Implementation of an Hierarchical Hybrid Intrusion Detection Mechanism in Wireless Sensor Network Based on Energy Management

Lamyaa Moulad[1(✉)], Hicham Belhadaoui[2], and Mounir Rifi[2]

[1] ENSEM/EST, University Hassan II, Casablanca, Morocco
Lamyaa.moulad@gmail.com
[2] EST, University Hassan II, Casablanca, Morocco

Abstract. In the last few years, Wireless Sensor Networks (WSN) 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 to improve security and protect all resources related to a WSN.

Different detection methods have been proposed in recent years for the development of intrusion detection system, In this regard, we propose an integral mechanism which is in fact a hybrid Intrusion Detection approach based Anomaly, Detection using support vector machine (SVM), specifications based technique 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 energy.

Keywords: WSN · IDS · Misuse detection · Anomalies
Specification-based detection · DOS attacks · Hybrid intrusion detection system
Support vector machine (SVM) · False alarm · Detection rate

1 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 it very expensive and difficult to replace or charge these sensors' batteries.

J. Mizera-Pietraszko et al. (Eds.): RTIS 2017, AISC 756, pp. 360–377, 2019.
https://doi.org/10.1007/978-3-319-91337-7_33

Recently, 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 emergency evacuations security, health monitoring, soldiers in battlefield, biometric application in airport, etc.. Thus, WSN are exposed to various malicious attacks, which can generate an overconsumption of energy. Therefore, controlling energy consumption is important 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 of this vital resource.

The goal of this work is to implement an integral mechanism, a new hybrid intrusion detection system [4] for WSN using the clustering algorithm, to reduce the information forwarded and decrease the consumption of resources, especially energy. In general we have combined two main techniques, anomaly-based detection, that class data into normal and abnormal (binary classification), to detect malicious behaviors. We have also, applied misuse detection technique called also (signature) to determine known attack patterns, specifications based technique, and other techniques. Therefore, the combination of those techniques, the benefit from the advantages of the two detection techniques, can absolutely offer a high detection rate and low false positive. This mechanism can make a better decision in order to detect new kinds of intrusions.

The paper is organized as follows: In Sect. 2, we provide a background information about IDS in WSNs and related works. Section 3 elaborates on the proposed scheme and architecture of our proposed Hybrid Intrusion Detection System. Section 4 contains The simulation results with analysis of the proposed scheme are discussed. In Sect. 5, We conclude our work with a further discussion of research directions

1.1 Background of Ids Security in WSNs

This paper examines one of the most important axes of Wireless Sensor Networks, which is security and particularly Intrusion Detection Systems (IDS) [14]. As already stated, Intrusion detection systems are defined as the second lines of defense; However, 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 attacks and all kinds of intrusions (Intrusion is defined as an unauthorized activity in a network.) (Fig. 1).

Fig. 1. Intrusion detection architecture

Each IDS [27] contains 3 modules:

(a) Data Collection modules: collect the information sent, received and forwarded by the sensors.
(b) 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.
(c) Intrusion detection module: In case of abnormal behavior the ids send an alarm to the rest of components, and remove the intruder.

IDSs are classified into 3 main techniques: Anomaly based, Signature based and Specification-based detection (Fig. 2).

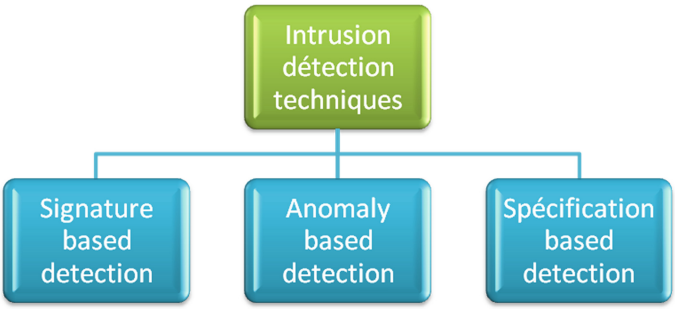

Fig. 2. Intrusion detection techniques

Misuse detection (Signature): Misuse detection based IDS have a predefined set of rules that are designed on the basis of previously known security attacks, so the behavior of nodes is compared with well-known attack patterns already existing in database. The disadvantages are that this technique needs knowledge of attacks' patterns and can't detect new attacks, 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 has the ability 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 model is based on deviations from normal behaviors which are defined by neither machine learning techniques not by training data. Yet, specifications are defined manually and describe what normal behavior is and monitor any action with respect to these 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.

2 Related Works

In previous works, and as we consider proposing hybrid HIDS system, there are some proposed hybrid schemes integrated for clustered sensor networks.

In [16] a detection system is proposed for WSN. To get an hybrid model, the combined version of Cluster-based and Rule-based intrusion detection techniques is used and eventually evaluated the performance of intrusion detection using hybrid technique and detection graph shows ratings like attack rating, data rating and detection net rating with the attack name and performs better in terms of energy, but the model proposed still weak and it can not detect new intrusions.

In [15], Su et al. proposed energy efficient hybrid intrusion prohibition system for CWSNs. They use intrusion detection and intrusion prevention techniques to get an hybrid security system. Their system contains collaboration-based intrusion detection subsystem which uses cluster head monitoring and member node monitoring. In this scheme, member nodes monitor the cluster heads and the cluster heads monitor their own cluster members by using alarm table and HMAC. This scheme can detects the intruder in case of member nodes are monitors, but when cluster nodes are monitors, the scheme fail because of using the only shared key between cluster head and member node.

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

Yan et al. proposed hierarchical IDS (CHIDS) based on clusters. The authors took advantage of this approach and install on each cluster-head an IDS agent (core defense). This agent contains three modules: a supervised learning module, an anomaly detection module based on the rules and decision-making module. The simulation results showed that this model has a high detection rate and lower false positive rate. But, his main disadvantages of this scheme is: The IDS node is static (runs only in the cluster-head), in this case the intruder uses all his strength to attack this hot element and subsequently disrupts the network. The implementation of this detection mechanism requires many calculations in cluster-heads, and that can decrease the network lifetime.

Hai et al. 4 proposed a hybrid, lightweight intrusion detection system integrated for sensor networks (SN), using the scheme of Roman et al. [5]. Intrusion detection scheme takes 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 (both agents are in the same node). 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] 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. implemented a lightweight Framework for securing WSN that combines the advantages of cryptography and IDS technology in order to detect the most dangerous network attacks, and provide a trust environment based on clusters. The results show that the model performs well in terms of detection rate, and generates high overhead and energy consumption.

Yassine Maleh et al. implemented a hybrid, lightweight intrusion detection model integrated for sensor networks, intrusion using cluster-based architecture. This model uses anomaly detection based on support vector machine (SVM) algorithm and some of signature rules. 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.

3 Proposed Hybrid IDS

The proposed model contains specification based technique, signatures based technique using some fixed rules representing most dangerous attacks in Wireless Sensor Network, and anomaly detection based on SVM technique, which is designed to confirm

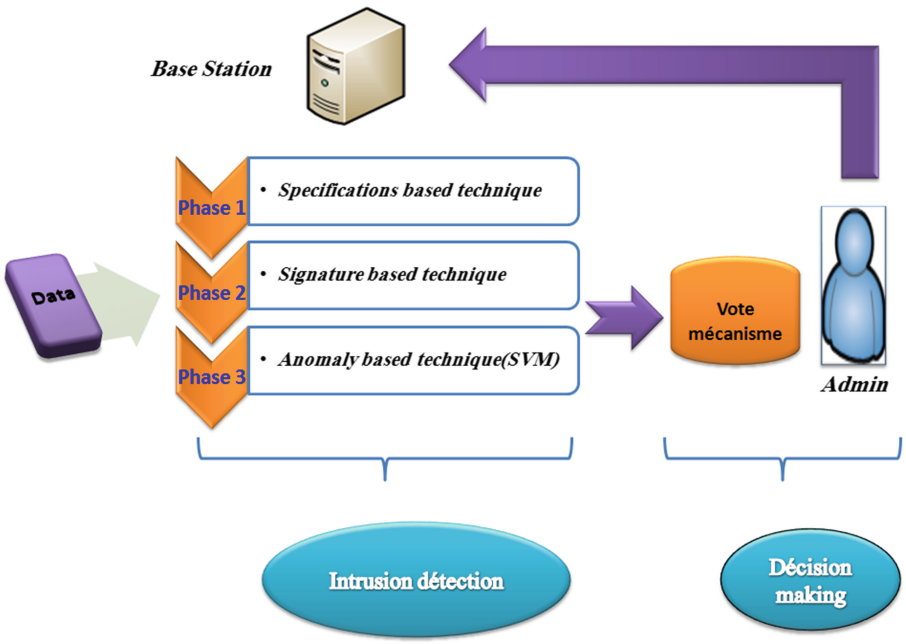

Fig. 3. Architecture of proposed hybrid IDS.

the malicious behavior of a target identified by behavior detection technique, and analyze data for classification (Fig. 3).

3.1 Intrusion Detection Used Techniques

Phase1: 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 test to determine if an instance belongs to this model or not. The bodies that have a low probability of being generated from the learned model 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 Non 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.

Phase2: Anomaly Detection Using SVM

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

Support Vector Machines

Support vector machines are a set of supervised learning techniques used for classification of network behavior. The aim of SVM classifier is to determine a set of vectors called support vectors to construct a hyperplane in the feature spaces. In our context, a distributed binary classifier to normal and abnormal, which permits detection of every malicious act.

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

$\sum_{i=1}^{n}\varepsilon_i$ is the constraints on the learning vectors, and C is a constant that controls the trade off between number of misclassifications and the margin maximization (Fig. 4).

The Eq. (1) can be deal by using the Lagrange multiplier [17]:

Classification hyperplane Given the training datasets,

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

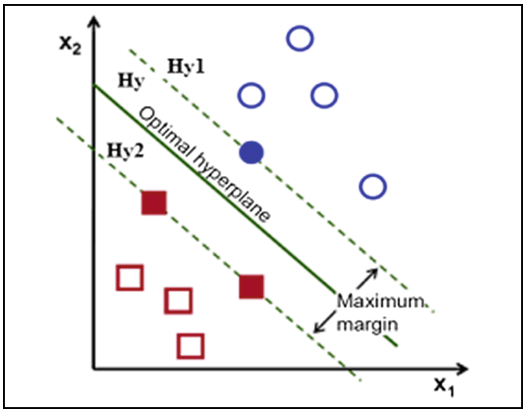

Fig. 4. Hyperplane

We want to find the hyperplane that have a maximum margin:

$$W \,.\, x = b$$

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

$$\begin{aligned} &\textit{maximise } l(\alpha) = \sum_{i=1}^{n} \alpha_i - \tfrac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \alpha_j y_i y_j k\left(x_j, x_i\right) \\ &\textit{subject to} \sum_{i=1}^{n} y_i \alpha_i = 0, \textit{ and } 0 \le \alpha_i \le C \textit{ for all } 1 \le i \le n \end{aligned} \tag{2}$$

$K(x_j,x_i)$ 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 Eq. (2) is found, we get [17]:

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

Thus the decision function is written as:

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

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].

Phase 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 (greater than threshold δissrbh). Finally, the rule to detect the wormholes attack is the power signal (above the threshold δissrhwh).

Phase 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 reports 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.

3.2 Network Structure and IDS Agents Location Process

(A) Structure of the network:

As mentioned before, the detection approach uses cluster-based topology to decrease the quantity of packets forwarded through the network while 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 trough 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 (Fig. 5).

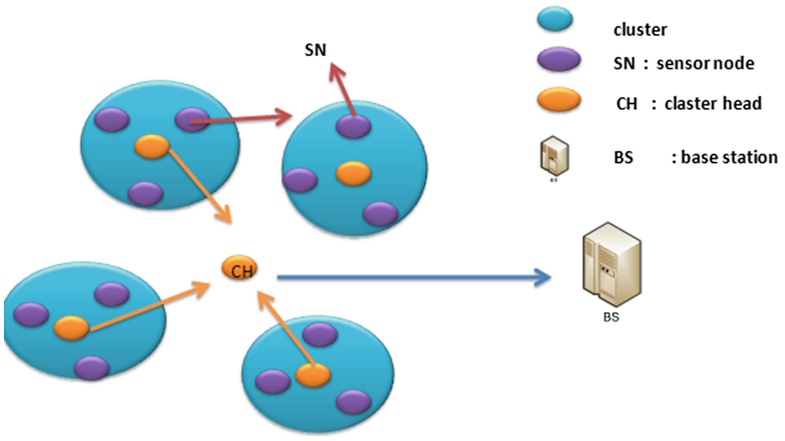

Fig. 5. Network Structure

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 obtained value, Base station calculates the average value and average deviation. Then CH is elected dynamically according to his residual energy.

CH starts the CH election procedure for nodes. Old CH broadcasts a message about the withdrawal of authority. New CH sends alert messages to the member nodes. CH is responsible for authentication of the other members of the cluster, and the base station is responsible for CH authentication. Because of limited battery life and resources, each agent is only active when needed [24].

(B) IDS location process

In this proposed scheme, an IDS [26] agent is located in every sensor node. Each cluster contains two kinds of agents: local IDS agent and global IDS agent. Because of the limited battery life and 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 cluster-head and the base station. 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. When the cluster-head transmits the data to the mobile sink, the energy of the cluster-head is reduced [11, 12].

Figure 6 below describes the process of IDS agents location in network.

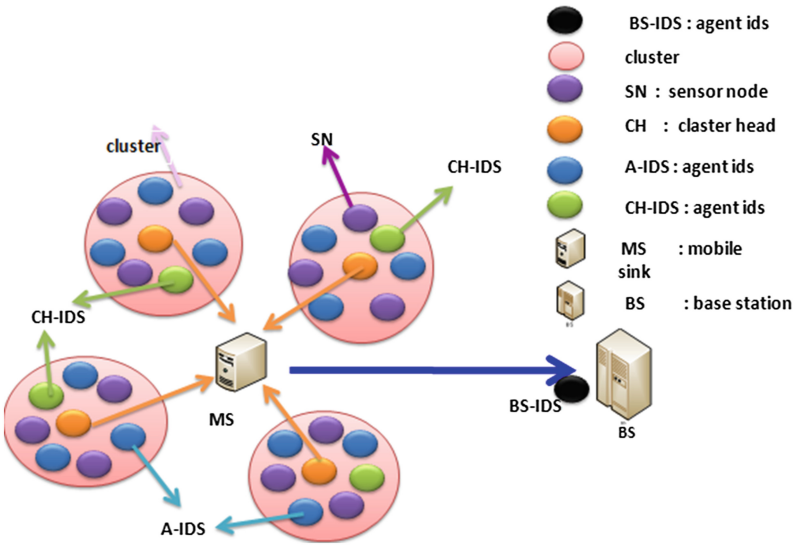

Fig. 6. Location of IDS in wireless sensor network

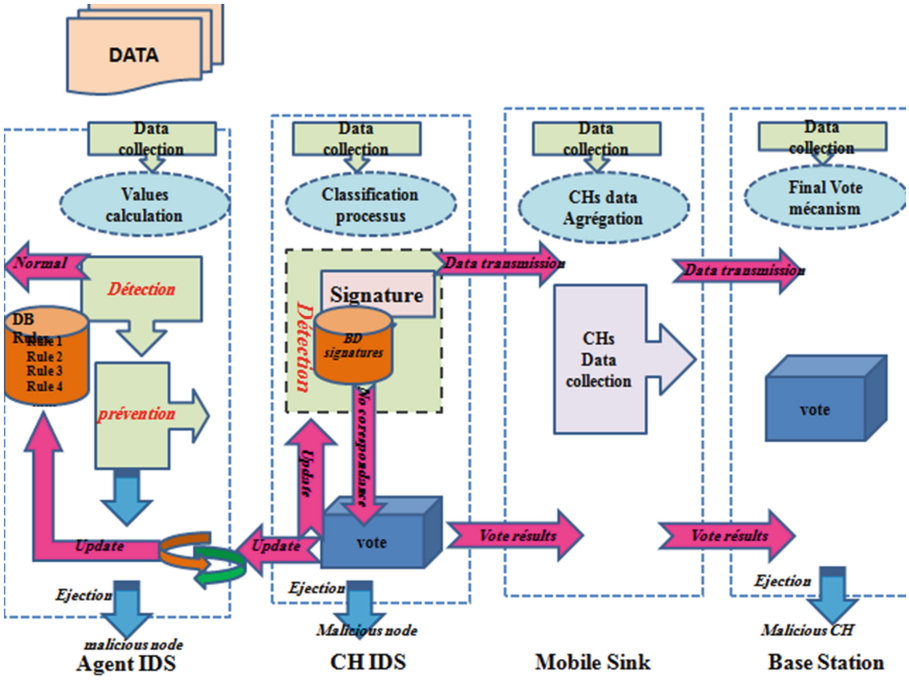

Fig. 7. Process of detection between WSN IDS agents components

In this hybrid IDS architecture, and by using hierarchical architecture, Our aim is to utilize cluster-based protocols in energy saving, to reduce computational resources and data transmission redundancy. In this context, we propose an intrusion framework based information sharing (Fig. 7).

- Intrusion detection at Member nodes:

Data Collection modules, and intrusion detection are in general, the principal components in this type of agent.

1. Data Collection Module:
   Is responsible to collect the information sent, received and forwarded by sensor. This node stores in his database id of the node analyzed and compute values of some parameters such Energy, NPD, NPS, RSSI, NRM, JITTER… in every node.
2. 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.

- Intrusion detection at CHs:

Proposed clustering algorithm chose for each cluster, the CH that has more power resources to manage and aggregate data from cluster members. This powerful node is composed of 3 modules:

1. Data Collection Module:
   Is responsible of collecting packets sent by the IDS agent. This message includes 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 behaviour 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}

}
```

2. 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 (Sect. 3. phase 3), then transmitted to the abnormality detection module for learning and classification process.

3. Voting mechanism:

Regarding collaborative process, the cluster-head uses the voting mechanism. if there is no correspondence 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 appropriate rule of this new intrusion detected. 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 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

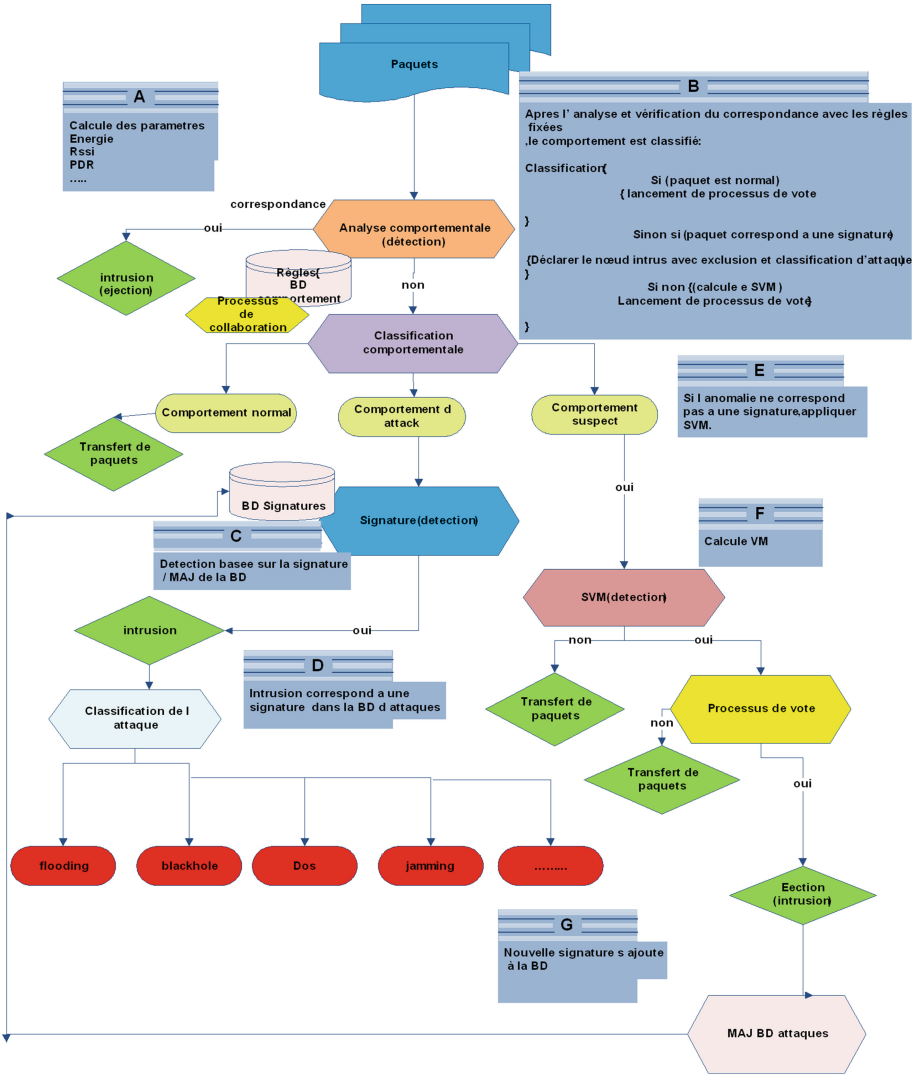

Fig. 8. Structure of the proposed intrusion detection model

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 base station for a monitoring process.

- Intrusion detection at Base station:

The CH monitoring sends to the base station a report of intrusion, includes the CH suspect, if exist, and the type of attack detected. The base station performs a polling mechanism to identify malicious nodes. In the case where more than ½ of the votes are in favor of the attack, the CH is excluded from the sensors network and a new CH is elected (Fig. 8).

3.3 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 cluster head. The older ones are designated as ordinary. Then new IDSs election depends on the residual energy and the placement strategies suggested by Khalil et al. new IDS nodes are elected, they compute locally the SVN and the distributed algorithm for training SVMs is performed as alluded above. This can protect the network from energy depletion and prolonging the network lifetime.

4 Experimental Evaluation

To evaluate the performance of the proposed hybrid IDSs. we have used the KDDcup'99 dataset [10] as the sample to verify the efficient of the hybrid detection mechanism and valid it by compare with one proposed by Abduvaliyev et al. [14] and Su and Chang [15]. [13] according to the false positive rate (false alarm), detection rate and energy generated by IDS agents, in order to determine the effectiveness of our scheme.

4.1 Dataset

The KDD 99 intrusion detection dataset is developed by MIT Lincoln Lab in 1998, each connection in the dataset has 41 features and it's categorized into five classes: normal and four attack behaviors (Dos, Probe, U2r, R2 l).

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:

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

$$False\ Positive\ Rate = \frac{Number\ \ of\ misclassified\ connections}{Number\ \ of\ \ normal\ \ connections} \times 100\%$$

$$\text{Total energy consumption } E_t = E_A + E_M$$

1 - Detection Rate: is the percentage of attacks detected on the total number of attacks;
2 - False positive rate (false alarms): is the ratio between the number classified as an anomaly on the total number of normal connections;
3 - Total energy consumption: it calculate the total amount of energy consumed in all nodes in the network.

4.2 Simulation Results

The sensor nodes are deployed in a randomized grid fashion, The network is composed of 10 clusters that contains 1–7 nodes over all the nodes 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 1 below (Fig. 9).

Table 1. Simulation parameters

Parameter	Value
Simulation time	900 s
Simulation area	100 *100 m
Number of nodes	100
Radio Model	Lossy
Number of cluster	10
IDS agents per cluster	1–7
Routing Protocol	HEED modifier
MAC	TDMA
Radio range	20 m
Initial energy	5 J
Power consumption for transmission	1.6 W
Power consumption for reception	1.2 W
Power consumption in idle state	1.15 W

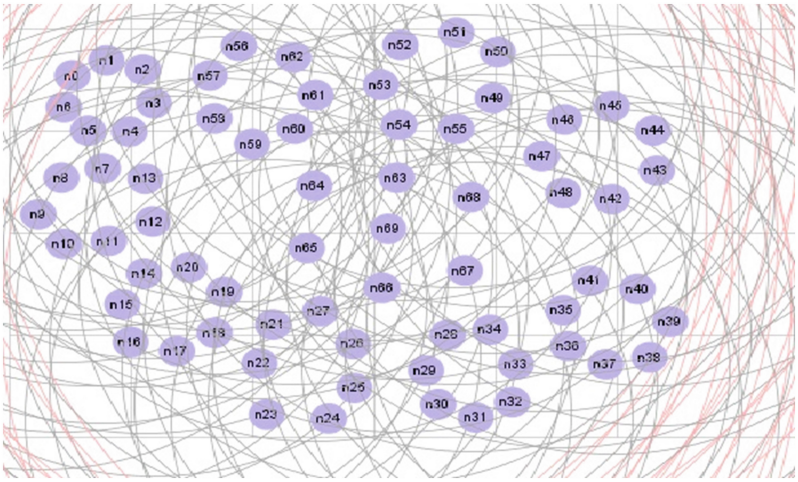

Fig. 9. Senario of 10 clusters

- ***Detection rate:***

The proposed scheme in Fig. 10, is effective when the number of 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 98.5% comparing to schemes proposed by Abduvaliyev et al., W.T. Su and K.M. Chang.

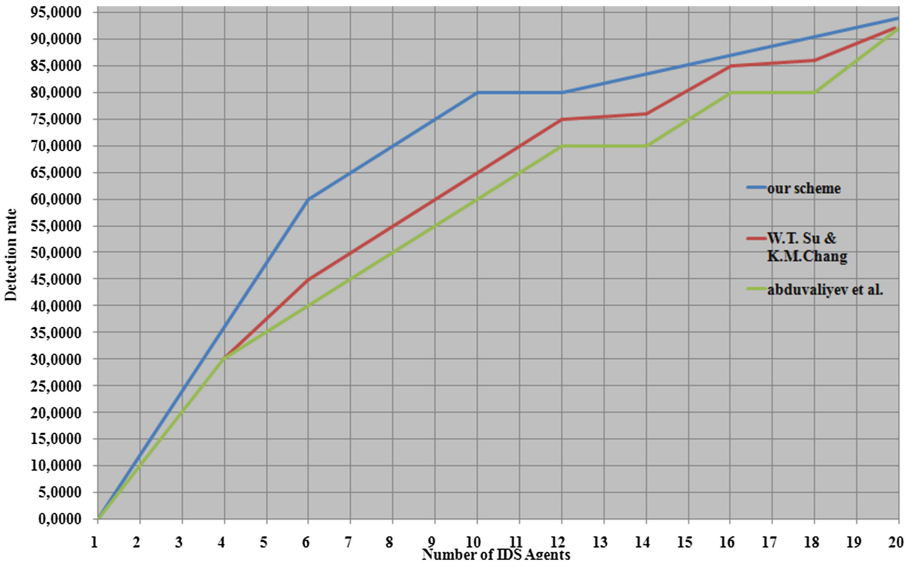

Fig. 10. Detection rate

- ***false positive rate***

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

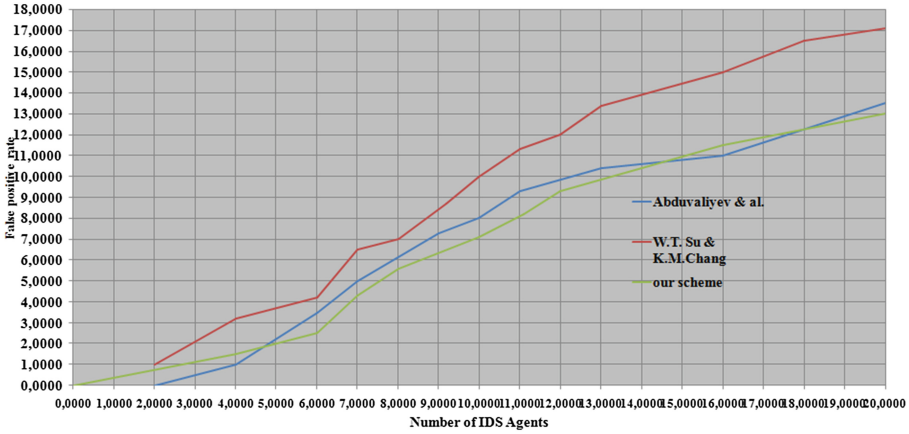

Fig. 11. False positive rate

- ***Energy Consumption***

Figure (12) illustrates the total amount of energy consumed in the network. 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 (j)

Detection and false positive rates were respectively of the order of 98.5% and 1.8%. As shown in Figs. (10) and (11) the two diagrams show a high detection rate with 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.

5 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, w**e** 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.

References

1. Houngbadji, T.: Réseaux ad hoc: système d'adressage et méthodes d'accessibilité aux donnée, Thesis 2009, école polytechnique de Montreal (2009)
2. Akyildiz, I.F., et al.: Wireless sensor networks: a survey. Comput. Netw. **38**, 393–422 (2002)
3. Karl, H., Willig, A.: A short survey of wireless sensor networks. IJCT (2004)
4. Strikos, A.A.: A full approach for intrusion detection in wireless sensor networks. School of Information and Communication Technology, March 2007
5. Mitchell, R., Chen, I.-R.: Department of Computer Science, Virginia Tech, Falls Church, VA 20191, United States 'A survey of intrusion detection in wireless network applications'. Comput. Commun. **42**, 1–23 (2014)
6. Masri, W.: Dérivation d'exigences de Qualité de Service dans les Réseaux de Capteurs Sans Fil sur TDMA, Thesis (2009)
7. Haboub, R., Ouzzif, M.: Secure and reliable routing in mobile Ad hoc networks. (IJCSES) (2012)
8. Moulad, L., Belhadaoui, H., Rifi, M.: Estc/Ensem UH2C Implementation of a security mechanism of WSN based on energy management. IJEAT (2013)

9. Prasanna Venkatesan, T.: An effective intrusion detection system for manets. Int. J. Comput. Appl. (IJCA) (0975–8887). International Conference on Advances in Computer Engineering and Applications (ICACEA-2014) at IMSEC, GZB
10. Sedjelmaci, H., Feham, M.: Novel hybrid intrusion detection system for clustered wireless sensor network. (IJNSA) **3**(4), July 2011
11. Huh, E.-N., Hai, T.H.: Lightweight intrusion detection for wireless sensor networks, Thesis (2009)
12. Maleh, Y., Iaeng, M., Ezzati, A.: Lightweight intrusion detection scheme for wireless sensor networks. IAENG, IJCS
13. Madhumathi, C.S.: Efficient cluster head selection and mobile sinks for cluster-based wireless sensor networks. Int. J. Sci. Eng. Res. (IJSER)
14. Abduvaliyev, A., Lee, S., Lee, Y.-K.: Energy efficient hybrid intrusion detection system for wireless sensor networks. In: 2010 International Conference on Electronics and Information Engineering, ICEIE 2010, Department of Computer Engineering, Kyung Hee University, Suwon, Korea (2010)
15. Su, W.T., Chang, K.M., Kuo, Y.H.: eHIP: an energy efficient hybrid intrusion prohibition system for cluster-based wireless sensor network. J. Comput. Netw. **51**, 1151–1168 (2007)
16. Deshmukh, R.: An intrusion detection using hybrid technique in cluster based wireless sensor network. J. Eng. Res. Appl. (IJERA) **3**(4), 2153–2161 (2013). ISSN: 2248–9622
17. Yan, K.Q., Wang, S.C., Wang, S.S., Liu, C.W.: Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network. In: Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology, China, pp. 114–118 (2010)
18. KDD Cup 1999 Data (1999). http://kdd.ics.uci.edu/databases/kddcup99/task.html
19. Nurtanio, I., Astuti, E.R., Purnama, I.K., Hariadi, M.: Classifying cyst and tumor lesion using support vector machine based on dental panoramic images texture features. IAENG Int. J. Comput. Sci. **40**(1), 29–37 (2013)
20. Yuan, L., Parker, L.E.: Intruder detection using a wireless sensor network with an intelligent mobile robot response. IEEE Southeastcon **1**, 37–42 (2008)
21. Patel, M., Aggrwal, A.: Security attacks in wireless sensor networks: a survey. In: International Conference on Intelligent Systems and Signal Processing, March 2013
22. Meena Kowshalya, A., Sukanya, A.: Cluster in algorithms for heterogeneous wireless sensor networks - a brief survey. Int. J. Ad Hoc Sensor Ubiquitous Comput. **2**(3), 57–69 (2011)
23. Hai, H., Khan, F., Huh, E.: Hybrid intrusion detection system for wireless sensor networks. LNCS, vol. 4706, pp. 383–396, August 2007
24. Maleh, Y., Ezzati, A.: Contributions to Security in Wireless Sensor Networks and Constrained Networks in Internet of Things, Thesis (2017)
25. Abduvaliyev, A., Pathan, A.K., Zhou, J., Roman, R., Wong, W.: On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. **15**(3) (2013)
26. Sedjelmaci, H., Senouci, S.M.: A lightweight hybrid security framework for wireless sensor networks. In: IEEE International Conference on Communications (ICC), vol. 1, pp. 3636–3641, June 2014
27. Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F., Dimitriou, T.: Cooperative intrusion detection in wireless sensor networks. LNCS, vol. 5432, pp. 263–278, February 2009