Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks

Somia Sahraoui[1], Souheila Bouam[2]

[1,2]LaSTIC Laboratory, Computer Science Department, University of Batna, Algeria.
[1]somiasahraoui@ymail.com, [2]souheila.bouam@yahoo.fr

***Abstract*:** Popularity of wireless sensor networks (WSNs) is increasing continuously in different domains of daily life, as they provide efficient method of collecting valuable data from the surroundings for use in different applications. Routing in WSNs is the vital functionality that allows the flow of information generated by sensor nodes to the base station, while considering the severe energy constraint and the limitations of computational and storage resources. Indeed, this functionality may be vulnerable and must be in itself secured, since conventional routing protocols in WSNs provide efficient routing techniques with low power consumption, but they do not take into account the possible attacks. As sensor nodes may be easily captured and compromised, the classical cryptographic solutions become insufficient to provide optimal routing security, especially, for cluster-based WSNs, where cluster heads can be still among the compromised nodes. In this work, we propose a hierarchical, robust and well-adapted intrusion detection system, named THIDS (Threshold Hierarchical Intrusion Detection System), which is intended to be integrated into the secure hierarchical cluster-based routing protocols. We have chosen the protocol RLEACH to be equipped with the proposed IDS. The results of simulation performed under NS2 simulator show that the resulting protocol ORLEACH is much more resistant to compromised nodes exercising the most dangerous attacks.

***Keywords*:** cluster-based wireless sensor networks, secure routing protocols, hierarchical intrusion detection system.

1. Introduction

The reason of being of a WSN is to monitor and control different events (or phenomena) in deferent environments. For this, the network is composed of a set of tiny sensor nodes, often randomly deployed, which are able to collect data of various types from the deployment field. Sensed data are then, communicated to the base station (BS) through wireless communications. The BS represents a downstream of all information coming from the sensor nodes.

According to the network topology, we distinguish two categories of WSNs: flat and hierarchical WSNs. In flat WSNs, all sensor nodes are in the same level of privilege; they are all charged of sensing and communication tasks. Moreover, data messages are communicated in a multi-hop policy. However, in hierarchical WSNs (HWSN) the network is organized in clusters. Each cluster contains one special node called cluster head (CH), and its member nodes. The CH is the router of data sent by its members to the BS. In this type of WSN, member nodes sleep the most of time to save energy. The figure1 illustrates the topology model in HWSNs.

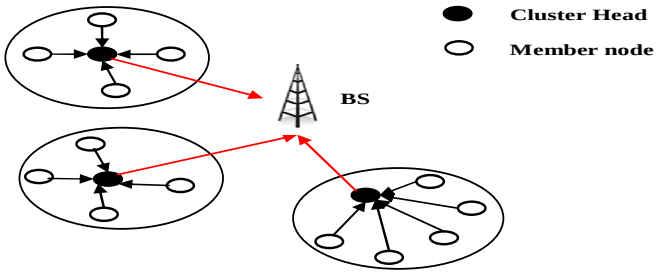

Figure 1. Simple model of cluster-based WSNs

Recently, the incorporation of WSNs to nowadays Internet, what is so-called Internet of Things (IoT), is seriously investigated. Although this novel trend improves the quality of service and living conditions, there are still several applications [1] that continue to use isolated WSNs (where Internet can be used just as a communication average of sensing reports to the task manager). This paper doesn't consider IoT scenario.

In certain applications, the mission of a WSN is very critical such as military, health-care and industry automation. In such a case, data as well as the process routing them to the BS must be secured. The hard imposed constraints on a WSN (especially: node size and the restrictions on the energy, computational and storage resources) make the security an extremely challenging task.

Recent studies and researches in WSNs, addressing routing aware techniques [2], and security solutions [3] are much more interested in HWSNs as an infrastructure because they present an appropriate and well-organized model of the network, providing easy control ways of network's functionalities, in addition to the included network lifetime prolonging. In this paper, we address the problem of secure routing enhancement in HWSNs.

Most of the existing secure hierarchical routing protocols focus only on the cryptographic solutions to achieve routing security goal. But, if the network includes compromised sensor nodes, these solutions become insufficient. In this context, we propose an intrusion detection system to be part of the hierarchical secure routing principle.

In the following sections, we give a literature review of routing, security and routing security in HWSNs. After that, we express the motivation behind the need in intrusion detection in HWSNs; we give also an overview on the relevant IDSs. We specify then, how secure routing in HWSNs could be optimized. Finally, we analyze and conclude the obtained results from the performed simulation.

2. Routing in Hierarchical WSNs

In WSNs, routing mechanism of the generated data to the BS should be efficient. This efficiency relates to less power consumption, limited inundation of messages and lower requirements on memory and computation resources.

Typically, hierarchical routing class, which target cluster based networks fashion; comply better with scalability and energy efficiency features. In such routing class, data are routed in tow steps: intra and inter-clusters. Within each cluster, member nodes communicate their data messages only to the CH. CHs perform then, an aggregation operation on the received messages and relay afterwards, the resulting messages to the BS. The communication between CHs and BS may pass by several hierarchy levels. Besides, the ordinary nodes which have no data to communicate to their CH (or which have already done it) turn off temporarily their radio devices. This allows network lifetime prolonging.

The main goal of a hierarchical routing protocol is to specify how the network hierarchy should be formed and then, it dictates the steps of data communication. In this section, we present some of the well known hierarchical routing protocols in WSNs.

2.1. Low Energy Adaptive Clustering Hierarchy (LEACH)

LEACH [4] is among the first and well-known cluster based routing protocols. Its operation is divided into several rounds. In each round, we find two phases: set-up phase and steady-state phase. In set-up phase, clusters are dynamically elaborated. Each sensor node decides if it acts as a CH or not in the present round. This decision takes on whether this node has recently acted as CH, and on if it has a sufficient residual energy. Each CH sends an advertising message (ADV) to the nodes of its neighborhood, informing them about its current state. Each member node chooses its cluster head, basing on the signal strength of the corresponding ADV message that should be the greatest. This choice is concretized by sending a joining message (JOIN) to the elected CH. On receiving all JOIN messages, each CH generates a TDMA (Time Division Multiple Access) scheduling frame and sends it to its member nodes. This process allows the indication of the right data transmission time for each of them.

In steady-state phase, data collected by sensor nodes are communicated to the base station in two steps. First, in each cluster, if the member node allocates a TDMA slot, it sends its data to the CH. Otherwise; it keeps its radio device turned off to save energy. Further, all CHs apply aggregation and compression functions on all data messages they received, and finally, they send the resulting messages directly to the base station.

By using the concept of the random rotation of the CH roles, LEACH prevents that nodes acted as CHs die rapidly, and ensures a uniform dissipation of nodes energetic reserves.

2.2. Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS [5] protocol is a variant of LEACH protocol. It adopts rather a particular hierarchical topology in which, nodes are organized into chain structure. This structure is set up in a greedy strategy, so that, each sensor node sends its data to the closest neighbor node in the next level making a chain towards the BS. Data are gradually aggregated as they transit on the established chain. This routing protocol has the advantage that it saves the spent energy in periodic clusters formation in LEACH. Nevertheless, it suffers from certain anomalies, in terms of the significant delay for the far situated nodes from the BS, and the ignorance of the energy status of the next hop node.

2.3. Hybrid Energy Efficiency Protocol (HEEP)

HEEP [6] protocol combines advantages of both LEACH and PEGASIS protocols. This is achieved through the application of chain concept inside clusters, between member nodes and their cluster heads. In each cluster, remaining nodes communicate their data messages to the CH over the chain. The CH doesn't transmit directly his aggregated message to the BS, but it forwards it to a neighbor CH, and reaches the BS after a multi-hop communication. HEEP maintains LEACH's principles related to the dynamic elaboration of clusters, while reducing the transmission distances, in both intra and inter clusters communications. For this reason, energy consumption and network latency are more likely improved.

3. Background of routing security in HWSNs

Since that sensed data in a WSN may be decisive, both data messages and sensor nodes have to be protected against malicious alterations and susceptible subversions. Wireless communication, resources limitations make the WSN vulnerable to several threats. In this section, we present briefly security issues, including, the secure routing issue and its context in HWSNs.

3.1. The basic security requirements

To achieve security in WSNs, the following requirements should be guaranteed:

- Confidentiality: only authorized nodes access network's messages.
- Integrity: prevent all malicious alterations and falsifications of messages.
- Authentication: the ability to verify the validity of messages source's identity.
- Freshness: control messages recentness and prevent message replay attack.
- Availability: ensure the accessibility to network's services and resources.

3.2. Threat models

Attacks in WSNs may appear under different models. They can be classified into the following classes [7]:

3.2.1. Outsider and insider attacks

Outsider attacks are launched by nodes that do not belong to the network. Whereas, insider attacks (that are the most dangerous) are due to the bad behavior of legitimate sensor nodes that have been captured and spoofed by a malicious person. This operation is called node compromising. Compromised sensor nodes benefit of all authorizations, exactly like the legitimate nodes.

3.2.2. Mote-class and laptop-class attacks

In mote-class attacks, attacker is a resources constraint node, quite like network nodes. In laptop-class attacks, adversary is much more powerful, it disposes a greater processing power, a very large transmission range and a sufficient energy reserve.

3.2.3. Passive and active attacks

Attacker's mission in passive attacks consists of interception (or eavesdropping) and traffic analysis actions. Contrariwise, in active attacks, attacker alters, misroutes, replays or blocks arriving packets. Hierarchical routing protocols in WSNs, could allow efficient and resources constraints aware routing, but they don't consider any risk in terms of the possible threats. In other words, these routing protocols assume that there will be no dangers, and all sensor nodes are honest, which is not always the case.

3.3. Routing attacks

Routing function in WSNs is vulnerable to various types of attacks. In the following points we enumerate the possible routing attacks in HWSNs [7] [8].

3.3.1. Alter, spoof and replay routing information

Attacker may alter, spoof and replay routing information, in order to empoison routing tables of attacked nodes.

3.3.2. Sinkhole

Attacker attempts to attract an important part of network traffic by broadcasting attractive routing information after that, it drops, alters or spoofs packets.

3.3.3. Sybil

Attacker announces multiple identities or geographic positions to maximize its chances to be part of several routing paths.

3.3.4. Selective forwarding

Attacker inserts at first itself into data flow way using sinkhole or Sybil attack, then, it drops randomly the received messages.

3.3.5. Black hole

The malicious node drops all messages it receives from the legitimate nodes.

3.3.6. Hello flooding

A laptop-class adversary broadcasts a powerful hello message to a large number of sensor nodes to give them the impression that it is their direct neighbor. Victim sensor nodes may not use, thereafter, routes advertised by the attacker if it is outside their radio range.

3.3.7. Denial of service (DoS)

In this attack, attacker may delete received messages, as it can behave in such a way to provoke exhaustion of node's resources (causing exhaustion of battery or the overflow of routing table).

3.4. Overview on the secure hierarchical routing protocols

Hierarchical routing protocols are by nature implicitly protected against some routing attacks. Once clusters are established, routes linking sensor nodes with the BS become explicit and wormhole attack couldn't have place. Moreover, the mechanism of node sleeping prevents DoS attack. However, an attacker can eavesdrop, delete or forge bogus messages. So, sinkhole, black hole, selective forwarding, sybil and other attacks are very possible. Consequently, it was necessary to secure routing function for HWSNs. Many hierarchical secure routing protocols have been proposed. In this section, we give an overview of a set of them.

3.4.1. SLEACH*:*

SLEACH protocol [9] is the first secure version of LEACH protocol, which prevents sinkhole, selective forwarding and HELLO flooding attacks by using the protocol SPINS (Security Protocol for Sensor Networks) and MAC for authentication. SLEACH prevents, thus, an intruder node (member or cluster head) to send falsified data messages. But it doesn't guarantee confidentiality and availability (insider adversary can decrease network's throughput by disrupting the time slot schedule of a cluster).

3.4.2. SS-LEACH

SSL-EACH [10] is another secure routing protocol based on LEACH protocol; its main goal is to offer security while being energy efficient. For that, it defines stochastic multi-paths cluster heads chains to communicate with the base station, which prolongs better the network lifetime. To ensure security, It employs key pre-distribution and self localization techniques. SS-LEACH is protected from selective forwarding, Hello flooding and sybil attacks, but it controls neither data integrity nor freshness.

3.4.3. RLEACH

RLEACH protocol [11] attempts to apply Random Pair-wise Key (RPK) scheme [12] onto LEACH. On the fact that RPK is a probabilistic key management protocol, it doesn't guarantee that all adjacent nodes have shared keys. For this reason, authors have proposed an improved version of RPK, so that it ensures security and connectivity in the network. In the modified RPK, nodes are pre-defined in several groups. Nodes within the same group can establish secure links between them. Prior to deployment, each sensor node is loaded with its identifier (ID) , an original key , m keys chosen randomly from the entire pool, and other relevant information. Like in LEACH, RLEACH operation is round based. It has three basic phases: shared-key discovery phase, cluster set-up phase and data transmission phase. In the shared-key discovery phase, nodes establish the secure links between them. Each sensor node broadcasts its ID and receives those of its neighbors. After that, it checks for each received ID whether the related node belongs to the same group. If it belongs, the shared-key is calculated. Otherwise, the two nodes exanimate their sub-pools of keys to find if they have a common key. In the cluster set-up phase, CHs emerge with the same conditions as in LEACH and diffuse their advertisement messages. The ordinary node chooses then its CH, where the criterion is about whether the CH has a shared-key. If many CHs have shared-keys, the nearest CH will be chosen. Once clusters are all set-up, CHs generate TDMA schedule for their members. Data communication between the CH and its members is authenticated by the use

of shared-keys. After the validation of the authentication, the CH aggregates and compresses received data, and then, it sends safely the new message to the BS, using its original key. RLEACH has the ability to resist to several attacks such as selective forwarding, sybil and hello flooding. Nevertheless, it is possible that an insider exercises sinkhole attack to be CH. Compromised node can also corrupt BS by the falsified data messages it sends.

In [13], authors highlight new research area for secure routing issue, in WSNs. In the opened trend, it is suggested that future secure routing protocols take into account sensor nodes mobility and/or base station replication (or mobility).

3.5. Problem statement

The existing secure hierarchical routing protocols in WSNs present security systems focused on cryptographic solutions and key management schemes. These security systems are very efficient to combat the external attacks. However, it is remarkable that most of the secure hierarchical routing protocols don't treat the insider attacks (exercised by the compromised nodes) as a serious problem in the routing security issue, which presents a major drawback.

Since an insider adversary disposes, by its nature, of the relevant cryptographic keys and any possible security material, it can despite everything be part of the routing path. In this way, a compromised node may success to be a CH and thus, it can perform several attacks on an entire group of sensor nodes. Consequently, cryptographic and key management solutions which resist to outsider attackers and reduce the impact of the insiders [12] [14], respectively, couldn't provide the desired security level for routing in HWSNs, even if the network contains only a few compromised nodes. For this reason, we suggest that hierarchical routing protocols integrate intrusion detection mechanisms, so that malicious behaviors may be detected, and the responsible nodes could be isolated.

4. Intrusion Detection in HWSN

In order to respond to the need to intrusion prevention in WSNs, researchers have investigated several solutions, from among, we find tamper proofing solutions like in [15], to convert the executable code of sensor's program, or checking its integrity as in [16], so that any possible falsification gets harder. These solutions are judged too expensive in terms of complexity, overhead and energy dissipation. In another side, researchers are carrying out massive studies to find an alternative and challenging solution which is the development of tamper-resistant sensor nodes, while maintaining their low cost. The last solution is a subject of a recent research work [17]. Until the preventive countermeasures could be effectively realized and approved, the present researches are much more oriented to the development of logical intrusion detection systems [18]. An intrusion detection system (IDS) is by definition a system that handles the detection and the isolation of intruders present in the network through a collection of monitor nodes (MNs). A MN is a sensor node which has to control network's traffic and to transmit alarm messages on detecting misbehaviors.

Although intrusion detection is an indispensable aspect in network's security, especially in networks where nodes are very prone to theft (just like WSNs), it receives a few attention in researches. In this section we emphasize in main points of IDS in HWSNs. The principal constraints [19] imposed on IDS design in WSNs are summarized in the points below:

- Less energy consumption: IDS must spend the minimum possible of energy.
- Lightweight and less overhead: the IDS program and the volume of control messages to be exchanged must not be very important.
- Effectiveness: IDS must still fulfill its mission with robustness even if the network contains a large number of intruders.
- Resistance: IDS should resist to any susceptible compromising of its MNs.
- Scalability: the IDS should be able to preserve its efficiency if the network expands.

There are four aspects to be considered when designing IDSs:

- The specification of the intrusion detection policy: specifying how the IDS detect misbehaviors.
- The selection of monitoring agents (MNs).
- The specification of the alerting system: indication of when to generate alarms and, how to communicate them in the network.
- The isolation mechanism: how the IDS isolates the detected attackers from the network.

Intrusion detection systems can detect different types of malicious behaviors **[**20**]** targeting different levels in OSI model, using conventional or special techniques [21]. Indeed, in wireless networks, IDSs architecture may be classified in three categories [19]: Stand-alone IDS; where MNs act independently with each other, the distributed and collaborative IDS; MNs exchange and share their relevant detection information, and finally, the hierarchical IDS.

The hierarchical IDSs concern HWSNs. In this type of IDSs, CHs and clusters members can monitor each other. Presentation of the recent hierarchical IDSs.

In [22], an isolation table intrusion detection system (ITIDS) for HWSNs is presented. It is characterized by a particular architecture; the network should have one primary cluster head (PCH) and the remaining sensor nodes are defined in multiple monitor groups, with secondary cluster heads. In ITIDS, sensor nodes of all kinds are concerned by monitoring task and control each other, to detect Hello flooding, DoS, denial of sleep, sinkhole and wormhole attacks. Basing on residual energy of sensor nodes and the well-known attack patterns, insider malicious nodes are detected. Besides, they are deposed using trust information stored in monitoring node's isolation tables. Isolating information are gathered in the PCH, which communicates them to BS. If the raised alerts reach a given threshold, the topology changes to ignore intruders. The particularity of the assumed architecture, as well as, the important number of MNs, risk complicating the IDS, which affects thus the energy consumption average. In [23], energy efficient hybrid IDS (eHIDS) is introduced. The detection scheme combines both misuse and anomaly rules in order to identify abnormal communications in HWSNs. eHIDS agents are implanted only on clusters heads, which reduces significantly its energy

consumption. The anomaly detection model includes general attacks on integrity, delay and transmission range. Whenever an intrusion is detected, MNs generate alarm. Authors claim that the proposed IDS has high detection rate, while it hasn't been evaluated with specific and various attacks.

In [24] a novel model of IDS architecture is developed for intrusion detection in WSN, which presents an alternative solution to layered IDSs. It is about a cross layer intrusion detection model to detect various types of attacks. It consists of a module that brings together information specific to several levels in the protocol stack (routing, MAC and physical layers). Interactions between cumulated information are exploited so that detection accuracy, latency and cost would be improved. The proposed IDS which is destined to HEEP based networks, has the ability to detect sinkhole, data falsification and sybil attacks at network layer level, and DoS (energy exhaustion) attack at MAC layer. In this IDS, all network's sensor nodes can play the role of a MN, and upon each intrusion detection, an alarm is generated and directly communicated to the BS. Performances of the proposed IDS have been evaluated with a fixed and reduced number of adversaries. Authors haven't taken into consideration the case of increasing number of intruders, however, in such a case, there will be a large number of both detection members and the generated alarms, which may augment the total of energy consumption and decrease the effectiveness of detection.

5. The proposed IDS: Threshold Hierarchical Intrusion Detection System (THIDS)

In order to address the problem of insider attackers for routing security in HWSN, we propose an HIDS that detects selective forwarding, black hole attacks, and prevents the sinkhole attack called THIDS. These three attacks are as well, the most dangerous, especially when applied by CHs attackers, because of their enormous impact on network performance. Unlike the most existent IDSs (even all), that have energy-expensive alerting systems, where alarm messages are directly sent to the BS each time an intrusion is detected, our IDS presents a lightweight alerting system, composed of two types of alerting messages: local and general alerts. Local alerts, which have a little energy cost, are generated frequently. However, general alerts are raised periodically, depending on threshold reaching.

THIDS is intended to be integrated into hierarchical secure routing protocols. So, it has to fully respond to the different requirements, in particular those related to the simplicity and low energy consumption.

5.1. Network architecture

The proposed IDS is destined to cluster based WSNs, especially those where clusters are dynamically and periodically formed. THIDS suggests that each cluster should have a certain number of MNs that control the behavior of their CH.

The number of MNs that should be defined in each cluster is determined according to a tradeoff between detection effectiveness and energy saving. Choosing a few number of MNs affects the detection accuracy, where a large number introduces network overhead and energy exhaustion.

MNs are selected in a dynamic and pseudo random manner, for security (resistance to MNs compromising) and simplification reasons. Moreover, a MN is not dedicated to the detection task; it performs monitoring, data sensing and communication functionalities. In addition, each time clusters change, the selected MNs change as well.

In THIDS, the CHs don't monitor their members. The justification is that if the compromised node couldn't be a CH, its effect is often not important. Whether it reports bogus data messages or it reports no messages, it can't affect, significantly, data consistence and/or network performance, unless the number of intruders is large.

5.2. System model

In THIDS, it is required that each sensor node (including MNs) has a local list called the isolation list (or blacklist). Selective forwarding and black hole attacks are detected after that member nodes relay their data messages. MNs in each cluster start monitoring their CH, by hearing exchanged messages, during a period of time. If the MN finds that there is no data message sent by its CH, this last is henceforth considered as attacker. Consequently, the MN puts CH's identifier in its blacklist, and diffuses a local alert message, containing the related ID to the neighboring nodes (which may be part of adjacent clusters). On the reception of the alert message, nodes update their blacklists by adding attacker ID. The monitoring and detection algorithm is detailed as follows:

```
Threshold : value of the threshold..
BL : the blacklist.
T : time of intrusion detection beginning.
Slot-time : time of TDMA slot.
msg : message.
CHid : cluster head ID.
Begin
  T ← (length (TDMA) * Time-slot) + random delay.
  if ((time = T) and (ID != CHid)) then
    Wakeup ().
    if ( isMONITOR = true ) then
      listening ().
      if (no data message of CH is heard ) then
        Add_in_list (BL , CHid ).
        msg [data] = CHid.
        Send_local_ alert (msg).
        if ( (length_liste (BL) mod Threshold) = 0) then
          msg [data] = BL.
          Send_general_alert (msg)  ;//directly to BS.
        end if.
      end if.
    end if.
  end if.
End.
```

Detected attackers, whose IDs appear in node's blacklist, will never be chosen as CHs in the future clusters reconstructions. This allows then sinkhole prevention. Insider malicious nodes finding themselves isolated from being CHs, may

transmit falsified reports to the BS. So, for a complete isolation, MNs as well as the legitimate sensor nodes should send general alarms carrying their blacklists, to the BS. On account of the important energy cost of direct communications with the BS, general alert messages are sent only if the number of the detected intruders, in the blacklist, rises by a step equal to a specified threshold, as it is described in the algorithm of isolation :

```
AttackerID : identifier of the malicious node.
ADV : an advertising message sent by a cluster head.
JOIN: the joining message to be sent to a selected cluster head.
Begin

    Receive_message (locale alert) ;
    AttackerID  = msg [data].
    if ( Is_in_list (BL , AttackerID ) = false) then
        Add_in_list (BL , AttackerID ).
        if ( (length_list (BL) mod  threshold ) = 0) then
            msg [data] = BL.
            Send_general_alert (msg) .
        end if.
    end if.
      - In a new clusters reconstruction phase.
    Receive_message (ADV)   //from cluster head "CHid".
    if ( Is_in_list (BL, CHid) = false ) then
        Send_ message (JOIN)
    end if.

End.
```

The threshold value should be carefully defined; a reduced value leads to overload the network and a big value affects the process of isolation coordination with the BS. On each time it receives such a general alert message, the BS updates its proper black list by adding the new intruders, allowing it to revoke the susceptible incoming malicious messages.

Since the detection mechanism of our IDS is related to the ability of a MN to intercept CH's data message, it is possible that a false positive detection occurs. In this case, the CH reports, normally, the data message to BS but, at least one of the MNs couldn't hear it, due to a susceptible collision. The probability of false positive P_F for a cluster MNs is estimated in equation 1:

$$P_F = P_{coll}\frac{(2^{C_{MN}} - 1)}{2^{C_{MN}}} \quad (1)$$

Where: P_{coll} is the probability of collision in a transmission link, and C_{MN} represents the number of MNs in a cluster.

The probability of false positive detection, P_{FD}, on one CH is calculated using the Binomial rule as:

$$P_{FD} = \binom{C_{MN}}{1}(1 - P_F)P_F^{\,C_{MN}-1} \quad (2)$$

Basing on equation 2, we can deduce the probability of false positive detection on X CHs in the entire network:

$$P_{FD} = \binom{T_{MN}}{X}(1 - P_F)^X P_F^{\,T_{MN}-X} \quad (3)$$

Where: T_{MN} is the total number of MNs in the network.

By its simplicity, the proposed IDS reduces extremely the induced cost for attacks detection. The limited number of MNs conscripted in each cluster, as well as, the introduction of threshold notion on general alarms generation, make THIDS energy efficient. The consumed energy by THIDS on a monitor node MN_i is calculated as:

$$E_{MN_i} = E_d + E_p + E_a \quad (4)$$

Where: E_d is the consumed energy to detect the intrusion on the CH. E_p, is the processing energy on the blacklist (the checking and updating operations). E_a, is the needed energy for the alerting mechanism; the sending of both local and general alarms.

6. Secure routing optimization in HWSN: case study RLEACH optimization

For an optimal and enhanced routing security level in the HWSNs, a secure hierarchical routing protocol should integrate adapted IDS. In other words, the secure protocols have to implement intrusion detection systems as a second line of defense, in addition to cryptographic tools. The integration of our IDS, in secure hierarchical protocols, takes place just after data communications within clusters, and just before a new phase of topology reconstruction.

In order to validate our assumption, we have chosen the protocol RLEACH to be equipped with our intrusion detection system (THIDS). RLEACH is considered as one of the most robust secure hierarchical routing protocols [25]. It gathers the basic security characteristics that would have a secure routing protocol (a probabilistic key management protocol RPK, the symmetric cryptography and so on). Although it resists against several attacks, it is still not well protected against sinkhole, selective forwarding and black hole attacks. A compromised node could be a cluster head, since it establishes communication links with nodes belonging to its group, and it shares, probably, keys with other nodes. In this case, network performances risk to be influenced, even if there exist few numbers of insiders in the network. To optimize RLEACH security, we add the proposed intrusion detection system as an additional phase in RLEACH operation, where nodes should execute THIDS. The resulting protocol is henceforth named ORLEACH, for Optimized RLEACH. ORLEACH operation is, therefore, divided into the following phases:

- Shared-key discovery phase.
- Cluster set-up phase, isolation of previously detected attackers and MNs selection.
- Data transmission phase.
- Intrusion detection and alerting phase.

7. Evaluation and Simulation results

In order to evaluate performances of ORLEACH protocol, including THIDS, we have used the network simulator NS2. We have implemented both RLEACH and ORLEACH protocols on the MIT's NS2 extension for LEACH [26]. The assumed network model is composed of 100 sensor nodes, randomly deployed on a surface of 100 m², where all nodes are supposed fixed. The rest of simulation assumptions are presented in the table 1 below.

Table1. Simulation parameters

Parameter	Value
Location of the base station	(20,175)
Number of clusters	5
Packet length	500 bytes
Simulation time	600 s
Initial energy	3 J
Transmission technology	IEEE 802.15.4
Number of groups in RLEACH	10
Number of MNs in each cluster	2
Threshold value in THIDS	5

In the figure 2, we present the results of detection effectiveness evaluation for THIDS in the proposed optimized RLEACH protocol.

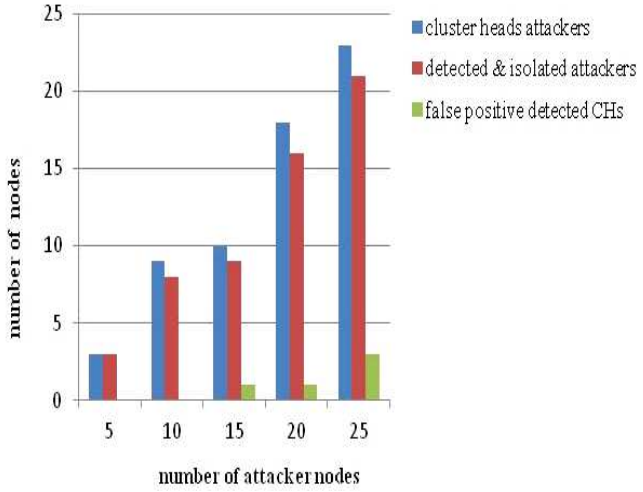

Figure 2. Detection evaluation in THIDS.

The above results, confirm that although the adoption of RPK scheme by RLEACH, insiders could still act as CHs. The proportion of detection and complete isolation of the intruders is 100% for a few numbers of attackers. This proportion becomes 91% when number of intruders is very important. This is justified by the possible collisions on the local alarms stemmed from adjacent clusters, which allows to the detected attackers to be CHs more than once. False positive detections on legitimate CHs are little. They are caused by collisions preventing messages hearing by at least one of the MNs in each cluster. We can judge THIDS detection process as sufficiently efficient.

The figure 3 shows the comparison results, between ORLEACH, RLEACH and LEACH protocols in term of the total delivered data to the BS, with the existence of variable and increasing number of compromised nodes. Those attackers attempt to be CHs at each new cluster set-up phase, and exercise selective forwarding or black hole attacks.

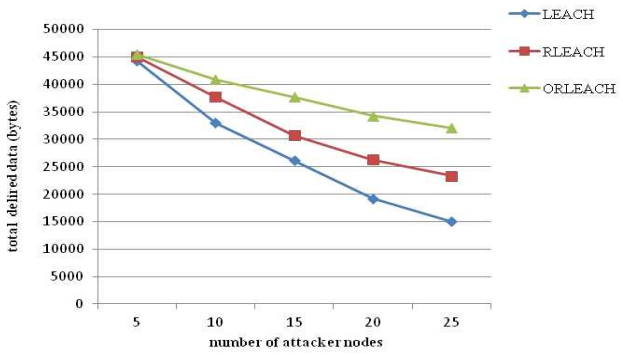

Figure 3. Total delivered data in ORLEACH.

The total of the delivered data in the network decreases, considerably, in LEACH and RLEACH protocols, each time the number of insider attackers augment, which isn't the case with ORLEACH protocol. This last (ORLEACH), seems much more resistant, thanks to the integrated THIDS.

In the figure 4 results corresponding to the total energy dissipation in the three protocols over the time are given.

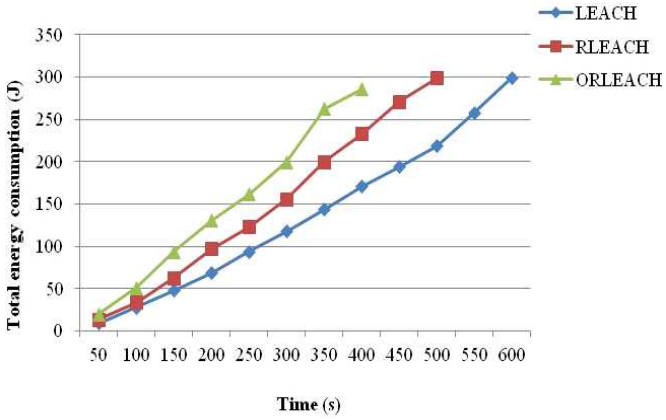

Figure 4. Total energy consumption in ORLEACH.

Logically, the integration of an IDS in the protocol RLEACH increases the energy consumption rate, which decreases, by consequent, the network lifetime. Our goal is to minimize as much as possible this rate. This goal is achieved through the simplification of the incorporated IDS. We find the additional devoted energy in the protocol ORLEACH is acceptable for an optimized routing security.

8. Conclusion

In this paper, we have presented an approach for constraints-aware optimization of routing security in HWSNs. We have first proposed an IDS (THIDS) that is prevented to be integrated in secure hierarchical routing protocols. THIDS has the ability to detect malicious CHs exercising the most dangerous attacks (sinkhole, selective forwarding and black hole). We have then, chosen the protocol RLEACH to be optimized by the proposed IDS.

Since the simulation results on the resulting protocol, ORLEACH, prove the validity of the prior assumptions. We recommend that each secure hierarchical routing protocol adopts adapted IDS. So, the design of the secure hierarchical routing protocols should consider intrusion detection as a necessity.

As a future work, we will extend our IDS to detect other types of attacks and thus, we think to adapt it and evaluate its performances in internet enabled WSNs, so-called 6LoWPAN networks.

References

[1] F. C. García-Hernández, et al, "Wireless sensor networks and applications : a survey," International Journal of Computer Science and Network Security (IJCSNS), vol. 7, No. 3, pp. 264-273, March 2007.

[2] R. Patel, S. Pariyani, V. Ukani, "Energy and throughput analysis of Hierarchical routing protocol (LEACH) for wireless sensor network," International Journal of Computer Applications, Vol. 20, No. 4, pp. 32-36, April 2011.

[3] K. Sharama, M. K. Ghose, "Security model for hierarchical clustered wireless sensor networks," International Journal of Computer Science and Security (IJCSS), vol. 5, No. 1, pp. 85-97, 2011.

[4] W. R. Heinzelman, A. Chandarkasan, H. Balakrishanan, "Energy efficient communication protocol for wireless micro sensor networks", 33rd IEEE International Conference on System Sciences, pp. 1–10, Hawaii, January 2000.

[5] S. Lindsey, C. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems", IEEE Aerospace Conference, pp. 1125-1130, 2002.

[6] D. E. Boubiche, A. Bilami, "HEEP (hybrid energy efficient protocol) based chain clustering," Int. J. Sensor Networks, vol. 10, No. ½, pp. 25-35, 2011.

[7] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks,'' IEEE communications surveys & tutorials, vol. 8, No. 2, pp. 2-21, 2006.

[8] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," University of California at Berkeley, 2003.

[9] A. C. Ferreira, et al, "On the security of cluster-based communication protocols for wireless sensor networks", Fourth IEEE International Conference on Networking (ICNŠ), Berlin, pp. 449–458, 2005.

[10] D.Wu, G. Hu, and G. Ni, "Research and improve on secure routing protocols in wireless sensor networks", Fourth IEEE International Conference on Circuits and Systems for Communications (ICCSC), pp. 853–856, Shanghai, May 2008.

[11] K. Zhang, C. Wang, C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management", IEEE Computer Society, pp. 1-5, 2008.

[12] H. Chan, A. Perrig, D. Song, "Random key pre-distribution schemes for sensor networks," Proceedings of the IEEE Computer Society Symposium on Security and Privacy, Piscataway, USA: IEEE, pp. 197-213, 2003.

[13] A.M. El-Semary, M. M. Abdel-Azim, "New Trends in Secure Routing Protocols for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, pp. 1-17, 2013.

[14] V. T. Kesavan, S. Radhakrishnan, "Multiple Secret Keys based Security for Wireless Sensor Networks", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 4, No. 1, April 2012.

[15] G. Wroblewski, "General method of program code obfusction," Proc. Int'l Conf. Software Eng. Research and Practise (SERP), June 2002.

[16] T. Park, S. Member, K. G. Shin, "Soft tamper-proofing via program integrity verification in wireless sensor networks," IEEE Transactions on mobile computing, vol. 4, No. 3, pp. 297-308, May/June 2005.

[17] http://cordis.europa.eu/projects/rcn/95511_en.html.

[18] A. Abduvaliyev, et al, "On the Vital areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, pp. 1223-1237, 2013.

[19] N. A. Alrajeh, S. Khan, B. Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", International Journal of Distributed Sensor Networks, pp. 1-7, 2013.

[20] E. Darra, S. K. Katsikas, "Attack Detection Capabilities of Intrusion Detection Systems for Wireless Sensor Networks", IEEE Fourth International Conference on Information, Intelligence, Systems and Applications (IISA), Piraeus, 10-12 July 2013

[21] H. Jalali, A. Baraani, "Process Aware Host-based Intrusion Detection Model", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 2, August 2012.

[22] R. C. Chen, C. F. Hsieh, Y. F. Huang, "An isolation intrusion detection system for hierarchical wireless sensor networks," Journal of networks, vol. 5, No. 3, pp. 335-342, March 2010.

[23] A. Abduvaliyev, S. Lee, Y. K. Lee, "Energy efficient hybrid intrusion detection system for wireless sensor networks," International Conference on Electronics and Information Engineering (ICEIE), Vol. 2, pp. 25-29, Kyoto, 2010.

[24] D. E. Boubiche, A. Bilami, "A cross layer intrusion detection system for wireless sensor network," International Journal of Network Security & Its Applications (IJNSA), vol. 4, No, 2, pp. 35-52, March 2012.

[25] S. Sharma, S. Kumar, "A survey on secure hierarchical routing protocols in wireless sensor networks," proceedings of ACM ICCCS'11, India, pp. 146-151, February 2011.

[26] "The MIT uAMPSns code extensions, Version 1.0," Massachusetts Institute of Technology. Cambridge, August, 2000.