false alarm.

II. Related Works

In previous works, and as we consider proposing hybrid HIDS system, there are some proposed hybrid schemes integrated for clustered sensor networks using the interesting study done by [4].

In [16], [4] a detection system is proposed for WSN and to get an hybrid model (HIDS), the version combine Cluster-based and Rule-based intrusion detection is used and evaluated the intrusion detection using hybrid technique and detection, the results performs better in terms of energy, but the model is still weak because it cannot detect new intrusions.

In [15], Su et al. [4] proposed energy efficient HIDS for CWSNs. They use intrusion detection and intrusion prevention techniques to form a hybrid security system. Their system combines collaboration-based intrusion detection and member node monitoring. The scheme fails because of using just the shared key between cluster head (CH) and member node (MN).

Abduvaliyev et al. [14], [25], [4] proposed a hybrid IDS (HIDS) based on two techniques, anomaly and misuse detection in a cluster WSN (CWSN) environment. The results showed that the model proposed give a high detection rate and low level of energy consumption. However, this model does not detect most known network attacks.

Yan et al. [4] proposed hierarchical IDS (CHIDS) based on clusters. The authors took advantage of this approach and install on each cluster-head an IDS agent that contains three modules: a supervised learning, an anomaly detection based on the rules and decision-making module. The simulation results showed a high detection rate and lower false positive rate. But, the implementation of this detection mechanism requires many calculations in cluster-heads, and that can decrease the network lifetime.

Hai et al. [23], [4] proposed a hybrid, lightweight intrusion detection system for sensor networks (SN), using the scheme of Roman et al. [5]. Intrusion detection scheme profit from advantage of cluster-based protocol to form a hierarchical network (HN) to give an intrusion framework based on anomaly and misuse techniques. In their proposition, IDS agent consists of two detection modules, local agent and global agent. The authors apply their model in a process of cooperation between the two agents to detect attacks with greater accuracy. But, the disadvantage of this scheme is the sharp increase in signatures, which can lead to an overload of the node memory.

In recent work, Coppolino et al. [6], [4] presented a hybrid, lightweight, distributed IDS (HDIDS) for WSN This IDS uses both misuse-based and anomaly-based detection techniques. It is composed of a Central Agent (CA), which performs highly accurate intrusion detection by using data mining techniques, and a number of Local Agents (LA) running lighter anomaly-based detection techniques on the motes.

Sedjelmaci et al. [4] implemented a new Framework for securing WSN that combines cryptography and IDS technology to detect the most dangerous network attacks, and provide a trust environment using clusters. The results show

that the model performs well in terms of detection rate, although it generates high overhead and energy consumption.

Y. Maleh et al. [24] implemented a hybrid, lightweight IDS model for sensor networks, the ids using cluster-based architecture. This model uses anomaly detection based (SVM) algorithm and signature. The proposed hybrid model give efficiency in terms of detecting attacks and false positives rates compared to previous schemes, however the charge of CH can cause an early dysfunction of this element.

III. Proposed Hybrid IDs

The proposed model contains specification based technique, signatures based technique using some fixed rules representing most dangerous attacks in WSN, and anomaly detection based on SVM [5], to confirm the malicious behavior of a target identified by behavior detection technique, and analyze data for classification.

Fig. 3 below provides our proposed hybrid model.

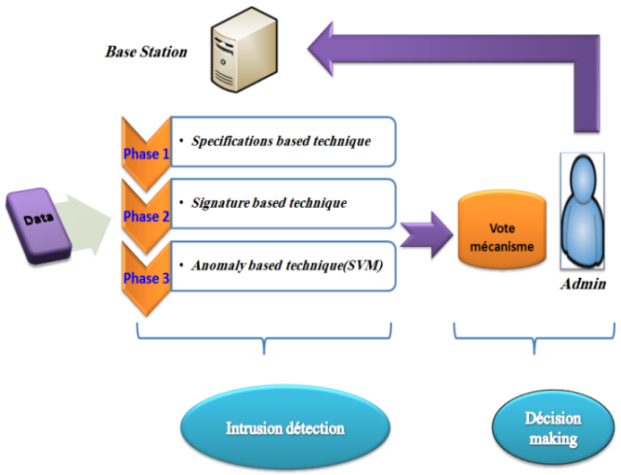

Fig. 3. Architecture of proposed hybrid IDS.

A. Intrusion Detection Used Techniques

1) Behavior based detection (specification-based)

This technique adopts the same principle as the detection based anomalies that, any deviation of normal behavior is considered as intrusion. This technique fit a statistical model (usually normal behavior) to the data provided. Then, It applies a statistical inference model to determine if an instance belongs to this model or not. When a low probability is being generated from the learned model, concerned bodies are reported as anomalies.

However, the definition of the behavior model is performed in a manual way and not automatically using a learning algorithm, because it uses thresholds defined by the user to identify areas of abnormal data. It is similar to a No parametric learning (statistical) the techniques that offer greater flexibility with respect to parametric learning techniques because they require no prior knowledge of the data distribution. This simplifies the detection system, and significantly reduces the rate of false negative detections. Compared to the detection based on anomalies, this technique seems to be best suited to the limitations of sensor networks.

2) Anomaly detection using SVM

In this section a detailed description of SVM and feature selection are presented:

a) Support vector machines

Support vector machines (SVM) [19] are defined as a set of supervised learning techniques used for classification of network behavior. The main goal of SVM classifier is to determine a set of vectors called support vectors to construct a hyperplane (see Fig. 4) in the feature spaces. Here, a distributed binary classifier to normal and abnormal, which permits detection of every malicious act.

$$w = \sum_{i=1}^{n} \alpha_i y_i x_i \quad \min\left\{\frac{\|w\|^2}{2} + C\sum_{i=1}^{n} \varepsilon_i\right\} \qquad (1)$$

$\sum_{i=1}^{n} \varepsilon_i$ is the constraints on the learning vectors, and C is a constant that controls the tradeoff between number of misclassifications and the margin maximization.

Equation (1) can be dealt by using the Lagrange multiplier [17]:

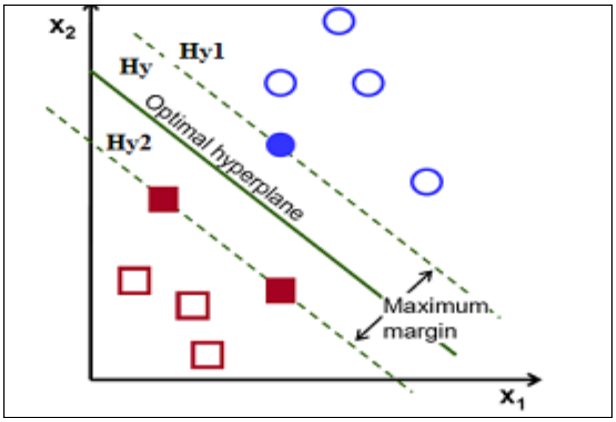

Fig. 4. Hyperplane.

Classification hyperplane given the training datasets,

(x_i, y_i) $i=1,...n$ $y_i \in \{-1,+1\}$, $x_i \in R^d$

The hyperplane that have a maximum margin:

$W.x = b$

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

$$maximise\ l(\alpha) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \alpha_j y_i y_j k(x_j, x_i) \qquad (2)$$

$$subject\ to \sum_{i=1}^{n} y_i \alpha_i = 0, and\ 0 \le \alpha_i \le C\ for\ all\ 1 \le i \le n$$

$K(x_j, x_i)$ is the kernel function and α_i are the Lagrange multipliers. Referring to the condition of Kuhn-Tucker (KKT), the x_is that corresponding to $\alpha_i > 0$ are called support vectors (SVs).

Once the solution to (2) is found, we get [17]:

$$y_i(w.x_i + b) \ge 1 - \varepsilon_i, \varepsilon_i \ge 0, 1 \le i \le n \qquad (3)$$

Thus the decision function is written as:

$$f(x,a,b) = \{\pm 1\} = sgn\left(\sum_{i=1}^{n} y_i \alpha_i k(X_j X_i) + b\right) \quad (4)$$

SVM is more suitable for intrusion detection in case where new signature is detected. Also, SVM provide low false positive and satisfied results with low training time compared to neural networks. [18].

3) Misuse based detection (Signature)

Misuse or signature based detection is used to prevent network against malicious behavior using a set of rules. There is five main rules for each attack, rule to detect an excessive demand of energy (E(d)>E. The rule to detect the Selective forwarding attack, represented by the number of packets dropped (PDR). The rule to detect the Hello flood attack is the received signal strength (ISSR) at the IDS agent, The rule to detect the Black hole attack is defined by the number of RDP. Finally, the rule to detect the wormholes attack which is the power of signal.

4) Cooperative decision making Approach (voting mechanism)

In this approach, each node participates in the detection and management of intrusion decision.

The goal of the decision making model is to analyze the results of all detection techniques used which are the behavior's specification, anomaly and misuse detection models and validate when an intrusion occurs or not. Then, it sends the results to the administrator of network, to help them handle the state of the system, update the database of signatures, make further countermeasures, and prevent the system by sending an alarm if an intrusion occurs.

B. Network Structure and IDS Agents Location Process

1) Structure of the network: As mentioned before, the detection approach uses cluster-based topology (see Fig. 5) [22] to decrease the quantity of packets forwarded through the network and increasing the network lifetime. by designating a leader of the group called cluster-head (CH) - via a cluster election - that collect data received from member nodes to prepare it for the mobile sink (MS) use, then and while moving through CHs, the MS aggregate data (collected by CHs), instead of sending it to the base station (BS), in order to reduce the charge and also support the CH.

The base station starts the process of CH election, CHs calculate residual energy using the equation Vi(t) = [Initial – Ei(t)] / r, where Initial is the initial energy, r is the current round of CH selection and Ei(t) is the residual energy. According to collected values, the Base station (BS) calculates the average value and average deviation .then a CH is elected dynamically according to his residual energy.

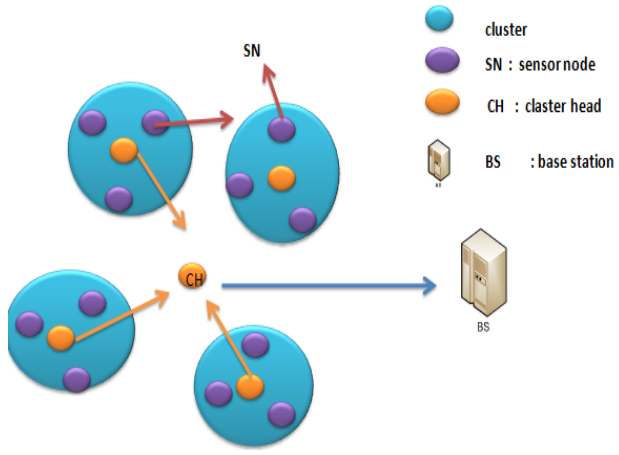

Fig. 5. Network structure.

2) IDS location process: In this proposed scheme, an IDS agent is located in each sensor node. Each cluster contains two kinds of agents: local and global IDS agents. Because of the limited energy resources, each agent is only active when needed, to avoid the above issues, we place a sensor node called mobile sink which act as an intermediate between the CH and the BS. The mobile sink (MS) is kept in moving state so that the intruder may not find the location of the node easily. The proposed cluster-based wireless sensor networks topology is shown in the (Fig. 6). The MS gathers the data from each of the cluster-head when it moves near to the corresponding clusters. The mobile sink reduces the work load of the cluster-head. While the cluster-head sending the data to the mobile sink, the energy of the cluster-head is automatically reduced [12], [11].

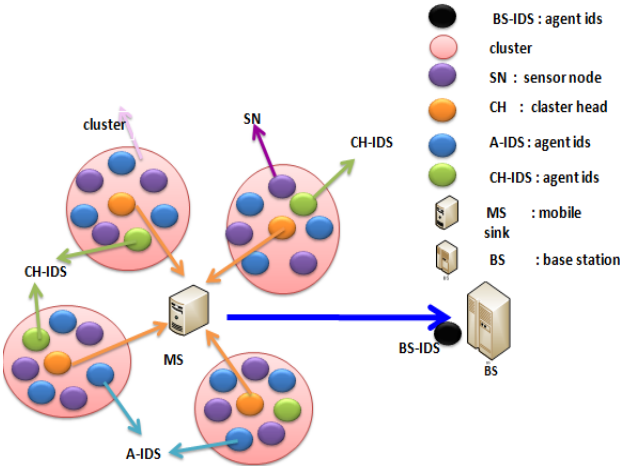

Fig. 6. Location of IDS in wireless sensor network.

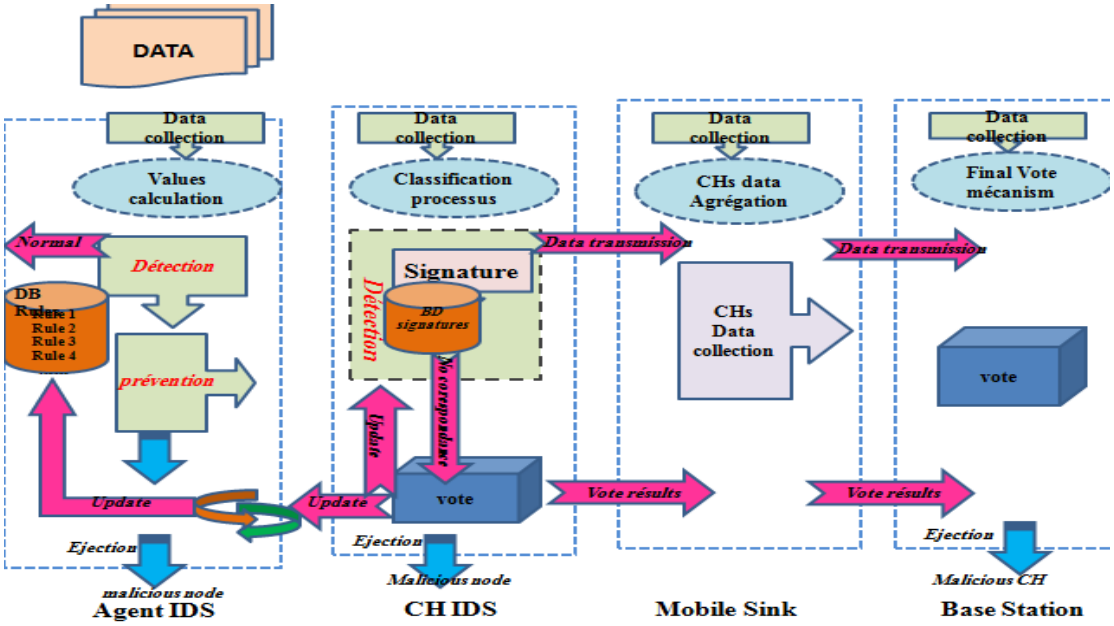

Fig. 7. Process of detection between WSN IDS agents components.

Fig. 7 explains well the process of IDS agents' location in network.

In this hybrid IDS architecture, and by using hierarchical architecture, our aim is to utilize cluster-based protocols to save energy, and reduce computational resources and data transmission redundancy. In this context, we proposed this enhanced intrusion framework based information sharing.

a) Intrusion detection at Member nodes: Data Collection modules and intrusion detection are in general, the principal components in this type of agent.

- Data Collection Module: Is responsible to collect the data sent, received and forwarded by sensor. This node saves in his database, the id of the node analyzed and compute values of some parameters, such as Energy, NPD, NPS, RSSI, NRM, JITTER … in every node.
- Intrusion Detection Module: This module apply a mechanism that the cluster have a special behavior, so any deviation of the normal values fixed for parameters mentioned, represent an abnormally that need to be fixed immediately, by alarming CH of the cluster. This IDS can supervise even the CH when needed.

b) Intrusion detection at CHs: Proposed clustering algorithm chose for every cluster, the CH that has more power resources to aggregate data from cluster members. This powerful node is composed of three modules.

- Data Collection Module: Is responsible of collecting packets sent by the IDS agent. This message contains the address of the node analyzed by the IDS agent then, transmitted to the abnormality detection module for intrusion detection process.

Behavior classifier:

Then the Behavior classifier classifies the node behavior of collected data already transmitted by the ids agent, as trustworthy if no match with database signature, attacker if rule signature is confirmed, and suspect if not an attack but the behavior still shows an abnormality in this case we need to apply detection module for learning based on SVM.

After computation and analysis of the values collected and the fixed rules, the behavior is classified into:

```
Classification {

If (packet is Normal)
  { Launch of voting process }

Elseif (packet matches a signature)
  {Declare the intruder node with exclusion and
classification of the attack)
 }

Else { (calculate SVM)
 Launching voting processes}
}
```

- Intrusion Detection Module: (Signature + SVM) This kind of IDS uses discovery protocol based on the fixed rules signatures representing most dangerous attacks in Wireless Sensor Network (Section III, Phase 3), then transmitted to the abnormality detection module for learning and classification process.
- Voting Mechanism: Regarding collaborative process, the cluster-head uses the voting mechanism. If there is no match between the intrusion detected by predefined signatures attackers and the anomaly detection, IDS agent sends a message to the CH, this one use voting to make a final sure decision on the suspect node. If more than ½ of IDS nodes located in the same cluster voted

for malicious suspected target, the CH rejects that node and calculates the rule of this new intrusion detected. The CH sends an update message to all IDSs that are in the same cluster and CHs neighbors. This message contains the ID of the malicious node and this new rule (and signatures).When IDS agent receives this message it is an update of its signature table.

Mobile sink:

Each mobile sink (MS) gathers the data from each of the cluster-head in the same radio coverage area when it moves near to the corresponding clusters to reduce the work load of the cluster-head. When the cluster-head transmits the data to the mobile sink [32], the energy of the cluster-head is reduced ,this information will be transmitted to the base station for a monitoring process.

c) Intrusion detection at Base station (BS): Each mobile sink gathers the data from each of the cluster-head in the same radio coverage area when it moves near to the corresponding clusters to reduce the work load of the cluster-head. When the cluster-head transmits the data to the mobile sink, the energy of the cluster-head is reduced; this information will be transmitted to the BS for monitoring process.

Fig. 8 below explains the global Structure of our effective hybrid proposed intrusion detection model.

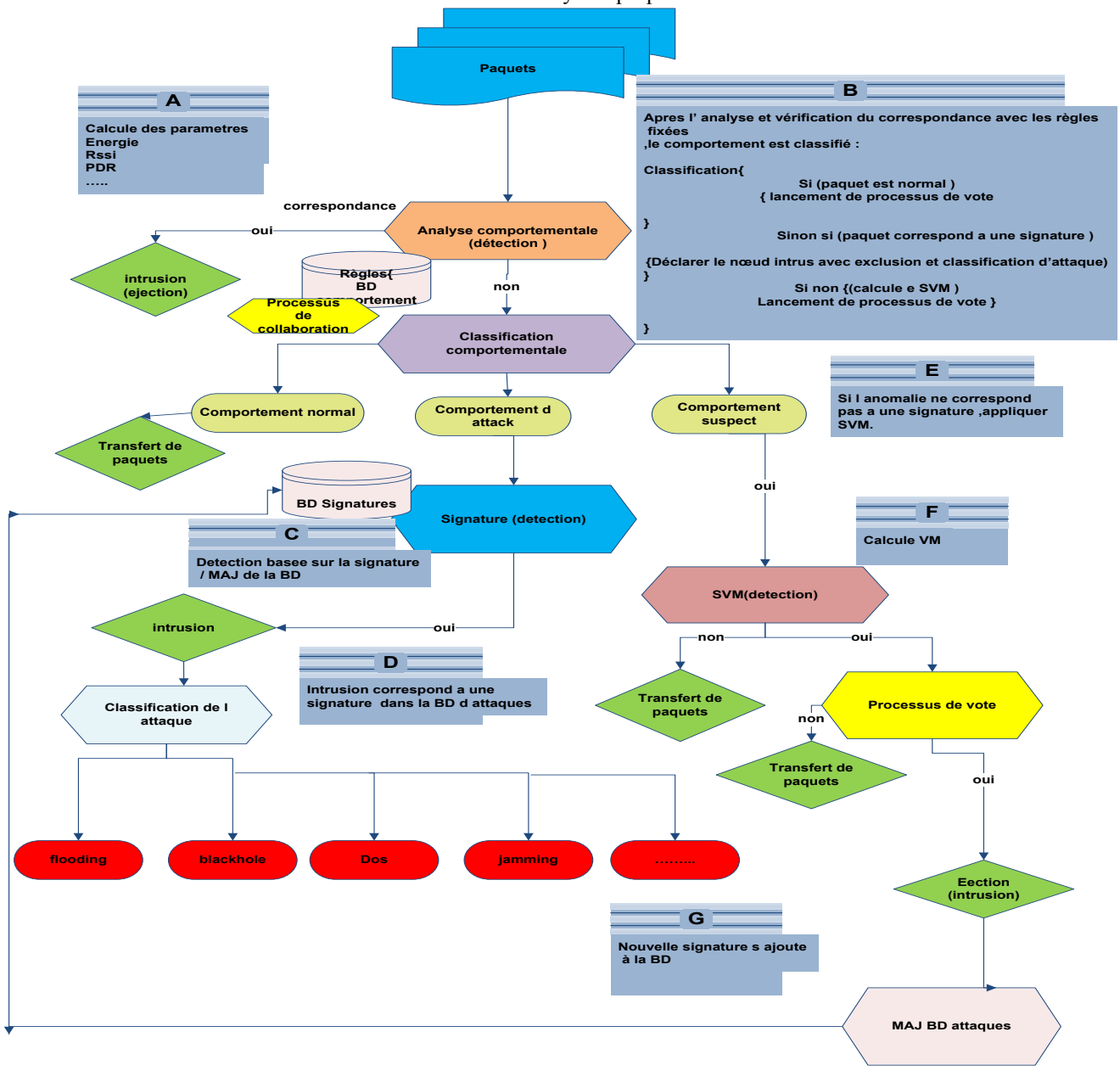

Fig. 8. Structure of the proposed intrusion detection model.

C. Dynamic Process for Intrusion Detection System

In the suggested approach, if (1/2) of IDS nodes within the cluster have consumed more than 25%, 50% and 75% (in tree level) of their energy; new IDSs are elected and receive the actual set of intrusion signature from the CH. New IDSs election depends on the residual energy and the placement process proposed by Khalil et al. new IDS nodes are elected, they compute locally the SV and the distributed algorithm for training SVMs is performed. This model helps to save energy of network components.

IV. Experimental Evaluation

To evaluate the proposed hybrid IDSs, we used the KDDcup'99 dataset [10] as the sample to verify the efficient of the hybrid detection mechanism and valid it by comparing the results with scheme proposed by Abduvaliyev et al. [14] and W. T. Su, K.M. Chang [15]. According to [13], the false positive rate (false alarm), detection rate and energy generated by IDS agents were to determine the effectiveness of our proposed scheme.

A. Dataset

The KDD 99 intrusion detection dataset is developed by MIT Lincoln Lab in1998, each connection in the dataset has 41 features and it's categorized into five classes: normal and four attack behaviors (Dos, Probe, U2r, R2l) [12].

Our analysis is performed on the "KDD" intrusion detection benchmark by using its samples as training and testing dataset. We focus on all categories of attacks and specially Dos attacks, which are defined as anomalies behavior.

The training data used at each IDS comprises of 50 normal and 50 anomalous samples include Dos attacks [17].

To determine the effectiveness of our proposed hybrid intrusion detection system we tried to analyze some important metrics, which are: detection rate (DR), the false positive rate (FP) and energy, according to the formulas:

$$Detection\ Rate = \frac{\text{Number of detected attacks}}{\text{Number of attacks}} * 100\%$$

$$False\ Positive\ Rate = \frac{\text{Number of misclassified connections}}{\text{Number of Normal connections}} * 100\%$$

$$Total\ Energy\ consumption\ Et = \text{EA} + \text{EM}$$

1) Detection Rate (DR): is the ratio of attacks detected on the total number of attacks;

2) False positive rate or false alarms (FR): is the ratio between the number classified as an anomaly on the total number of normal connections;

3) Total energy consumption (EC): it calculate the total amount of energy consumed in all nodes in the network.

B. Simulation Results

The network is composed of 10 clusters that contain 1-7 nodes over all the nodes that are static, distributed in a field of 100×100, an interference model for radio simulations. The rest of the specifications of a sensor node for detection module are defined in the table below (see Table 1, Fig. 9).

TABLE I. Simulation Parameters

Parameter	Value
simulation time	900 sec
simulation area	100 *100m
Number of nodes	100
radio Model	Lossy
Number of cluster	10
IDS agents / cluster	1-7
routing Protocol (Rp)	HEED modifier
MAC	TDMA
radio range	20m
Initial energy	5 Joules
Power consumption for transmission	1.6W
Power consumption for reception	1.2W
Power consumption in idle state	1.15W

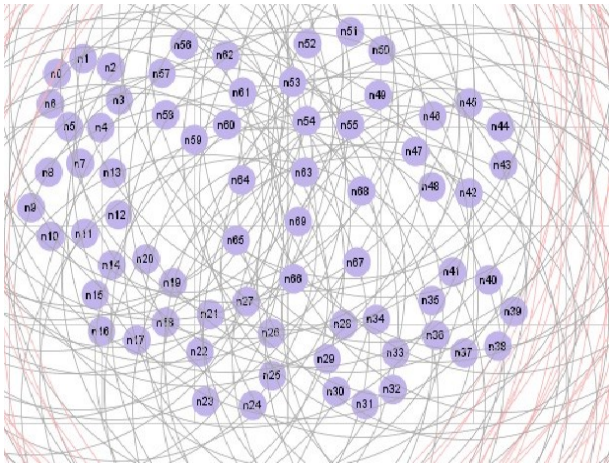

Fig. 9. Scenario of 10 clusters.

1) Detection rate: Fig. 10 shows that if we increase the number of nodes, the scheme become very effective. So, our proposed model performs better in term of detection rate, exceeding over 98.5% comparing to schemes proposed by Abduvaliyev et al. and W. T. Su, K.M. Chang.

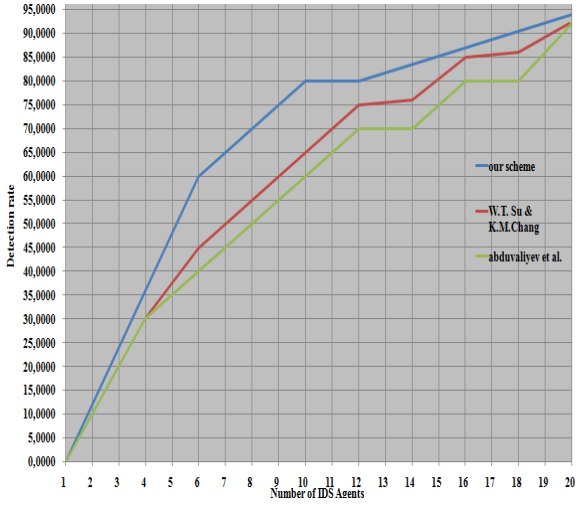

Fig. 10. Detection rate.

2) False positive rate: The probability of false alarms is given in Fig. 11. It indicates that the increasing number of nodes provide an increasing in the probability of a collision. Fig. 11 shows a low false alarm (1.8%) and a short detection time, compared to the scheme proposed by Abduvaliyev et al. and W. T. Su, K.M. Chang.

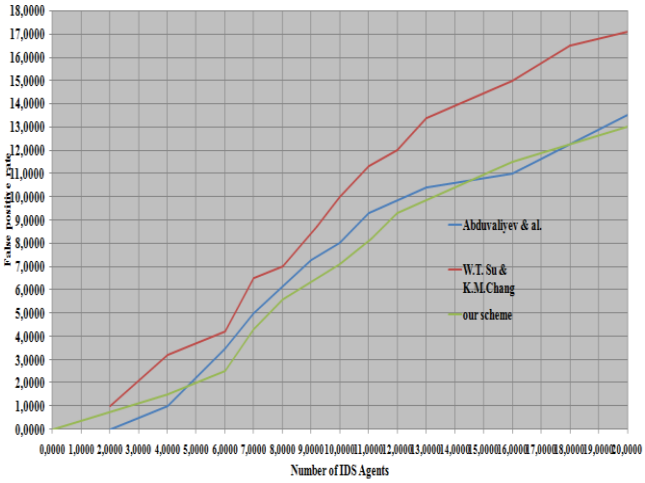

Fig. 11. False positive rate.

3) Energy Consumption: Fig. 12 illustrates the total of energy consumed in the sensors network deployed. It is clear that our model is the less energy consuming scheme comparing to the other schemes proposed by Abduvaliyev et al. and W.T. Su, K.M. Chang.

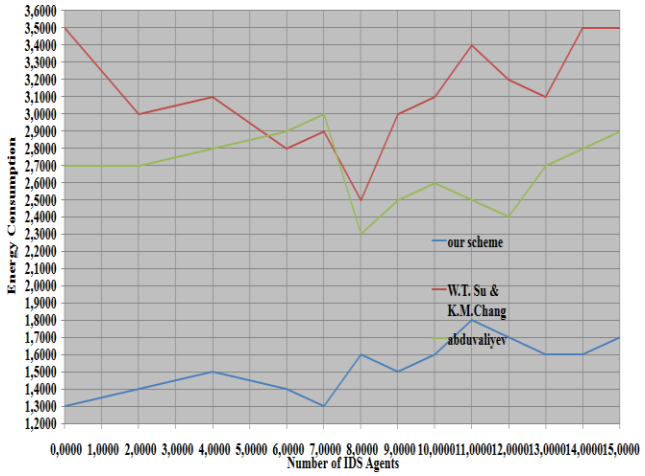

Fig. 12. Energy consumption.

Detection and false positive rates were respectively of the order of 98.5% and 1.8%. As shown in Fig. 10 and 11, the two diagrams show a high detection rate and low false alarms and a short detection time, compared to the scheme proposed in the reference.

Furthermore, our detection model requires less energy to detect these attacks, compared to the approach used by the authors mentioned. This improvement was achieved through our use of a cluster-based topology that aims to select a single node in a cluster (cluster-head) to transmit data aggregated at Mobile sink, which allows grouping packets from cluster-heads, then send it to the base station, especially that each IDS agent is based on a policy that minimizes packet transmission, which, in turn, will save energy. In conclusion, we can say that our approach improves network lifetime.

V. Conclusion

In this paper, we have implemented a security mechanism which is a hybrid Intrusion Detection approach based Anomaly Detection, based on support vector machine (SVM), specifications, and the Misuse Detection WSN, using the clustering algorithm to decrease the consumption of resources specially the energy by reducing the amount of information forwarded, so, our aim was to a safe WSN without damaging the network, by the good management of resources specially the energy. All results show that all attacks are detected with low false alarm and high detection rate.

As the future research directions, we will analyze, evaluate and implement our model with various attacks in a real environment; also a soft hybrid model will be proposed and compared to this present model and implemented in a large-scale sensors network.

References

[1] Houngbadji Thérence, Réseaux ad hoc : 'système d'adressage et 277ultime d'accessibilité aux donnée' Thesis 2009, école polytechnique de Montreal.

[2] I. F. Akyildiz et al, "Wireless Sensor Networks: a survey," Computer Networks, Vol. 38, pp. 393-422, March 2002.

[3] H. Karl and A. Willig, "A short survey of wireless sensor networks" IJCT(2004).

[4] Y.Maleh A.Ezzati,Y. Quasmaoui and Mohamed Mbida."Aglobal hybrid intrusion detection system for wireless sensor networks" ,procedia computer science,2015.

[5] Robert Mitchell, Ing-Ray Chen , Department of Computer Science, Virginia Tech, Falls Church, VA 20191, United States 'A survey of intrusion detection in wireless network applications' , Computer Communications 42 (2014) 1–23.

[6] Wassim Masri, 'Dérivation d'exigences de Qualité de Service dans les Réseaux de Capteurs Sans Fil sur TDMA', Thesis 2009,

[7] R.Haboub and M. Ouzzif 'Secure and reliable routing in mobile Adhoc networks', (IJCSES),2012 .

[8] Lamyaa Moulad ,Hicham Belhadaoui,Mounir Rifi Estc/Ensem UH2C 'Implementation of a security mechanism of WSN based on energy management' IJEAT 2013.

[9] T. Prasanna Venkatesan 'An Effective Intrusion Detection System for Manets' International Journal of Computer Applications® (IJCA) (0975 – 8887) International Conference on Advances in Computer Engineering & Applications (ICACEA-2014) at IMSEC,GZB.

[10] Hichem Sedjelmaci, and Mohamed Feham,'Novel hybrid intrusion detection system for clustred wireless sensor network' , (IJNSA), Vol.3, No.4, July 2011 .

[11] Eui-Nam Huh and Tran Hong Hai, 'Lightweight Intrusion Detection for Wireles Sensor Networks' ,Thesis 2009 .

[12] Yassine MALEH, Member, IAENG, and Abdellah Ezzati,'Lightweight Intrusion Detection Scheme for Wireless Sensor Networks' ,IAENG, IJCS 2013.

[13] Madhumathi C S, 'Efficient Cluster Head Selection and Mobile Sinks for Cluster-Based Wireless Sensor Networks', International Journal of Scientific Engineering and Research (IJSER).

[14] Abror Abduvaliyev, Sungyoung Lee, Young-Koo Lee, Department of Computer Engineering,Kyung Hee University, Suwon, Korea 'Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor

Networks' 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[15] W. T. Su, K.M. Chang, and Y.H. Kuo, 'eHIP: An energy efficient hybrid intrusion prohibition system for cluster-based wireless sensor network', journal of Computer Networks, Vol.51, pp. 1151-1168, 2007.

[16] Rachana Deshmukh 'An Intrusion Detection Using Hybrid Technique in Cluster Based Wireless Sensor Network'Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.2153-2161.

[17] K. Q. Yan, S. C. Wang, S. S. Wang, C. W. Liu, 'Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network', Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology, China, pp. 114-118, 2010.

[18] KDDCup1999Data,http://kdd.ics.uci.edu/databases/kddcup99/task.html; 1999.

[19] 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.

[20] 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.

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

[22] A. MeenaKowshalya, A.Sukanya,'Clusterin algorithms for heterogeneous wireless sensor networks - a brief survey', International Journal of Ad hoc, Sensor & Ubiquitous Computing,

[23] H.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.

[24] Y.MALEH,, and A.Ezzati, ' CONTRIBUTIONS TO SECURITY IN WIRELESS SENSOR NETWORKS AND CONSTRAINED NETWORKS IN INTERNET OF THINGS , Thesis 2017 .

[25] A. Abduvaliyev, A.K Pathan, J. Zhou, R. Roman and W. Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", Communications Surveys & Tutorials, IEEE Volume

15, Issue 3, 2013.

[26] 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.

[27] 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.

[28] A.A. Strikos, "A full approach for intrusion detection in wireless sensor networks", School of Information and Communication Technology, March 2007.

[29] A. Louzani "sécurisation d un protocole inter-couches pour les réseaux LR-WPAN,thesis, 2015.

[30] S. Sahraoui, "mécanisme de sécurité pour l'intégration des RCSFà l'IoT , thesis 2016.

[31] D. Boubiche une approche inter-couches pour la sécurité dans RCSF , thesis 2014 .

[32] S. Nithyakalyani and S.Kumar,"Voronoi Fuzzy clustering approach for data processing in WSN" international of computational intelligence system 2014.