International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 11 No. 4 Jun. 2015, pp. 894-907

http://www.ijias.issr-journals.org/

Monitoring behavior-based Intrusion Detection System for 6loWPAN networks

Anass RGHIOUI, Anass KHANNOUS, and Mohammed BOUHORMA

Laboratory of Informatics, Systems and Telecommunications,
Faculty of Science and Technology of Tangier,
Abdelmalek Essaadi University,
Morocco

ABSTRACT: Even when 6LoWPAN has an ideal cryptography line defense, it is still necessary to implement an intrusion detection system (IDS) to deal with threats targeting network performance such as DoS attacks. IDS discover and stop most attacks that make changes on the operation of the network. However, few IDS solution has been proposed for 6LoWPAN networks. IDS missions are to monitor and raise an alarm about any possible threats and pass it to the system to restart the keying process for eliminating the attackers. New technique has been proposed recently based on the principle that neighbor nodes have a trend to have the same behavior, so the detection of the malicious node is based on the detection of the abnormal node that has a bad behavior different than it neighbors. The security goal is to provide a monitoring system that will attempt to detect anomalous malicious behavior and to prevent it from harming the network performance basing on the neighbors nodes behavior monitoring.

KEYWORDS: 6LoWPAN, RPL, IDS, Neighbor-based IDS, Security.

1 INTRODUCTION

One of the most important aspects to be taken into account when creating a 6LoWPAN network is setting the security mechanisms and maintain it. 6LoWPAN networks are inherently open to the attackers whose can eavesdrop the information exchanged within the network, or injecting false packets into the network.

It makes it more complicated the impossibility of application of current security systems used in today's networks, for several reasons, being limited resources and high consumption of energy, making it difficult to provide the protection systems of complex computations, which need high-performance resources and consume a lot of energy. Any proposal to resolve the terms of the security of 6LoWPAN network must take into account two factors; the need to use limited resources and the need for minimal consumption of energy, any proposal that consumes a lot of energy will be ineffective and sentenced to failure.

Among the complications is the ease to capture 6LoWPAN devices, because of their small size and their location in insecure places, so an attacker can steal their data, re-programmed and re-integrated them in the network as an intruder device to eavesdrop data or to damage the network. Generally, threats aim to introduce false information affecting the cost-effectiveness and quality of the network, or to tamper the functioning of the full network as a whole or a part of them as Denial of Service attacks. Attacks can be done via a malicious node, a powerful machine placed approximately to the 6LoWPAN, or remotely through the Internet.

A new approach to intrusion detection has recently been proposed for identifying malicious nodes in 6LoWPAN networks. It is based on the fact that nodes that are in the same neighborhood tend to have the same behavior, i.e. the same number of packets sent, received, and rejected, the same signal strength generated. A node is considered malicious if its behavior significantly differs from its neighbors in the same group. These techniques has many advantages as it does not require prior training, localized and capable of adapting to changing network dynamics, also, it has the most suitable mechanism for a total

Corresponding Author: Anass RGHIOUI

encrypted network as a node does not require to analyze its neighbors data to detect their behavior change. Moreover, some attacks in 6LoWPAN networks can be observed only by the neighbors of the malicious node [1]. The authors in [2] -[5] use this concept to detect a number of attacks in low power networks. In all these works, the IDS agents monitor their neighbors to detect internal attacks. Monitoring is to collect intrusion data from messages sent in their radio range, and then analyze these packets based on selected like packet-dropping rate, the number of transmitted packets and the strength of received signal, etc. However, the common disadvantages of these propositions are analyzing the signals from all the neighboring nodes, which leads to excessive energy consumption, and the strategy of the location of IDS agents in the network is an important aspect and has not been considered in these researches.

We propose an IDS solution adapted for 6LoWPAN networks. Our simulations and performance analysis shows that our solution provides security, and it is efficient in computation, communication, and storage. We give a preliminary study about IDS systems that are been proposed for resource-constrained networks, especially 6LoWPAN networks to choose the most adequate system to use it for 6LoWPAN networks. In addition, we propose an IDS system based on the preliminary study results and well adapted for 6LoWPAN networks.

The paper is structured as follow. Section 2 gives an overview of the challenges of the application of an IDS in a 6LoWPAN network, Section 3 discusses our proposed security model to deal with these challenges, and Section 4 presents a theoretical analysis and simulation tests of this model. Finally, Section 5 concludes the paper.

2 IDS : INTRUSION DETECTION SYSTEM

Before Unlike cryptography, the system has the ability to detect with high accuracy internal attacks. Cryptography protect the network only from outside attackers, a compromised node can launch attacks from inside and will not be detected as it is considered as legitimate node. Mainly 6LoWPAN's devices are weak secure and are deployed in non-secure wireless environment. In order to address this problem, an intrusion detection system must be used as a second line of defense and a wall against internal threats. This mechanism is used to detect abnormal or suspicious activities on the analyzed target and trigger an alarm when malicious behavior occurs. The cryptography mechanisms are not effective when protecting against insider threats, also it cannot defend against some external threats like a Denial of Service attack from the Internet to the 6LoWPAN network.

The main components of an IDS agent. IDS agent is installed in the application layer, it consists of three components (or modules). These components are defined as follows:

- Data Collection: this module is responsible for packet capture in the radio range of the node IDS.
- Intrusion Detection: IDS agent analyzes the captured packets in a policy based on detection. Among these policies, there's the signature-based detection of attacking and anomaly detection. These techniques will be detailed in the next chapters.
- Prevention: intrusion prevention is a set of tasks designed to anticipate and stop attacks. These tasks can be defined such as sending an alarm by the IDS to the base station, the latter subsequently ejects the suspect node of the network and apply the update key.

2.1 IDS IN A 6LOWPAN

The IDS solutions developed for ad hoc networks cannot be applied directly to 6LoWPAN networks, and this is due to the difference of these two types of networks [6]:

- In ad hoc networks, each node is typically handled by a human user. Unlike 6LoWPAN where all nodes are independent, these sensors send their collected at the base station data. The latter is usually controlled by a human user.
- Energy resources are more limited in the 6LoWPAN nodes compared to ad hoc nodes.
- The task of the 6LoWPAN network is very specific, for example the measurement of the temperature in an agricultural field. Therefore, the hardware modules and communication protocols must depend on the intended application.
- The density of nodes in 6LoWPAN networks is higher than in the ad hoc networks.

Thus, it is necessary to introduce a mechanism for detecting the own 6LoWPAN network intrusion.

2.2 IDS IMPLEMENTATION REQUIREMENTS

Much research in the application of the solution of IDSs in ad hoc networks have been done compared to 6LoWPAN networks, due to limited resources of 6LoWPAN nodes in terms of computing capabilities and communication. The design of an IDS solution for such networks should consider the following limitations [7]:

- Waste of energy: most of the energy consumed in a 6LoWPAN is mainly due to the communication interface, not the calculation process. Therefore, IDSs must preserve their transmission power and minimizing the data exchange between nodes.
- Distributed IDS: in 6LoWPANs, the base station cannot handle a large number of audit data (intrusion detection) from the network to detect any intrusion. In addition, the nodes cannot transmit a large number of packets because energy resources are not used optimally. This is due to a significant packet transmission to the base station. In this case, a distributed detection based on the cooperation of IDS agents is a desirable solution.
- No node is trustworthy: each IDS agent monitors its neighbors, based on the fact that even the IDS node can be malicious.
- Real time: to minimize the impact of a possible attack in critical applications, it is important that an IDS works in real time.
- Support adding new nodes: in practice, it is likely that new nodes can join the network after deployment thereof. The IDS must support this transaction and distinguish normal node from malicious node.
- Accuracy: the accuracy of an IDS in 6LoWPAN is another major problem. It can be defined as the ability of an IDS to determine whether the node in question is malicious or not.
- Availability: an IDS must run continuously and be transparent to users.

2.3 EVALUATION METRICS

To evaluate the effectiveness of any proposed IDS model, there is a set of metrics to be adopted to quantify the level of security and the best use of resources such as energy and storage. These performance indicators will enable a network administrator to choose the best intrusion system [8] and the optimization of the location of the agents in the IDS. Accordingly, the following metrics are considered important characteristics for effective design of IDSs in 6LoWPAN:

- Detection rates: represents the percentage of detecting attacks within the total number of attacks.
- False positives rate (false alarms): This is the ratio between the number of classified as an anomaly on the total number of normal connections normal connections.
- False negative rate: it is the opposite of the detection rate; this metric is defined as the ratio of false detections of attacks on the total number of attacks.

2.4 IDS AGENTS' LOCATION

An important criterion for achieving the IDS mechanisms in the 6LoWPAN is the location of its agents in this type of network. Many researchers have worked on this problem [9]–[11].

The network-based approach puts the IDS agent at the base station to receive and analyze data from monitored nodes. In this way, we benefit from the base station strong resources and its global vision of the entire network, which helps detect cooperation attacks. However, the disadvantage of this architecture is that it creates a lot of communication overhead and is not performing at detecting local attacks.

Otherwise, the host-based approach puts the IDS agents at each node, where each one of them has to monitor data, analyze it and decide for itself. The benefit of this approach is the reduction of monitored traffic. However, it puts more computational work on the node, which shortens its life by consuming its resources. One advantage of this approach is the ability to detect local attacks, but it lacks the global vision, which does not detect cooperation attacks.

There is another approach, the hierarchical approach [11]. It consists of combining the two previous solutions in the network. It places the IDS agents on three levels. The first is the level of the cluster members, which are used to control the behavior of their neighbors and collect audit data. These nodes have the ability to analyze their own data to identify malicious neighbors to isolate them. The second is the level of cluster-heads, which are used as coordinators to consolidate

audit data from their cluster nodes, analyze and make decisions to identify intrusions. The highest level is the base station, which collects data to monitor its cluster-heads and detects attacks across multiple clusters.

The main advantages of this architecture are the ability to detect distributed attacks and ensure scalability. Audit data collected from different points of view of the network also allows robust and fault-tolerant architecture [11]. The clustering architecture in 6LoWPAN is similar to the 6LoWPAN graph topology (RPL DODAG) [12] where the border router 6LBR is placed on the side of Internet and acts as a base station (Fig. 1). The border router is typically a wired device connected to the Internet so that it can be considered unlimited resource.

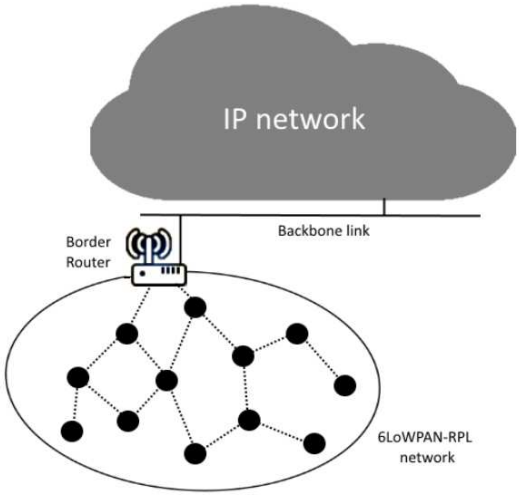

Fig. 1. 6LoWPAN-RPL network architecture

The DODAG roots will act as cluster heads for controlling operation of sensor nodes. Algorithms for attacks supervision in each DODAG will be slightly different because each uses a different objective function and follow DODAG varied routing rule. It is not in the clustering topology where cluster-heads implement the same algorithm. However, it does not affect cooperation between DODAG roots because the border router always has a global vision.

3 DISCUSSION

The IDS systems have become a very attractive research area for intrusion detection. Centralized intrusion detection systems are energy efficient as they are implemented in a powerful node (base station) [13]. However, this solution requires that all sensor nodes are required to submit their data to the base station, which introduce a high communication overload. On the other hand, systems of distributed intrusion detection provides detection performance slightly lower than the previous approaches because they use simple techniques and computationally light detection. In addition, the amount of information exchanged between the nodes is not important, unlike centralized model where all the nodes send their packets to a remote location; the distributed approach therefore is better adapted to the constraints of the resources of the 6LoWPAN devices.

The hierarchical architecture requires low energy consumption. Apply for a distributed intrusion detection in a topology based on clusters will result in a secure network solution that meets the requirements of 6LoWPAN nodes. Our research problem of IDS in the 6LoWPAN network resides on the use of specification-based intrusion detection agent and the location of these agents in the 6LoWPAN nodes. It is interesting to place the IDS agents optimally in the network to cover the entire network and have a global view of the sensor nodes. This leads to the detection of all packets generated by malicious attackers. We proposed and designed an IDS to counter the most threatening attacks for 6LoWPAN network.

The proposed security approach security is applied based on that all nodes in the same group have a similar behavior. We show the performance of our detection model simulation under Tossim and then by an experimental study. We evaluate its performance against several types of attacks. Specifically, we calculate the rate of detection, false positive rate, power consumption and time needed for IDS agents to detect attacks (average efficiency). According to the simulation results and experimental, our model has high accuracy of detection, low power consumption and a short time of detection.

4 PROPOSED SOLUTION

The Basics propositions from the papers that were a source of inspiration for this work are summarized in these solutions; the insider attacker detection scheme [2], the group-based intrusion detection scheme [3], the neighbor-based intrusion detection [4] and Intrusion detection framework of cluster-based wireless sensor network [5].

An IDS system for a 6LoWPAN network must satisfy the following properties: simplicity, full network coverage, utility and scalability. In other words, the system would cover all of the nodes in the network, is simple enough to run on limited devices to detect most attacks that would be designed for and it would be possible to implement new mechanisms to detect new types of attacks easily without having to rebuild the existing system.

We propose to build the IDS as powerful global IDS agent running on the border router and a lightweight agent running on each node. Global agent has access to information of all network nodes. On the other hand, the node's agents can operate with only the information from their neighbors. However, this information is very rich due to wireless nature of communication. Each node upon receiving any message should consider whether it is for the node itself or another node. Then, each node contains information about its neighborhood. For saving energy, it should be possible for a node to turn off its agent to reduce battery consumption.

Symptoms of selected attacks that pose risks of security must be integrated into the node agent detection component. Results of detections are organized in a database alert data. Nodes are marked as suspicious or malicious there. Finally, a cooperative component can be activated when the communication with other parts of the system or neighborhood is necessary.

The global agent consist of a data acquisition component that collects data from the received packets. These data are processed for further analysis. The processed data is stored using a statistical component. A detection component uses the information stored by the component of the statistics and analysis attacks symptoms.

Our intrusion detection system explores the spatial correlation of neighborhood activities and unlike other systems; it does not require prior training. The algorithm is localized, which means that information is exchanged only in the limited neighborhood. In addition, apart from the requirement of no prior training, is that it has a pattern that is generic, it is not related to a specific types of attacks. It can monitor many aspects of the behavior of the 6LoWPAN network at a time. The way this is achieved will be described in more detail in the following paragraphs. The basic idea is that in some areas neighboring nodes that are physically close to each other must be taken with the similar network traffic and provide similar values of their sensors. Then it is possible to watch all the attributes for some spatially correlated group of nodes and nominate these nodes, which differ significantly in some aspects as attackers.

We know in a wireless environment, a node *N* is able to listen to messages coming to its neighbor N_i no matter whether or not it is involved in the communication. The node *N* creates a model of network behavior of the node N_i as a q-component attribute vector

$$f(N_i) = (f_1(N_i); f_2(N_i); \dots; f_q(N_i))$$

with each component describing an N_i's activity in one aspect. The component f_j represents actual monitoring results of some behavioral aspect of the node N_i for each and fixed j. For example, it might be a measured value from the sensor, the number of dropped packets per burst period, packet delivery ratio per some period of time, etc. Behavioral aspects are chosen as appropriate and quantifiable properties, which represent statistics that are used to evaluate symptoms of attacks that should be detected by the IDS. The authors in [2], [3] assume that for any local area of normal sensor nodes N_i, all $f(N_i)$ follow the same multivariate normal distribution.

The data acquisition component of the node N gathers information from its neighborhood and creates the set

$$F(x) = f(f(N_i)) = f(f_1(N_i); f_2(N_i); \dots; f_q(N_i))$$

of attribute vectors, where $N(N)$ is the set of neighbors of the node N. This set of attributes is broadcast within the neighborhood $N(N)$ and is taken as a source of statistics for the detection component. This approach eliminates the need of the training phase and storing its results permanently in the database of the detection component of the IDS. In each period, the normal behavior of a node is defined as the "center" of the set $F(N)$.

Suspect intruders are considered as nodes, which are far from the "center" of the set $F(N)$ that the threshold θ. Details on calculating of this distance can be found in the cited papers, as well as determining the threshold θ. The final decision

about the suspect nodes in our solution is made in the level of the border router, this latter may invoke the MCU remote server for help. Different nodes mark the attacker on the basis of information from different neighborhoods. If a local IDS agent finds a suspect, it alerts the entire group with a warning message about the node. If there are more such messages, the entire group wakes up and all of the nodes monitor the proposed malicious node. If abnormal behavior is detected, the border router is alerted and the actual suspect node is blocked from routing tables until the final decision. The border router revoke a node if it is considered suspect by a majority of its neighbors, and it presents an attack and not just a malfunctioning, after that it's excluded from nodes routing tables, reported in the database alert and announced to the remote server.

4.1 IDS AGENTS' LOCATION

We propose a new concept detection to identify and prevent different types of attacks in sensor networks. This detection approach is based on specifications, but without the need for continuous updating of rules to maintain the intrusion detection system reliability. We used the concept screened by the works [2], [3] in a hierarchical topology based on DODAG. We adopt this method as we demonstrated in the previous chapters that the hierarchical topology is most suitable for 6LoWPAN networks using the RPL as the routing protocol. The following studies [2], [3] proved that the nodes that are in the same group or the same cluster tend to have the same behavior. Since the nodes in 6LoWPAN regrouped in DODAGs, we assume that the nodes are in the same group if they are physically close to each other and tend to have the same behavior. If we have an heterogeneous nodes distributed in the same network where they differ from each other even if they are physically close to each other, in the same DODAG we can make sub-groups of the nodes that are from the same type, i.e. the monitoring node collects audit data about its neighbors but only those from the same type. We have developed a new detection model based on this concept to detect the most dangerous attacks for 6LoWPAN. In the presence of several types of attacks, the proposed intrusion detection approach is evaluated using four metrics; the detection rate, the number of false positives, the average efficiency and the total consumed energy.

In what follows, we describe our detection proposition based on the concept of the normal distribution and detection rules for a set of behavioral change signs in a node. Our goal is to protect the network from attacks aimed at tampering it by detecting the anomaly of the malicious node whatever its type. Each node has an abnormal behavior must be suspect to be an intruder. The final decision should be made following statistical analysis that will confirm if the node is really an intruder or it just present a malfunctioning. The advantage of this approach that it provides flexibility by the detection of new attacks that were not defined by the standards, since it is not tied to a specific type of attack. Subsequently, we present the design of the proposed detection model and its operating principle.

4.2 INTRUSION DETECTION TECHNIQUES

Solutions that adopt the concept of neighbor monitoring are based on the determination of the threshold by calculating the mean of the observed phenomena, which means that the node has compared a given phenomenon generated by its neighbor node with a definite value. The result of this comparison is not exact since the phenomenon is a variable that can take a correct value in a large field, more or less than the calculated mean. This explains the high rate of false negative in these solutions. To deal with that, we adopt a new detection techniques based on the concept of the normal distribution (Gaussian distribution) proposed by [5] to detect attacks and allow a normal functioning of the 6LoWPAN network.

An observed value can be considered as random and normally distributed. The mean of the normal distribution is then considered as the real value of the observed value, the dispersion of the law then provides information on the error of observation. That is to say, it is possible to calculate an approximate value of the probability that a variable following a normal distribution is in a around the mean .This is to obtain an approximation of the value of indicator observed by considering errors due to changes in the environment or a malfunction.

In a concept of normal distribution, the mean μ and standard deviation σ of the data are calculated. This data is properly distributed if they are within three standard deviations from the average. In our approach, we assume that all nodes that are located in the same DODAG have the same behavior. Therefore, a node is considered an attacker if its behavior differs from its neighbor in the same DODAG.

4.2.1 ATTACKS INDICATORS

We focus in our study about the most known attacks that can be detected by surveying the communications between the nodes and that are detectable only by an IDS. We was based in our study on [14]-[16] to determine the indicators of these attacks in order to determine the parameters to be monitored. We describe in what follows the main indicators.

- Sending ratio (SR): number of packets sent by a node N.
- Reception ratio (RcR): number of packets received by a node N.
- Forwarding ratio (FR): number of packets received by a node N and forwarded by this node to their destination.
- Retransmission ratio (RtR): number of retransmission of the same packet by a node N.

Each indicator shows its efficiency only in protecting the network from one or some attacks but not all, this why each node must take them all in consideration. Wherever there is other indicators, but a 6LoWPAN node cannot monitor them all because it is limited in resources. Therefore, the IDS needs to prioritize the attacks depending on the scenario. Our approach is based on cooperation between the chosen indicators to monitor all these priority threats.

4.2.2 BEHAVIOUR MONITORING

Behavior monitoring of a node $N_i$by IDS agent is modeled by the following function:

$$f(N_i) = (f_1(N_i); f_2(N_i); \dots; f_q(N_i))$$

where q is the number of monitored behavior defined by:

$$f_1(N_i) = \mathrm{SR}$$
$$f_2(N_i) = \mathrm{RcR}$$
$$f_3(N_i) = \mathrm{FR}$$
$$f_4(N_i) = \mathrm{RtR}$$

All of these behaviors follow the same multivariate normal distribution in any local area within the DODAG. All values associated with these indicators are in the range of three standard deviations around their mean values. The writing normal distribution function is

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}}\ \mathrm{e}^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}.$$

To determine whether the nodes within the same DODAG have the same behavior, the standard deviation σ and the Euclidean distance E of the indicators must be calculated. Each IDS agent calculates the standard deviation of the set $f_m(N_i), \dots, f_m(N_n), i = 1, \dots, n\}$, where n is the number of monitored nodes by this agent and m is the selected behavior.

$$\sigma(f_m(N)) = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(f_m(N_i) - \mu\, f_m(N))^2}$$

When σ is above a certain threshold θ, the IDS finds that monitored nodes could be an attacker. To determine the node that has a malicious behavior, the IDS agent calculates the E of $f_m(N_i)$ in the center of the set $f_m(N_i), \dots, f_m(N_n)$, given by calculating the mean μ of its components. When *E* is above a certain threshold θ, the node is considered as an attacker.

$$E\big(f_m(N)\big) = f_m(N_i) - \mu(f_m(N))$$

Knowing that: $\mu\,(f_m(N)) = \sum_{i=1}^{n}\frac{f_m(N_i)}{n}$

Our goal in this solution is to provide a reliable mechanism for detecting intrusion in terms of attack detection and lightweight in terms of computation process and communication, i.e. obtaining a low overhead. Therefore, our detection mechanism is mainly based on the concept that all nodes in the same DODAG should have similar behaviors. These behaviors are represented by the noted indicators previously described. In our solution, we used a hierarchical architecture based on the DODAG topology.

4.3 INTRUSION DETECTION TECHNIQUES

In our scheme, each node has the ability to enable its intrusion detection agent. When a node performs the heavy calculations, it can disable detection to conserve energy for a while. For the analysis and detection process, we propose two detection agents: node IDS N_{IDS} and global IDS G_{IDS}, located respectively at the nodes and the border router. The first applies a detection based on the behavior of neighbors to identify malicious nodes. The second aims to reduce the number of false positives that occurred when the N_{IDS} agents suspects a normal node as an attacker.

4.3.1 NODE IDS (N_{IDS})

The strategy of the location of N_{IDS} agents in the network is a very important point, since the increase of the number of agents in a network leads to a communication and calculation overhead, and therefore a decrease in the lifetime of the network. Our solution is that each node is monitored by its one-hop neighbors in the DODAG as they are intended by its messages and because they are in its radio range. Therefore, this strategy leads to detect all malicious nodes with low overhead.

The N_{IDS} has the following missions:

- Data collection: it is responsible for collecting packets in the radio range of N_{IDS}, storing the physical address of the analyzed node and calculating indicators behavior, is related to each node.
- Detection: it aims to implement the policy of detection based on the fact that in each DODAG, the indicators behaviors should follow normal distributions. The N_{IDS} agent monitors its one-hop neighbors by calculating the standard deviation and the Euclidean distance of their behavior.
- Prevention: when abnormal behavior occurs, the N_{IDS} off an alarm as a message to the G_{IDS}, so that it can confirm the malicious nature of the suspected node. This alarm message includes the suspect node (physical address) and detected attack type. In this case, the N_{IDS} receiving such a message will trigger an alarm counter. When this counter reaches a certain threshold θ, the N_{IDS} will make a final decision.

4.3.2 GLOBAL IDS (G_{IDS})

Each G_{IDS} agent has the following missions:

- Data collection: it receives an alarm message from N_{IDS} agents. This message contains the suspect node and detected attack type.
- Decision: N_{IDS} stores the address of the suspect node in a database (blacklist) and increases a specific counter of malicious nodes. The latter is calculated as the number of times N_{IDS} agents within the same DODAG identifies a node as malicious. When this counter exceeds a threshold θ, the corresponding node will be ejected from the network. When the N_{IDS} identifies a node as normal and the N_{IDS} agent detects it as malicious one, the N_{IDS} stores the address of the N_{IDS} in a blacklist and the counter associated with this agent is increased. When this counter exceeds the threshold θ, this N_{IDS} will be designated as the intruder who tries to tamper the network by false information, it will be ejected when the other N_{IDS} agents identify it as a malicious node and the N_{IDS} affirmed that decision.

4.3.3 COMMUNICATION ACTIVITIES BETWEEN IDS AGENTS

In 6LoWPAN networks, the communication process requires a large amount of energy compared to the process of calculation. Therefore, our detection approach aims to reduce the cost of communication between agents of intrusion detection to increase the lifetime of the network. This is achieved by minimizing the amount of information exchanged between N_{IDS} agents and between N_{IDS} and G_{IDS}. The N_{IDS} sends two types of messages: the first is for the G_{IDS}, the second to all N_{IDS} agents that are located on its radio range. They contain the address of the suspect node and the type of detected attack.

In addition, the mechanisms of cooperation between IDS agents can be classified into two approaches: Each IDS agent exchange intrusion data with other agents. This approach generates high communication load. Each IDS agent works with its neighbors agents to make a final decision about the suspect node (intruder or not). In this approach, the IDS agent only sends an alarm message to its neighbors, where the length of the message is much smaller compared to the previous approach, which indicates a low communication load. Accordingly, our detection scheme is based on this cooperative approach to detect malicious nodes with high accuracy and low power consumption.

Cooperative approach is used for the information exchange between IDS agents running of different nodes. When network density is low and there is not enough nodes monitored by a single IDS agent, it is helpful that an agent collaborates with its one-hop neighbors; the neighboring nodes exchange the information about the suspect nodes they have gathered. Alternatively, this can be done among nodes that are two or more hops away from each other, but we limit our solution to one-hop to reduce the number of monitored nodes and also, in order to reduce false alarms as some indicators may differ only if the monitor node is far from the other. The IDS agent would not extend the number of nodes it is monitoring but only refine the information about them.

The result of these cooperative information are sent to the G_{IDS}. These information will help it as data for its statistical technique that used for analyzing the relationship between the received alarms from the network N_{IDS} for potential threats. Evaluating only one indicator of a suspect node behavior can be seen normal in given range; but, evaluating alarm messages in a combined manner can indicate a threat.

4.4 INTRUSION DETECTION MODULES

In order to establish a system adapted to the distributed nature of 6LoWPANs networks, we have designed a distributed detection system. It locates nodes with abnormal functioning by listening to the traffic. After treatment, it decided to discard the package or transmit it to the next hop. Each node that receives a packet from its neighbor node, it treats it in two modules: local control and data collection. The local control module verifies the legitimacy of the neighboring node sending the message. If this is the case, that mean that sending node is not reported malicious, the node processes the packet and perform other normal tasks. At the same time, the data collection module interprets the header information to be used by the intrusion detection system. The interval of the threshold already determined, if the result of the treatment is different from the predicted value, an alarm is generated, the node is declared abnormal and action must be taken to detect if it is malicious or just a dysfunction.

4.4.1 LOCAL CONTROL

The local control unit the audit engagement and validation of received packets. It verifies the identity of the sender and decides to reject the package or transmit to treatment. This module listens systematically all communications that took place in the radio field. He decides for each packet to treat or reject it. It deals only with packets received from neighboring nodes to a jump, so his children or his parents. The intrusion detection processing will take place only if the sending node belongs to this category, and it is not reported as malicious.

4.4.2 DATA COLLECTION

Generally, sensor nodes listen jumble communication exchanged between neighboring nodes residing in its radio range. Since 6LoWPANs nodes have very limited memory and storage space, the data collection unit will not store data, it will be limited to listening to the data and transmit them to the processing unit. This unit acquired the information required by interpreting the header. The detection strategy is applied once the data is being processed. If the result shows a different level of the predicted value, an alert is issued. After collaboration with neighboring nodes, the local agent says the node as normal or abnormal. Results are sent after the overall agent to determine if the node is malicious to take the necessary measures against him.

4.4.2.1 INTRUSION DETECTION

A number of rules have been chosen to detect a variety of attacks that are determined by the established indicators to set their thresholds after the normal execution of the 6LoWPAN network. As explained in previous sections, the threshold values are set using the normal distribution. These rules are represented as follows:

- Low: if the value of the result is below the minimum ”$\mu - \sigma$”, in the case where he has an attack pattern.
- High: if the value of the result is greater than the maximum threshold ”$\mu + \sigma$”, if it has any attack pattern.
- Normal: if the value is between the minimum and the maximum threshold, but it shows no attack pattern.

5 EVALUATION

5.1 INTRUSION PERFORMANCE EVALUATION

In our study, we use the TelosB in Tossim simulator as we did on the previous simulations of the security keys establishment, in order to evaluate the performance of our model in terms of the detection rate of true positive and false positive rates. IDS works well should have a false positive rate near to 0% and a very high rate of detection rate. According to these metrics, we determined the optimal detection thresholds for each attack (relative to the standard deviation and the Euclidean distance) to meet the requirements of our target.

Subsequently, we simulated our model to assess experimentally the average efficiency resulted in the time required for IDS agents to detect all attacks in the network, the number of true positives and the number of false positives. In addition, we evaluated the total energy consumed during the execution of our model. In what follows, we present the simulation results of our detection model.

5.2 THE ATTACK SCENARIOS

A 6LoWPAN network can undergo several types of attacks as we studied in the previous chapters. In our solution, it is not intended for a specific attacks as explained, but our approach is based on the study of the normal operation of the network indicators, their disturbance will indicate the network exposure to an attack whatever this attack. A number of malicious nodes was randomly chosen from all scenarios. We chose to implement the most known and most dangerous attacks for the test; these attacks are ”hello flood”, ”blackhole” sinckhole ”,” wormhole ”,” selective forwarding ”,” crash ”and” jamming ”. The threshold is obtained after running the simulation for 15 times in each case.

5.2.1 SENDING RATIO

In a kind of attack, the attacker sends a large number of packets, so the sending rate among attackers nodes is high compared to others. Fig. 2 shows an analysis of the sending rate, we note that the average packet forwarding among attackers nodes is very large compared to normal nodes.

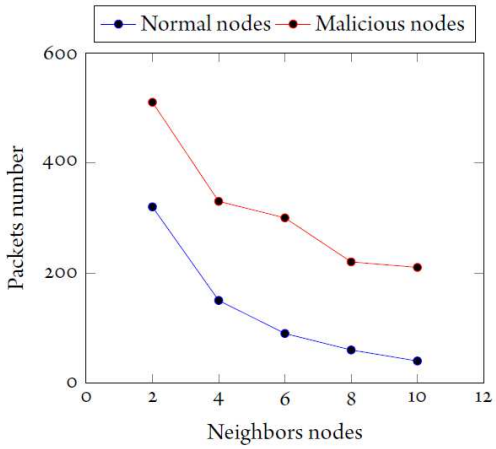

Fig. 2. Sending ratio

5.2.2 RECEPTION RATIO

In one type of attack, the attacker aims to get a large number of packages, so the receiving rate for this node has very high average. Note that the number of nodes was increased relative to other nodes. Fig. 3 shows an analysis of the rate of receipt of the network nodes; we see that the nodes that have been selected to carry out such attacks receives a greater number of packets than other nodes.

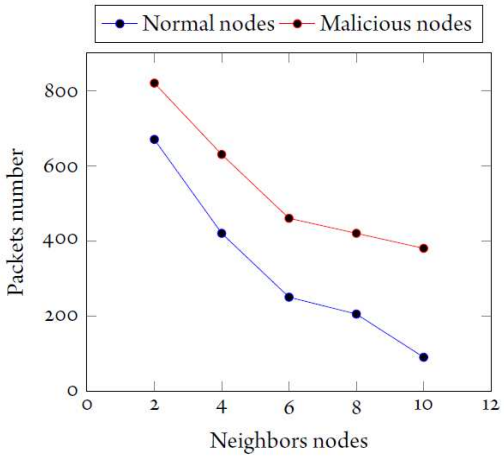

Fig. 3. Reception ratio

5.2.3 FORWARDING RATIO

There are attacks that aim to disrupt information exchanged in the network, like the non-forwarding of some packages, which generates false information. The attacking node records a lower average packet transfer to other nodes. Fig. 4 shows an analysis of the data rate; we note that the average forwarding of malicious nodes is less than that of other nodes.

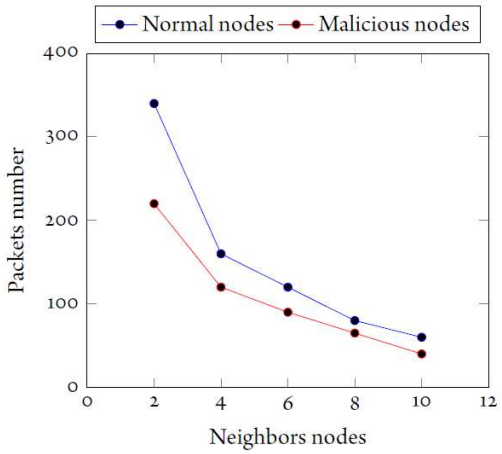

Fig. 4. Forwarding ratio

5.2.4 RETRANSMISSION RATIO

Unlike previous attacks, a kind of attack is to retransmit the same packet multiple times. Therefore, the transmission rate of the attackers is much more important than the other nodes. Fig 5 shows an analysis of the transmission rate; we note that the average retransmission among attacker nodes is more important than the other nodes.

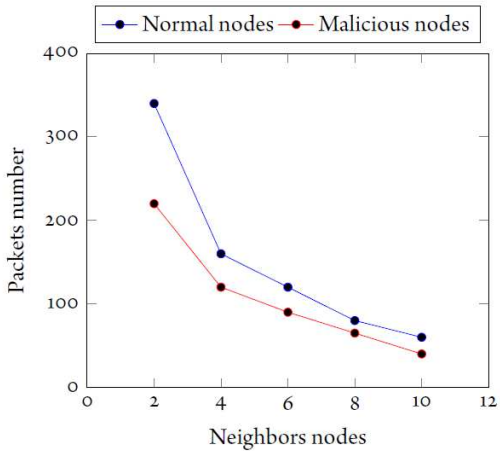

Fig. 5. Retransmission ratio

5.3 SIMULATION

We considered in the simulations of a network of sensors 40 static nodes deployed in a random manner in a square area of 100 x 100 m2. The simulation time was for 800 seconds. In the approach, where the NIDS agent determines in its radio coverage as an indicator of a neighboring node does not follow a normal distribution, the Euclidean distance on this behavior is calculated to detect the likely suspect node execute an attack. Our results show that IDS is running efficiently and accurately with a very low false positive rate of less than 10% and a high of more than 90% true positive rate (Fig. 6). Moreover, nodes generally consume less energy. As illustrated in the IDS model performance graph, the detection rate is almost 94% when the number of nodes IDS is high (more than 10 agents). However, we have noticed an increase in energy consumption when the number of nodes exceeds 20 IDS agents.

The combination of the detection based on indicators and the collaboration between nodes allows the model intrusion detection to achieve a high rate intrusion detection with a very small number of false alarms, when the number of IDS is large (i.e. greater than 10 agents). Thus, the use of our approach based on the normal distribution for intrusion detection can meet the requirement of the application in terms of detection rates of attacks and number of false alarms generated by IDS agents.

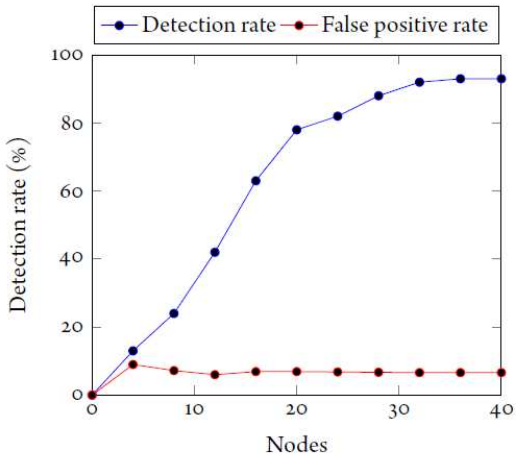

Fig. 6. Detection rate

5.4 ENERGY CONSUMPTION

About the energy, from energy consumption graph, it is clear that our detection model has low power consumption. This improvement is achieved by the fact that IDS agents generate a low charge of communication and computation (low overhead communication and computation). In addition, our detection modules involve energy consumption less than the

techniques proposed in previous work (Fig. 7), based on the core protocols of the 6LoWPAN network and limiting the number of monitored nodes, and the context of our application implies a low density of nodes, which also has impact on energy consumption. Yet our detection frame has been evaluated and it has been shown to be effective, even when the density of the network is high. Therefore, we can say that our model improves the detection of network lifetime.

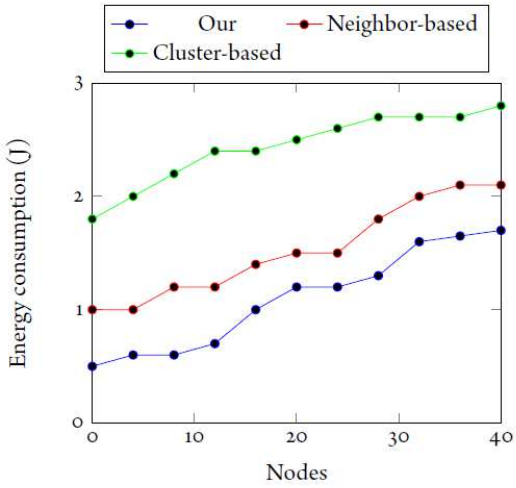

Fig. 7. Energy consumption evaluation

6 CONCLUSION

We proposed a new detection approach based on behavioral concept of neighboring nodes. This is based on the fact that the nodes that are in the same group have the same behavior. This is a new intrusion detection approach was recently proposed for the identification of malicious nodes in LoWPANs networks, it is based on the fact that the neighbor nodes tend to have the same behavior, that is to say, the same number of packets transmitted, received, and rejected, the same strength of the generated signal, etc. In addition, we have applied this concept to detect attacks that can cause significant damage in 6LoWPAN networks. In our approach, we assume that all nodes that are located in the same DODAG have the same behavior. Therefore, a node is considered an attacker if its behavior differs from its neighbor in the same DODAG.

We focus in our study about the most known attacks that can be detected by surveying the communications between the nodes and that are detectable only by an IDS. We determined the indicators of these attacks in order to determine the parameters to be monitored. Our IDS research problem in 6LoWPAN networks was in the use of intrusion detection policies by IDS agent and the location of these agents in the network nodes. In the first, two major detection techniques have been proposed in the literature; signature-based and anomaly-based detection. Each technique has advantages and disadvantages. Our idea was the use of the advantages of these techniques to counter attack with a maximum load limit of computing and communication generated by IDS agents. In the second point, we tried to place them optimally in the network to cover the entire network and have an overall view of the sensor nodes. This leads to the detection of all malicious packets generated by the attackers.

REFERENCES

[1] A. H. Farooqi and F. A. Khan, “Intrusion Detection Systems for Wireless Sensor Networks: A Survey,” in Communication and Networking, D. Ślęzak, T. Kim, A. C.-C. Chang, T. Vasilakos, M. Li, and K. Sakurai, Eds. Springer Berlin Heidelberg, 2009, pp. 234–241.

[2] I. Butun, S. D. Morgera, and R. Sankar, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks,” IEEE Commun. Surv. Tutor., vol. 16, no.1, pp. 266–282, 2014..

[3] F. Liu, X. Cheng, and D. Chen, “Insider Attacker Detection in Wireless Sensor Networks,” in IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications, 2007, pp. 1937–1945.

[4] G. Li, J. He, and Y. Fu, “Group-based intrusion detection system in wireless sensor networks,” Comput. Commun., vol. 31, no. 18, pp. 4324–4332, Dec. 2008.

[5] A. Stetsko, L. Folkman, and V. Matyáš, "Neighbor-Based Intrusion Detection for Wireless Sensor Networks," in 2010 6th International Conference on Wireless and Mobile Communications (ICWMC), 2010, pp. 420–425.
[6] H. Sedjelmaci, S.-M. Senouci, and M. Feham, "Intrusion detection framework of cluster-based wireless sensor network," in 2012 IEEE Symposium on Computers and Communications (ISCC), 2012, pp. 000893–000897.
[7] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in 3rd IEEE Consumer Communications and Networking Conference, 2006. CCNC 2006, 2006, vol. 1, pp. 640–644.
[8] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," in Proceedings of the 1st ACM International Workshop on Quality of Service; Security in Wireless and Mobile Networks, New York, NY, USA, 2005, pp. 16–23.
[9] A. Stetsko and V. Matyas, "Effectiveness Metrics for Intrusion Detection in Wireless Sensor Networks," in 2009 European Conference on Computer Network Defense (EC2ND), 2009, pp. 21–28.
[10] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty, "On optimal placement of intrusion detection modules in sensor networks," in First International Conference on Broadband Networks, 2004. BroadNets 2004. Proceedings, 2004, pp. 690–699.
[11] P. Techateerawat and A. Jennings, "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks," in 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops, 2006. WI-IAT 2006 Workshops, 2006, pp. 227–230.
[12] T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks."
[Online]. Available: https://tools.ietf.org/html/rfc6550.
[13] A. H. Farooqi and F. A. Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey," in Communication and Networking, D. Ślęzak, T. Kim, A. C.-C. Chang, T. Vasilakos, M. Li, and K. Sakurai, Eds. Springer Berlin Heidelberg, 2009, pp. 234–241.
[14] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Commun. Surv. Tutor., vol. 11, no. 4, pp. 42–56, Fourth 2009.
[15] M. K. G. Sharma Kalpana, "Wireless Sensor Networks: An Overview on its Security Threats," Int. J. Comput. Appl., 2010.
[16] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Comput., vol. 7, no. 1, pp. 74–81, Jan. 2008.