CROSS LAYER INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK

Djallel Eddine Boubiche[1] and Azeddine Bilami[2]

LaSTIC Laboratory, Department of Computer Sciences, UHL Batna, ALGERIA
dj.boubiche@gmail.com[1], abilami@yahoo.fr[2]

ABSTRACT

The wireless sensor networks (WSN) are particularly vulnerable to various attacks at different layers of the protocol stack. Many intrusion detection system (IDS) have been proposed to secure WSNs. But all these systems operate in a single layer of the OSI model, or do not consider the interaction and collaboration between these layers. Consequently these systems are mostly inefficient and would drain out the WSN. In this paper we propose a new intrusion detection system based on cross layer interaction between the network, Mac and physical layers. Indeed we have addressed the problem of intrusion detection in a different way in which the concept of cross layer is widely used leading to the birth of a new type of IDS. We have experimentally evaluated our system using the NS simulator to demonstrate its effectiveness in detecting different types of attacks at multiple layers of the OSI model.

KEYWORDS

Wireless sensor networks, Cross layer architecture, intrusion detection system, WSN security.

1. INTRODUCTION

Wireless sensor network (WSN) is an emerging technology that shows great promise for various applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks, which presents a demand for providing security mechanisms in the network.

Major challenge for employing an efficient security scheme comes from the resource constrained nature of WSNs like size of sensors, memory, processing power, battery power etc. and easy accessibility of wireless channels by good citizens and attackers. Currently, research on providing security solutions for WSNs has focused mainly on three categories:

1. Key management: A lot of work has been done [1] in establishing cryptographic keys between nodes to enable encryption and authentication.

2. Authentication and Secure Routing: Several protocols [2] have been proposed to protect information from being revealed to an unauthorized party and guarantee its integral delivery to the base station.

3. Secure services: Certain progress has been made in providing specialized secure services, like secure localization [3], secure aggregation [4] and secure time synchronization [5].

All mentioned security protocols are based on particular assumptions about the nature of attacks. If the attacker is “weak”, the protocol will achieve its security goal. This means that an intruder is prevented from breaking into a sensor network. If the attacker is “strong” (i.e., behaves more maliciously), there is a non-negligible probability that the adversary will break in.

DOI : 10.5121/ijnsa.2012.4203

Because of their resource constraints, sensor nodes usually cannot deal with very strong adversaries. So what is needed is a second line of defence: An Intrusion Detection System (IDS) that can detect a third party's attempts of exploiting possible insecurities and warn for malicious attacks, even if these attacks have not been experienced before.

An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of the wireless network system. Intrusion detection mechanisms can detect malicious intruders based on those anomalies. Intrusion detection system (IDS) attempts to monitor computer networks and systems, detecting possible intrusions in the network, and alerting users after intrusions had been detected, reconfiguring the network if this is possible [6], [7]. Usually, the neighbors of a malicious node are the first entities learning those abnormal behaviors. Therefore, it is convenient to let each node monitor its neighbors such that intrusion detection mechanisms can be triggered as soon as possible.

There are currently only a few studies in this area (Intrusion Detection System), in addition all of these studies propose layered security solutions. Indeed layered approach of security solutions tries to provide security either to all the layers which may be unnecessary or concentrate on just a single layer of the protocol stack. The following are the limitations of the layered security solutions:

- Layered approach can provide security services for only one layer. Moreover some of these layered solutions address a particular kind of attack only. For example: providing security solution in link layer without securing the physical layer which results in a WSN with a weak security provision [8].
- The above mentioned point doesn't mean that security is to be provided in each and every layer blindly. If it is done, such mechanism would drain out the WSN of all its limited resources like power, computation capacity, memory, battery life [9].

In this study, we emphasized that the layered approaches have noticeable shortcomings such as the redundancy and/or inflexibility of the security solutions, which made the layers security solutions often inefficient and inadequate. It was, however, beneficial to construct the security approach for the WSNs based on cross-layer interaction between all components in different layers of the protocol stack. Consequently, these new approaches surely gave a new direction towards the issue of security for wireless sensor networks.

In this paper new intrusion detection system is proposed. Our basic idea is the use of the cross layer interaction concept to detect different types of attacks on several layers of the OSI model. In our proposal, the MAC layer uses the cross layer information from network and physical layers in order to detect possible intrusions. Once intrusion is detected, various kinds of actions (like dropping a packet, flagging a neighbor etc.) can be taken. However in this paper we focus only on intrusion detection and hence do not discuss solutions to handle intrusions.

This paper is organized as follows: In Section 2, we briefly survey existing IDS. Then, we introduce a scope of our work in Section 3. In Section 4, we present our cross layer intrusion detection system. Finally, we evaluate the performances of our security solution in Section 5 and we conclude in Section 6.

2. RELATED WORK

Intrusion detection is an important aspect in the large domain of computer network security. Several studies have been proposed in this domain where most offer intrusion detection mechanisms dedicated to ad hoc networks. As a result they pay no attention to the constraints and limitations of WSNs. There is some research trying to adapt the solutions previously proposed to WSNs and propose new solutions dedicated for them.

Similar IDS systems proposed by Da Silva [10] and Onat et al. [11] contain certain monitor nodes in the network which are responsible of monitoring their neighbors, looking for intruders. They listen to messages in their radio range and use a buffer to store specific message fields that might be useful to an IDS system running within a sensor node, but no details are given concerning how this system works. In these architectures, there is no collaboration among the monitor nodes. Both papers lead to conclude that the buffer size is an important factor that greatly affects the rate of false alarms.

Two more IDSs for routing attacks in sensor networks are described by Loo et al. [12] and Bhuse and Gupta [13]. They assume in both papers that routing protocols for ad hoc networks can also be applied to WSNs: Loo et al. [12] assume the AODV (Ad hoc On-Demand Distance Vector) protocol while Bhuse and Gupta [13] use the DSDV and DSR protocols. Intruders' detection uses specific characteristics of these protocols like "number of route requests received". Though, to our knowledge, these routing protocols are not attractive for sensor networks.

Continuous monitoring may consume energy, which is not desirable in WSNs. consequently; a cluster-based detection approach for WSNs is proposed in Ref. [14]. In this approach, a network is divided into clusters. Each cluster head monitors its cluster members. All the members in a cluster are further divided into groups and the groups take turns to monitor the cluster head. The overall network energy cost is reduced because not all the sensor nodes keep monitoring.

Sinkhole attacks can be detected through the algorithm proposed by author in [15], even in presence of colluding nodes. The first step consists of finding a list of suspected nodes through estimating the attacked area. Authors assume that the base station has a rough understanding on the location of nodes, e.g. obtained through various localization mechanisms. Data inconsistencies can be detected by base station using the following statistical method. Let X1,... ,Xn be the sensing data collected in a sliding window, and X be their mean. Define f(Xj) as:

$$f(X_j) = \sqrt{\left(\frac{(xj - \bar{x})^2}{\bar{x}} \right)} \qquad (1)$$

Then, and if f(Xj) is greater than a certain threshold a node is suspected, since the data from this node is different from others in the same area. Henceforth, the position of the sinkhole is estimated by the base station which circles a potentially attacked area containing all suspected nodes. The radius of the circle is chosen to cover all suspected nodes.

Secondly, the intruder will be identified through analyzing the routing pattern in the affected area. In detail, a request message containing the IDs of all affected nodes is broadcasted by base station. A timestamp is included in a request signed with the private key of the base station to prevent replay attacks. The affected node replies with its own ID the ID of the next-hop node and the routing cost (e.g. hop-count) to that node on receiving the request. The reply message is sent along the reverse path in the broadcast, as the next-hop and routing cost could already be affected by the attack. At the base station, constructing a tree using the next-hop information allows to analyze the routing pattern. In a sinkhole attack, all network traffic flow towards the same destination which reveals the identity of the intruder.

Routing attacks in sensor networks are detected through a method presented in [16]. A clustering algorithm is used to build a model of normal traffic behavior. Abnormal traffic is detected thanks to this algorithm. Consequently, unseen attacks are detected using this approach, as it is not based on signatures. Power consumption is significantly reduces since the intrusion detection scheme does not require communication between sensor nodes. A wide range of routing attacks can be detected. In their approach, each node is equipped with IDS which should work independently and detect intrusions locally. No collaboration exists with other nodes. The node's own routing table and all packets the node received are the only information used. A set of twelve features to detect routing anomalies in a variety of routing protocols are identified by the authors.

An energy-efficient hybrid intrusion prohibition system (eHIP) was proposed in [17]. eHIP combines intrusion prevention and intrusion detection. The authors assume a cluster-based WSN, in which data is routed through the cluster heads to the sink. Two authentication mechanisms are used to prevent intrusions, one for control messages (such as routing messages) and the other for sensed data. To detect intrusion attack the authors implement a collaboration-based intrusion detection system to monitor cluster heads as well as member nodes. In cluster head monitoring, the member nodes cooperate to detect misbehavior, whereas the cluster head is responsible for monitoring the member nodes. The authors claim that attacks like packet dropping, packet duplicating, and packet jamming can be detected, but no details are given. Their simulation focuses on energy-efficiency and makes no statements about detection accuracy.

With using only partial and localized information, Krontiris et al. [18] design IDS to detect the blackhole and the selective forwarding attack. In order to detect the attacker, every node monitors its neighborhood and collaborates with its nearest neighbors. They can detect deviations from normal behavior by following a rule-based approach (rate of messages dropped above a certain threshold); the attacker node is identified, if more than half of the watchdog nodes raise an alert for this node. This approach is extended in [19], in order to detect sinkhole attacks.

In [20] is presented an insider attacker detection algorithm using only localized information. The spatial correlation existent among the networking behaviors of sensors in close proximity is explored by this algorithm. Similar communication and computation workloads should exist between neighboring sensors, in a typical sensor network. Malicious behavior is thus indicated through deviations from these characterises. In their approach, the behavior of the immediate neighbors is monitored by each sensor. The algorithm considers multiple attributes simultaneously in node behavior evaluation, without requiring prior knowledge of what normal/abnormal behavior is. If the behavior of a node is significantly different from that of nodes in the same neighborhood, it is considered malicious. In that case, a report is generated and sent to the base station.

In general, four phases compose the algorithm: first, collection of local information, second; filtering of collected data, third; identification of initial outliers using Mahalanobis distances, and fourth; applying of the majority vote to obtain a final list of outlying sensors. In order to remove falsified information by an attacker, it is necessary to filter the data. A trust value is then assigned to each neighbor in the range [0, 1], where a value closer to 1 indicates a higher possibility that the node is a normal sensor. According to the degree of the node's deviation from the neighborhood activities, the trust value is computed.

In [21] the authors propose a framework of a machine learning based intrusion detection system. An intrusion detection agent is implemented by each node to overhear the traffic of its neighbors, but there is no cooperation among nodes to detect attackers. The intrusion detection agent begins the detection process by detecting if the node itself is attacked. For this purpose a local Intrusion Detection Component (LIDC) was proposed to analyze local features (packet collision ratio, packet delivery waiting time, RTS packets rate, neighbor count, routing cost, power consumption rate, sensing reading report rate...).

To monitor the neighbor and find the attacker, the intrusion detection agent uses packet based Intrusion Detection Component (PIDC). The PIDC analyses and monitors: Distribution of packet type, packet received signal strength, sensing data arrival rate, sensing reading value changing ratio, RTS packets rate, packet drop ratio and packet retransmission rate. A rule-learner called SLIPPER [22] is used to build the detection model, they which is then used to classify observed traffic into normal and abnormal traffic.

Krontiris et al. [23], presents a more generalization of the collaboration of sensor nodes. Thus, the approach does not focus on specific attacks, but rather on cooperative techniques. The problem of intrusion detection is formally defined and necessary and sufficient conditions on the solvability of the cooperative intrusion detection are identified. However, only the case of a single attacker is investigated. The algorithm is lightweight enough to run on sensor node, which is demonstrated by their implementation.

A localized algorithm is proposed by Dimitriou and Giannetsos to detect wormhole attacks [24], which can always prevent wormholes. Connectivity information obtained from the underlying communication graph is analyzed in their approach. They assume some initial time interval, which is free of attacks and allows nodes to establish neighborhood information. A node executes a test to check whether it is safe to add the new id to its neighbor list as it receives a message with a new node id. This test tries to find a small path to the new node id which excludes all suspected nodes (nodes with an unseen node id are included in the list of suspected nodes). This link if it exists, allows the node to be part of the network. Thus, it might be the case, that a legitimate node is denied access to the network.

In [25] authors present a hybrid intrusion detection system, which represents a combination of centralized and decentralized IDS. In this architecture, intrusion detection is performed both locally and globally. Local agents running on every node and a central agent compose this architecture. The local agent analyzes packets routed through the node and tries to detect anomalies analyzed by local agent, which are reported to the central agent. Central agent receives the alerts which are then verified using a form of attack signatures. Local agents, who are in charge of taking further actions, receive response messages. The detail of how anomalies can be detected is not described by the authors.

Authors In [26] proposed an IDS base on clustered sensor networks and is able to detect several routing attacks, based on neighbor knowledge and routing rules. In their architecture, an IDS agent is contained in every node which belongs to a single cluster. There are two intrusion modules, a local and global IDS agent. Sent and received packets by the node are monitored by local agent. In addition, a list about malicious nodes in the network (blacklist) is kept. Communication of the neighboring nodes is monitored by the global agent. The overheard communication is checked using pre-defined and two-hop neighbor knowledge, and this to detect anomalies. The cluster head receives alerts, and decides if there is an attack or not. If the number of alerts concerning a specific node is greater than a certain threshold, this anomalous event is considered as attack. In that case, a blacklist update is sent to the nodes to isolate the attacker from the cluster. The selective forwarding, sinkhole, hello flood, and wormhole attacks are detected by the used pre-defined rules.

3. Scope of Our Work

3.1. Communication Model and Topology Assumptions

In our work we assume a hierarchical cluster-based network topology. This topology divides the network into several clusters, and selects as cluster head *(CH)* node which has the greatest energy reserves in the cluster.

We assume the same multi-hop routing protocol we proposed in [27], which consists to establish a chain of neighborhood nodes at each cluster. The base station is responsible of the formation of clusters, the election of CHs and the establishment of chains of node based on routing information (identifier, geographical position and energy reserve) sent by all nodes in the network. All the network nodes will transmit collected data to their CH through the chain of neighboring nodes. Then CHs take the responsibility of transmitting received data directly to the base station (BS), or indirectly through the neighboring CHs. Figure 1 shows the organization of the network.

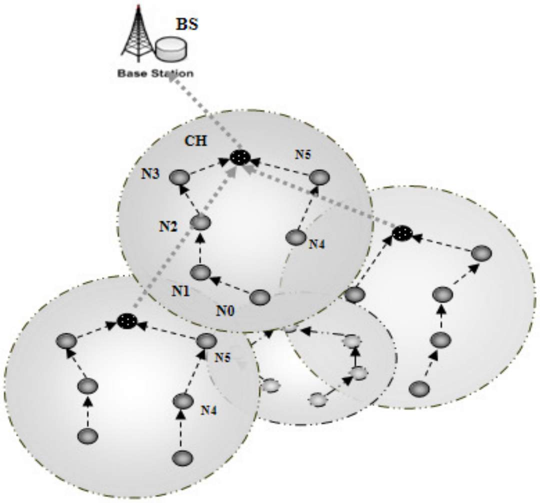


Figure 1.Chains cluster organization.

We used the SMAC protocol [28] to access the medium. To reduce energy consumption generated by the idle listening, nodes must periodically sleep. S-MAC also sets the radio to sleep during transmission of other nodes. We assume the use of RTS / CTS [29] mechanism in the process of data transmission. Source node initiates the process by sending a Request to Send frame (RTS) to the destination node. Then destination node replies with a Clear to Send frame (CTS).

3.2. Security Assumptions

We assume that communication between the network nodes and the base station is secured using security protocols based on symmetric keys. We opt for using the same protocol proposed in [30]. It consists on establishing keys following a pre-distributed approach which seems more appropriate for sensor networks. In this approach (secret) key information is distributed to all sensor nodes prior to deployment.

3.3. Description of the problem

Sensor networks are vulnerable to different types of attacks and intrusions. These can target several layers in the OSI model. The different solutions proposed in the previous section offer layered intrusion detection systems. Thus, they can detect an intrusion at the network layer without detecting it at the MAC or physical layer, which therefore makes these systems less effective. However, the implementation of a detection system for each layer can greatly increase the load (processing power, energy consumption ...) on sensor nodes.

To remedy this problem, we developed an intrusion detection system that operates on different layers of the OSI model. So instead of offering IDS for each layer, we have developed a single intrusion detection system that can detect different types of attacks on several layers of the OSI model. The following section describes its architecture and operating principle.

4. PROPOSED INTRUSION DETECTION SYSTEM

The proposed intrusion detection system is based on a cross layer architecture that exploits interaction and collaboration of three adjacent layers in the OSI model i.e. network, Mac and physical layers. The basic idea of our intrusion detection system is to detect intruders when they attempt to communicate with the network nodes.

After receiving RTS packets of the intruders node by the targeted node, our detection system checks if it is one of the neighbors in the routing path (by consulting the routing table at the network layer). In addition the authenticity of the intruder node will be checked by measuring the RSSI (Received Signal Strength Indicator) of the received packet (at the physical layer).

By using the routing information at the MAC layer, each sensor node can previously know the source of packets that will be received. Thus, any node trying to communicate (receive RTS or CTS packet) with the sensor nodes is immediately detected as an intruder if it is not included in the routing path.

When a node receives a packet, it is difficult to find out if the packet came from the claimed sender unless explicit authentication is used. V. Bhuse and A. Gupta [13] address this problem by using Received Signal Strength Indicator (RSSI). Recently proposed embedded operating systems like TinyOS [31] provide functionality to get the RSSI value. For wireless medium, received signal strength is related to the distance between nodes.

At the physical layer each node knows the signal strength of the packet sent by its neighbors (calculated previously by the base station). Therefore, the authenticity of the intruder node can be detected as the signal strength of the packets will not be equivalent to calculated RSSI. Then, by combining RSSI value with neighborhood routing table, the detection ability is significantly improved.

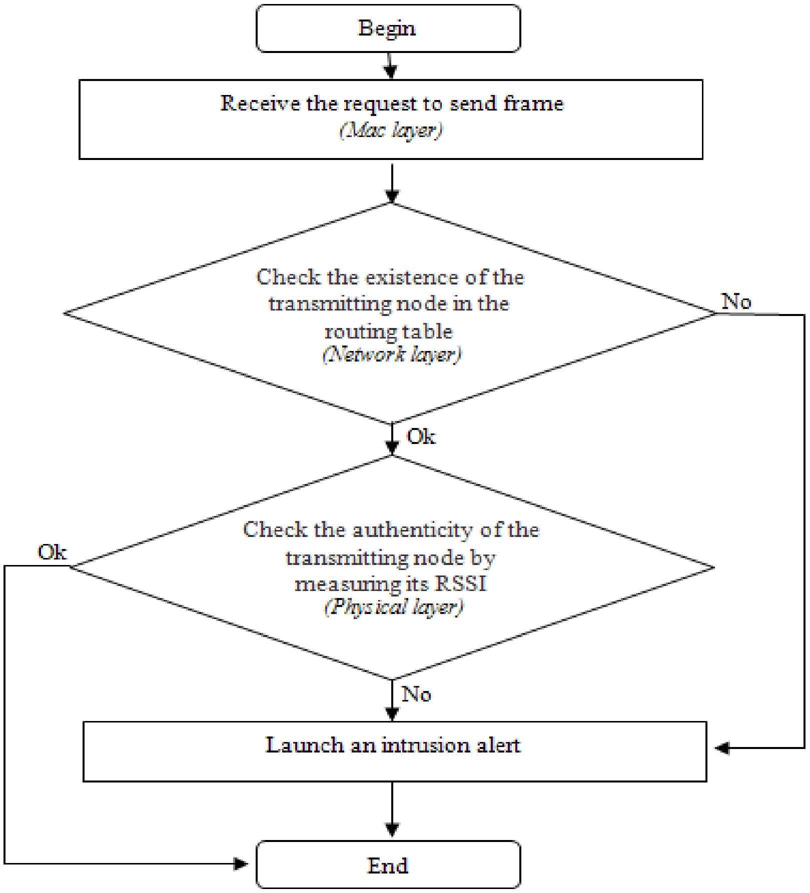

Begin
Receive the request to send frame
(Mac layer)
Check the existence of the transmitting node in the routing table
(Network layer)
No
Ok
Check the authenticity of the transmitting node by measuring its RSSI
(Physical layer)
Ok
No
Launch an intrusion alert
End

Figure 2.Algorithm of our proposed IDS.

The probability of detection of an intruder, P_{Det}, depends on two factors: number of attacked nodes in a cluster and probability of a missed detection of an attacked node. We defined *A* as the number of attacked nodes. In our IDS the intruder node can not be detected only if the attacked node doesn't receive any packet from the intruder node. Then the probability of a missed detection is equivalent to the probability of a collision occurring in a transmission link P_{Col}

By using the Binomial rule we can define the probability of detection of an intruder as:

$$P_{Det}= \binom{A}{1}(1- P_{Col})\, P_{Col}^{\,A-1} \qquad (2)$$

Basing on equation 2 we can calculate the probability of detecting X intruder in the network:

$$P_{Det}= \binom{A}{X}(1- P_{Col})^{X}\, P_{Col}^{\,A-X} \qquad (3)$$

In our proposal all network nodes can detect the intruders and the probability of detection augments gradually with the expansion of the number of attacked nodes and the decreasing of collusion amount. In the other side, majority of proposed IDS must augment the number of monitor nodes to enhance their detection probability which is not suitable for energy efficiency.

We assume the intruder node attacks all nodes in the range of its radio antenna. Therefore the average number of attacked node by an intruder can be equal to:

$$A= (N-1)\, \pi\, r^2 / a \qquad (4)$$

Where: a is the area of the range region, N is the number of nodes in that region and r is the intruder transmission radius.

Our proposed IDS is energy efficient, since we reuse the already available data generated by network, Mac and physical layers, our approach incurs very little additional cost and thus is ideally suited for resource constrained WSNs.To estimate the total energy consumed by our IDS, we calculate the consumed energy of IDS on every attacked node.

$$EA_i = E_{rx} + E_p + E_{tx} \qquad (5)$$

Where: EA_i is the energy consumed to detect the intrusion on node i, E_{rx} is the power consumption due to receiving of packet from intruder, E_p is the power consumption due to processing of intruder detection algorithm and E_{tx} is the power consumption due to sending the alarm message.

Then the amount of energy consumed by our IDS to defend the network from x attacker *(at)* nodes is equal to:

$$Energy\_IDS = \sum_{at=0}^{at=X} \; \sum_{i=0}^{i=A} ER_i \qquad (6)$$

Contrarily to other IDS (*that use a fixed monitoring nodes*), the amount of energy consumed by our IDS decreases, as the number of intruder nodes and attacked nodes is reduced. That preserves more energy and enhances the network lifetime.

4.1 Proposed IDS architecture

The architecture of our IDS maintains the traditional layered architecture and adopts the principle of communication via a cross layer entity named CLIDA (Cross-Layer Intrusion Detection Agent). This choice is based on the multitude of benefits of this architecture namely: the conservation benefits of the layered architecture, particularly in terms of modularity, thus contributing to the longevity and compatibility with the OSI model. The presence of cross-layer entity provides a cross layer individual evolution and continues to both layers and the entity itself without disturbing the overall system. Another advantage is that this entity has a free access to all the layers, making decisions more objective. It also allows easy and simple integration of new cross layer algorithms and data without changing the rest of the architecture. The following figure shows the cross-layer proposed architecture.

The intrusion detection agent CLIDA is the entity through which the layers and applications communicate. It includes essentially two parts: the interaction interface and cross-layer data module.

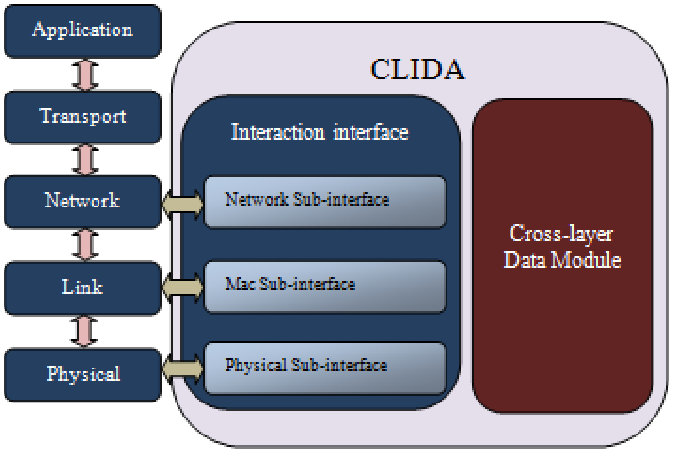


Figure 3.Cross-layer proposed architecture.

4.1.1 Interaction interface

Interaction interface facilitates the contact between the layers and application on one hand and the CLIDA agent on the other hand. The interaction interface takes as its main objective the management of sub-interfaces that provide access to the layers (IR: Network Interface, IL: Interface). Each sub interface describes methods for reading and writing to facilitate the manipulation of parameters of the corresponding protocol. Via these methods is made the collection and / or updating data (eg the value of the calculated RSSI, routing tables, etc.).

4.1.2 Cross-layer data module

The Cross-layer data module represents data in a special way to make them quickly accessible by all layer protocols. Data provided by this module are the basis for any Cross-layer adaptation and optimization. The module is also responsible of maintaining up to date data through Cross-layer interaction interfaces.

4.2 Example of possible attacks and their detection

In this section we provide some types of attacks and their detection by our intrusion detection system. We assume in our example that there are three intruder nodes in the network (NI_1, NI_2 and NI_3) where each one is capable of a different type of attacks:

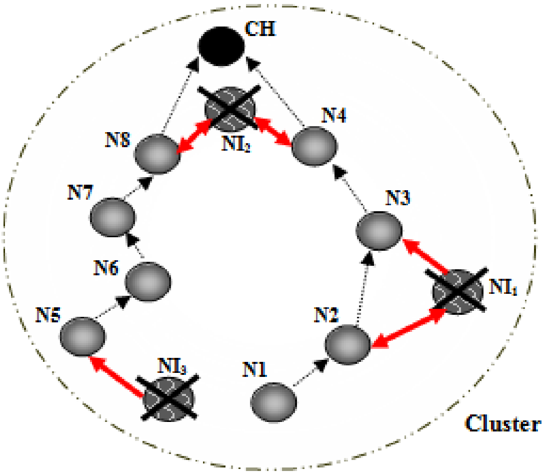


Figure 4.Example of intruder attacks.

4.2.1 Attack at the network layer

Case 1:

The first intruder node (NI_1) tries to integrate into the routing path to launch attack (spoofed routing information). Thus the node NI_1 intercepts the information routed from node N2, modifies (alter) them then transmits them to the next node in the routing path (N3). In addition, the node NI_1 can transmit falsified data several times to generate additional traffic; it can also create infinitely routing loops. In order to be undetectable, the intruder node can copy the identity of the node N2, this type of attack is called cloning nodes (cloned or replicated nodes).

In the first case the node NI_1 tries to connect to the node N3 in order to route the altered information. Upon receiving the connection request packet (RTS) of NI_1, N3 checks the belonging of this node to its neighboring routing nodes (routing table). Thus the intruder node will be immediately detected and corrupted data will not be passed to the node N3. If the node NI_1 is a copied identity from another node (N2), the intrusion will be detected (by the node N3) by comparing the received RSSI value of the RTS packet with the saved RSSI value of the node N2 (previously calculated).

Case 2:

Concerning the second intrusion case, the node NI_2 tries to play the role of CH in order to make Sinkhole attack. At the end of the data collection phase, the nodes managed by the same CH try to connect to it to send the collected data. The node NI_2 intercepts connection requests (packets RTS) and returns CTS packet to synchronize with the transmitting nodes. Upon receiving these, sensor nodes can detect the intrusion by consulting their routing tables. In addition, the RSSI value confirms the identity of the intruder node NI_2.

In the case where the sensor nodes do not receive acceptances (CTS packets) from CH node (node intruder), the connection will not be established and data will not be sent. In addition an anomaly alarm will be reported to the base station.

4.2.2 Attack at the link layer (Mac)

In this second type of attack, the node NI_3 launches DOS attack which consists of exhausting the energy reserves of the target sensor node (N5). Thus, the node NI_3 sends constantly multiple control messages (HELLO message) to the node N5. By receiving these messages the node N5 leaves its sleeping state to communicate with the node NI_3. Therefore, node N5 may be maintained unnecessarily in an active state to receive the unlimited number of HELLO messages, which means the exhaustion of its energy reserves. Figure 5 presents the energy exhaust attack lanced by attacker NI_3.

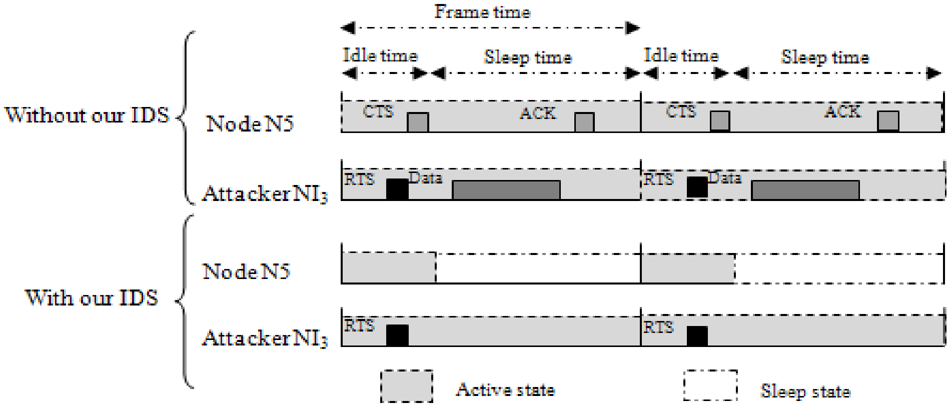


Figure 5.Energy exhausts attack.

With our detection system the previous scenario can be avoided. Since the node NI_3 must set up a connection (RTS and CTS packets) with the node N5 to begin the transmission of HELLO messages, the node N5 can detect the intrusion of the node NI_3 and deny its connection request. Therefore, the node N5 is maintained in a sleeping state and preserves its energy reserves.

5. Simulation

5.1 Simulation environment

Analysis of the performance of our intrusion detection is performed using the network simulator NS2. In this simulation, our experimental model is built on 100 nodes distributed randomly on a square surface of 100 x 100 m² presented in Figure 6.

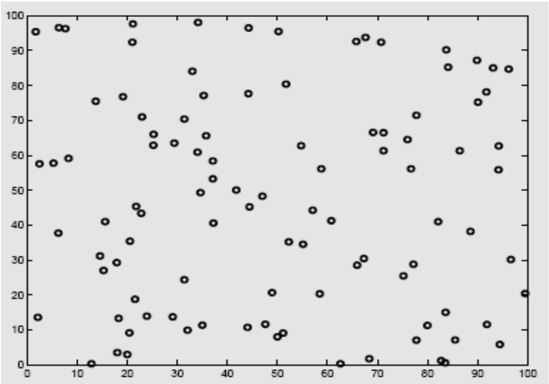


Figure 6.Experimentation model

We assume that all nodes have a fixed position throughout the simulation period. The simulation parameters used in our simulation model are summarized in the table below:

Parameter	Value
Surface of the network	100 m^2
Location of the BS	(50, 75)
Number of nodes	100
Number of clusters	5
Initial energy of nodes	2 J
Size of data packet	500 Byte
E_{el}	50nJ/bit
εfs	10nJ/bit/m^2
MAC layer protocol	SMAC
Initial duty cycle	10%
RTS, CTS, ACK size	30 Bytes
Traffic type	CBR
Routing Protocol	HEEP
Antenna type	Omni-Antenna
Channel bandwidth	20kpbs

Table 1.Simulation parameters

The transmission bandwidth is set to 20kbps, the latency of transmission and reception of a data packet is equal to 25µs, and the size of a data packet is 500 Bytes, with a packet header measuring 25 bytes. The communication energy parameters are set as: E_{elec}=50nJ/bit, εfs=10pJ/bit/m^2, εmp=0.0013pJ/bit/m^4 and the energy for data aggregation is set as E_{DA}=5nJ/bit/signal. The range of radio antennas is 2 meters.

All network nodes start the simulation by an initial energy equal to 2 J and an unlimited amount of data to be transmitted to the base station. In addition, the energy of the base station is considered as unlimited. Each node uses its limited reserves of energy throughout the duration of simulation, which involves the depletion of it. Thus, any node which has exhausted its energy reserve is considered dead. Therefore, it cannot transmit or receive data.

In our simulation model, we assume that there are 10 intruder nodes randomly deployed in the well field. All intruders' nodes pass through a period of passive listening and then try to connect with nodes randomly targeted. All simulation results presented later are the average of 10 performed simulation operations. The duration of each simulation is set to 1000 sec.

5.2 Simulation Results

First, we measured the number and percentage of intruder nodes detected as the simulation progresses. We assume that attacker nodes target and attack randomly network nodes after being in passive state (random time period) and send every tow frame time an RTS packet. The following figures (figure 7 and figure 8) show the results.

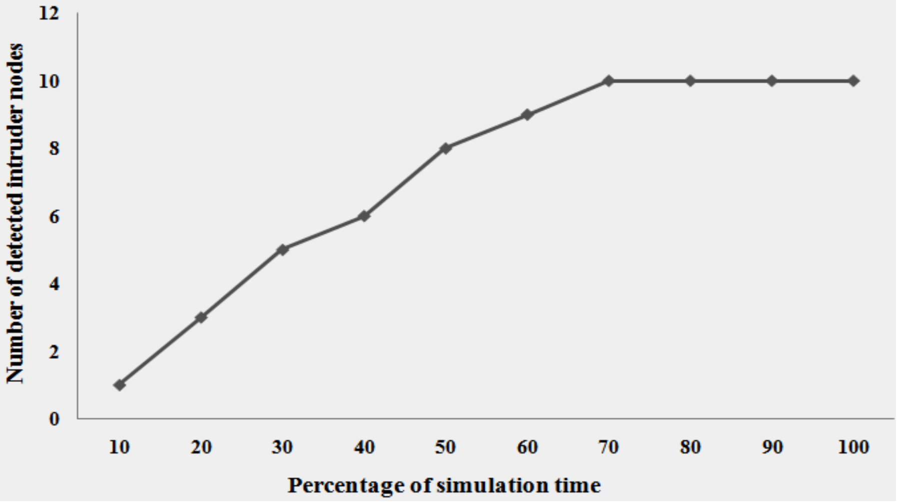


Figure 7.Number of detected intruder nodes compared to the percentage of simulation time.

Indeed the number of detected intruder nodes with our IDS is strongly linked to moments when they decide to launch their attacks.

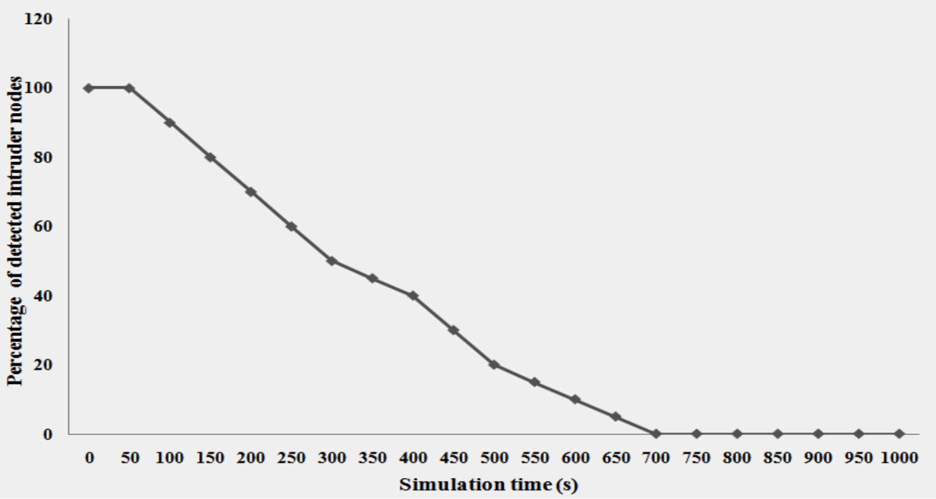


Figure 8.Number of detected intruder nodes over the simulation time.

The second evaluation step is to analyze the behavior of our IDS in case of Sinkhole and selective routing attacks. For this, we measured the total of received messages by the base station throughout the simulation period. All intruder nodes try to make their attacks in random periods. In our simulation, the intruder nodes which are closest to the CHs try to create a sinkhole to divert a larger number of data. However, other intruder nodes (distant from CHs) perform selective routing attacks targeting all nodes that are within the range of their radio antenna. Figure 9 shows the results:

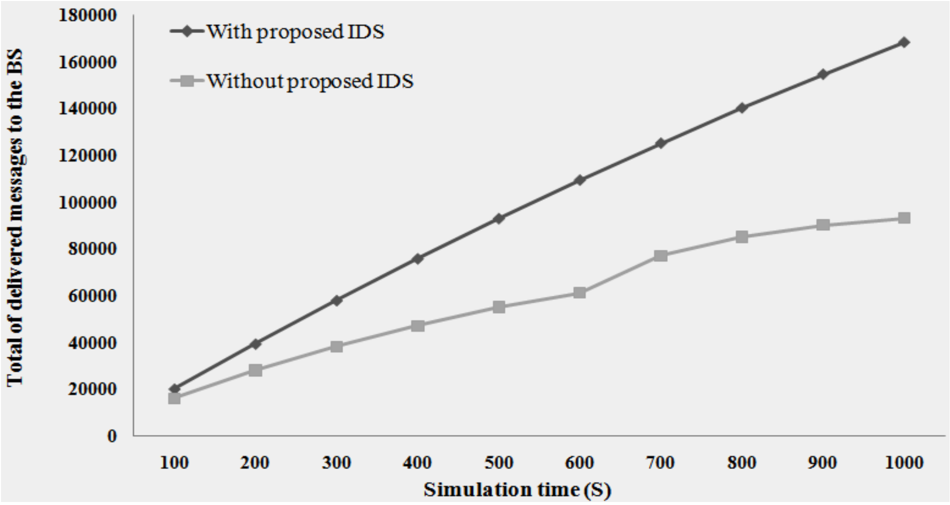


Figure 9.Total of delivered messages to the BS over the simulation time.

Based on simulation results, we demonstrated that our IDS can prevent major attacks that affect data routing at the network layer. The previous figure shows that data routing is not affected by the intruder nodes attacks as the number of messages delivered to the BS continues to expand as the simulation progresses. However, the results obtained without the use of our IDS illustrate the problems of routing data generated by the attacks of intruder nodes.

To evaluate the performance of our IDS against attacks at the MAC layer, we conducted a third simulation in which the intruder nodes perform attacks of exhaustion of energy. We measure as well the total energy reserves of the network nodes throughout the simulation period. Figure 10 shows the results:

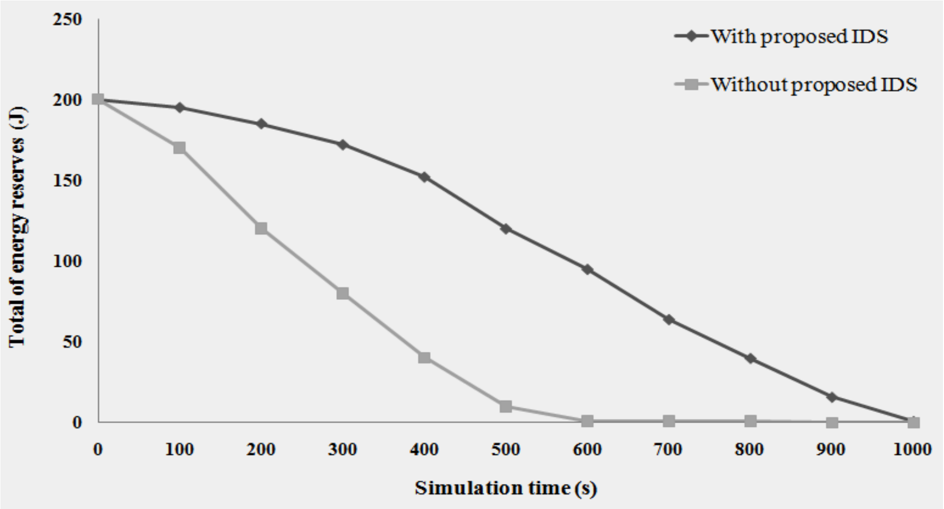


Figure 10.Total of energy reserves over the simulation time.

The graph clearly illustrates the effectiveness of our new IDS in preventing attacks of energy exhaustion at the MAC layer. With our IDS the sensor intruder nodes consume their energy reserves regularly to transmit their collected data. But without our IDS the intruder nodes targeted by the attacks exhaust quickly their energy reserves, which directly affects the life of the network.

To show the number of activated nodes in the network, we take a random snapshot of awaked nodes after 250 seconds of simulation time, which gives us as result Figure 11 with proposed IDS and Figure 12 without proposed IDS.

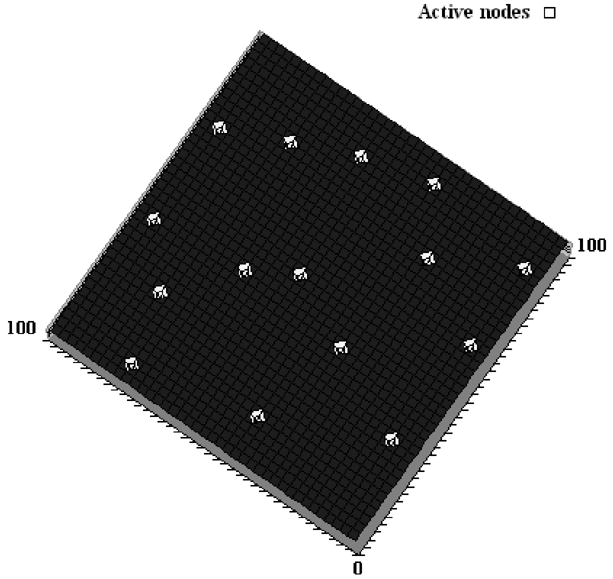


Figure 11.Activated nodes map with proposed IDS (under energy exhaust attacks).

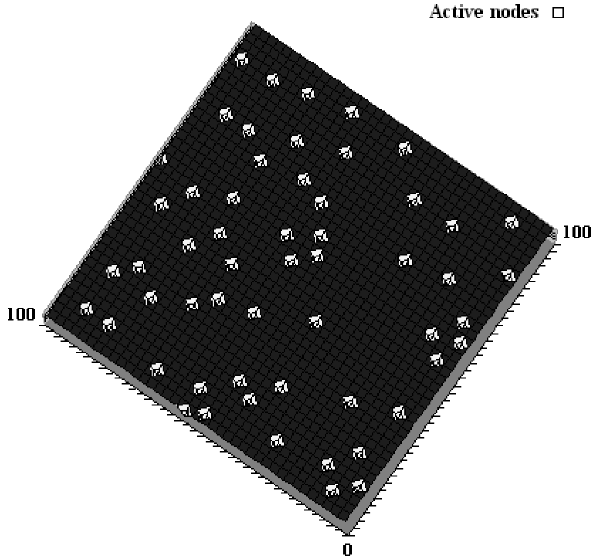


Figure 12.Activated nodes map without proposed IDS (under energy exhaust attacks).

We can clearly observe that the number of unnecessary activated nodes is much higher without our proposed IDS.

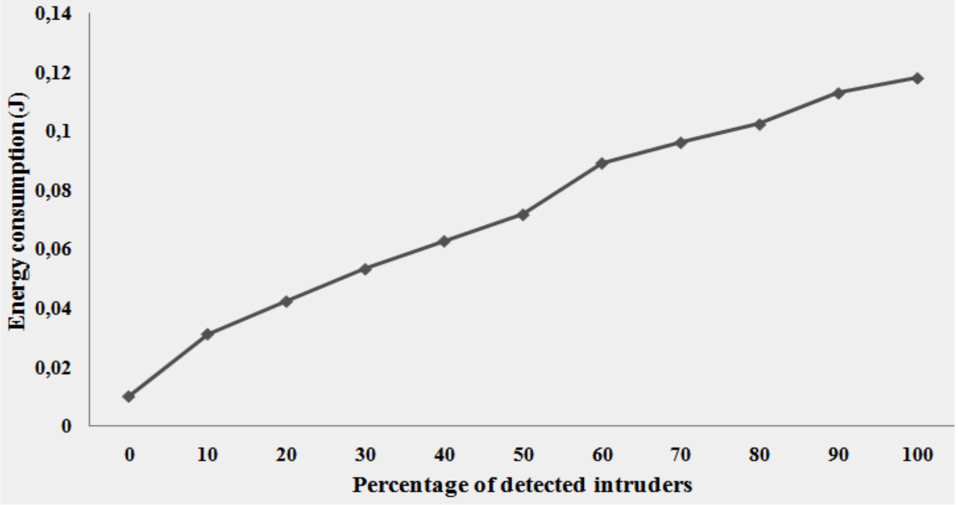


Figure 13.Energy consumption over the percentage of detected intruders.

In figure 13, we evaluate the amount of energy consumed by our IDS. As shown, proposed IDS consume negligible additional power for implementing intrusion detection based on cross layer security solution. Also, it is extremely energy-efficient compared to conventional layered security solution. Indeed in the previous experimental simulation our IDS consume 0,118J to detect 10 intruder nodes which represent 0.06 % of the overall network power.

6. CONCLUSIONS

Taking security as main objective, we proposed an intrusion detection system dedicated for wireless sensor networks. In our proposal the problem of intrusion detection is discussed in a new way in which the Cross layer interaction is heavily exploited. Our approach is to provide a single cross layer IDS to several layers of the OSI model instead of offering an IDS for each layer. The proposed approach doesn't claim to be immune from all security attacks but this new approach should give a new direction towards WSN security. Simulation results demonstrate the performance provided by our IDS in terms of prevention and detection of different intrusion types.

REFERENCES

[1] S. Camtepe and B. Yener, (2005) “Key distribution mechanisms for wireless sensor networks: a survey,” Rensselaer Polytechnic Institute, Troy, New York, Technical Report 05-07.

[2] E. Shi and A. Perrig, (2004) “Designing secure sensor networks,” *IEEE Wireless Communications*, Vol. 11, No. 6, pp. 38–43.

[3] L. Lazos and R. Poovendran, (2005) “Serloc: Robust localization for wireless sensor networks,” ACM Transactions on Sensor Networks, Vol. 1, No. 1, pp. 73–100.

[4] T. Dimitriou and I. Krontiris, (2006) “Security in Sensor Networks,” *CRC Press, 2006, ch. Secure In-network Processing in Sensor Networks,* pp. 275–290.

[5] S. Ganeriwal, S. Capkun, C.-C. Han, and M. Srivastava, (2005) "Secure time synchronization service for sensor networks," *in Proceedings of the 4th ACM workshop on Wireless security* (WiSe '05), pp. 97–106.

[6] Jun Zheng and Abbas Jamalipour, (2009) "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE.

[7] R. Bace, (2000) "Intrusion Detection", MacMillan Technical Publishing.

[8] Ayman Khalil, Matthieu Crussière and Jean-François Hélard, (2010) "Cross Layer Resource Allocation Scheme under Heterogeneous constraints for Next Generation High Rate WPAN," International Journal of Computer Networks and Communications(IJCNC) Vol 2, No. 3.

[9] Mingbo Xiao,Xudong Wang,Guangsong Yang, (2006) "Cross-Layer Design for the Security of Wireless Sensor Networks," P*roceedings of the 6th World Congress on Intelligent Control and Automation*, June 21 - 23, Dalian, China.

[10] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, (2005) "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 (Q2SWinet '05).* ACM Press, October, pp. 16–23.

[11] I. Onat and A. Miri, (2005) "An intrusion detection system for wireless sensor networks," *in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Vol. 3, Montreal, Canada, pp. 253–259.

[12] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, (2005) "Intrusion detection for routing attacks in sensor networks," International Journal of Distributed Sensor Networks.

[13] V. Bhuse and A. Gupta, (2006) "Anomaly intrusion detection in wireless sensor networks," Journal of High Speed Networks, Vol. 15, No. 1, pp. 33–51.

[14] C.C. Su, K.M. Chang, Y.H. Kue, and M.F. Horng, (2005) "The new intrusion prevention and detection approaches for clustering-based sensor networks," *in Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05),* Vol. 4, New Orleans, L.A., pp. 1927-1932.

[15] Edith C. H. Ngai, Jiangchuan Liu, and Michael R. Lyu. (2006) "On the intruder detection for sinkhole attack in wireless sensor networks," *In Proceedings of the IEEE International Conference on Communications*, pages 3383–3389.

[16] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami. (2006) "Intrusion detection for routing attacks in sensor networks," International Journal of Distributed Sensor Networks, Vol 2, pp. 313–332.

[17] Wei-Tsung Su, Ko-Ming Chang, and Yau-Hwang Kuo. Ehip, (2007) "An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks," Computer Networks, Vol 51, pp. 1151–1168.

[18] Ioannis Krontiris, Tassos Dimitriou, and Felix C. Freiling. (2007) "Towards intrusion detection in wireless sensor networks," *In Proceedings of the 13th European Wireless Conference*.

[19] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos. (2008) "Intrusion detection of sinkhole attacks in wireless sensor networks. In Algorithmic Aspects of Wireless Sensor Networks," Vol 4837, pp. 150–161. Springer Berlin / Heidelberg.

[20] Fang Liu, Xiuzhen Cheng, and Dechang Chen, (2007) "Insider attacker detection in wireless sensor networks," In INFOCOM 2007. *26th IEEE International Conference on Computer Communications. IEEE*, pp. 1937–1945.

[21] Zhenwei Yu and Jeffrey J.P. Tsai. (2008) "A framework of machine learning based intrusion detection for wireless sensor networks," *In IEEE International Conference on Sensor Networks*, Ubiquitous, and Trustworthy Computing, pages 272–279,

[22] William W. Cohen and Yoram Singer, (1999) "A simple, fast, and effective rule learner," *In Proceedings of the sixteenth national conference on Artificial intelligence and the eleventh Innovative applications of artificial intelligence*, pp. 335–342.

[23] Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C. Freiling, and Tassos Dimitriou, (2009) "Cooperative intrusion detection in wireless sensor networks," *In Proceedings of the 6th European Conference on Wireless Sensor Networks*, pp. 263–278.

[24] Tassos Dimitriou and Athanassios Giannetsos. Wormholes no more, (2010) "localized wormhole detection and prevention in wireless networks," *In Distributed Computing in Sensor Systems*, pp. 334–347. Springer Berlin/Heidelberg.

[25] Luigi Coppolino and Luigi Romano. (2010) "Open issues in ids design for wireless biomedical sensor networks. In Intelligent Interactive Multimedia Systems and Services," Vol 6, pp. 231–240. Springer Berlin Heidelberg.

[26] Tran Hoang Hai, Eui-Nam Huh, and Minho Jo. (2010) "A lightweight intrusion detection framework for wireless sensor networks," *Wirel. Commun. Mob. Comput.*, 10(4), pp. 559–572.

[27] D.Boubiche, A.Bilami, (2011) "HEEP (Hybrid Energy Efficiency Protocol) Based on Chain Clustering", Int. J. Sensor Networks, Volume 10 Issue 1/2, pp. 25 - 35.

[28] W. Ye John Heidemann and Deborah Estrin, (2002) "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *INFOCOM 2002*.

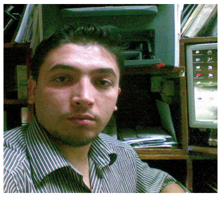
[29] Wei Ye, John Heidemann and Deborah Estrin, (2004) "Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, Vol. 12, No. 3, pp. 493-506.

[30] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, (2005) "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 2, pp. 228–258.

[31] http://www.tinyos.net/.

Authors

Djallel Eddine Boubiche is currently a PhD student at the Computer Science Department,-University of Batna, Algeria He is a member of LaSTIC Laboratory. His research interests include wireless communication and sensor networks.



Azeddine Bilami is the director of LaSTIC Laboratory. He is currently serving as a Full Professor at the Computer Science Department at University of Batna, Algeria. His research interests are wireless and mobile networks, TCP/IP, internet, system on chip architectures; high performance interconnects for parallel architectures and multiprocessors.