

Document downloaded from:

<http://hdl.handle.net/10251/137581>

This paper must be cited as:

Mehmood, A.; Lloret, J.; Sendra, S. (2016). A Secure and Low-Energy Zone-based Wireless Sensor Networks Routing Protocol for Pollution Monitoring. *Wireless Communications and Mobile Computing*. 16(17):2869-2883. <https://doi.org/10.1002/wcm.2734>



The final publication is available at

<https://doi.org/10.1002/wcm.2734>

Copyright John Wiley & Sons

Additional Information

A Secure and Low-Energy Zone-based Wireless Sensor Networks Routing Protocol for Pollution Monitoring

Amjad Mehmood¹, Jaime Lloret², Sandra Sendra³

¹Institute of Information Technology, KUST, Kohat, KPK, Pakistan

²Integrated Management Coastal Research Institute, Universidad Politecnica de Valencia, Spain

³Signal Theory, Telematics and Communications Department (TSTC), Universidad de Granada, Spain
amjad.mehmood@kust.edu.pk, jlloret@com.upv.es, ssendra@ugr.es

Abstract

Sensor networks can be used in many sorts of environments. The increase of pollution and carbon footprint are nowadays an important environmental problem. The use of sensors and sensor networks can help to make an early detection in order to mitigate their effect over the medium. The deployment of wireless sensor networks (WSNs) requires high energy efficiency and secure mechanisms to ensure the data veracity. Moreover, when WSNs are deployed in harsh environments, it is very difficult to recharge or replace the sensor's batteries. For this reason, the increase of network lifetime is highly desired. WSNs also work in unattended environments which is vulnerable to different sort of attacks. Therefore, both energy efficiency and security must be considered in the development of routing protocols for WSNs. In this paper, we present a novel Secure and Low-Energy Zone-based Routing Protocol (SeLeZoR) where the nodes of the WSN are split into zones and each zone is separated into clusters. Each cluster is controlled by a cluster head. Firstly, the Information is securely sent to the zone-head using a secret key; then the zone-head sends the data to the base station using the secure and energy efficient mechanism. This paper demonstrates that SeLeZoR achieves better energy efficiency and security levels than existing routing protocols for WSNs.

Keywords: Pollution Monitoring, WSN, Security, Clusters, Key Management, Hierarchical Protocol.

1 Introduction

Wireless Sensor Networks (WSNs) are composed by a large number of low-cost and tiny devices and are used in many applications including environmental monitoring, weather forecasting, medical services, military surveillance, tracking objects and so on [1, 2]. However, these devices or nodes present a set of hardware limitations that do not let them work always unattended. Two of the most important challenges faced by WSNs are the energy efficiency and security issues. It is also difficult to ensure the wireless communication as the data in WSNs are transmitted over a broadcast channel. Attackers can simply eavesdrop, insert, interrupt, and change the transmitted information which is spread through the medium. When WSNs are physically deployed in insecure locations, attackers can easily take control over the sensor nodes, recover the cryptographic material from the nodes to decrypt the information and attack the network by spoofing any node and sending error messages to all other nodes. Therefore, in order to waste a node's battery and deplete its bandwidth with the purpose of disable it, the attackers can repetitively send packets to the node in order to reach their goal [3]. Therefore, it is desired to design energy efficient protocols to extend the network lifetime of the WSN [4, 5].

In recent years, researchers have identified some effective schemes focused on increasing the scalability and the lifetime of the WSNs [6]. They are mainly focused on the use of clusters [7, 8] and group-based topologies [9, 10]. The energy efficiency and the network lifetime of WSNs are extremely related to self-organization and clustering mechanism, because of their benefits in these issues. Furthermore, in cluster-based WSNs, efficiency is further affected by the distance between sensor nodes and the cluster head (CH) and the distance between a CH and a base station (BS). Parameters such as the time to select the CHs, the size of the cluster and the workload balance among clusters are also important to determine the energy consumption of the entire network.

Finally, it is important to apply some mechanisms to improve the network performance and the security issues. This is case of cooperative decision algorithms [11], where the nodes use the network information and the information provided by the user to take intelligent decisions. These techniques are applied in several fields, like environmental monitoring [12].

This paper presents a new zone-based wireless sensor network routing protocol for pollution monitoring called SeLeZor. This protocol also implements several improvements to enhance the issue of energy consumption and data vulnerability. SeLeZor divides the network area into zones, and each zone is divided in clusters. Hence, the data are exchanged between intra and inter-zone communication by using a secure and powerful key at each level in order to identify the malicious data while maintaining the network performance.

The rest of this paper is organized as follows. The related work is presented in Section 2. Section 3 shows the proposed network model. The details of SeLeZoR are presented in Section 4. Section 5 provides the performance results. Finally, Section 6 concludes the paper.

2. Related Work and Motivation

Nowadays, the issue of detecting environmental problems such as the presence of contaminants and natural disasters is a great concern to the scientific community. Nonetheless, there are very few proposals where researchers develop systems and design protocols focused on these issues. However, we found hundreds of proposals about protocols that could be applied for environment monitoring. Thus, this section presents some proposals focused on the development of protocols for environmental monitoring systems.

T. Jain [13] presented a proposal which senses multiple attributes in an environment for producing an alarm if any absurd condition is predicted. The proposed WSN is focused on detecting tsunamis. The author proposed the use of a hybrid and bidirectional protocol. In

addition, the proposal implemented data aggregation to minimize data transmissions, energy consumption and to be faster. Finally, the protocol is based on the concept of distributed computing which facilitates the data analysis.

In order to improve the network lifetime of nodes in WSNs several routing protocols have been developed, including those based on tree, chain, grid, and hybrid topologies among others [14]. Cluster based protocols, in which the sensor nodes in a WSN are divided into a set of clusters or groups, are most energy efficient [10].

The zone based protocols are also focused on increasing the network lifetime of a WSN by balancing the workload among clusters [15]. In this distributed architecture, the node with the highest level of energy in a zone is selected as a Zone Head (ZH), and the node with the highest level of energy in the cluster is selected as a CH. After performing aggregation, the CH sends the fused data to the ZH, which then sends them to the BS. This section presents a brief summary of the most popular cluster, zone and group based protocols for WSNs.

Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol [16] is a hierarchical protocol specially developed for reducing the energy consumption of the nodes in order to increase the network lifetime. In LEACH, the nodes are separated into clusters where a node performs its tasks as the leader or CH node. All non-leader nodes transmit their data to the CH, while the CH sends data from all the cluster members to the BS. Before this, CH performs the task of data processing (e.g., data aggregation). LEACH works by rounds. In each round, leader nodes are swapped over in order to deal the network power consumption. A round consists of two phases: clusters grouping phase and communication phase. During the phase of clustering, leaders nodes are selected using a distributed algorithm, and the source nodes tend to join to the nearest CH. In the communication stage, data are transmitted to the BS.

L.B. Oliveira et al. investigated security issues and also addressed secure communication among nodes. They proposed Security Based LEACH (SecLEACH) [17]. We can find two LEACH-based protocols with improved network efficiency called Energy-LEACH [18] and Multi-hop LEACH [19]. Energy-LEACH (E-LEACH) protocol improves the selection method of the CH by selecting nodes having more remaining energy as CHs in the next round. The Multi-hop LEACH protocol, which sends the data to the BS via other intermediate nodes, represents an extension of the LEACH to save energy in WSNs. Finally, M. Tong, and M. Tang, proposed Balanced LEACH (LEACH-B) [20] which selects a CH randomly, like LEACH protocol, in the first round. But it selects a number of CHs by taking the residual energy into account in the second round, which helps to find optimal number of CHs per round.

Other protocols based on similar principles are PEGASIS [21] protocol and Hybrid Energy Efficient Distributed Clustering (HEED) [22], which were developed to help to reduce the energy consumption.

Many researchers are interested on improving the network life time and also addressing security issues separately [23]. However, the purpose of this paper is to improve the energy efficiency and the network security using simultaneously a zone-based system. This provides better performance for upper layer functionality such as number of messages sent, broadcasting, data aggregation, etc.

In Secure Communications in Group-based Wireless Sensor Networks [24], authors presented a group based mechanism which divides the communication into intra-group communication and inter-group communication. The intra-group provides secure communication within the group while inter-group offers the secure communication between different groups. Due to limited memory and processing capability of sensor nodes, the symmetric cryptographic technique with a single key for all members of the network was used.

A. Noack [25] proposed a solution for alarming issues in dynamic networks, e.g. flexible memberships, group signatures and distributed signatures. In some cases, this kind of solutions includes some mechanisms to increase the network lifetime. This is the case of N. Nasserel et al. [26], who proposed a Secure and Energy Efficient Multipath Routing Protocol (SEEM) which provides multipath communication between two nodes while the network lifetime is increased.

Finally, we can find several proposals for environmental monitoring based on WSNs. This is the case of C. Alippi et al [27] who presented a marine environmental monitoring system based on a WSN characterized by the use of energy harvesting. The system is based on a star topology where nodes perform the local transmission from sensor nodes to the gateway and data is stored in a DB for real-time visualization. The entire system used a power-aware and adaptive TDMA protocol for the local transmission that guarantees robustness and adaptability to network changes. The hardware and software were selected to guarantee high quality of service (QoS), optimal solar energy harvesting, storage and energy awareness. The monitoring system was deployed in Queensland, Australia, for monitoring the underwater luminosity and temperature to control the health status of the coralline barrier.

Finally, L. Parra et al. [28] proposed a system based on a smart algorithm which was able to detect, track and locate pollution stains, such as oil spills. The system was composed by wireless nodes that were able to move towards the end of the stain seeking its edge. Nodes use IEEE 802.15.4 protocol and the Global Position System (GPS) to estimate the final position of the stain. Finally, authors tested the operation of the system, using the routing protocols Ad hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV). The results show that the system registers better behavior when reactive protocols were used.

Unlike existing systems, our proposed system's security technique not only improves the security of the data exchanged in the network but also avoids the presence of malicious users. Moreover,

the zone based technique helps to improve the energy-efficiency in both sparse and dense environments.

3. System Parameters and Network Features

This section describes our network architecture and how it works. For simplification, we are going to use a circular sensor network which contains several sensor nodes and one BS (See Figure 1). The following assumptions are taken:

- The network consists of N nodes.
- BS is in the center of the network.
- All the nodes and the BS are static.
- Nodes are equally distributed in the network.
- All sensors are location aware, i.e., nodes can send the information of their location to the BS in the initialization phase.
- Initially, all sensor nodes have a unique Identifier (ID) and a secret key.
- All nodes sense the data and send the information to the CH.
- The packet size has L bits.
- The CH aggregates the data.
- The energy consumption in data gathering process is lower than the energy of reception or transmission process.
- CH sends the aggregated data to the ZH.
- The transmitted energy depends on the distance (from the source to the destination) and the size of the data packet.
- For simplicity, initially, all nodes have the same energy level

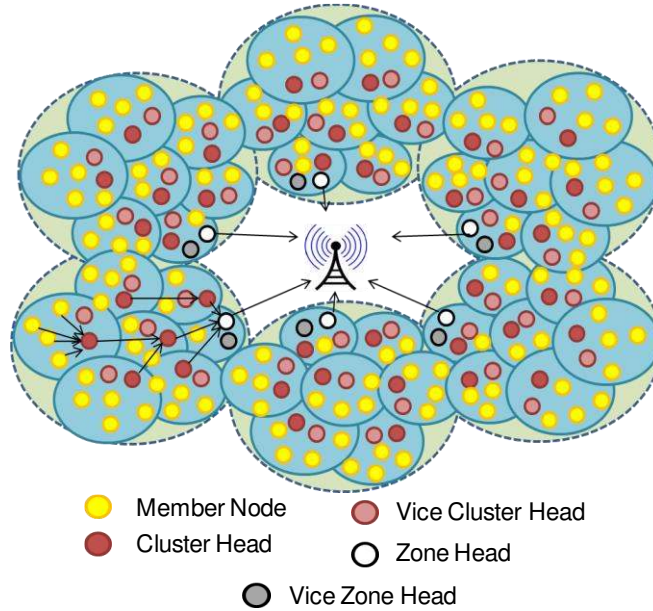


Fig.1 The network structure of SeLeZoR

In this case, the following tasks are assigned to each kind of node:

- **Member Node (MN):** Senses the data and transfers the information to the CH.
- **Cluster Head (CH):** Performs data aggregation, encryption of the data sent by the nodes belonging to its cluster and sends these data packets to the Zone Head (ZH).
- **Vice Cluster Head (VCH):** It takes the role of the CH in case the CH has low energy.
- **Zone Head (ZH):** Receives messages from CHs and transmits these data packets to the BS.
- **Vice Zone Head (VZH):** IT takes the role of ZH in case of ZH low energy.
- **Base Station (BS):** The BS is very powerful and has the biggest computational capacity.

The fact of assigning different roles to the nodes allows us to simplify the network management and reduce the power consumption due to the processing and sending data.

4. SeleZoR Description

This section presents a detailed explanation of our proposed SeleZoR scheme. This section also includes some mathematical expressions and pseudo-codes used to implement our protocol.

In order to improve the energy efficiency and have an efficient storage and key establishment, the entire network is distributed into zones and clusters. The division of the network into zones is carried out by the BS. This division allows decreasing the number of messages sent to the BS. These zones are further divided into clusters. The clusters have unequal size. The clusters further away from the BS have greater sizes than those clusters nearer to the BS. Therefore, cluster heads nearer to the BS can reserve some energy for the inter-cluster data transmission. Each zone has a ZH and each cluster has a CH. Because ZH and CH have several responsibilities, their energy is consumed faster than MNs. Therefore, their chances of death are higher than of the rest of nodes. If the energy level of ZH and CH goes down below a certain threshold value, the proposed technique introduces the VZH and VCH to overcome this issue [29, 30] (See Fig 1).

To ensure a secure communication between WSN nodes, various kinds of keys are established and defined by the key management system. All types of communication have to be secured in order to ensure the entire WSN. For the secure communication, the secure keying procedures proposed in this paper offer a combination of different kind of keys and ensure that the nodes, CH and the ZH (using these keys) route securely the messages to their last hop, i.e., the BS.

4.1. Key management system

It has been demonstrated that the use of a single keying technique is not secure enough to ensure all the message types that circulate through the WSN. Key management is the procedure in which keys are formed, stored, transmitted, used between approved parties and removed when they are no longer needed [31, 32]. Key management creates essential keys that offer integrity, privacy, and confirmation services. Due to the sensor node energy constraints and limited memory resources, sensor networks cannot use complex security algorithms. The main aim of key

management is to be sure that WSN security requirements are met by encoding messages and authentication of nodes when the connection process is performed. For securing the entire WSN, all types of messages need to be secured. Before presenting the keys used in this paper, the different kind of WSN communication messages have to be presented. These are:

- Zone Head/Vice Zone Head to Cluster Head/Vice Cluster Head or Cluster Head/Vice Cluster Head to Zone Head/Vice Zone Head communication messages
(ZH/VZH : CH/VCH or CH/VCH : ZH/VZH)
- Zone Head to Vice Zone Head or Vice Zone Head to Zone Head communication messages
(ZH : VZH/VZH : ZH)
- Cluster Head to Vice Cluster Head or Vice Cluster Head to Cluster Head communication messages (CH : VCH/VCH : CH)
- Cluster Head/Vice Cluster Head to Node communication messages (CH/VCH : N)
- Node to Cluster Head/Vice Cluster Head communication messages (N : CH/VCH)
- Zone Head/Vice Zone Head to Base Station communication messages (ZH/VZH : BS)
- Base Station to Zone Head communication messages (BS : ZH)

For secure communication the following keys are used.

- Secret Key (Ks): It is initially used by every node. Ks is used for (N : BS) communication.
- Network KEY (Kn): Kn is used for (BS : Z) communication.
- Head Key (Kh): Kh is used for (ZH/VZH : CH/VCH) as well as (CH/VCH : ZH/VZH) communication messages.
- Neighbor Head Key (Knh): Knh is used for (ZH : VZH) as well as (VZH/ZH, CH : VCH, VCH : CH) communication messages.

- Cluster Key (K_c): K_c is used for (CH/VCH : N) communication messages as well as (N : CH/VCH) communication messages.
- Zone Key (K_z): K_z is used for (ZH/VZH : BS) communication messages.

4.2. Key Usage

It is necessary that all nodes identify their own key K_s . The Initial Message (IM) sent by the member node to the CH is shown in expression 1:

$$Message(M) = \{ K_c, TS, IM \} \quad (1)$$

Where Timestamp (TS) is used to avoid message repeating. The initial message from a node is encrypted using K_c to communicate with CH. CH encrypts the aggregated data using the K_h and sends the message to the ZH. The format of the message is shown in expression 2:

$$CH\ Message(CHM) = \{ K_h, \{ K_c, TS, aggregated(M) \} \} \quad (2)$$

ZH communicates with BS and encrypts the message (See expression 3) using the K_z :

$$ZH\ Message(ZHM) = \{ K_z, \{ K_h, \{ K_c, TS, (CHM) \} \} \} \quad (3)$$

When a MN sends a message to its CH, the CH checks that the message has a key. If it finds the key, the message is decrypted using the key K_c . Otherwise the message is discarded since it can possibly be generated by an attacker who is trying to have access to the network.

4.3. Setup Phase

In the deployment phase of the network, all nodes are equally deployed in a specific region. All nodes have a unique ID and a secret key, the same initial energy and equal processing and communication capacity. When the BS achieves a specific power level, it broadcasts a welcome message. Every node can estimate their distances to other nodes and to the BS based on the received signal strength from them. All network nodes send their ID and current location to the BS using the initial secret key (K_s). BS creates a table and saves the information of each node

and according to the nodes' location, the BS generates the zones and clusters. BS uses the algorithm 1 to divide the network into zones and the unequal clusters.

//Variables definition

- $N \leftarrow$ total no. of nodes //100
- $Z \leftarrow$ total no. of zones //4
- $NZ \leftarrow$ total no. of nodes in each zone //25
- $TAZ \leftarrow$ total number of nodes in all zones //100
- $CZ \leftarrow$ clusters in a zone //4
- $NC \leftarrow$ nodes in a cluster //6
- $TCZ \leftarrow$ total clusters in all zones //16

$Z \leftarrow N/NZ$
 $TAZ \leftarrow Z * NZ$
 $CZ \leftarrow NZ/NC$
 $NC \leftarrow NZ/CZ$
 $TCZ \leftarrow Z * CZ$

Algorithm 1. Pseudo-Code to carry out the Clustering setup phase

The BS also chooses the ZH for each zone and the CH for each cluster according to their location in the zones and clusters. Then, the BS chooses the nearest MN as a VZH and VCH, respectively. After that, the BS sends a message to each zone to identify the ZH, VZH, CHs and VCHs of the clusters in its zone. The CH sends a message to all nodes in the cluster to announce which node is the CH and VCH. The selected CH broadcasts an announcement message to its neighbor nodes. During a specific interval of time the neighbor nodes collect the announced message and then they send a “join REQ” message to the nearby CH. The “join-REQ” message is received by the CH and builds a list of CH members. The MN receives and save the message for data transfer [33]. The nodes of the same cluster try to find each other using the “Neighbor finding phase”. When the neighbors are recognized, each node stores the information on their neighbors in the ‘Neighbor info table’. After “Neighbor finding phase” is finished, the security keys are distributed in the network, see Fig. 2.

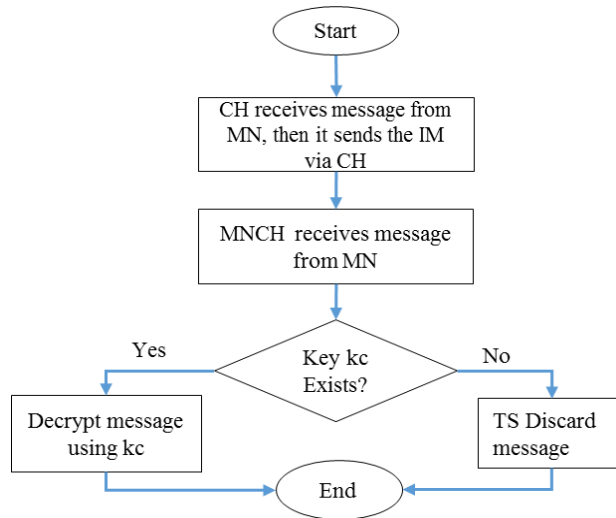


Fig. 2 . Communication Algorithm

4.3. Base Station Algorithm

This subsection presents the BS algorithm and how it works to carry out its tasks. BS initiates the routing process once the clustering, the distribution of nodes in zones and the key distribution are performed. When the sensor nodes send a join request to the BS, the secret key (K_S) is used for encrypting this request. Then, the BS is only able to decrypt the request message from actual nodes of the network. After authenticating all nodes, BS issues the network key (K_N). If a node joins the network, it has to send a request to the BS for acquiring the K_N . This request, which is encrypted by the K_S , is sent by all the nodes to the BS. BS sends the K_N to the requesting nodes and encrypts it with the K_S . Only reliable nodes can decrypt messages by using the K_N . After that, BS sends a message to the ZH using the zone key (K_Z). This message contains information in regard to the ZH-ID, VZH-ID, CH-ID, VCH-ID. The ZH receives this message encrypted by the key K_Z . In this case, the received message contains the information of their corresponding clusters. On the other hand, the cluster receives an encrypted message (using the cluster key (K_C)) from the ZH and this message contains the information of the CH-ID and the MNs. If the data is

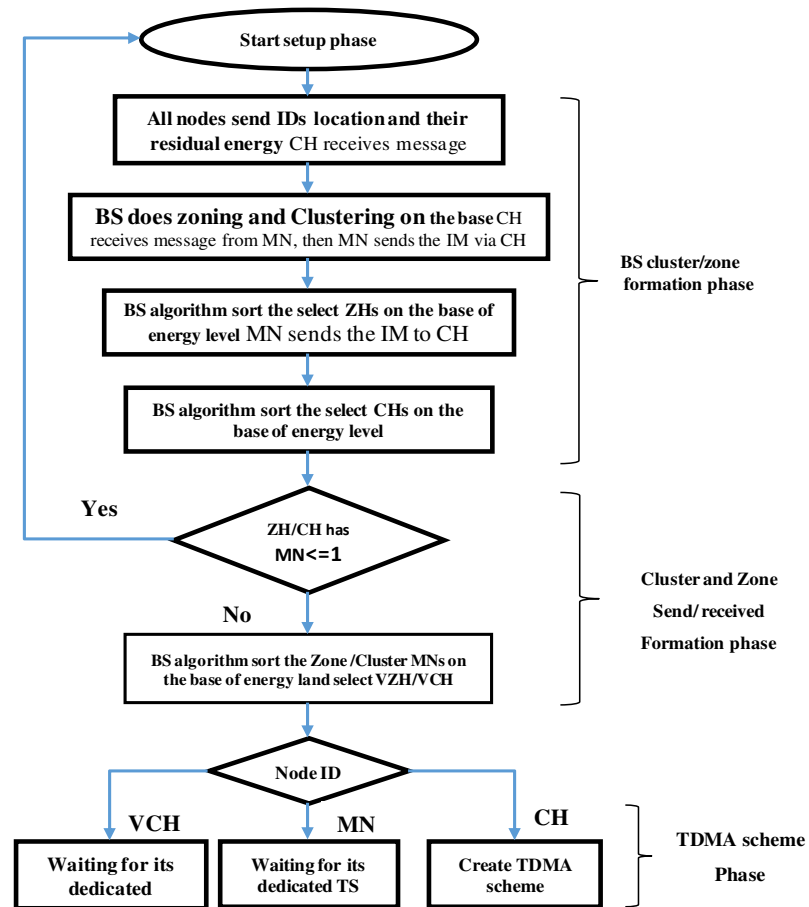


Fig.3 SeLeZoR setup phase flow chart

4.4. TDMA schema phase

SeLeZoR uses the Time Division Multiple Access (TDMA) technique in order to efficiently use the transmission channel. The TDMA phase is created by the ZH. TDMA Time Slots (TS) are shown in Fig. 4a.

ZH arranges TDMA scheme as follows:

TSs for MNi:

- 1) Two TSs are allocated for CH Data Aggregation (CHda) and CH Data Sending (CHds)
- 2) Last two TSs are assigned for ZH Data Receiving (ZHdr) and ZH Data Transmit (ZHdt)

In the steady state phase, once the CH decides to give up its role in favor of the VCH, as an alternative to create a new TDMA, the VCH uses the same TDMA already created, but creates new TSs for CH and gives CH TSs, as shown in Fig.4b. When the ZH gives its role to the VZH, instead of creating a new TDMA, the VZH uses the same TDMA already created, but it only changes the last two TSs, as shown in Fig.4c.

Then, the ZH announces its TDMA scheme by sending a message to its CHs holding the assigned TS. Each CH sends the TDMA scheme message to its MNs. Once MNs collect this message all nodes know their assigned TSs for data transmission and go to sleep till their assigned TS. The steady state phase is started when the zones and clusters are formed, keys are distributed and TDMA schemes are created and distributed.

(a)	N1	N2	...	Ni-1	Ni	CHda	CHds	CHdr	CHdt	
(b)	N1	N2	Ni-1	Ni	CH	VCHda	VCHds	ZHdr	ZHdt
(c)	N1	N2	Ni-1	Ni	CH	VCHda	VCHds	VZHdr	VZHdt

Fig.4 TDMA Scheme (a) before applying VCH and VZH (b) after applying VCH (c) after applying VCH and VZH

4.5. Steady state phase

The network needs to know the environment status. For this reason this subsection explains how the system operates to get the information from the environment.

The MNs sense an area to get information from the environment. Then, all MNs send data about the environment and the information about their remaining energy to the CH using the minimum transmission power. In order to determine the exact value of minimum transmission power, MNs use the received signal strength when advertisement message is received so that, taking into account this factor, the minimum quantity of energy is used to communicate with other nodes. Using the RSSI (Received Signal Strength Indicator), we can know the minimum energy needed

to ensure the correct communication between 2 devices (See Fig. 5), we can calculate the minimum energy needed to transmit the packets from a node to another (See Fig. 6). In our case, we have estimated that the minimum energy transmission is that one that warrants a RSSI equal to -70 dBm. If there is some meteorological factor that can affect the process, [34] these factors will be taken into account. In this case, we will ensure a RSSI of -60 dBm.

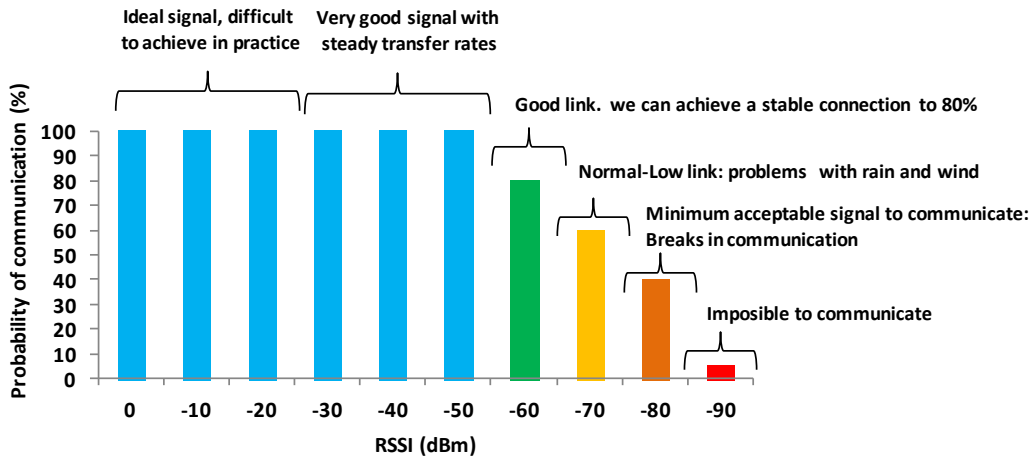


Fig. 5 Values of RSSI and its probability of communicating

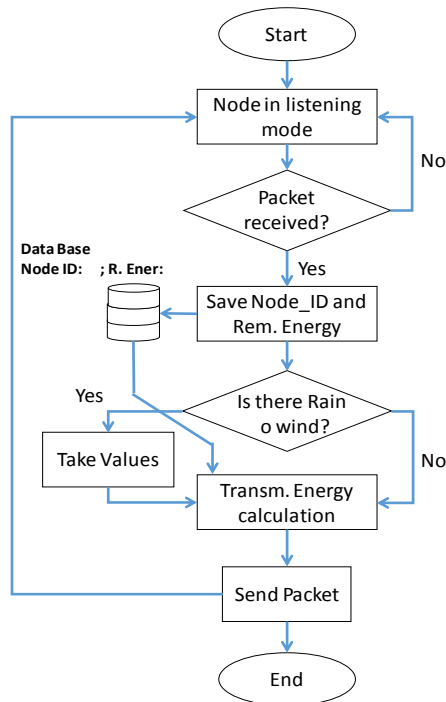


Fig. 6 Energy calculation phase flow chart

Updated information about the MNs is maintained by the CH. Each cluster member can be switched off until TS assigned to the node reaches. When CH receives all the data from the cluster members, the CH node performs the task of data aggregation in order to include the information into a single packet. The packet is encoded and sent to the ZH. The ZH receives messages from the clusters belonging to its zone and transmits these data packets to the BS. Transmission between nodes can be done using TDMA, as Fig. 7 shows.

During the data transmission, when the energy level of ZH reaches the 10% of the maximum value, it must give up its role in favor of the VZH. The ZH sends a message to all clusters in its zone informing them about the changes of roles between ZH and VZH. Therefore, CHs establish a connection with the VZH, and VZH starts to listen to the network information, getting and transferring data packets to the BS. Finally, when the CH energy level reaches values lower than 10%, it gives up its role to the VCH. Before a CH steps down its role, it must broadcast its decision to all the members in its cluster and to the ZH. In that moment, the current CH becomes MN and VCH becomes CH and nominates a new VCH. Then, starts receiving, aggregating and sending data to its neighbor CH (inter-cluster) or ZH till its energy level reaches levels of energy lower than 10%. After CH and VCH, all Cluster groups can select their own CH based on its remaining energy. The residual energy of the MNs is included in the data packet from MNs to CHs.

Based on the information used to the CH election, CHs maintains an energy list. If the CH presents an energy level lower than the 10%, the node with the next maximum energy level will be elected as next CH. In this way, if the CH losses its energy during the next repetition, the next CH will assume the role of the main CH [35, 36].

Fig. 8 shows the message exchange between the network nodes during the process for determining the next CH. To ensure that our network works properly, the protocol is in charge of

sending a set of messages to the ZH, VZH, CH, VCH and Nodes. In the first step, the BS has to send the IDs and Keys used to encrypt the information to the rest of nodes with independence of their roles. Because the TDMA is implemented by the ZH, this node sends the slot time during which a node can send data. After the nodes' authentication, each node sends to its upper node a request to join the cluster. After this step, the network is created. During the slot time assigned to each node, they can transmit the collected data. This information is sent from each node to their upper nodes until the BS registers the data. As Fig. 8 shows, depending on which node generates the information, the network will generate a set of messages that will be sent to the immediately upper and lower nodes.

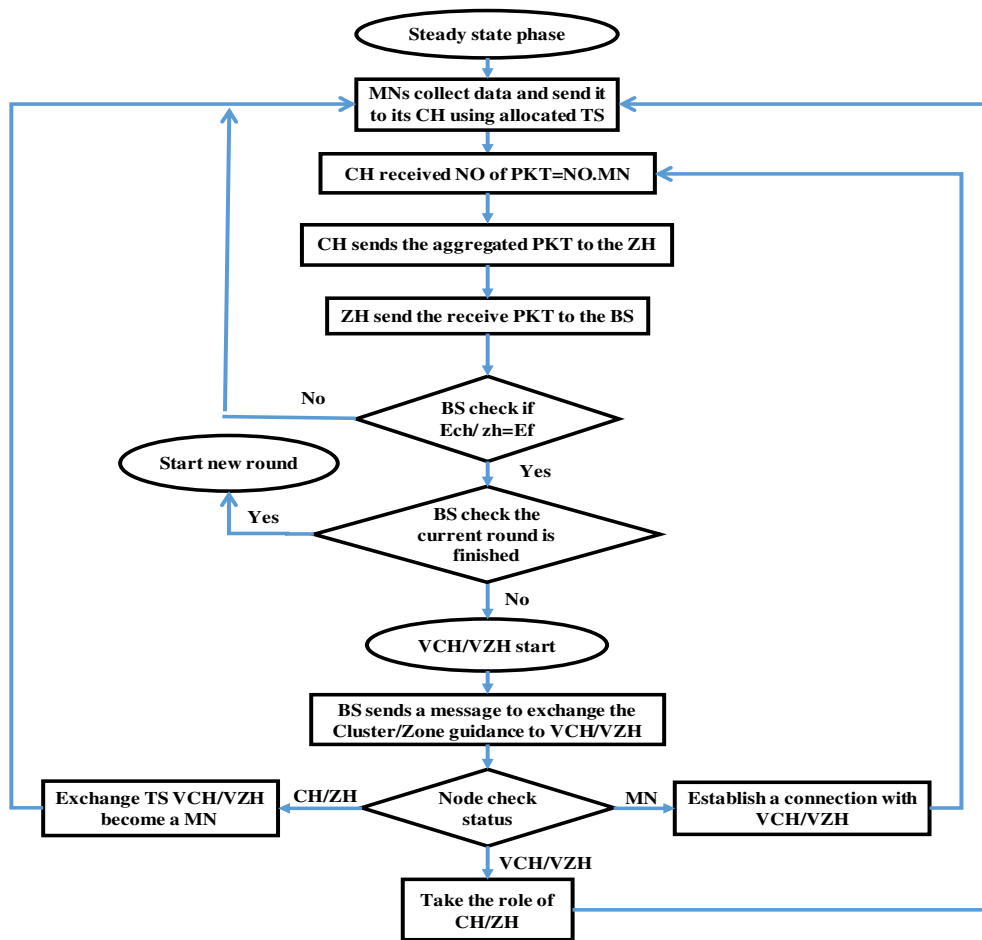


Fig. 7 SeLeZoR steady phase flow chart

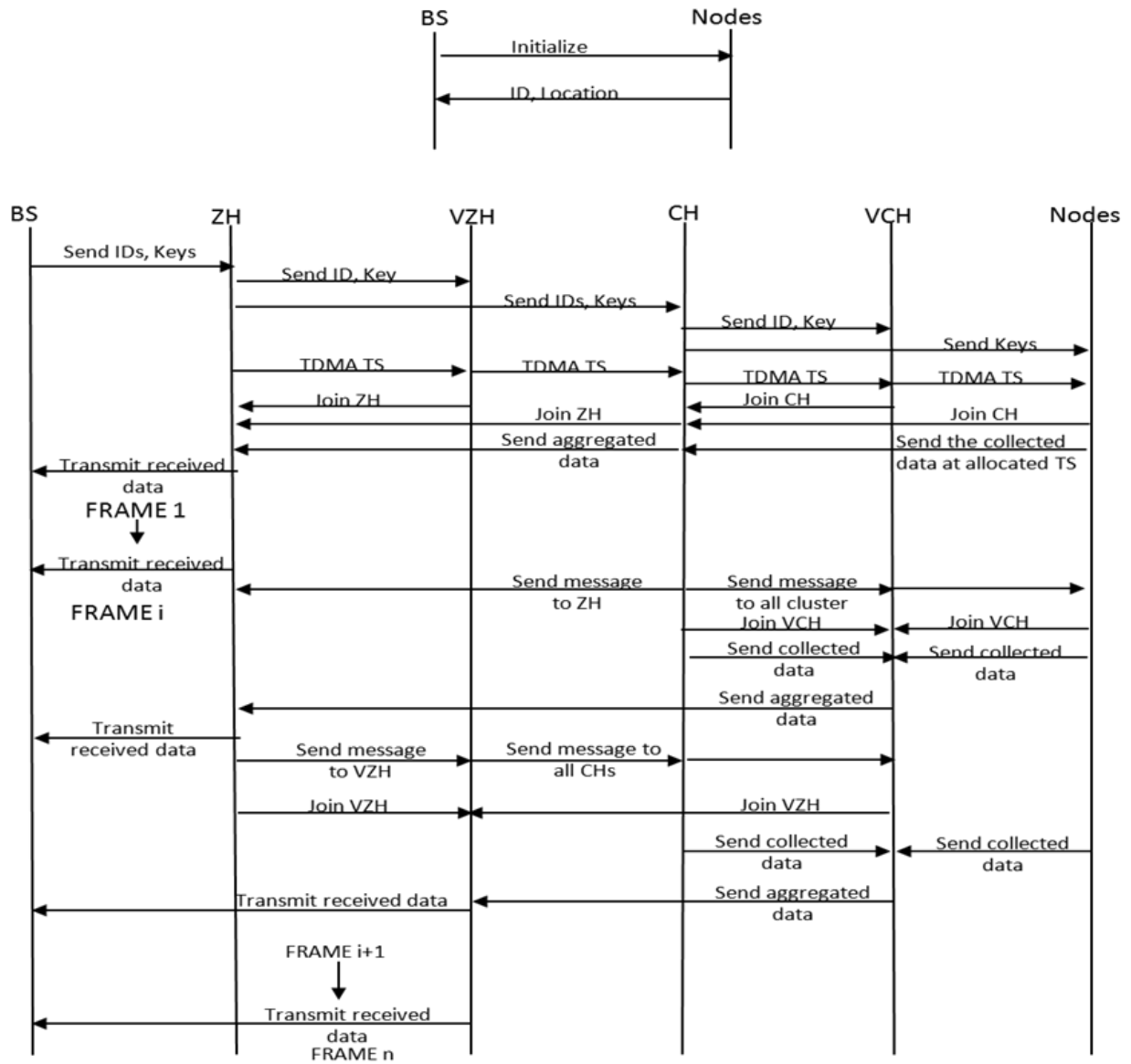


Fig. 8 SeLeZor protocol's working

5. Performance Evaluation

The last important step during the protocol design is the performance evaluation [37]. In order to emphasize the value to SeLeZoR, we have to estimate and compare its performance with existing solutions that implement saving energy techniques to prolong the network lifetime and support

the security mechanisms to ensure data veracity. In order to evaluate the energy consumption of the computational overhead when security is implemented in communication, we consider six important factors during the network performance evaluation:

- **Network Lifetime (i.e. the time of first node dead (FND)):** It shows the time during which the sensor network is completely efficient. Therefore, maximizing the time of FND will mean that a WSN will extend the network lifetime.
- **The number of alive nodes:** The ability of detecting and gathering data in a WSN hangs on the set of alive nodes. Thus, we evaluate the WSN functionality depending on calculating the number of alive nodes in the network.
- **Network Energy Consumption:** It states the quantity of energy used by a WSN. We evaluate the difference of energy consumption in secure data transmission.
- **Packet Delivery Ratio (PDR):** this value indicates the ratio of the successfully delivered data packets to the destinations generated by Constant Bit Rate sources.

$$PDR = N_r / N_t \quad (2)$$

Where N_r is the number of data packets successfully received and N_t is the number of data packets transmitted.

- **End-to-End Delay:** It shows the time needed by the data to reach the destination from the source.
- **Energy Consumption:** It is expressed in mWh.

Three additional considerations about the WSN status and the compromised node are considered:

- (1) A compromised node is present in the network. It has the same basic capabilities as authentic sensor nodes.

(2) The compromised node plays a part in the network activities, but it may deliver false data in its link.

(3) The compromised node may also drop, modify, or divert the traffic that goes through it.

In order to test the performance operation of our protocol and compare it with another one, we have selected the one who present the closest features. In this case, SeLeZoR has been compared with SecLEACH [13]. In order to perform the performance evaluation, we have used MATLAB as a software tool to emulate the operation of both protocols.

5.1. Simulation parameters

In order to evaluate our proposal, we have to assume and determine several parameters. The values of the parameters used in the simulation are listed in Table 1.

Table 1: Parameters used in our simulations

Parameter	Value
Network size	500 m* 500 m
MAC	802.11
Routing Protocols	SELEZOR and SecLEACH
Number of zones	6
Number of clusters	42
Number of nodes per cluster	3-4
Transmission Rate	250 m
Node distribution	Random position of nodes as Ad hoc Network
Initial energy	17 J
Data packet size	512 Bytes
Bandwidth	2 Mbps
Frequency	2.4 GHz
Traffic type	Variable Bitrate (VBR)
Payload size	30 to 70 Bytes
Number of packets	200 Packets
Propagation limit (dbm)	-111.0 dbm
Path loss model	Two ray model
Antenna type	Omni directional
Channel bandwidth	20 Kbps
Transmit Power	0.395 W
Receiving power	0.660 W
Idle power	0.035 W

No. of Attackers	2,4,6,8,10
-------------------------	------------

One of the most important issues is to know when the network starts to fail. Fig.9 shows the FND time for the two protocols under analysis. The confidence intervals are applied to the simulation results. Simulations have been performed with a network of 100 nodes randomly distributed. The confidence level is fixed at 90%. As we can see, SeLeZor presents the highest FND time (around 185 s) while SecLEACH presents a FND time of 49 s, which indicates that when running SeLeZor protocol the first node will die later than in SecLEACH. The FND time in SeLeZor is larger than SecLEACH due to the security overhead in the computation process which seems to be lower in SeLeZor.

Fig.10 shows the comparison of the number of alive nodes using SeLeZor and SecLEACH. The simulation results make evident that the network lifetime offered by SeLeZor is longer than the one offered by SecLEACH.

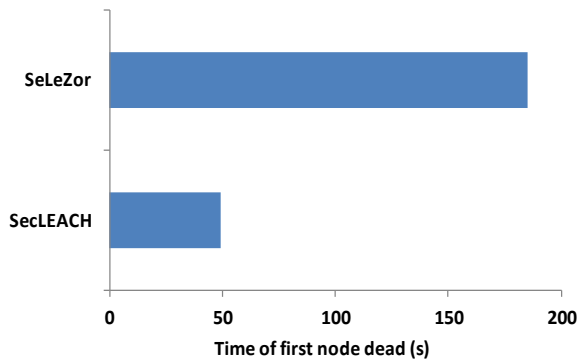


Fig.9 FND time for each protocols

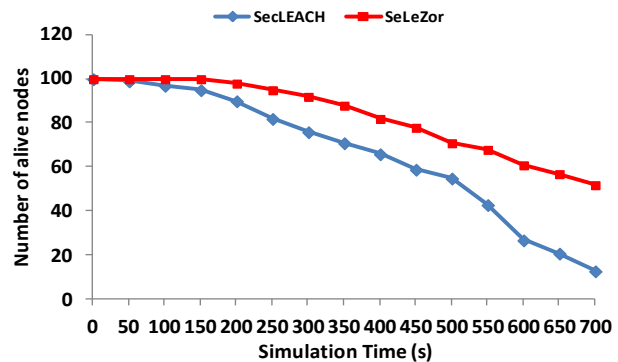


Fig.10 Number of alive nodes for each protocol along the time.

Fig.11 shows the total power consumption of all sensor nodes distributed in the network. It also shows the stability of energy consumption in the network. The simulation has been performed

with a network of 100 nodes randomly distributed. In both cases, the energy consumption follows a logarithmic behavior but SeLeZor presents lower energy consumption along the simulation.

On the other hand, the Packet Delivery Ratio (PDR) decreases as the network size increases as it is shown in Fig.12. If we compare the PDR vs. number of nodes, SeLeZor presents a slightly higher percentage of delivered packets than SecLEACH.

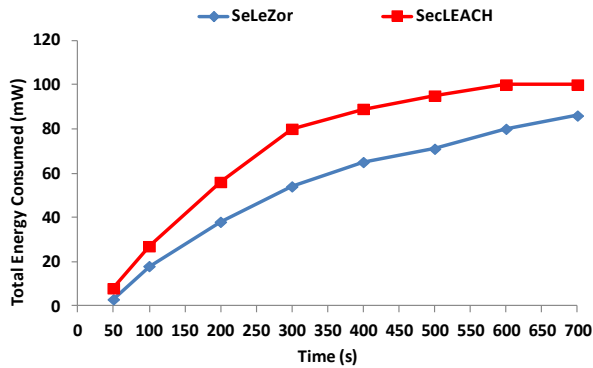


Fig.11 Comparison of energy consumption in different protocols

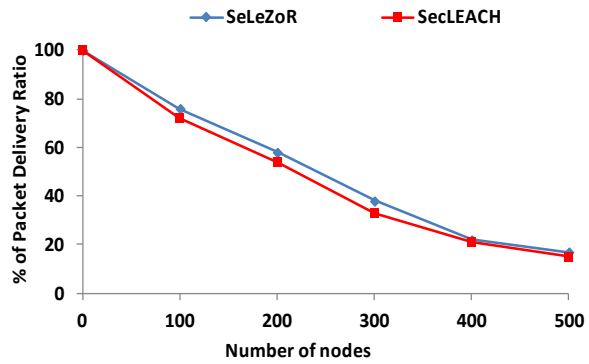


Fig.12 Comparison of %PDR vs. Network Size

Fig.13 shows the End-to-End delay in seconds for both protocols when the percentage of compromised nodes is increased up to 70%. As we can see, both protocols present a lineal behavior. However, the difference in End-to-End delay between both protocols is higher when the number of compromised nodes increases. This proves the efficiency of SeLeZor security mechanism.

Fig.14 compares the average power consumption in mWh when the network varies with the presence of 30 % of compromised nodes. The end to end power consumption decreases in both protocols because of the operation of the clustering mechanism. The difference between both is about 100 mWh.

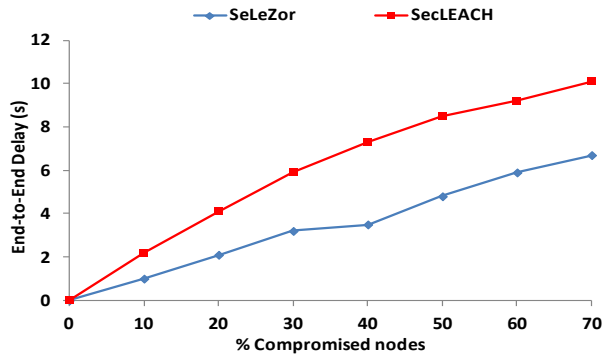


Fig.13 Comparison of % compromised nodes Vs. End-to-End delay

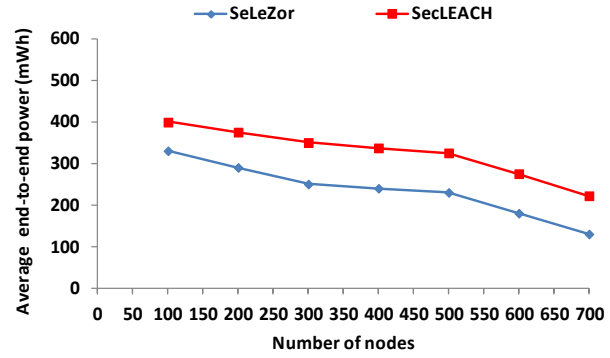


Fig.14 Average end-to-end power consumption

One of the main features of SeLeZoR is that it minimizes the node capture attacks. Fig.15 illustrates the effect of PDR on the proposed protocol when the number of attacks increases while packets are sent from source node to the destination node. The proposed protocol keeps the delay stable between 1 s and 1.5 s. Moreover, SeLeZor keeps stable the delay under various network attacks. It has also proven that the proposed protocol mitigates the illegitimate user and it is able to work normally. As a conclusion of these results, we can say that when the number of attacks increases, the delay also increases.

Fig. 16 shows the PDR when the number of attacked nodes increases. Generally, the PDR decreases when the number of attacks increases. We can conclude that many packets are dropped during the communication, so the performance between the source and destination is low. The results show that our proposed protocol presents higher PDR as a function of the number of attacks. In addition, SeLeZor presents a PDR higher than 50% when 30 attacks are registered while SecLEACH only has a PDR of 40% for the same number of attacks. SeLeZor is able to detect and handle an illegitimate user and can smoothly carry its communication.

Finally, Fig. 17 shows the network overhead as a function of the number of attacks. Generally, an increasing number of attacks would affect the routing overhead. However, SeLeZor is able to manage the increase of the number of attacks while maintains a relatively low routing overhead.



Fig.15 End to End delay vs number of attacks

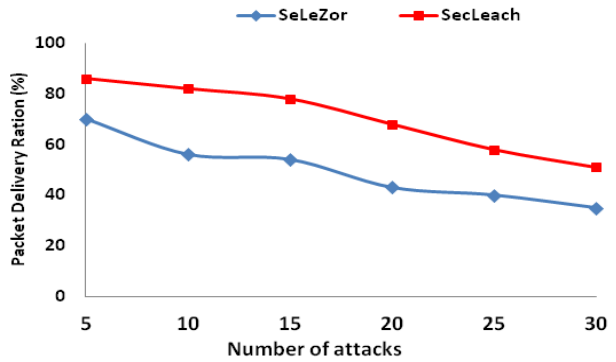


Fig.16 Packet delivery ratio vs number of attacks

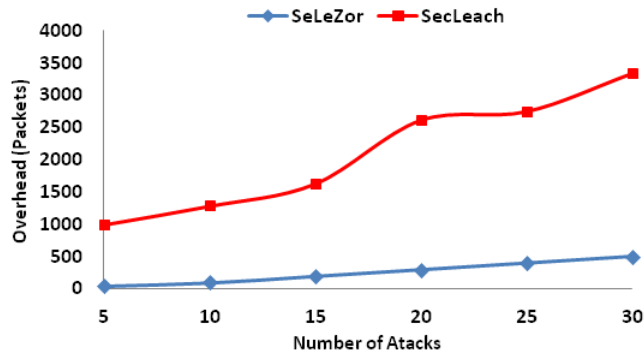


Fig. 17 Routing overhead vs number of attacks

These results proved that SeLeZor is able to keep the network communication with lower overhead than SecLEACH and mitigates the intruder actions.

6. Conclusion and Future Work

The main objective of a routing protocol scheme in WSN is to keep in mind the energy efficiency and increase the lifetime of the network [38]. A Secure and Low-Energy Zone-based Routing Protocol known as SeLeZoR is presented and its performance is evaluated in this paper.

In SeLeZoR, zones are used in order to reduce communication messages with the BS. Moreover, CHs use unequal sizes of clusters. The clusters nearer to the BS have smaller sizes than those clusters away from the BS. For inter-cluster transmission, the CHs nearer to the BS can reserve some energy and the Clusters away from the BS can reserve some energy for long-distance transmission. Thus, the energy consumption is lower. This paper also addresses the important issue of packet loss in the network, which makes the network unreliable. Therefore, SeLeZor has proposed the Vice Head mechanism for ZH and CH recovery to avoid the Heads from being a single point of failure. On the basis of the zoning and clustering structure, SeLeZor reduces the needless waste of energy.

This paper enhances the security and energy-efficiency of WSNs' protocols. SeLeZoR protocol provides the secure key management in which all the communication types of WSN are encoded and authenticated the connecting nodes. Similarly, a zone based technique is introduced for intra and inter-zone communication, which increases the lifetime of the network.

As future work, we are going to include an intelligent mechanism for security and energy efficiency using artificial neural network and genetic algorithms [39]. After introducing such intelligence in the protocol, it would be more adaptive, robust and reliable as well.

References

- [1]Sendra S, *Deployment of Efficient Wireless Sensor Nodes for Monitoring in Rural, Indoor and Underwater Environments*, Editorial Universitat Politècnica de València. 2013.
- [2]Garcia M, Bri D, Sendra S, Lloret J. Practical deployments of wireless sensor networks: A survey. *International Journal on Advances in Networks and Services* 2010; 3(1 & 2):136–178.
- [3]Javaid N., Qureshi TN., Khan AH., Iqbal A., Akhtar E., Ishfaq M. (2013). EDDEEC: Enhanced Developed Distributed Energy-Efficient Clustering for Heterogeneous Wireless Sensor Networks. *Procedia Computer Science*, 2013; 19 :914-919.

- [4]Men S, Chargé P, Pillement S, A Robust and Energy Efficient Cooperative Spectrum Sensing Scheme in Cognitive Wireless Sensor Networks, *Network Protocols and Algorithms* 2015; 7(3): 140-156.
- [5]Sendra S, Lloret J, Garcia M, Toledo JF, Power Saving and Energy Optimization Techniques for Wireless Sensor Networks, *Journal of Communications* 2011; 6(6): 439-459.
- [6]Papadopoulos GZ, Kotsiou V, Gallais A, Chatzimisios P, Noel T, Low-Power Neighbor Discovery for Mobility-Aware Wireless Sensor Networks, *accepted to be published in Elsevier AdHoc Networks journal* 2016, 48 (-): 66-79.
- [7]Latif K, Ahmad A, Javaid N, Khan ZA, Alrajeh N, Divide-and-Rule Scheme for Energy Efficient Routing in Wireless Sensor Networks. *Procedia Computer Science* 2013;19(-):340-347.
- [8]Zhang W, Han G, Feng Y, Lloret J, Shu L, A Survivability Clustering Algorithm for Ad Hoc Network Based on a Small-World Model, *Wireless Personal Communications* 2015; 84(3):1835-1854.
- [9]Garcia M, Sendra S, Lloret J, Lacuesta R, Saving Energy with Cooperative Group-Based Wireless Sensor Networks, *Cooperative Design, Visualization, and Engineering. Series Lecture Notes in Computer Science* 2010; 6240(-): 73-76
- [10]Garcia M, Sendra S, Lloret J, Canovas A, Saving energy and improving communications using cooperative group-based Wireless Sensor Networks, *Telecommunication Systems* 2013; 52(4): 2489-2502.
- [11] Garcia M, Lloret J, Sendra S, Rodrigues JJPC, Taking Cooperative Decisions in Group-Based Wireless Sensor Networks, *Cooperative Design, Visualization, and Engineering, Lecture Notes in Computer Science* 2011; 6874(-): 61-65
- [12]Garcia M, Lloret J, A Cooperative Group-Based Sensor Network for Environmental Monitoring, *Lecture Notes in Computer Science* 2009; 5738(-): 276-279.
- [13]Jain T, Wireless Environmental Monitoring System (WEMS) Using Data Aggregation in a Bidirectional Hybrid Protocol, *In Proc. of the 6th International Conference ICISTM 2012, Grenoble, France, March 28-30, 2012.* (414-420)
- [14]Sahraoui S, Bouam S. Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks. *International Journal of Communication Networks and Information Security (IJCNIS)* 2013; 5(3): 178-185.

- [15]Senouci MR, Mellouk A, Senouci H, Aissani A. Performance evaluation of network lifetime spatial-temporal distribution for WSN routing protocols. *Journal of Network and Computer Applications* 2012; 35(4): 1317-1328.
- [16]Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. *In proc. of the 33rd Annual Hawaii International Conference on System Sciences 2000*. January 4-7, 2000 Maui, Hawaii; (pp. 10).
- [17]Oliveira LB, Ferreira A, Vilaça MA, Wong HC, Bern M, Dahab R, Loureiro AA, (2007). SecLEACH—On the security of clustered sensor networks. *Signal Processing* 2007; 87(12): 2882-2895.
- [18]Xiangning F, Yulin S. Improvement on LEACH protocol of wireless sensor network. *In proc. of the 2007 International Conference on Sensor Technologies and Applications(SensorComm 2007)*. October 14-20, 2007 - Valencia, Spain. (pp. 260-264).
- [19]Biradar RV, Sawant D, Mudholkar D, Patil D. Multi-hop routing in self-organizing wireless sensor networks, *International Journal of Computer Science* 2011; 8(1): 154–164.
- [20]Tong M, Tang M, LEACH-B: An improved LEACH protocol for wireless sensor network. *In proc. of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM 2010)*, 23-25 Sept. 2010, Chengdu City, China (pp. 1-4).
- [21]El-Basioni BM, Abd El-kader SM, Eissa HS, Zahra MM, An Optimized Energy-aware Routing Protocol for Wireless Sensor Network, *Egyptian Informatics Journal* 2011;12(2): 61–72.
- [22]Bojkovic ZS., Bakmaz BM., Bakmaz MR, Security issues in wireless sensor networks. *International Journal of Communications* 2008; 2(1): 106-115.
- [23]Younis O., Fahmy S.. Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach. *In proc. of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004)*, Hong Kong. 7-11 March 2004
- [24] Garcia M, Lloret J, Sendra S, Lacuesta R, Secure Communications in Group-based Wireless Sensor Networks, *International Journal of Communication Networks and Information Security* 2010; 2(1); 8-14.
- [25]Noack A, Spitz S, Dynamic Threshold Cryptosystem without Group Manager, *Network Protocols and Algorithms* 2009; 1(1): 108-121
- [26]Nasser N, Chen Y. SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. *Computer Communications* 2007; 30(11): 2401-2412.

- [27]Alippi C, Camplani R, Galperti C, Roveri M, A Robust, Adaptive, Solar-Powered WSN Framework for Aquatic Environmental Monitoring, *IEEE Sensors Journal* 2011; 11(1):.45-56
- [28]Parra L, Sendra S, Jimenez JM, Lloret J, Smart system to detect and track pollution in marine environments, in proc. of the 2015 IEEE International Conference on Communication Workshop (ICCW 2015), 8-12 June 2015, London. (pp.1503 - 1508)
- [29]El-Azeem NS., El-Kader SM., Zahra MM. Cluster Head Recovery Mechanism for Hierarchical Protocols. *International Journal of Computer Science Issues (IJCSI)*, 2013; 10 (5).
- [30]Mehmood A, Lloret J, Noman M, Song H, Improvement of the Wireless Sensor Network Lifetime using LEACH with Vice-Cluster Head, *Ad Hoc & Sensor Wireless Networks* 2015; 28 (1&2):1-17.
- [31]A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2005.
- [32] Atto M, Guy, Routing Protocols and Quality of Services for Security Based Applications Using Wireless Video Sensor Networks, *Network Protocols and Algorithms* 2014; 6(3): 119-137.
- [33]Liu Z, Zheng Q, Xue L, Guan X. A distributed energy-efficient clustering algorithm with improved coverage in wireless sensor networks. *Future Generation Computer Systems* 2012; 28(5): 780-790.
- [34]Bri D, Sendra S, Coll H, Lloret J, How the Atmospheric Variables Affect to the WLAN Datalink Layer Parameters," in proc. of the 2010 Sixth Advanced International Conference on Telecommunications (AICT 2010) Barcelona, Spain. 9-15 May 2010. Pp.13-18.
- [35]Ganesh S, Amutha R. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. *Journal of Communications and Networks* 2013; 15(4): 422-429.
- [36]Amjad M, (2014) Energy Efficient *Multi Level and Distance Clustering Mechanism for Wireless Sensor Networks*. PhD thesis, Kohat University of Science & Technology, Kohat, 2014.
- [37]Papadopoulos GZ, Kritsis K, Gallais A, Chatzimisios P., Noel T, Performance Evaluation Methods in Ad-Hoc and Wireless Sensor Networks: A Literature Study, *IEEE Communications Magazine, Ad Hoc and Sensor Networks Series* 2016, 54(1):122-128.
- [38] Bagci F, Energy-efficient Communication Protocol for Wireless Sensor Networks, *Ad Hoc and Sensor Wireless Networks* 2016,30(3-4): 301-322.

[39]Meghanathan N, A Generic Algorithm to Determine Maximum Bottleneck Node Weight-based Data Gathering Trees for Wireless Sensor Networks, *Network Protocols and Algorithms* 2015, 7(3):. 18-51.