I. J. Computer Network and Information Security, **2016, 7, 50-60**
Published Online July 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.07.07

Intrusion Detection System to Overcome a Novel Form of Replay Attack (Data Replay) in Wireless Sensor Networks

Yasmine Medjadba
Science and Technology Department, Beijing Normal University, Beijing, 100001, China.
E-mail: yasmine.med1@yahoo.com

Somia Sahraoui
LaSTIC laboratory, Computer Science Department, University of Batna 2, Batna, 05000, Algeria.
E-mail: somiasahraoui@ymail.com

Abstract—Wireless Sensor Networks (WSNs) are widely and successfully employed in various application domains. They are easily deployed to collect valuable information and monitor potential environmental phenomena. However, the special nature of WSNs as well as their severe constraints and resource limitations make them vulnerable to various types of threats. Replay attack, is one example. According to this attack, the adversary intercepts and replays several times the same (old) message leading either to missed alerts or to false alerts. Many solutions have been proposed to mitigate message replay attack. However, all these solutions are of cryptographic natures and consider only external attacks exercising a trivial scenario of replay attack. In fact, the attacker could be a lot smarter, and in this case, it replays only the data field in the message while keeping the remaining fields updated. This novel form of replay attack is much more dangerous and difficult to be detected. We call this attack variant by data replay attack. As sensor nodes may be easily captured and compromised, the worst scenario occurs if data replay attack is performed by an internal intruder. In this paper we propose an efficient intrusion detection framework to overcome data replay attack in WSNs. The proposed intrusion detection system is named *DR-IDS* (Data Replay Intrusion Detection System). The performance evaluations performed under NS2 simulator show that the proposed solution is sufficiently robust.

Index Terms—Wireless sensor networks, security, replay attacks, data replay, intrusion detection system.

I. Introduction

Nowadays wireless sensor networks (WSNs) [1] and their wide application fields are becoming progressively more popular because of their low cost, flexibility, ease of deployment and self-organization ability. Sensor nodes in a WSN capture the information of interest (e.g. temperature, humidity, image …) from the surroundings and communicate it in the form of messages to the base station (BS), through wireless and multi-hop communications. The BS represents a downstream of all information coming from the sensor nodes.

Regarding 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 detection and communication tasks. 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.

Sensor networks have great advantages in various applications [2] such as: battlefield monitoring, habitat monitoring, intelligent agriculture, home automation, etc. where the quality of services is substantially improved due to the remote monitoring and real-time reporting and reaction. Recently, the integration of WSNs into the Internet is highly investigated [3].

WSNs are prone to diverse models of attacks targeting different network levels Security in sensor networks is a real challenge because of the numerous constraints (like the random deployment in unattended areas), and the limitations related to the energetic, computational and storage resources, which prevent the adoption of robust and highly complicated security mechanisms.

The replay attack [4] is known to be among the most dangerous attacks that target the freshness feature of network messages. In its common scenario, the attacker simply replays the same message (application data and signaling information) many times leading to missed or false alerts, all depending on the replayed message. Indeed, the attacker could be more intelligent, and therefore replays only the data field in the message. This novel scenario of replay attack is much more dangerous in WSNs where the sensed data are often sensitive and need to be fresh.

Several research works have been conducted to prevent replay attacks in WSNs. These works focus generally on the cryptographic solutions. But, if the network includes compromised sensor nodes, these solutions become

insufficient. In this context, we propose an intrusion detection system (IDS) for the assumed scenario of replay attack in WSNs.

In the following sections, we give review of related works. After that, we express the motivation behind the need in intrusion detection for data replay attack. Finally, we describe the context of the performance evaluation of our solution and we present and discuss the obtained results. Finally, we conclude the paper.

II. Background of Security in WSNs

Security is of paramount importance for the successful missions of WSNs. However, the wireless nature of links and limited resources make the network vulnerable to many threats. In this section, we present a brief review on security concerns in WSNs.

A. WSN Vulnerabilities

The principal vulnerabilities of wireless sensor networks are summarized in the following points [5, 32]:

- **Random deployment in harsh and unattended areas:** This is a major reason of exposure to failures and compromising risks, where a malicious party may capture sensor nodes and alter their programs so that they behave in a malicious way once they are reintroduced in the network.
- **Wireless and multi-hop communication:** The wireless transmission medium opens a door of insecurity. Thus, data can be easily intercepted and analyzed by an attacker who is in the same communication range. The short radio range of the sensor nodes and the necessity of multi-hop communications for data routing give the opportunity to attackers to interpose between terminal sensor nodes and the base station.
- **Limited resources:** Sensor nodes are seriously limited in memory, computational and particularly energetic resources. Thus, the limited energy reserves of each sensor node must be carefully managed to prolong, as much as possible its lifetime. An attacker may exploit this constraint to launch attacks that exhaust the energy and overload mote's memory and computational resources.

B. Threat Models

Attacks on sensor networks can be classified into different models. They can be classified Into the Following classes [6]:

- **Outsider attacks:** In this type of attack, the adversary is not part of the deployed nodes and it has no internal network information.
- **Insider attacks:** (that are the most dangerous) are due to the bad behavior of legitimate sensor nodes that have been captured and compromised. This operation is called node compromising.
- **Mote-class attacks:** In this type of attacks, attacker is a resources-constraining node, quite like network nodes.
- **Laptop-class attacks:** Adversary is much more powerful, it disposes of a greater processing power, a very large transmission range and a sufficient energy reserves.
- **Passive attacks:** The goal of the attacker is to listen to the traffic to intercept and collect data in order to extract secret information about the network.
- **Active attacks:** The attacker tries to exploit vulnerabilities in protocols used in the network to launch a variety of attacks, such as alters, misroutes, replays or blocks arriving packets.

C. Security Requirements

To ensure security in sensor networks, the following conditions must be guaranteed:

- **Confidentiality:** Protect the information so that to be communicated secretly by preventing unauthorized entities from access it.
- **Authentication:** Ensure that communication between nodes is authentic via the identity validation techniques of each node.
- **Integrity:** Ensure that exchanged messages haven't been modified and falsified during transmission.
- **Availability:** Guarantee the accessibility to network's services and resources.
- **Freshness:** Ensure that data is recent and old messages are not replayed.

D. Replay Attack Context

Replay attack aimed primarily the messages exchanged between the nodes of the network, where the adversary captures packets in an old context and retransmits, repeatedly in another, targeting the freshness property of data. The figure1 illustrates replay attack.

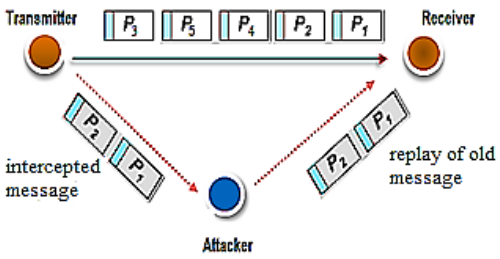

Fig.1. An Example of Replay Attack.

According to this type of attack the adversary simply replays the same message (data and header) many times, which has an important impact on data freshness and network performances. It has also many other negative effects not less important, such as:

- In the routing phase, the attacker communicates old information on the state of neighborhood nodes,

which can lead to the construction of bogus routing tables, which will further affect the connectivity and overall network topology consistency.
- This attack can also be used in the phase of key distribution, where the adversary replays the new key with the old one so that it could easily intercept the encrypted data.
- Also, replay attack can be exploited to perform other types of attacks such as DoS (Denial of Service) attacks.

Thus, replay attack has many crucial effects on applications. By replaying old messages, we may prevent the reporting of an emergency (such as the case of forest fires detection), or the generation of a false alarms, creating a conflict situation with the current state of the monitored environment.

III. Related Works

Security in sensor networks is a challenging task because of the severe constraints and resource limitations characterizing WSNs. Therefore, it becomes mandatory to design models highly aware of these constraints while providing a good level of security.

In this section, we present a state-of-the-art of the proposed solutions for secure sensor networks against the replay attack. The proposed solutions are mainly focused at the link and network layers. Some solutions exploit the interactions between the different layers for the development of cross-layer security solutions.

A. SPINS

SNEP as part of SPINS protocol [7] among the first solutions that take into account this type of attack. Based on the synchronization technique where in a counter is maintained at each node increases with the reception of a valid message. The drawbak of this solution is that each node maintains a counter of all the network nodes for communication, which is not feasible with the resource-limitated nodes. Also, if the packet is lost, the count between the transmitter and the receiver becomes incompatible.

B. Framework

Several architectures have implemented at the link layer in order to provide different security mechanisms requested. TinySec [9] is a popular link layer security protocol, offers several approaches to protect against replay attack, which are:

Counter: based on the use of a counter introduced by TinySec_AE format. Over a sliding window maintained at each node is used to store the received packets in order. Upon each reception, the counter is compared with the previous received, if lower will be compared with those introduced in the window. In the case of equality with a value, package considered replayed and rejected. The disadvantage is that a window is created for each node which affects the resources of the node.

Hash function: The same principle of counter approach, except that it is replaced by a value generated by using the hash function SHA-1. However, it accepts as input a message of length less than 264 bit and outputs 160 bits. The receiver compares the received value with those of the window, if packet exist is rejected. The route of the window takes time, which affects real-time applications.

Bloom Filter: the Bloom filter is a probabilistic data structure to test whether an element is a member of a set or not, with the possibility of false positives. At the receiver, k hash function is applied to each incoming packet. Each case of Bloom is checked if equal to 1 then the packet is replayed and rejected otherwise be accepted. The algorithm uses multiple hash functions to minimize the probability of false positive, such that k hash functions with probability ($1/2^K$). The small probability of false positive leads to accept packets replayed and several hash functions require computing power and high energy that affects the state of the sensor.

MiniSec [10] is another framework implemented at this level, which runs in unicast mode and broadcast called respectively MiniSec-U and MiniSec-B. It offers ways to prevent replay attack as the counter, the approach of the sliding window and the approach of Bloom Filter.

Counter: this type of security is used only in unicast mode, where a counter is maintained between two nodes before starting communication. However, it is encrypted by the OCB function to make a single value attached to each packet. At the time of communication packets sent contain the last x bits (last bit) of the counter to minimize energy consumption. However, the receiver checks if the counter is maintained at this higher level, then the packet is accepted and the counter will be incremented. Other different value, the packet is discarded. In case of loss, the counter is incremented to avoid implicit synchronization between nodes. Disadvantage is that a counter is maintained for each node, the result using a lot of resources. If packet loss is high, the counter value will be incompatible requiring heavy resynchronization mechanisms. The implicit incrementing the counter can accept packets replay.

Sliding window: this approach is applied MiniSec-B mode, where a defined period of time and chatting to sub periods between pairs of nodes, in the form of a time window. Each period has a length calculated according to the time of ΔT synchronization error and the time of maximum latency ΔN network under form. The packets are encrypted using the OCB function that uses the number of its period (as a nonce) to prevent the replay of earlier periods packages. At the time of receipt, decrypting packets leads to get a nonce value indicates the time of transmission. Thus, the window is more vulnerable to the replay attack so, it is ineffective for this type of attack.

Bloom filter: at the nodes, bloom filters are maintained to keep packets accepted on both current and prior periods. Indeed, the received packet matches with the current BF; if the result is true it is replayed considered and will be rejected. If the packet is accepted is recorded

at BF before. Bloom filter suffers from the same problem of False Positives.

Another framework implemented at the link layer works on the same principle; such as: FlexiSec [11], SenSec [12] and LLSP [13].

C. μSec "MicroSec"

μSec [14] another link layer-based solution that offers multiple techniques to ensure security in unicast mode. It implements the same meter based on synchronization mechanism applied by MiniSec in order to prevent replay of messages. In effect, the counter encoded on four bytes, and only the last eight bits which are integrated in the package. At the time of communication, the receiver accepts the packet only if the counter equal maintained at this level, followed by incrementing its value by one. This mechanism leads to disadvantages that the advantages offered because of the overhead added at the nodes. Thus, the synchronization problem on the meter requires significant resynchronizations mechanisms. In addition, the attacker can easily inject old packages at the network level and keep the counter current.

D. The Freshness of Aggregated Data

Security mechanism applies the principle of a hash function, to ensure security in the aggregate data phase [15]. Based on the hash function and a value , the collected data is concatenated with the value ; apply the hash function on the results and the holes concatenated with the data collected in the clear. Upon receipt of the message at each node; calculate the difference between data with those received in the clear before node and apply the hash function. The format of the message to convey is:

$$(D1//H(D1//V0))//(D2-D1//H((D2-D1//V0))//.....//(D1-D1//H(D1-D1//V0))$$

Upon receipt of the data by the reader, it computes the hash of plaintext data using the same value ; the value obtained is compared with that of the hash function received, if are equal then the message is accepted otherwise be ignored. At the end of each session, the aggregator node to update the value and broadcast all son nodes. Disadvantage is during the broadcast of , the attacker can retrieve and influence communication and if it compromises the aggregator node, all communication will be falsified.

E. CARP "Clustered Anti-Replay Protection"

Based on the use of a table of size equal to the number of nodes, and a counter [16]. CARP requires a uniform distribution in the area to be monitored. Traffic is routed through the cluster-head in each group of this; the table is allocated only to the level and consists of two fields: ID (member nodes and other cluster-heads) and the corresponding counters. As the members maintain only the head of the counter. The communication is initiated by an authentication phase. At each dispatch, the counter is incremented and attached to the message, at the receiver, verifying that the counter is less than the message packet is therefore accepted, otherwise will be rejected. The disadvantage is if the number of neighbor nodes is large enough that the space allocated in the table, can replace some input by others, saturation of the node. It protects the network against the replay attack, but has no explicit mechanism described for maintaining the basic security properties.

F. AASP

AASP protocol [17] implements two mechanisms, which are: the last MAC and authentication handshake. The protocol based on the authentication phase. Used to send the current message with the MAC code generated for the package in front. At the receiver, if the MAC calculated for the preceding packet is equal to that of the message, then the packet is accepted. In case the packet is lost, the protocol uses the principle acknowledgment. The disadvantage is that the connection between nodes is lost re-authentication will be rejected because the node is considered an attacker. Using ACK leads to a large amount of data exchanged.

G. SecSyWiSeSec

SyWiSe protocol [18] resists the replay attack by counter mechanism. Communication is preceded by the synchronization time distribution between nodes and shared only when active, in order to safeguard energy load. The protocol used between the source node (base station) and allows sensor nodes to ensure the periodic distribution of messages on all nodes in a fixed time interval. The synchronizations of messages disseminated take the following structure:

$$m = (ID, tsp, c, sig(h(tsp \,||\, c)))$$

Each transmission of the message counter is increased by the base station and accepts the nodes if it is greater than the last received counter, that is keep locally. Moreover, the value of the signature if it is valid. The disadvantage is that because of certain transmission conditions, nodes do not receive the synchronization message which leads to lose the count.

H. Sec-LEACH

Sec-LEACH protocol [19] is a secure version of LEACH routing protocol. The protocol provides mechanisms against the replay attack to prevent the construction of groups of old configuration requests. At the time of configuration, each cluster-head broadcasts a packet on the nodes to join its group contain its id and nonce used to ensure the freshness of queries sent. Indeed, nodes wishing to participate in a given group, spread a message contains the nonce the corresponding head to facilitate him to accept the request only if the nonce value equal to that maintained its level.

Protocol also ensures the freshness at the time of communication by sharing a meter between the leader and the station, which increases with each sending

aggregated data valid. The disadvantage is that the attacker can play the role of cluster-head that affects the communication.

I. SHEER

SHEER protocol [20] based on the principle of nonce to prevent replay attack. The protocol has four phases: an initiation phase, neighbor discovery phase, clustering phase, and data message exchange phase. After network deployment, the base station generates using the key escrow table and HMAC function. It generates a broadcast authentication nonce N_R, and encrypts it using KR as: $N'_R = E_{KR}(N_R)$ and pre-loads each sensor with N'R. To send an initiation call, it broadcasts the following message: $N_b||I_R||OR||E_{KR}(init||N_B||N_R||N''_R)$ nonce generated by the base station to prevent a replay of the message by an adversary. When a node receives the message decrypts the N'_R using K_R as: $D_{KR}(N'_R) = N_R$, if the obtained N_R is the same as that received in, the node is assured that the base station is the source of the message. It replaces N'_R with the new encrypted revocation nonce (N''_R) then initializes its timer and starts the neighbor discovery phase. If the attacker managed to decrypt the message; it can easily reply the request with an old once. The principle of nonce only limited to prevent external attacks.

J. NSKM

NSKM protocol [21] another security protocol of the network layer, implements the technique of time-stamp and to prevent replay attack. Defined as a field directly at the packet level proposed by the protocol. NSKM use three categories of keys. It is requisite for all the sensor nodes to hold and maintain their keys. Many control messages transmitted between nodes with the integration of time-stamp for each message and synchronize it values. If the attacker knows the encryption key, it can capture the packet and desynchronized the state of time stamp, and replay data easily.

K. ZigBee/IEEE 802.15.4 Standard

The standard ZigBee [22] defines by default protection mechanism against message replay on the principle of shared counter. That is incremented for each transmission of a message. The major drawback of this mechanism is that each node must maintain a counter for all neighbors, which influences the limited resources and led the performance degradations.

L. NEKAP

NEKAP protocol [23] applied at the link layer. It is modified to make the protocol less vulnerable to replay attack depending on ACKs and time stamp (time-stamp). The protocol offers several different types of keys, depending on the message to send. At each transmission, the request is encrypted by the global key and authentication using another key, to prevent its modification. At the time of communication, each message sending followed by ACKs, if ACK received during a defined time, the transmitter node is considered honest, if the AC is dismissed with saved data. The node considered as a malicious and all information will be rejected. The disadvantage is the ACK mechanism makes the slow communication and if an attacker manages to find the keys can affect the network.

In the table bellow, we give a general comparison between the highlighted solutions, Where *, /, +, ++, -- denote respectively: supported, not mentioned, important, very important and very low.

Table 1. General Comparison between Existing Security Solutions for Message Replay Attack

Protocol		Technical	Goal		Operational layer			Mode function	Severity level	Overhead
			Prevent	Detect	MAC	network	Cross layer			
SPINS		Counter	*		*			Unicast	+	++
Mixed Sequencing		Counter explicit & implicit	*		*			Unicast	+	++
Fram work	Tiny-Sec	Counter	*		*			Unicast	+	++
		Hash function						/	+	++
		Bloom Filter						Broadcast	++	++
	Mini-Sec	Counter	*		*			Unicast	+	++
		Sliding window						Broadcast	--	+
		Bloom Filter							++	++
µSec		Counter	*		*			Unicast	+	++
NEKAP		ACK & Tsp	*		*			Unicast	++	++
Zigbee		Counter	*			*		Unicast	+	++
Freshness of aggregated data		Hash function	*			*		Unicast	++	+
Sec-LEACH		Nonce	*			*		Broadcast	++	++
		Counter	*					Unicast	+	+
CARP		Table & counter	*				*	Unicast	+	+
AASP		Last MAC & authentication handshake	*				*	Unicast	++	++
SHEER		Nonce	*				*	/	++	+
NSKM		Time-stamp	*				*	/	++	++
SecSyWise		Counter	*				*	Broadcast	+	+

IV. Problem Description

The most of the existing security solutions against replay attack in WSNs are focused on cryptographic solutions and key management schemes [24]. These security systems are efficient enough to face external replay attacks. However, it is remarkable that no solution takes into account the internal replay attacks (exercised by the compromised sensor nodes) where the attacker can replay messages, even with the adoption of cryptographic countermeasures, which presents a serious security problem affecting the freshness of sensing data (often highly critical). Consequently, cryptographic and key management solutions couldn't provide alone the desired security level in WSNs, even if the network contains only a few compromised nodes. For this reason, the integration of intrusion detection mechanism is highly suggested, so that malicious behaviors may be detected, and the concerned nodes could be isolated.

In addition to the internal replay attacks scenario, we assume the attacker to exercise intelligently replay attack in such a way that it replays only the effective data contained in the messages while updating the signaling information carried in the appended protocol headers. We name this special form of replay attack by data replay attack.

Data replay seems to be much more harmful than message replay attack in data-centric networks like WSNs.

V. Intrusion Detection in WSNs

An intrusion detection system (IDS) is a system that manages the detection and isolation of these intruders in the network through a set of control nodes (MNs). MN is a sensor node having to monitor network traffic and transmit alarm misbehavior detection messages. Although the intrusion detection is an essential aspect of network security, especially in networks where nodes are very prone to theft (as sensor networks). Researchers are carrying out massive studies to find IDSs, to all kinds take Considerations the overhead the dissipation of energy and the cost of complexity. The principal constraints [25] 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 an intrusion detection system [26]:

- 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.

VI. The Proposed IDS: Data Replay Intrusion Detection System (DR-IDS)

The replay attack qualified among the most dangerous attacks, due to the damage inflicted on the network. However, it is very difficult to determine their attendance in the communication or even guess especially if it is an internal attack. Maintain and implement all the most advanced security mechanisms such as cryptography, against this kind of attack, this would not be enough to eliminate its impact. Indeed; the essence of Replay attack is a compromised node that is easily operated, because of the lack of control over the network.

The primary objective of the replay attack is to assign the actual data that form the state of the monitored field and reflects the true network deployment target, the entire message replay attacks that are generally easy to be detected and faced. according to the novel attack scenario, the attacker replays only the data field while keeping the signaling information in the packets up to date so that to make the detection task much more difficult. The expected scenario is particularly harmful in WSNs, where data are often critical and freshness-requiring. The figure2 illustrates an example of replay data.

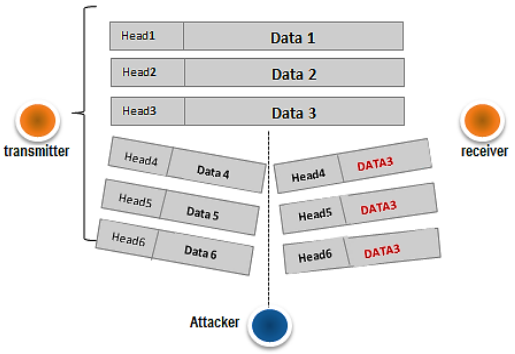

Fig.2. An Example of Data Replay Attack.

Cryptographic solutions that have a preventive nature are insufficient in case of existence of insider attacks. An intrusion detection system is suggested in this case to deal with internal data replay attack. Many IDSs have been proposed for protecting WSNs from different types of attacks as sinkhole, Sybil and black hole, etc [26, 27, 28, 29]. However, none of these systems treat the case of replay attacks. It remains a threat to the network regardless of the means of prevention available.

In this paper, we propose the first intrusion detection for data replay in WSNs. 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, uses in case the data are not encrypted, helped to the base station to confirm the identification of the attacker. However, general alerts sent by the base station, are raised periodically, depending on threshold reaching.

DR-IDS is intended to be integrated into the network layer especially, in routing protocols operation as replay attack targets the routing feature. So, it has to fully respond to the different requirements, in particular those related to the simplicity and low energy consumption.

A. *Network Model*

It is obvious that sensor node compromising affects network security and performances, but the most crucial is a successful compromise of a cluster head node in a hierarchical cluster-based WSN since the cluster head plays an important role in the network. In order to deal with such a case, we consider in our solution the case of clustering WSN.

The specification of detection policy is a very important step in the design of IDSs. To get an ideal level of detection effectiveness (misbehavior discovery and intruder identification). The proposed IDS is destined to cluster-based WSNs, especially those where clusters are dynamically and periodically formed.

Detection agents: They are network entities charged of detecting and intruders and identifying the typology of the exercised attacks. The operational entities in the proposed IDS are:

- **Monitor Nodes (MN):** A subset number of sensor nodes in each cluster are commissioned to play the role of anomaly detectors. It's worthy to note that we should realize a trade-off between a high level of detection accuracy and low resource consumption when choosing the number of monitor nodes in the network. Indeed, a few numbers of MNs affects the detection effectiveness, where a large number introduces network overhead and energy exhaustion. Another interesting aspect to be considered when deciding the number of MNs is related to coverage of radio communications inside each cluster. As sensor nodes have generally short transmission range, a much reduced number of MNs may not provide a large coverage of all communicating nodes in a cluster. Furthermore, MNs are selected in a dynamic and pseudo random manner, for security (resistance to MNs compromising) and simplification reasons. If data transmitted from CHs to the BS are encrypted, detectors are not selected since they do not know the decryption key. So, the MNs are operational only in the case where the data are not ciphered.
- **The base station:** To consolidate our IDS, the base station acts as a detector of possible malicious CHs. It can be active at any time for the observation of anomalies. Indeed, resource availability, and all information on the nodes at the BS, making it easy replay detection process. In DR-IDS, the CHs don't monitor their members. The motivation 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 consistency and/or network performance, unless the number of intruders is important

B. *The Detection Process*

Our intrusion detection scenario is as follows:

At level of monitor nodes, sensor nodes maintain a list (including collector's knots) to keep malicious CHs and help to isolate these nodes from the network. Each MN-detector acts as CH in its coverage area, so that monitors and listen to traffic sent by its neighbors. Indeed, after the transmission of collected data to the head, detectors welcome but only by nearby nodes. However; receiving the data collected by the detectors is followed by the data aggregation and to perform the role of CH, the detector nodes collaborate with each other so that they get the overall aggregation of all cluster members. After the aggregation phase, the detectors are starting to control the CH and listen to the traffic routed to the BS. Indeed; if the data is the same as that calculated by each detector while the communication is successfully completed in this level. But, if the value sent by CH is different from the detectors it is considered as an attacker and placed in the insulation list. A local alarm is sent to inform neighboring nodes. Figure 3 shows the detection process in each cluster.

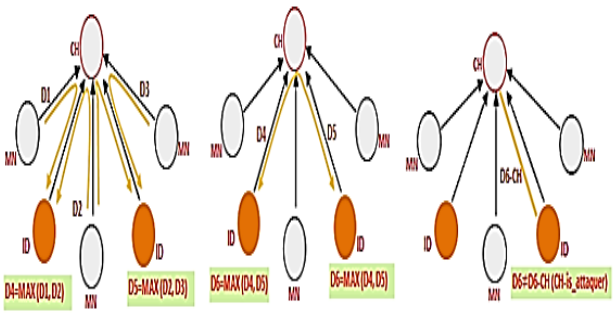

Fig.3. The Detection Process in Each Cluster.

However, breaches of confidentiality and integrity do not affect our detection system.The detection algorithm at the monitor nodes is as follows:

```
nodeID: node detector;
Time: TDMA duration;
Data: data;
Is_attaquer: list of attackers;
MN: member's knots;
Begin
   If (Time) then
      Reception (Data, MN);
   end If.
   If (CH == true) then
       Data-CH -> Aggregation (Data);
   end If.
   If (nodeID == true) then
       Data-nodeID -> Aggregation (Data);
         If (Data-CH != Data-nodeID) then
             Add_List (Is_attaquer, CH);
             Send_Local_ Alert (Is_attaquer);
         end If.
   end If.
End.
```

At level of the base station, the base station keeps the old data already sent by CHs and defines a threshold in order to effectively assert data replay attack and avoid false positive (false alarm). BS compares each time the value of the received data with the old kept; in the case of equality an observation value is incremented for this node. After a preset threshold, the base station decides with detectors if the CH is in the list of attacker, if it is found the replay is certified and a general alert broadcast on the network. The detection algorithms at level of base stations are :

```
Data-old: old data;
CH: the Head node;
Obs: value of observation;
Begin
   Reception (Data, CH);
   If (Data == Data-old) then
      Obs++;
      If ((obs == threshold) && (is_attaquer (CH))) then
         Send _General_ Alert (is_attaquer (CH));
      end if.
   end if.
End.
```

```
CH-attacker: malicious node;
ADV: an advertising message sent by a cluster head.
JOIN: the joining message to be sent to a selected cluster head.
Begin
   Reception_Alert (is_attaquer(CH));
   CH-attacker = is_attaquer (CH);
   If (check_list (is_attaquer, CH) == false) then
      Add_List (Is_attaquer, CH-attacker);
   end if.
   Reception (ADV);
   If (check_list (is_attaquer, CH) == false) then
      Send (JOIN);
   end if.
End.
```

VII. Evaluation and Simulation Results

In order to evaluate performances of DR-IDS, we have used the network simulator NS-2 [30] and the use of hierarchical routing protocol LEACH (Low Energy Adaptive Clustering Hierarchy) [31]. 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 table 2.

Table 2. 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 MNs in each cluster	2
Packet length	500 bytes

The number of attackers in the simulation is varied. The attackers are CHs to have an influence on the data sent to the base station. We present the results of the evaluations proposed IDS's performance in the case where data transmitted from CH to BS plain and also, if the data is encrypted.

A. *Energy Consumption*

We are interested in the energy consumption of nodes as an essential evaluation parameter.

Case of unencrypted data: Incorporating our IDS in the network operation increases the amount of consumed energy, which consequently reduces the lifetime of the network, because of additional functionalities and the new exchanged messages. The figure bellow depicts the obtained results in this case.

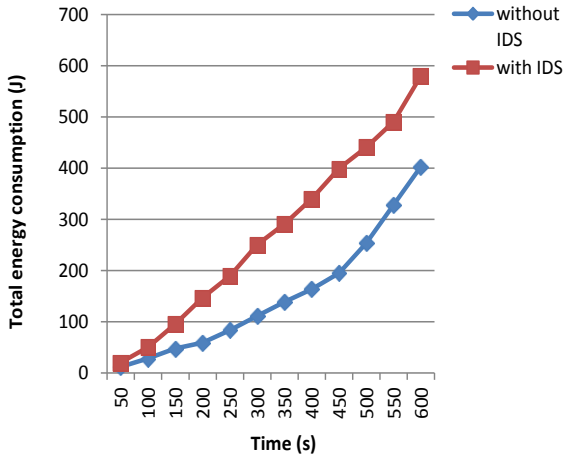

Fig.4. Total Energy Consumption by IDS in the Case of Unencrypted Data.

Case of data encryption : here we evaluate the energetic costs of DR-IDS in the case of messages encryption between the cluster head nodes and the base station. The obtained results are presented in the figure 5.

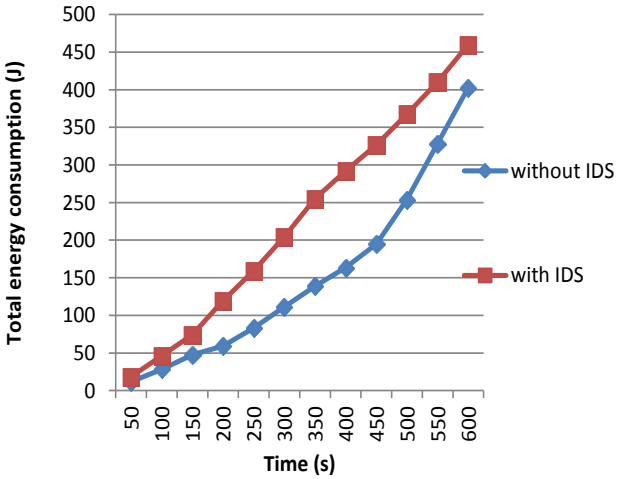

Fig.5. Total Energy Consumption by IDS in the Case of Data Encryption

The excess amount of energy consumed in this case is caused by the communication of alerting messages, including false alarms that are sent by the base station and destined to all network nodes.

B. *Detection accuracy*

Data replay detection accuracy is evaluated. The rates of detected and isolated attackers in DR-IDS are given in figure 6.

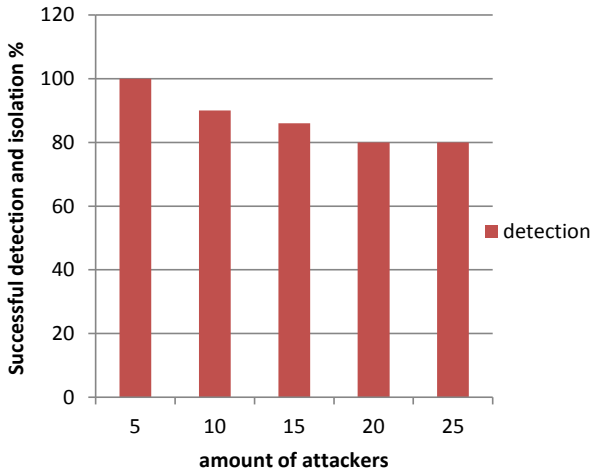

Fig.6. Data Replay Detection Effectiveness in DR-IDS.

The detection level is the same in both cases of the non-encryption and data encryption. The results show that the detection rate and complete isolation of intruders is about 100% when the number of attackers is reduced. But, when their amount becomes relatively important, the proportion of attack detection and intruder isolation decreases slightly down to 80% due to collisions that occur upon the communication of detection alarms.

C. *False Positive Detection*

The case of false positive detection occurs when monitoring entities make accidently a wrong detection and generate accordingly false alarms leading to the isolation of legitimate nodes that act correctly. False positive detection is a decisive parameter that affects detection accuracy in an IDS. In DR-IDS, the choice of the alerting threshold value is the main factor that influences detection credibility.

We evaluate the amounts of false positive detection in DR-IDS with different threshold values in the case of encrypted and unencrypted communications between CHs and the base station.

Case of unencrypted data: in such a case, detectors in each group help the base station to confirm the identities of attackers and avoid false positive detections. False alarms are generated in this case only because of collisions generated within clusters by the detectors, led to a false aggregate value and different from that of the CH, the latter being regarded as an attacker. The following figure shows the obtained results.

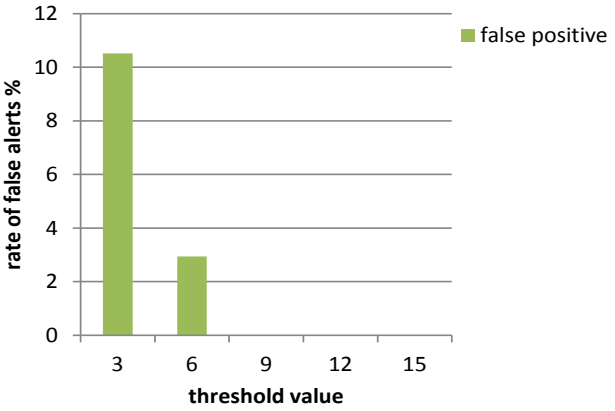

Fig.7. False Positive Rate in the Case of Unencrypted Data.

In such a case, detectors in each group help the base station to confirm the identities of attackers and avoid false positive detections. False alarms are generated in this case only because of collisions generated within clusters by the detectors, led to a false aggregate value and different from that of the CH, the latter being regarded as an attacker.

Case of data encryption: the choice of threshold value is very important in this case because it is the only parameter considered in the decision nodes isolation decisions (no confirmation alerts are sent by monitor nodes). The less the threshold value is, the more false alarms are raised, and vice versa. The rate of false alarms decreases with increasing values of the threshold. Therefore, the choice of the threshold should be done in such a way that a trade-off between detection credibility and reasonable resources consumption could be realized.

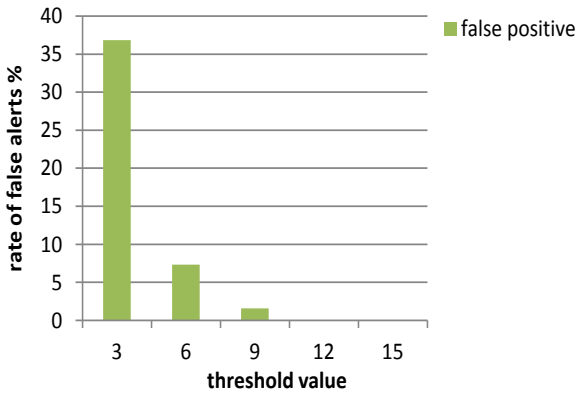

Fig.8. False Positive Rate in the case of Encrypted Data.

VIII. Conclusion

In this paper we have presented a detective solution to mitigate a novel and smarter variant of replay attack in WSNs. Unlike traditional scenarios where the attack principle was generally trivial enough, in data replay scenario the attacker replays only data (sensed information) part carried in each targeted message. Indeed, data replay is much more difficult to be faced and it has a great negative impact on network services as the reported data in a WSN are generally sensitive.

Cryptographic solutions can prevent efficiently an outsider attacker from replaying network messages. With the existence of insider adversaries (compromised sensor nodes), these solutions become unable to deal with the attack. So, this is also applicable in case of internal data replay attack.

Accordingly, intrusion detection is highly recommended. We have proposed an adapted intrusion detection system to overcome data replay attack in clustering WSNs. The assessment results show the effectiveness of the proposed solution.

For an enhanced security against replay attacks in WSNs, the proposed solution can be associated with cryptographic countermeasures.

References

[1] P. Rawat, K. Deep Singh, H. Chaouchi, J. M. Bonnin, " Wireless sensor networks: a survey on recent developments and potential synergies", The Journal of Supercomputing, Vol. 68, No. 1, pp 1-48, April 2014.

[2] S. Kalantary, S. Taghipour, "A survey on architectures, protocols, applications, and management in wireless sensor networks", Journal of Advanced Computer Science & Technology, Vol. 3, No. 1, pp. 1-11, 2014.

[3] J. Gubbi, R. Buyya, and S. Marusic, M. Palaniswamia, "Internet of Things (IoT): A vision, Architectural Elements, and Future Directions," ELSEVIER Journal: Future Generation Computer Systems, pp. 1645-1660, 2013.

[4] S. Malladi, J. A. Foss, R. B. Heckendorn "On Preventing Replay Attacks on Security Protocols", Idaho Univ Moscow Dept of Computer Science, 2002.

[5] K. Khan, W. Goodridge, D. Ragbir, "Security in Wireless Sensor Networks", Global Journal of Computer Science and Technology Network, Web & Security, Vol. 12, No.16 , 2012.

[6] 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.

[7] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D. E. Culler, "SPINS: Security Protocols for Sensor Networks" Wireless Networks, Vol. 8, pp. 521-534, 2002.

[8] M. G. Gouda, Y. Choi, A. Arora, "Antireplay Protocols for Sensor Networks", pp.1–20, August 23, 2004.

[9] D. C. Jinwala, D. R. Patel, Members, IAENG, S. Patel, K. S. Dasgupta, "Optimizing the Replay Protection at the Link Layer Security Framework in Wireless Sensor Networks".

[10] M. Luk, G. Mezzour, A. Perrig, V. Gligor, "MiniSec: A Secure Sensor Network Communication Architecture".

[11] D. C. Jinwala, D. R. Patel, K. S. Dasgupta, "Configurable Link Layer Security Architecture for Wireless Sensor Networks," Proceedings of the World Congress on Engineering 2008.

[12] I. Krontiris, T. Dimitriou, H. Soroush, M. Salajegheh, "WSN Link-layer Security Frameworks".

[13] S. M. AlMheiri, H. S. AlQamzi, "Data Link Layer Security Protocols in Wireless Sensor Networks: A Survey", IEEE 2013.

[14] A. Ghosal, S. Sur, S. DasBit, "μSec: A Security Protocol for Unicast Communication in Wireless Sensor Networks", DPM 2012 and SETOP 2012, LNCS 7731, pp. 258–273, 2013.

[15] S. A. Ch, M. M. Omair, I. A. Khan, T. A. Malik, "Ensuring reliability and freshness for Data Aggregation in Wireless Sensor Networks". International Journal of Machine Learning and Computing, Vol. 1, No. 3, August 2011.

[16] D. R. Raymond, R. C. Marchany, S. F. Midkiff, "Scalable, Cluster-based Anti-replay Protection for Wireless Sensor Networks", Proceedings of the 2007 IEEE.

[17] L. Gheorghe, R. Rughiniş, R. Deaconescu, N. Tapus, "Authentication and Anti-replay Security Protocol for Wireless Sensor Networks", 2010 Fifth International Conference on Systems and Networks Communications.

[18] J. Barnickel, U. Meyer, "SecSyWiSe: A Secure Time Synchronization Scheme in Wireless Sensor Networks", 2009 IEEE

[19] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, A. A. F. Loureiro, "SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks", 2006.

[20] J. Ibriq, I. Mahgoub, "A Secure Hierarchical Routing Protocol for Wireless Sensor Networks".

[21] N. Sastry, D. Wagner, "Security considerations for IEEE 802.15. 4 networks", In Proceedings of the 3rd ACM workshop on Wireless security, ACM, 2004.

[22] I. S. Gawdan, C. O. Chow, T. A. Zia, Q. I. Sarhan, "A Novel Secure Key Management for Hierarchical Clustering Wireless Sensor Networks," In Proceeding of 2011 Third Conference on Computational Intelligence, Modeling and Simulation (CIMSiM), 2011, pp. 312 - 316.

[23] D. Zhang, Y. Zhao, X. Wang, J. Choi, "A Robust and Efficient Neighborhood-Based Security Protocol for Wireless Sensor Networks", 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

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

[25] 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.
[26] S. Sahraoui, S. Bouam, “Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks”, International Jorunal of Communication Networks and Information Security (IJCNIS), Vol. 5, No. 3, pp.178-185, 2013.
[27] 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.
[28] 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.
[29] 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.
[30] T. Issariyakul, E. Hossain, “Introduction to Network Simulator NS2”, Springer, 2012.
[31] 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.
[32] V. Seema, Pratchi, "A Comparative Study of Key Management Protocols for WSN," International Journal of Computer Network and Information Security (IJCNIS), vol. 6, No. 4, pp. 29-36, 2014.

Authors’ Profiles

Yasmine Medjadba PhD student at Science and Technology Department, Beijing Normal University, Beijing, China. Her research interests include communication security in wireless sensor networks.

Somia Sahraoui PhD student at Computer Science Department, University of Batna 2, Algeria. Her research interests are mainly focused on communication security in Wireless Sensor Networks and the Internet of Things.

How to cite this paper: Yasmine Medjadba, Somia Sahraoui,"Intrusion Detection System to Overcome a Novel Form of Replay Attack (Data Replay) in Wireless Sensor Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.7, pp.50-60, 2016.DOI: 10.5815/ijcnis.2016.07.07

