REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA
Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie
Département d'informatique

N° d'ordre : RTIC07/M2/2021

Mémoire

Présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : **Réseaux et Technologies de l'Information et de la Communication (RTIC)**

Titre : Conception d'un protocole de routage sécurisé pour les réseaux de capteurs sans fil.

Par :
CHADLI MOHAMED ISHAK

Soutenu le ../../…. devant le jury composé de :

Nom Prénom	grade	Président
Nom Prénom	grade	Rapporteur
Nom Prénom	grade	Examinateur

Année universitaire 2020-2021

Acknowledgments:

Bissmilah rahman rahim, wassalat wasslam alla achraf morsalin Mohamed amin alayhi salat wsalam, in the name of the mighty allah and upon Mohamed his servent and messenger. First of all, I wanna ta thank allah for everything he gave me and everything and every strength he gave me.

I would also like to give my supervisor DR.Imene Aloui a great thanks for guiding me through this battel that I gave and show me the right direction to be able to be a better person and to accomplish the task of my work.

I would also like to acknowledge my dead cat minocho, thanks for being with me all the time and share with me the college state, my new cat shadow also he needs big thenks to make my life little better, mom dad my brothers my family all of them are big part of my success today.

My friends Wahab and soufian, walid, Djamel and amir all of them thank you for everything.

ملخص :

تشكل شبكة المستشعرات اللاسلكية ، والتي يشار إليها باسم WSN ، ثورة علمية في مجال الاتصالات اللاسلكية والأنظمة المدمجة ، حيث فتحت الطريق لإنشاء جيل جديد من التطبيقات في مجالات متنوعة مثل البيئة ومراقبة الطقس والمراقبة الصحية وفحص سلامة المباني والمنشآت والأمن. مثل كشف المتسللين والاقتحام للمناطق المحظورة وحركة المرور واكتشاف الحرائق

نقل البيانات في هذا النظام الأساسي غير محمي ويعتبر خطيرًا إذا كانت المعلومات التي نريد استشعارها حساسة وذات أهمية خاصة بالنسبة لنا.

في هذه الرسالة سوف نناقش طرق حماية هذه الشبكة. سنختار بروتوكول SPIN معدل باستخدام ، سننشئ نظام أمان عن طريق تشفيره بمستويين باستخدام التشفير المتماثل بواسطة خوارزمية AES والتشفير غير المتماثل باستخدام خوارزمية RSA

Abstract:

Wireless Sensors Network, which is referred to as WSN, constitutes a scientific revolution in the field of wireless communications and embedded systems, as it has opened the way for the creation of a new generation of applications in fields as diverse as the environment, weather monitoring, health monitoring, building and facility safety inspection, and security. Such as detecting intruders, intrusions into restricted areas, traffic and fire detection.

The transmission of data in this platform is not protected and is considered dangerous if the information we want to sense is sensitive and of particular importance to us.

In this thesis, we will discuss ways to protect this network. We will choose a modified SPIN protocol using, we will create a security system by encrypting it with two levels using the Symmetric encryption by AES algorithm and Asymmetric encryption using RSA algorithm

Resume:

Le réseau de capteurs sans fil, appelé WSN, constitue une révolution scientifique dans le domaine des communications sans fil et des systèmes embarqués, car il a ouvert la voie à la création d'une nouvelle génération d'applications dans des domaines aussi divers que l'environnement, la surveillance météorologique, la surveillance de la santé, l'inspection de la sécurité des bâtiments et des installations et la sécurité. Comme la détection d'intrus, les intrusions dans des zones restreintes, la détection de trafic et d'incendie.

La transmission de données sur cette plateforme n'est pas protégée et est considérée comme dangereuse si les informations que nous souhaitons capter sont sensibles et revêtent une importance particulière pour nous.

Dans cette thèse, nous discuterons des moyens de protéger ce réseau. Nous choisirons un protocole SPIN modifié à l'aide, nous créerons un système de sécurité en le cryptant à deux niveaux à l'aide du cryptage symétrique par algorithme AES et du cryptage asymétrique à l'aide de l'algorithme RSA

Contents:

General introduction

Chapter 01: Wireless Sensor Network

1. Introduction……... 03
2. Wireless sensor networks……. 04
   2.1 Definition…….. 04
   2.2 Elements…… 04
   2.3 Sensors in wireless sensor networks……. 05
3. Protocol stack…….. 07
4. WSN application …… 07
5. COMMUNICATION MODEL IN WSN……... 11
6. CHARACTERISTICS of WSN…….. 12
7. Advantage /disadvantage of WSN…… 13
8. Energy consumption in WSN…….. 13
   6.1 Challenges……..... 14
   6.2 Reason of Energy Waste…… 14
   6.3 How to save energy…… 15
   6.5 energy model …… . 15
9. Routing protocols in WSN…… 16
   9.1 Routing Challenges and Design Issues in WSNs….. 16
   9.2 Network Structure .…… 17
10. Conclusion …… 19

Chapter 2: Aspect of security in sensor networks and state of the art on existing works

1. Introduction …… 20
2. Security……... 21
3. Security measures in WSN…… 21
   3.1 Data Confidentiality…… 21
   3.2 Data Freshness…… 21
   3.3 Self-organization…… 22
   3.4 Time synchronization……. 22
   3.5 authentication …… 22
4. WSN Vulnerabilities, Threats and Attacks…… 22
5. Functional security blocked in WSN…….. 23

6. Security mechanisms ……. 24
6.1 Cryptography…… 25
6.2 cryptographic tools…… 26
7. security protocols in WSN'S……. 27
7.1 Spins…… 28
7.2 Tinysec…… 29
7.3 Minisec…… 29
7.4 Zigbee……. 30
7.5 Leap…… 31
8. Conclusion …… 32

Chapter 3: conception of a new secure routing protocol

1. Introduction …….. 33
2. Global description of Secure GR-SPIN……..... 34
3. Detail's description of Secure GR-SPIN……. 35
3.1 Step 0: generating RSA keys…… 35
3.2 Step 1: initialization and encryption with RSA…… 36
3.3 Step 2: Data advertising and decryption with RSA …. 36
3.4 Step 3: Data requesting and decryption with RSA…… 38
3.5 Step 4: Data transmitting and encryption with AES … 39
3.6 Step 5: Data saving and decryption…… 41
4. General operation …….. 44
5. Conclusion ……. 46

Chapter 4: implementation and results

1. Introduction …… 47
2. Development environment……. 48
2.1 Software…… 48
2.2 Hardware ……. 48
3. Network model ……. 49
4. Sensor model……. 49
5. Simulation……. 51
6. Project structure……... 51
6.1 Functions…… 51
6.2 Buttons …….. 53
7. Results …….. 66
8. Conclusion …… 68

General conclusion …… 67

Bibliographies …… 68

Figure's list:

Figure 01: Wireless Sensor Network…….. 04

Figure 02: sensor examples …… 05

Figure 03: components of sensor nodes …… 05

Figure 04: Protocol Stack ……... 07

Figure 05: WSN applications..…….……... 08

Figure 06: : example military application in WSN ……. 08

Figure 07: example health application in WSN ……. 09

Figure 08: example environmental application in WSN …… 09

Figure 09: the main subcategories Flora and Fauna applications ……. 10

Figure 10 example environmental application in WSN ..…… 10

Figure 11: example urban application in WSN……. 11

Figure 12: WSN one hop model …….…… 11

Figure 13: WSN multi hop model …….……. 12

Figure 14: Energies consumed by a sensor ……..……. 14

Figure 15: Routing protocols in WSN's based Network structure …… 17

Figure 16: Taxonomy of challenges and security solutions in WSN's…… 24

Figure 17: Symmetric Encryption……. 25

Figure 18: Asymmetric Encryption……... 26

Figure 19: how digital signature works…… 26

Figure 20: Hash function in cryptography……... 27

Figure 21: Principle of message authentication codes (MACs)…….. 27

Figure 22: shows the comparison of these security protocols in terms of their energy consumption and security provided by them…… 32

Figure 23: General process for secured GR-Spin…… 35

Figure 24: RSA key pair generation……. 36

Figure 25: general process of data advertising and decryption with RSA…… 37

Figure 26: general process of data requesting stage…… 39

Figure 27: general process of sending and encryption data with AES…….. 40

Figure 28: AES encryption steps…….. 41

Figure 29: AES decryption…… 42

Figure 30: global architecture of our solution…….. 43

Figure 31: sequence diagram for the solution proposed…… 45

Figure 32: MATLAB icon …… 48

Figure 33: dell latitude 3580……. 48

Figure 34: deployment with 200 nodes …… 49

Figure 35: block diagram of TelosB……. 50

Figure 36: project application structure …… 52

Figure 37: security button function…… 53

Figure 38: RSA_GEN.m …….. 53

Figure 39: Deployment button…….. 54

Figure 40: inisialize.m function source code…… 55

Figure 41: intialisationgraph.m source code…… 55

Figure 42: RSA_ENC.m function…… 56

Figure 43: capturing data…… 57

Figure 44: fcapture.m function……. 57

Figure 45: AES encryption function……. 58

Figure 46: adv from source node to the sink…… 58

Figure 47: adv.m function…… 59

Figure 48: RSA_Dec.m function…….. 59

Figure 49: requesting data…… 60

Figure 50: frequest.m function……. 60

Figure 51: sending data to the sink…….…… 61

Figure 52: senddata.m function…… 61

Figure 53: aes_decryption function……. 62

Figure 54: Savedata.m function…… 62

Figure 55: save data and display…….. 63

Figure 56: drawline.m function…… 63

Figure 57: energy consumption and total energy…… 64

Figure 58: avergenergy.m function……... 64

Figure 59: energycons.m function…… 65

Figure 60: Task.m function…… 66

Figure 61: simulation results…….. 67

Figure 62: simulation results…….. 67

Figure 63: energy consumption……. 68

Table lists:

Table 1: Sensor Components …….……... 06

Table 2: WSN Advantages/Disadvantages…… 13

Table 3: shows comparison between WSN security protocols…… 32

Table 4: TelosB settings …… 50

Table 5: Network simulation settings ……... 51

Table 6: nodes type…….. 51

List of Abbreviations

WSN	Wireless sensor network
ADV	Advertise
RQS	Request
msg	Message
RSA	Rivest–Shamir–Adleman
AES	Advanced Encryption Standard
SPIN	Sensor Protocols for Information via Negotiation
GRASP	Greedy Randomized Adaptive Search Procedure

General Introduction:

In a modern-day wireless telecommunication play a big role in our lives, the rise of this technologies allowed us to view a new offer and achieves new perspectives int the telecommunication fields. In comparison with the wired environment, the wireless environment allows flexibility of access and the ease of manipulation of information through mobile computing units such us (laptop, pc or PDA, sensors….).

Wireless sensor network is a combination of hundreds or thousands of small devices each with sensing, processing and communication capabilities to monitor the real-world environment, since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

In addition to traditional security issues like secure routing and secure data aggregation, security mechanisms deployed in WSNs also should involve collaborations among the nodes due to the decentralized nature of the networks and absence of any infrastructure. In real-world WSNs, the nodes cannot be assumed to be trustworthy apriori. Researchers have therefore, focused on building a sensor trust model to solve the problems which are beyond the capabilities of traditional cryptographic mechanisms.

In this thesis to that we will propose we will propose a security routing protocol that will help our network to be secured. By using an optimized version of spin protocol called GR-SPIN and make it secure so we can allow our network to be compact and energy efficient and highly secured, using two types of encryptions that will provide to level of security, a symmetric encryption with AES and asymmetric encryption with RSA.

The structure of our application is as follow:

GENEREAL INTRODUCTION

The chapter 1 will present Wireless sensor network (WSN) in general, and the sensor nodes including the definition and architecture...etc. we also talk about the routing protocols using in WSN and the energy consumption.

The chapter 2 we explain the security in general and its mechanisms and how to apply it, we also speak about security in WSN and how to apply it and also the different protocols in WSN security and the difference between each one.

The chapter 3 we introduce our secure GR-SPIN solution and how it works and all its functions.

The chapter 4 presents the simulation tools that we used, the network models and at the end we shown the results of the simulation and differences between secured and non-secured solution.

Chapter 1: Wireless Sensor Network

CHAPTER 1: WIRELESS SENSOR NETWORK

1.1 Introduction:

Wireless sensor networks (WSNs) begun to gain a huge appeal worldwide in recent years, especially after the introduction of MEMS or Micro-Electro-Mechanical Systems a technology that helped in accelerating the pace in which smart sensors are developed, Wireless Sensor Networks consists of a set of low-cost and small-sized sensor nodes having limited communication range, energy, processing, and storage capacity. WSNs are classified into two types structured and unstructured network in the former, the deployment of nodes is made with proper planning while in latter the same is done in an ad hoc manner.

A WSN has so little infrastructure. It is just combination of a large number of sensor nodes (few tens to thousands) that are working together to monitor a region or to obtain data about the environment. In the two types of WSNs the unstructured WSN is the one that contains a dense collection of sensor nodes. these sensor nodes can be placed in an ad hoc manner and once they are deployed in the field, they can serve no matter the conditions.

:

1.2 Wireless sensor network:

a. Definition:

Wireless sensor network (WSN) is a combination of various sensor nodes connected with each other to a sink or more in a zone called sensing zone, it can be deployed in any part of the world to collect information like temperature, pressure, vibration and sound…etc. to be analyzed [1].

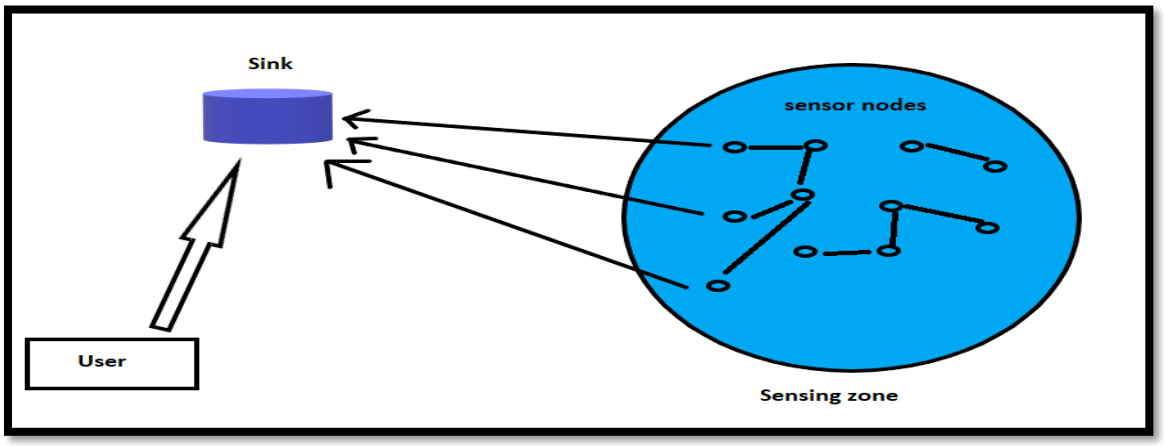


Figure 1: Wireless Sensor Network [2]

b. Elements:

WSN is combination of many elements and they all make the entire network, and they are as follow:

1- Sensors:

sensor is a device used to measure a property, such as pressure, position, temperature, or acceleration, and respond with feedback [4]

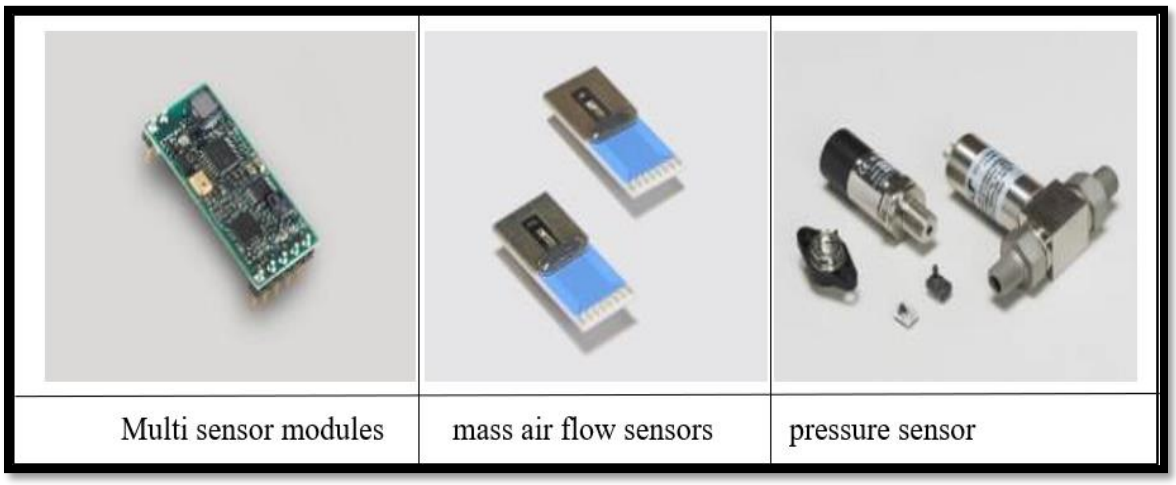


Figure 2: Sensors examples [4]

c. Sensors in wireless sensor networks:

Wireless sensors and nodes are a device that allows you to remotely monitor and diagnose systems quickly and can gather sensory information, and detect changes in local environments and provides data to optimize your operation, they are easy to install and set up, it eliminates expensive cable runs, and run integrated machines that were not previously network capable.[5]

A wireless sensor node is composed of 4 main units such as sensing unit, processing unit, transceiver unit, and a power unit which is in figure 5:

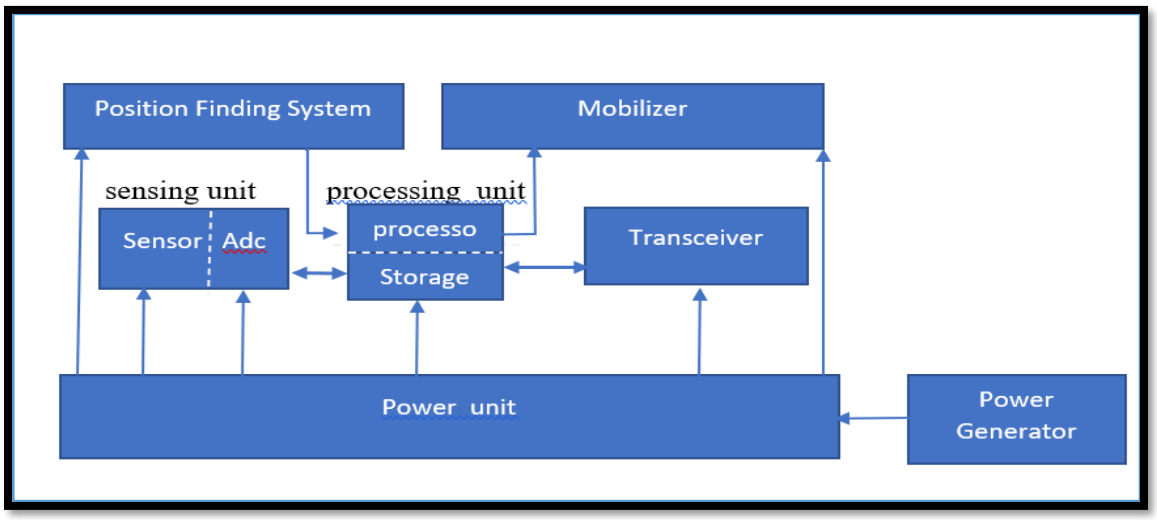


Figure 3: component of sensor nodes [3]

- **Power unit**: is the unit who is responsible for power delivery to the sensor it will often be an AA battery normal of about 2.2 - 2.5 Ah operating at 1.5, it can be also supported by solar cells that convert light to electric power [7][8].
- **Communication unit**: it's the unit who is manly focused on transmitting data to other nodes, it is composed of a radio module transmitter/receiver which allow the sensor to communicate with other nodes on the network using radio waves [7][8].
- **Sensing unit**: this unit is the physical heart that allowing the measurement, it composed a sensor which will obtain digital measurements on the environmental parameters and analog to digital sensor (adc) that will goes to convert the recorded information and transmit it to the processing unit [7][8]
- **Processing unit**: it's the main component of the sensor and it's composed of two interfaces one for the communication unit and the other for sensing unit, it has two processor and an operation system (tiny os) all data received will be stored in the memory [7].

There are also many components of sensors so we can achieve deferent results as they shown in the table 1:

Components	Details
Sensor	Used to capture and measuring a value relating to its Environment
Aggregator	Collect messages he receives from the sensors and send iyyt to the sink, for limiting traffic and expend the life time of the sensor
Gateway	It has two network interfaces, allows the sensors to connect to traditional network
Sink	All data send to him measured by the network of sensors

Table 1: Sensor Components [9]

1.3 Protocol stack:

The protocol stack implemented for the set of communication protocols of the sensor network.

The protocol stack comprises 5 layers which have the same functions as those of the

OSI model (Open Systems Interconnection). Each layer of the stack communicates with an adjacent layer (the one above or the one below). Each layer thus uses the services of the lower layers and provides them to the higher level one.

It thus includes 3 plants for energy management, mobility management and task management.

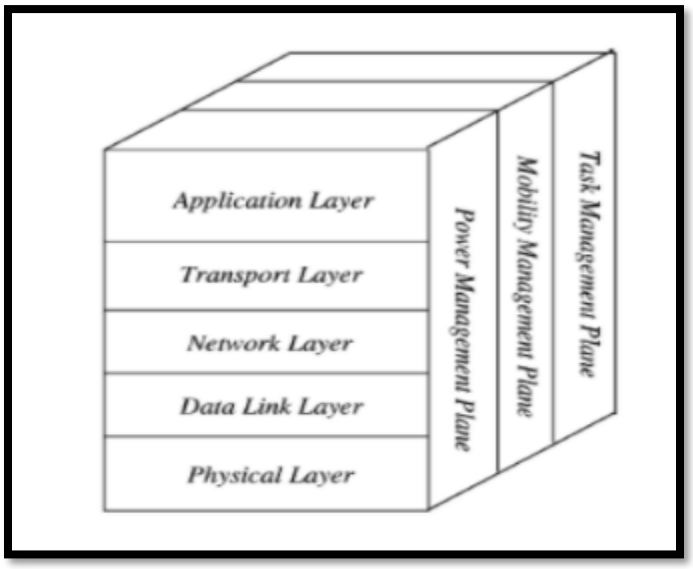


Figure 4: Protocol Stack [11]

1.4 WSN APPLICATIONS:

The application of WSN is in many fields today and some of them are already mature or still in development, they are classified due to their nature and use cases into six main categories which are presented in Figure 7:[21]

Figure 5: WSN applications

- **Military application:**

In this domain is not the first field of human activity of WSN's, but it is also considered to have motivate and improve the research in WSN, Therefore, the using in WSN military makes use of control and communications, sensing soldier status and other objects. [21]

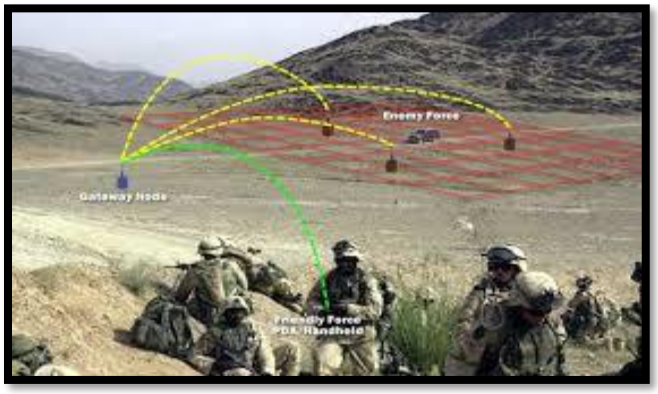


Figure 6: example military application in WSN [22]

- **Health:**

In the health domain, WSN plays a huge role in it and utilize advance medical sensor to monitor patients within a healthcare facility, as a hospital or within their home, as

well as to provide a real time monitoring of patient's vitals by utilizing and deployment of a wearable hardware. [21]

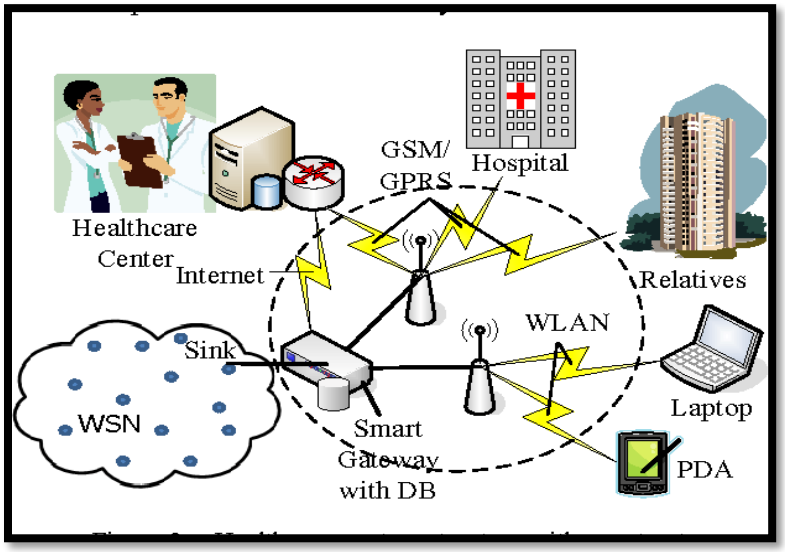


Figure7: example of health applications in WSN [23]

- **Environmental Applications:**

Environmental application that mainly demand continuous monitoring of ambient conditions at hostile, harsh and remote areas that can be improved by WSN, [21]

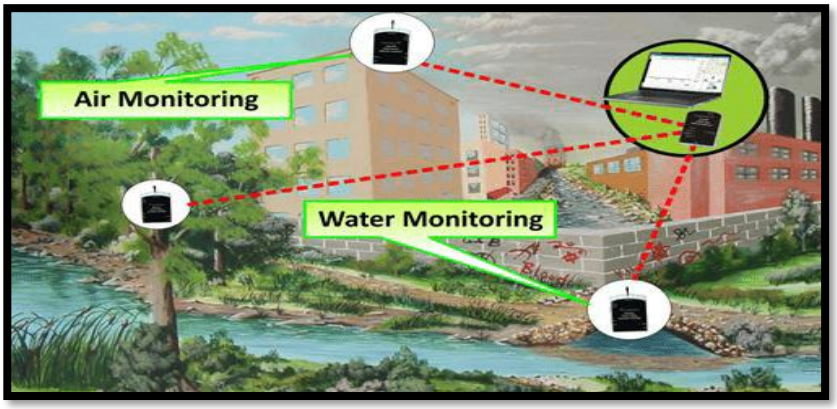


Figure 8: example of Environmental application [24]

- **Flora and Fauna applications:**

Both flora and fauna domains are vital for every country, in the figure 10 the main subcategories, they are namely greenhouse monitoring, crop monitoring, and livestock farming, [21]

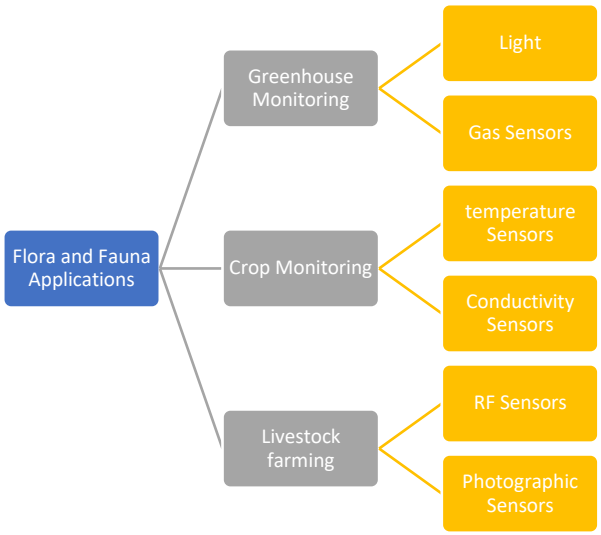


Figure 9: the main subcategories Flora and Fauna applications

- **Industrial applications:**

WSN can be applied in many various industrial applications to help solving related problems like technique problem, robotic problems, logistics and machinery health. [21]

Figure 10:example of industrial application in WSN

- **Urban applications:**

The variety of sensing abilities offered by WSN's also provides an opportunity to have an unprecedented level of information about a target area, a building, a room or outdoors. WSN are indeed a tool to measure a phenomenon in an urban environment. [21]

Figure 11: example of urban applications in WSN

1.5 COMMUNICATION MODEL IN WSN:

In WSN there is two modes of communication:

- **One hop model:** this is one of the simplest ways to deploy and represent a direct communication, in this approach every node in our network directly transmits the data to the BS (Base Station), this type of communication not only saves energy but only good in coast too, the down side is that the nodes have a limited range of communication

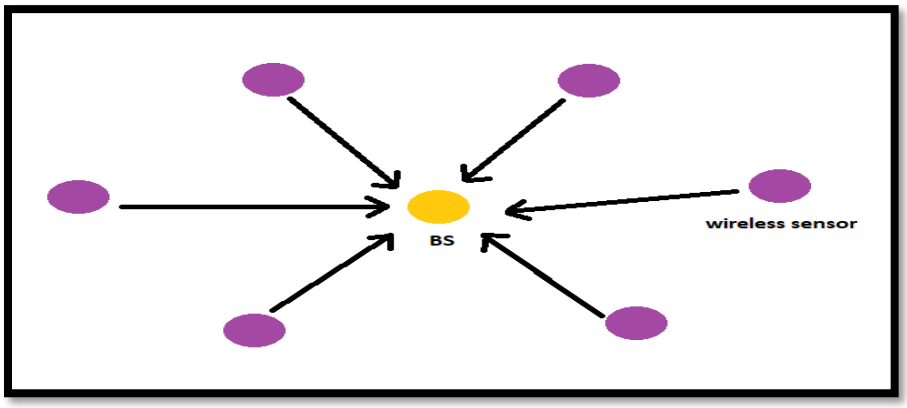


Figure 12: WSN one hop model

- **Multi hop model:** In this model the node transmit data by passing it to his neighbor node which is close to the BS, by this the data are traveling by hops from a node to another, from source until it reaches the destination.

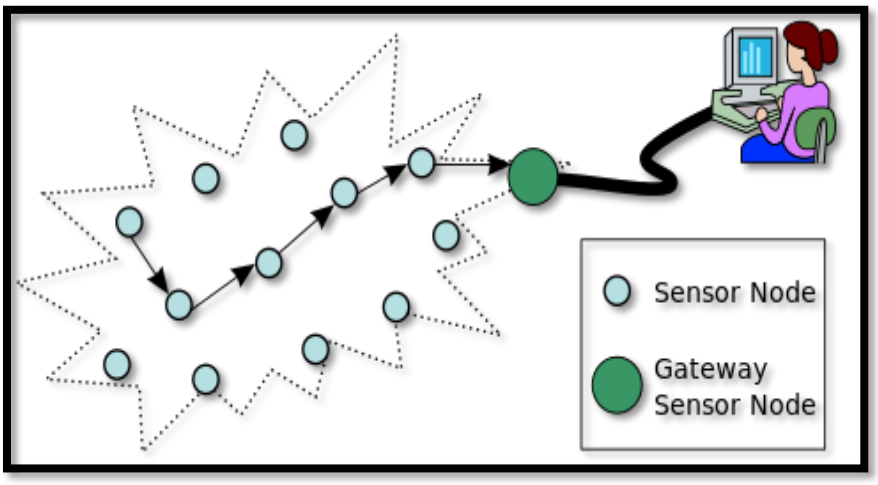


Figure 13: WSN multi hop model [27]

1.6 CHARACTERISTICS OF WSN:

Today in wireless networks that include types like Lan, Bluetooth, adhok and so on. all have some characteristics based on as similar WSN must be consider for efficient deployment of the network, and here are the significant characteristics of WSN [13][14]:

- **Low cost**: in our network we are deploying thousands of nodes and the size of battery are limited and memory to so we must consider the cost of each node.[13][14]
- **Battery size**: in WSN the nodes energy used for different reasons such as computing and communication. Therefore, the protocols and the algorithm that used must consider the battery size in advance. [13][14]
- **Communication**: in general, WSN communication used radio waves over a wireless channel. and we'll deploy a thousand of sensor and the range is tens to several hundred meters, because the sensor will be easily influenced by natural environment, and for that the software of WSN must be robust and fault-tolerant, security and resiliency. [13][14]
- **Security and Privacy**: in WSN security is great major to consider and it must be. Each sensor node should have a working security mechanism in order to stop any unwanted access, attacks, and unintentional damage in the information of the sensor nodes.[13]

- **Dynamic**: it means we can manage our sensor nodes if some nodes fail or go out of battery, and we can add other nodes to our infrastructure, the sensors of WSN must be embedded with functions of reconfiguration and self-adjustment.[13][14]
- **Self-Organization**: in our network the sensor nodes must have the capability of organizing themselves as they are deployed in unknown pattern and hostile environment, the sensor nodes which it can collaboratively adjust itself perform and distribute algorithm.
- **Multi-hop communication**: in WSN a large sensor is deployed, so if a sensor needs to communicate to other nodes the feasible way is with a sinker or base station with the help of neighbor nodes through routing path. If one node needs to communicate with other nodes or the base station which is beyond the frequency coverage it must be through the multi-hop route by neighbor or an intermediate node.[13][14]
- **Application relevance (oriented)**: WSN is different from the conventional network due to its nature, and its highly dependent on application, it's ultimate work is acquiring the environment data ranges from military, health environmental...etc. [13][14]

1.7 Advantage /disadvantage of WSN:

As of any technology WSN is not perfect and there is some good in it as there is down flows, in here the advantages and disadvantages of WSN in the table below [15]:

Advantages	Disadvantage
- WSN are effective in harsh and hostile environments - WSN's offer easy scaled solution - Enable long-distance data transmit and collection	-Security risk -WSN introduce practical issues with their deployment -Limited battery life and transmitting capabilities

Table2: WSN Advantages/Disadvantages

1.8 Energy consumption in WSN:

In every day technology is evolving as so WSN technology, and at the same time it faces a large problem of energy constraints in terms of restricted battery life. That because each node depends on energy to do it task, and because of that it become major consequence in WSN, if one node fail it can interrupt the overall system.[16]

The energy consumed by a sensor node is mainly due to the operations

following: capturing, processing and communicating data [19].

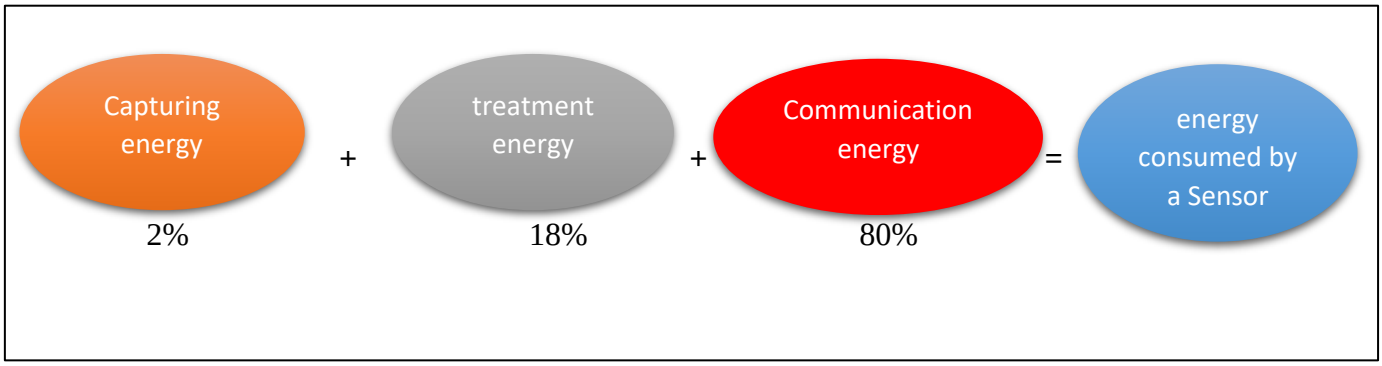


Figure 14: Energies consumed by a sensor [19]

1.8.1 Challenges: in overall WSN faces many challenges especially in energy consumption, and the main challenges are:

- The path between a sensor to a sink is selected depending on the network topology chosen.
- The same path is shared between many sensors to save data, and energy saving, that will cause a link failure.
- A many large number of sensors sending data to a sink might increases the complexity of the problem.
- The delivery ration for path/link increases the retransmission as well as increase transmission delay and also the energy consumed.

1.8.2 Reason of Energy Waste:

There are many reasons why energy is wasted, for us WSN energy is released during sensing process, transmitting, or receiving, and here the famous reasons why we waste energy:

a) Collision: when nodes receive more than one information in a time, these data may collide. All the information that causes that are to be discarded and retransmission of data is done.

b) Overhearing: the sensor is set to listen in all the sensing time and not put in sleep or energy saving mode at all

c) Control packet overhead: a minimal number of control packet should be used for enabling data transmission.

d) IDLE listening: this is one of the major sources of energy wasting. It happens when a node is listening to an idle channel in order to catch and receive possible data traffic.

1.2 How to save energy:

the steps taking for saving energy which is affected by communication and other reason:

1. Charging the transmission range between sensing nodes.
2. Avoid the interference with unwanted data like in the case of overhearing
3. Schedule the state of the node.
4. Efficient and data collecting methods are taking into consideration.

1.6.5 Energetic Model:

For starter the energy consumption is called **Ec** is defined as so:[19]

Ec = Es/sensing + Es/processing + Es/communication where:

Es/sensing: the energy consumption of sensing unit

Es/processing: the energy consumption of processing unit

Es/communication: the energy consumption of communication unit, it equals the sum of two values:

ETXwhich is energy transmissionandERXwhich is energy reception

Es/communication = ETX + ERX(2) where :

ETX (k, d) = (Eelec * k)+(Eamp *k * d2)

ERX (k) = Eelec * k(4) where:

K:the packet size (bits)

d: the distance between the transmitter and receiver

Eelec:energy to run the transmitter or receiver circuitry

Eamp:Transmit Amplifier

1.9 Routing protocols in WSN:

In WSN routing is very importing thing that must be handle carefully. Routing technique is needed to transmit and send data between sensor sondes and the base station. As so the routing techniques faces a large number of problems such as energy, security and the type of network we use [17]

1- Routing Challenges and Design Issues in WSNs:

Despite of the large number of WSN application, it has several restrictions like limited energy, security and others. These factors must be overcome and faces before efficient communication can be achieved in WSNs. The following we see the routing challenges and design issues that affect our routing process [18][17]:

- **Node deployment**: in WSN nodes deployments can affects the performance of the routing protocol. Therefore, there is two ways of deployment, a deterministic way where the nodes are manually placed and data is routed through pre-determined paths. The other one is randomized where the node randomly placed in ad hock manner.
- **Energy Consumption without losing accuracy**: generally, the power of a sensor is so limited in the tasks .as such, energy conserving forms of communication and computation are essential. The malfunctioning of some sensor does to power failure can cause a dramatic change in the topological changes and might require rerouting.
- **Data Reporting model**: Data sensing and reporting is dependent on the application and time criticality of the data reporting.
- **Fault Tolerance**: In a critical condition some of the sensor may fail due to many reasons like physical damage, low power or an environmental interference. As so the failure of the sensor nodes should not affect the overall task of the network, but if many

nodes fail, MAC and routing protocols must recreate a now formation for the links and routs to the data collection base station.

❖ **Security:** In wireless sensor is used in many critical fields. Therefore, data transmitted must be highly secured from any attack or unauthorized access.[20]

❖ **Network Dynamics:** Most network architecture assume that the sensor is stationary. But, mobility of the Base Station and the sensor nodes is sometimes necessary in many apps. Routing messages from moving nodes it far challenging and difficult as rout stability becomes an important factor.

2- Network Structure:

In general, the WSN routing is divided into a flat-based routing, hierarchical-based routing and location-based routing on the network structure.

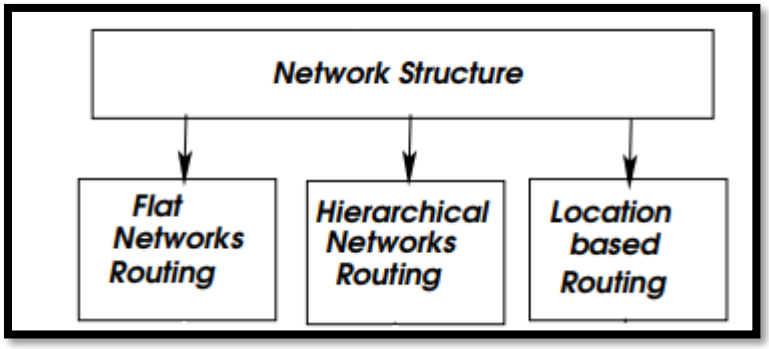


Figure 15: Routing protocols in WSN's based Network structure [17]

Flat based routing:

Is a multi-hop routing where all nodes operate at the same moment and time. And manly our network is typically quite large and the nodes are assigned in the same sensing task. Therefore. Since all nodes are transmitting data, redundancy will which definitely will lead to high and large energy consumption. The base station or sink can ask for some data in the region so all the nodes in the region will send data after an event happened .and here some of flat routing scheme:

- Sensor Protocol for Information via Negotiation (SPIN)
- Directed Diffusion (DD)
- Rumor Routing (RR)
- Gradient based Routing (GBR)

• Constrained Anisotropic Diffusion Routing (CADR)

• Energy Aware Routing (EAR)

• Minimum Cost Forwarding Algorithm (MCFA)

• Active Query forwarding in sensor network (ACQUIRE).

• Sequential Assignment Routing (SAR).

- **Location-based:**

In this scheme, the location of nodes is known through a low power GPS on every node. So, nodes are addresses by their own location, but not all nodes are demanded to work together. So, they can save energy and be sleeping condition while others are sensing the events. The distance between the sensor nodes can be detected the strength of the signal received from those nodes.

• Sequential assignment routing (SAR).

• Ad-hoc positioning system (APS).

• Geographic adaptive fidelity (GAF).

• Greedy Perimeter Stateless Routing (GPSR)

• Graph Embedding for Routing (GEM)

• Location Aided Routing (LAR)

• Geographic distance routing (GEDIR).

• Geographic and energy aware routing (GEAR).

- **Hierarchical base routing:**

In hierarchical routing the nodes are not able to communicate to a very large distance. Therefore, cluster based, hierarchical routing becomes a very good solution, the import of this protocol is by implemented data aggregation causing decreasing of the energy consumption, where the packets are sent to the sink

And here are some of the hierarchical routing

• Low energy adaptive clustering hierarchy (LEACH)

• Minimum energy communication network (MECN).

• Power efficient gathering in sensor information

systems (PEGASIS).

• Self-Organizing Protocol (SOP)

• Threshold Sensitive Energy Efficient Protocols: TEEN and APTEEN

1.10 Conclusion:

In this chapter, we have introduced the basic of WSN technology and it's elements like the sensor nodes, and we saw also the architecture of the WSN and some its function, we also have talked about its characteristic, the advantages/disadvantages of the WSN and the energetic model, lastly, we mention some of the routing protocols and their classification and the applications of WSN, in the next chapter we will see security in WSN and its measures and state of the art on existing works.

Chapter two: Aspect of security in sensor networks and state of the art on existing works

CHAPTER 2: SECURITY IN WIRELESS SENSOR NETWORK

2.1 Introduction:

In a world of perceived uncertainty and danger, the need of security becomes a main goal of political thought and action, against the threats that have an impact to us. This multidimensional nature of security results in both a society and industry have no clear understanding of a definition for the concept of security.

Therefore, security breaches are commonplace in computers, and it happen around the world every day, some of them are considered minor with small impact in our systems, but many of them are considered major, or even catastrophic.

CHAPTER 2: SECURITY IN WIRELESS SENSOR NETWORK

2.2 Security:

Security in computers is the protection of the items you value in it, [29]and so we live in a world fully connected so network security, is process of taking preventing measures to protect our network from unauthorized access, misuse or modification. so as so in WSN security play great major to make sure our commination is safe between all nodes and BS and it is a great problem need to resolve and take care of. [30]

2.3 Security Measures for WSN

WSN's are used in a big number of applications with different security requirements. E.g., military application for sensing an enemy or a highly defense systems, it demands a highly security levels.[31]

In that manner, a security protocol for WSN, must meet one or more of the security conditions:

2.3.1 Data Confidentiality

In our network, security mechanism should ensure that no message in our network is understood by anyone except intended recipient. In WSN the problem of confidentiality should address the following requirements.[31][32].

2.3.2 Data integrity

The mechanism should make sure to ensure that no message can be alerted by an entity as it's traverses from the sender to receiver.[31]

2.3.3 Data Freshness

It means that the data is new and recent, and ensure that no adversary our outsider can replay with and old messages. This requirement is very critical and important when the nodes use a shared-key for communication.

2.3.4 Self-organization

In WSN each node should be self-organizing. this future also makes a great challenge to security. The dynamic nature of WSN makes it sometimes hard, challenging and impossible to deploy any pre-installed shared key mechanism among the nodes and the sink.[33]

2.3.5 Secure -localization

In many cases, it becomes strictly necessary to require to locate itself in the network and automatically to locates each sensor node in the WSN. [31][34]

2.3.6 Time Synchronization

The majority of application in WSN require to be time synchronized. And also, in that manner any security mechanism should be time-synchronized.

2.3.7 Authentication

It makes sure that the communicating node is the one that it claims he is .in other way, an adversary can not only modify our data, it also can change a packet stream by injecting fabricated packet.[31]

2.4 WSN Vulnerabilities, Threats and Attacks

WSN vulnerabilities consists of many different attacks and threats, mostly of those attacks are similar to those that are applied in traditional network. In that manner an attack in node is totally new and distinct phenomenon that does not apply to traditional networks.[35]

The type of attack consists in distinguishing the passive attacks from the passive attacks:

- **The passive attacks**: these types of attacks are just limited to listening and analyzes exchanged the data traffic, this type of attack is easy to realize, and it’s too hard to detect. [37]

The passive attack consists of two phases:

Phase 1. Eavesdropping: this is very common violence against privacy. By interfering to someone personal data, the attacker easily learns the weakness of our system our learn the content of communication. [36]

Phase 2. Traffic Analysis: in here the messages are transferred over the network are so much vulnerable even if they are encrypted. There is a big possibility that someone can analysis the patterns of communication.[36]

- **The active attacks**: in active attacks, an attacker tries to modify or delete a certain part of the whole message, he can inject his own traffic in the network or replay to old messages to disturb the operation of the network or to cause a denial of service.[37], And here are some of the most common attacks in WSN:

- **Node capture Attack:** one of the distinct WSN's attacks, in this type of attack, the attacker is gaining full control of a sensor node through direct physical access. Then the attacker can gain a full access to the sensor node and extract the information in the sensor by simply reverse engineering process.[35]
- **DoSAttack:** Dos attacks re done by devastating the targeted server by putting an amount of extra traffic the maximum server capacity.[36]
- **Blackmail attack:** a malicious node make announce that another legitimate node is infected to eliminate this last form in the network. It the attacker node manage to tackle a significant number of nodes; it can disturb the whole operation.[37]
- **Replay Attack:** this type of attacks usually involves a passive imprisonment of the data unit and its succeeding retransmission for generating an attack. [36]
- **Selective forwarding:** In selective forwarding, a node act like router and tike it's roles, and it may refuse to forward the messages and simply just drop them.[37]
- **Wormhole Attack:** these types of attacks are extremely dangerous to our network, which an intruder records the stream of packets at a very specific position in the wireless network and send them to other location. [36]
- **Sybil Attacks:** this attack is defined as a malicious device illegally taking multiple identities illegitimately, he uses the other nodes to participate in distributed algorithms like elections.[36][37]
- **Sink hole Attack:** in it a malicious node represents itself as a black hole to appeal and catch all traffic.it will falsifies routing information to force the data to pass by him. It's main goal that nothing is transferred, creating a black hole in the network.[36][37].

- **Rushing Attack:** this attack is a latest threat that comes after DoS attack, the attacker distributes the malicious message very fast to genuine messages that reach later [37].

2.5 FUNCTIONAL SECURITY BLOCKED IN WSN

like it's shown in the following figure, we distinguished four of the blocks functionals in security solutions in WSN's: key management, routing security, data aggregation security, and channel access security.[38]

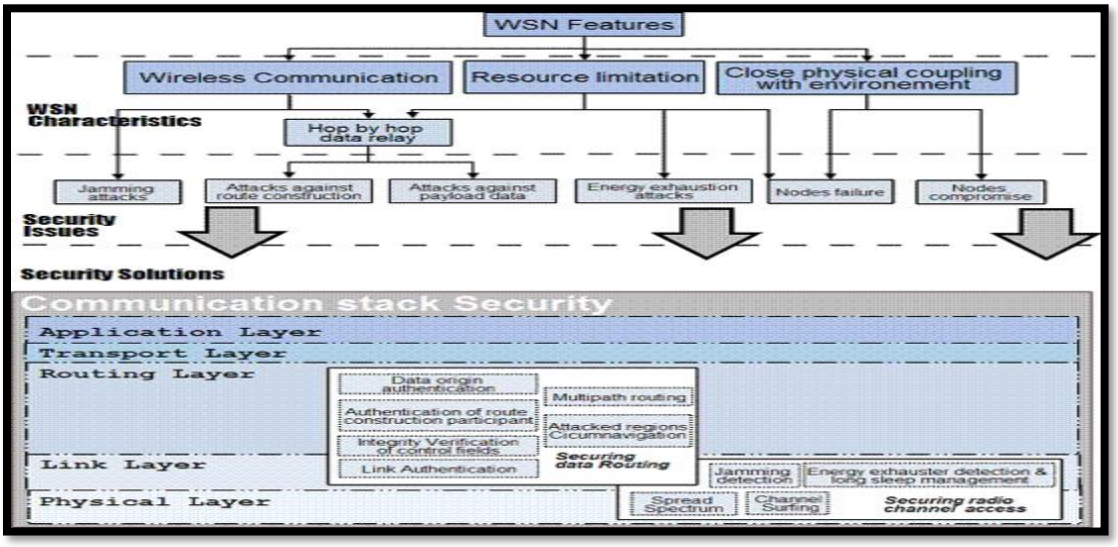


Figure 16: Taxonomy of challenges and security solutions in WSN's

2.6 SECURITY MECHANISMS:

There are different types of application in WSN and each one has specific need, and require different security requirements. For that encryption is the security solution many applicable in. [45]

2.6.1 Cryptography

Cryptography is simply the science of guarding the information and keeping them secure by transforming it into form that no unintended recipients can't understand. In this regard, a cryptographic algorithm can be set as a function that converts encrypted message in clear message n vice versa, by making use of a cryptographic key. The system of cryptographic might require some method to work and intended recipient to be able to make use of the encrypted message usually, but not always, by transforming the ciphertext back into plaintext. [45][46]

2.6.2 Cryptographic tools

Cryptography uses many tools to achieve its security goals, for that, here are the famous security tools we're using:

2.6.2.1 Encryption

By putting it simply, encryption is a method that takes the information and converted it into a secret form or code that simply hides Its original content. [47]

Encryption work simply by the sender must decide what cipher will best disguise the meaning of the message, and what the variable to use as a key to make for encoding, for that there is two types of encryptions.

- **Symmetric encryption:** this technique also called by secret key encryption, it works by using a single key shared between the sender and the receiver, the most widely used symmetric key cipher is the Advance Encryption Standard (AES).

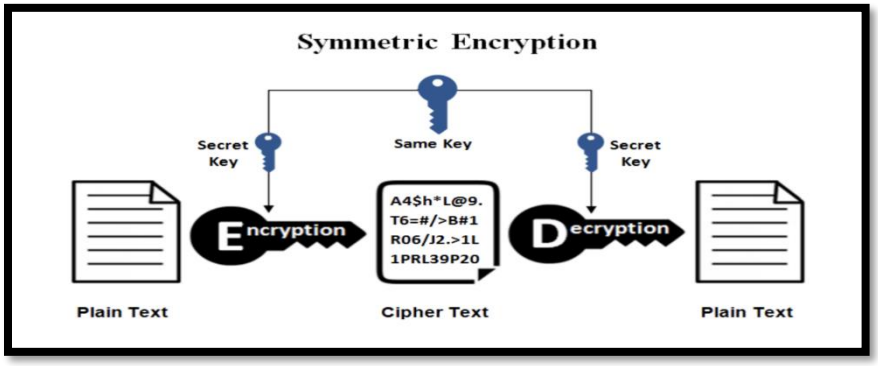


Figure 17: Symmetric Encryption [48]

- **Asymmetric encryption:** this technique uses two different keys—but logically linked. It's often uses a prime number to create keys since it's difficult to factor large numbers and it's hard to reverse-engineer the encryption, The Rivest-Shamir-Adleman (RSA) encryption algorithm is the mostly used.

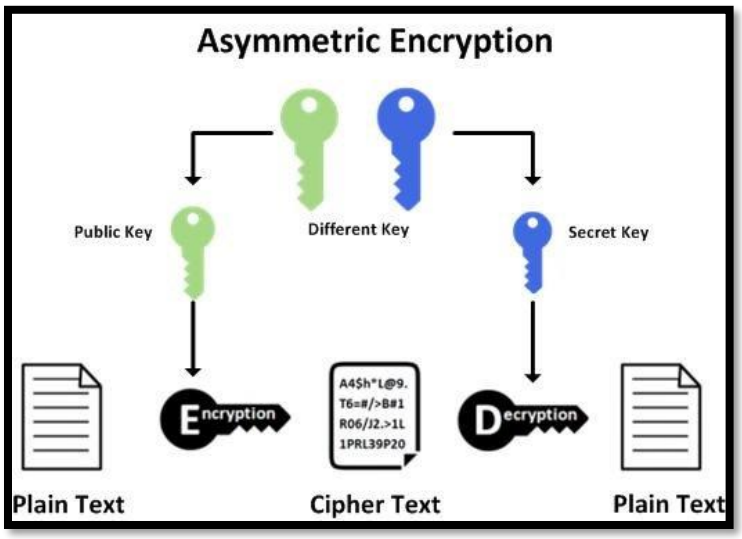


Figure 18: Asymmetric Encryption [49]

2.6.2.2 Digital signature

The digital signature is a cryptographic system ensuring the non-repudiation of the source. It is based on asymmetric keys. The sender (A) signs the data to be transmitted with his private key (A) by producing a digital signature (1). The latter is subsequently sent with the data (2). If it can be decrypted with the public key (A) by the receiver (B) and if its result I identical to the data received then the signature is valid [50].

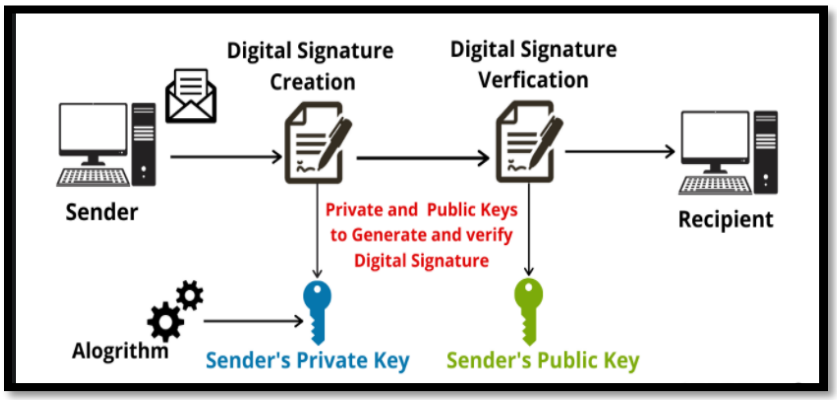


Figure 19: how digital signature works [51]

2.6.2.3 The hash functions

The hash functions are a term that refers to a function that is compresses a string arbitrary input to a string of fixed length. And it is one of the most important tools in cryptography, it is the one that assures authenticity, digital signatures, generation, digital steganography, digital time stamping etc.

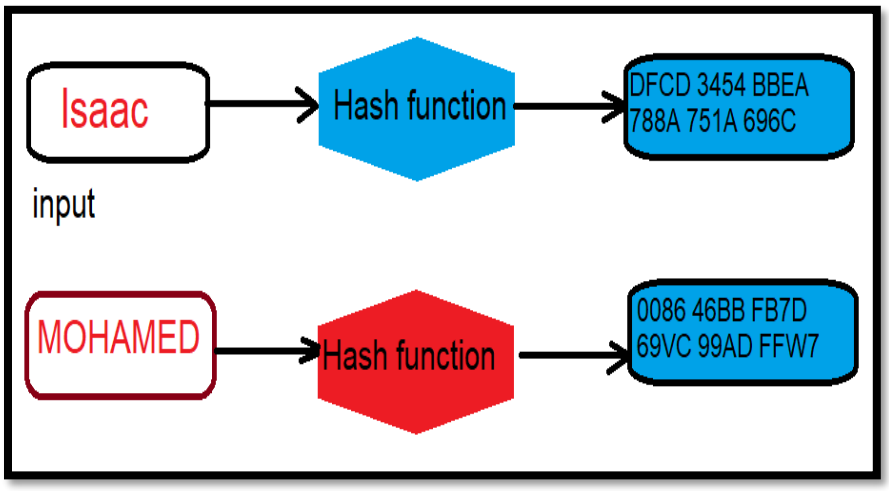


Figure 20: Hash function in cryptography

2.6.2.4 The MAC message authentication code

Also, knowns as a cryptographic checksum or keyed hash function, it's a symmetric-key schema, it appends an authentication tag to a message. The difference in crucial between each MAC and digital signatures is that the first is using a symmetric key k for both operation: authentication tag and verifying it. The function of MAC is as follow:

$$m = MAC_k(x)$$

We also can represent the Principe of MAC in the figure bellow:

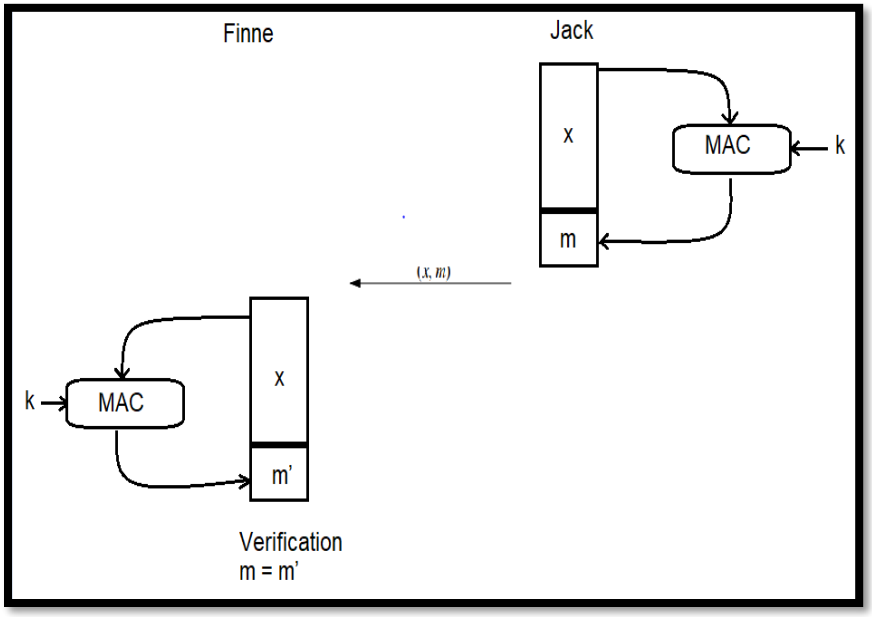


Figure 21: Principle of message authentication codes (MACs)

2.7 Security Protocols in WSN's

CHAPTER 2: SECURITY IN WIRELESS SENSOR NETWORK

Routing is one of the most critical and fundamental tasks in any network, that guarantee the delivery of message from source to destination. It a phase of two-steps that involves the phase of discovering a suitable and stable route between our source and destination, and forwarding the messages using this path we discovered. In traditional networks routing are specific to special nodes such as routers. However, in WSN is consisted of resource-constraint devices operating in ad-hoc that are requiring all our network operation to be done by these ordinary sensor nodes. Some real time applications are requiring that the routing protocols to facilitate timely delivery of messages. More so, such applications are heavy resource usage in WSN and require the routing protocol that can handle and balance energy consumption of all the networks. Furthermore, the number of operation nodes in WSN is far larger than the traditional network. Consequently, there is a need of large production of low-cost sensors nodes. More so, with the increasing of the number of sensor nodes to meet the demand, construction of applications, construction of each node to be tamper resistant would be very expensive. As a result, the nodes could be susceptible to capture attacks. Hence, routing protocol used in traditional network can't be applied in WSN, as a result of that, new arrays of routing protocols have been designed for WSN.[39][40]

Traditional Security protocols can't be applied to WSN network because of the decentralized infrastructure, so a lot of research is going on to produce a security protocols for these resource constrained networks, and most of security protocols take a large number of resources,[41]

2.7.1 SPINS (Security Protocols for Wireless Sensor Networks):

Spins are proposed by Adrian Perrig and al, it is consisting of two main protocols; SNEP and µTESLA. SNEP main focus is on data confidentiality and two-party authentication. While µTESLA provides authenticated broadcast for severely resource constrained networks. [41]

2.7.1.1 SNEP (Sensor Network Encryption Protocol):

It uses Shared counters, in SNEP, a block of plain text is encrypted with CTR encryption algorithm, the counter is not included in the message because the sender and

receiver update the shared counter after they have done their tasks (send or receive), every message has a MAC computed with CBC-MAC algorithm to encrypt the data, each time the MAC is computed for each package. When the receiver gets the message, it comparing it computed MAC with received MAC, if the two MAC are the same the message will be accepted else ways the message will be dropped [41]. The protocol SNEP has many advantages such:

- It uses a shared counter that mean it must not be transmitted with the message.
- It only adds 8 bytes to message so the size still small.
- It offers the following type of security:

i. Semantic security: since the sender and receiver share the counter between each other, and they increment it after each task, the same message may be encrypted in many ways each time.

ii. Data Authentication: the MAC are generated and sent with the message and the message will only be accepted if the MAC from sender matches the receiver, the receiver will assure that the message is authentic.

iii. Replay Protection: the counter value in the MAC stops the attacker from replaying to previous messages.

iv. Weak Freshness: if the authentic message is received and accepted, after that the message can ordered resulting in weak freshness.

v. Low communication Overhead: the counter is shared between both sender/receiver and that make the message short.

2.7.1.2 **µTESLA:** for assuring an Authenticated broadcast of the message an asymmetric encryption mechanism is needed, that have a high computing communication and storage overhead, so they can't access to more resource constrained sensor network, µTESLA protocol pass this problem by a simple thing, it present asymmetry through delayed disclosure of symmetric keys. A node stock the packet in a buffer till the key is disclosed, after that the sink diffuse the validation key to all the receivers, which the node can use to authenticate the packet that stored in the buffer.

Each MAC key is a sequence of keys generated by one way function F, the last key is chosen by the sender and repeatedly applies F to compute the keys $k_i = f(k_{i+1})$.[41]

2.7.2 TINYSEC

Is a link layer security architecture for wireless sensor networks, it provides the same major services as SNEP like authentication, message integrity and confidentiality. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16--32 bytes of overhead. The main deference between SNEP and TINYSEC is that no counters are used in TINYSEC.

There are two types available in TINYSEC and they are: TINYSEC-AE (authentication Encryption) and TINYSEC-Auth (Authentication Only) and the difference between them is the TINYSEC-Auth add mac in the end of its header.[41][42]

2.7.3 MiniSec:

Minisec is protocol that provide us a high security at low power consumption, it has lower energy then TINYSEC and higher security like Zigbee, it uses three techniques to achieve all of those results. The first one is block encryption method, that we used it to provide privacy and authentication with only one pass for the data. Second one is the initialization vector used a very specific few bit. And at the very last is the basic gaps, they're used during transmission in unicast and broadcast communication. In unicast the power consumption is reducing due to the making extra computation using synchronized counters. In the second one broadcast, a mechanism called bloom filtering is use, SkipJack is used as the encryption algorithm and OCB as the encryption mode. It is defenseless against DoS attacks.[43]

2.7.4 Zigbee

Zigbee is wireless standard based on IEEE802.15.4 that was constructed to address the very unique needs of the most wireless sensing control applications. This technology is very low cost, power and data rate highly reliable, highly secure wireless network protocol, it targeted towards automation and the remote-controlled applications. Zigbee is consists of three types of network devices, and they are as following [43][41]:

- **Zigbee coordinator:** this device is responsible starting the network communication, stores the information of the network and bridges the various networks.
- **Zigbee Router:** the Zigbee Router is helping to link the various devices with each other and provides a multi hop communication.
- **Zigbee End Devices:** last and not least the end devices in ZigBee are composed of many sensors, actuators and controllers that work to gather data and communicates with other Zigbee components.[43][41]

2.7.5 LEAP (Localized Encryption and Authentication Protocol)

LEAP protocol was proposed by Sencun zhuet et al, the localized encryption authentication protocol is a key management protocol for WSN designed specifically to support secure communication in the network, and it offers authentication and confidentiality services. In addition, LEAP has the following features:

- It provides four types of keys to each node an individual key shared with the bs, a pairwise key shared with the other sensor node, a cluster key shared with a group of neighbor nods, and lastly a group of keys shared by all nodes in the network.
- LEAP provides use of one-way key chains for a local broadcast authentication.
- Key sharing mechanism easily support in-network processing

all those protocols serve a one thing, is to get our network to be secure and make the communication safe, with also a low energy usage and consumption, in this graph we compare the level of security and the energy consumption between each protocol:

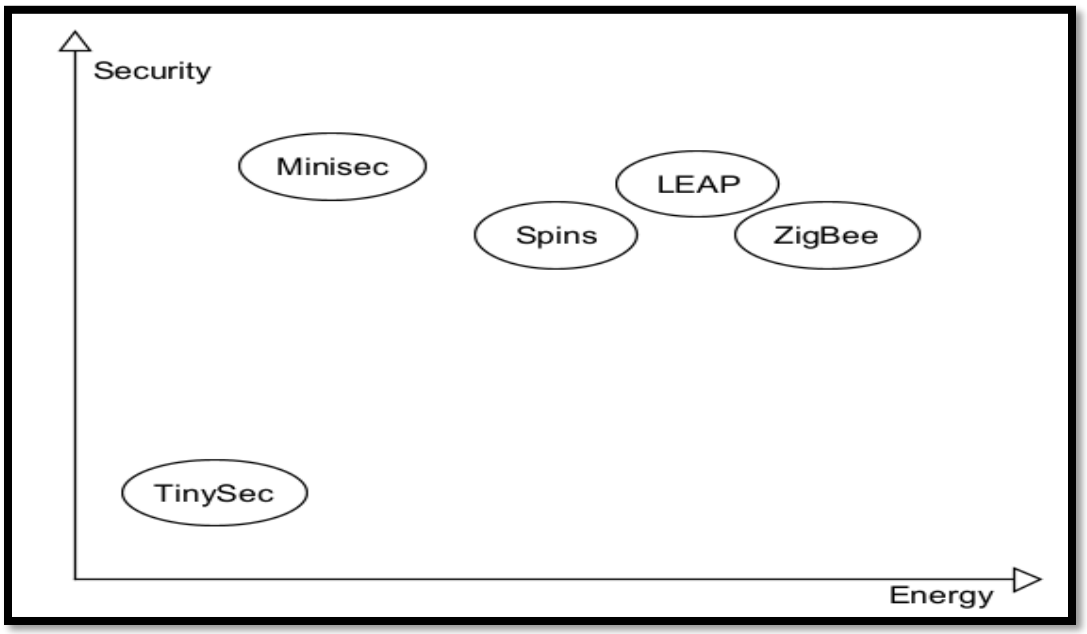


Figure22: shows the comparison of these security protocols in terms of their energy consumption and security provided by them

And in this table, we see table of comparison between each protocol:

	SPINS	TINYSEC	MINISEC	LEAP	ZIGBEE
Encryption	Yes	Yes	Yes	Yes	Yes
Mac Used	Yes	Yes	Yes	Yes	Yes
Freshness	Yes	No	Yes	No	Yes
Overhead (Bytes)	8	4	4+3	Variable	4.6 or 16
Key Agreement	Symmetric delayed	any	any	Pre-deployed	Trust-center

Table 3: shows comparison between WSN security protocols

2.8 Conclusion

In this chapter, we have introduced the basic security measures, and the security mechanisms, and the types of attacks we will face in our network and in WSN, and we see also the security mechanism of WSN and the protocols we use in WSN security, in the end we see what is secure rout and how it works.

Chapiter 3: conception of a new secure routing protocol

CHAPTER 3: PROPOSED SECURITY PROTOCOL

2

3.1 Introduction

As we saw in the previous chapter security descriptions in WSN, the classification of security and also security protocols in WSN, and also comparison between security protocols and show the benefits and the down side of each one.

We also see that WSN can be deployed anywhere because of that we must take control of the nodes that can access the information, the objective of this chapter is to provide the WSN with a secure routing protocol based on modified SPIN protocol called GR-SPIN, the main objective is to secure the nodes during the deployment faze using RSA encryption, and also during transferring data between the source node and the base station using AES encryption method, with that we can help our network to stay secured from intervention and threats that we face in common WSN attacks.

3.2 Global description of Secure GR-SPIN

- **Step 0: generating RSA keys**

This step simply will generate the private and public key for RSA encryption method

- **Step 1: initialization and encryption with RSA**

In this step we simply divided the network by four equal regions, after deployment finish immediately we will apply the RSA encryption method to the whole network (sink and nodes).

- **Step 2: Data advertising and decryption with RSA**

In order to a source node to advertise its data that he sensed in its sensing zone it must first decrypt the RSA value if it's the same, then it will discover the path that leads to the sink and send and adv message to it.

- **Step 3: Data requesting and decryption with RSA**

Now in the sink, after receiving a list of adv messages, the sink will first decrypt the RSA value first to be able to complete requesting, after the value is correct and decryption is complete the sink will decide who to send the request message to for asking data.

- **Step 4: Data transmitting and encryption with AES**

This phase any source node that receives a request from the sink will firstly encrypt the data with AES encryption and it will send it to the sink.

- **Step 5: Data saving and decryption**

After the sink receives the data, it will decrypt it and save it and show us the results.

Each of these steps are repeated for each region and each task.

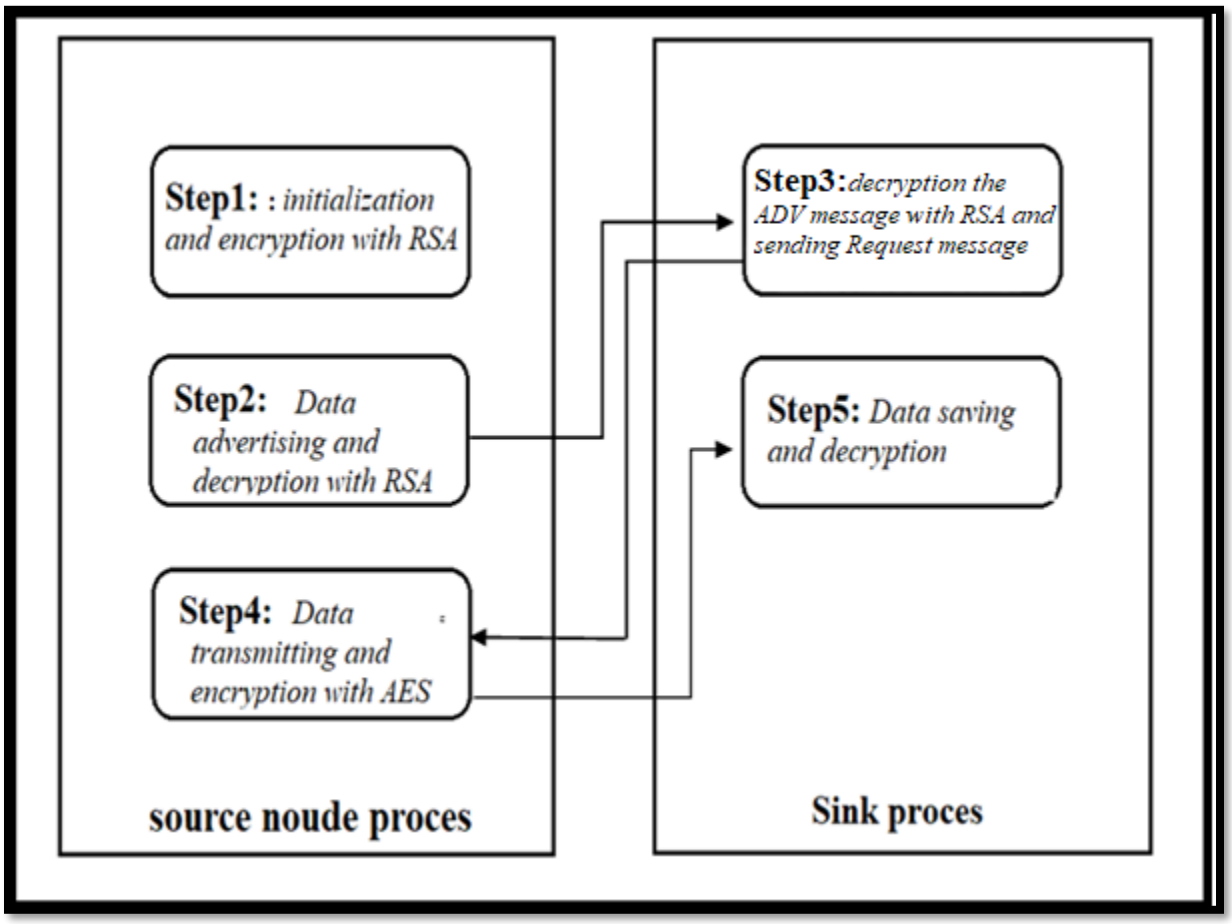


Figure 23: General process for secured GR-Spin

3.3 Detail's description of Secure GR-SPIN

In this part we will discuss in details our solution to improve security in wireless sensor network:

3.3.1 Step 0: generating RSA keys:

This step is so simple it consists of a simple method that will generate the public key and the private key for RSA encryption method.

To generate those to key we need to follow these 5 steps:

- Select two large prime numbers p and q. The prime numbers need to be large so that they will be difficult for someone to figure it out.
- The second step is to calculate n, and **n = p × q**.
- The third step is to calculate the totient function: **ϕ(n)=(x−1) (y−1).**

- Now we select an integer e, such e is co-prime to **ϕ(n)** and 1< e < ϕ(n). the pair of numbers (n, e) makes up the public key.
- In the last step we calculate d such that e.d = 1 mod ϕ(n). d can be found using the extended Euclidean algorithm. The pair (n, d) makes up the private key.

All these steps can be shown in the figure below:

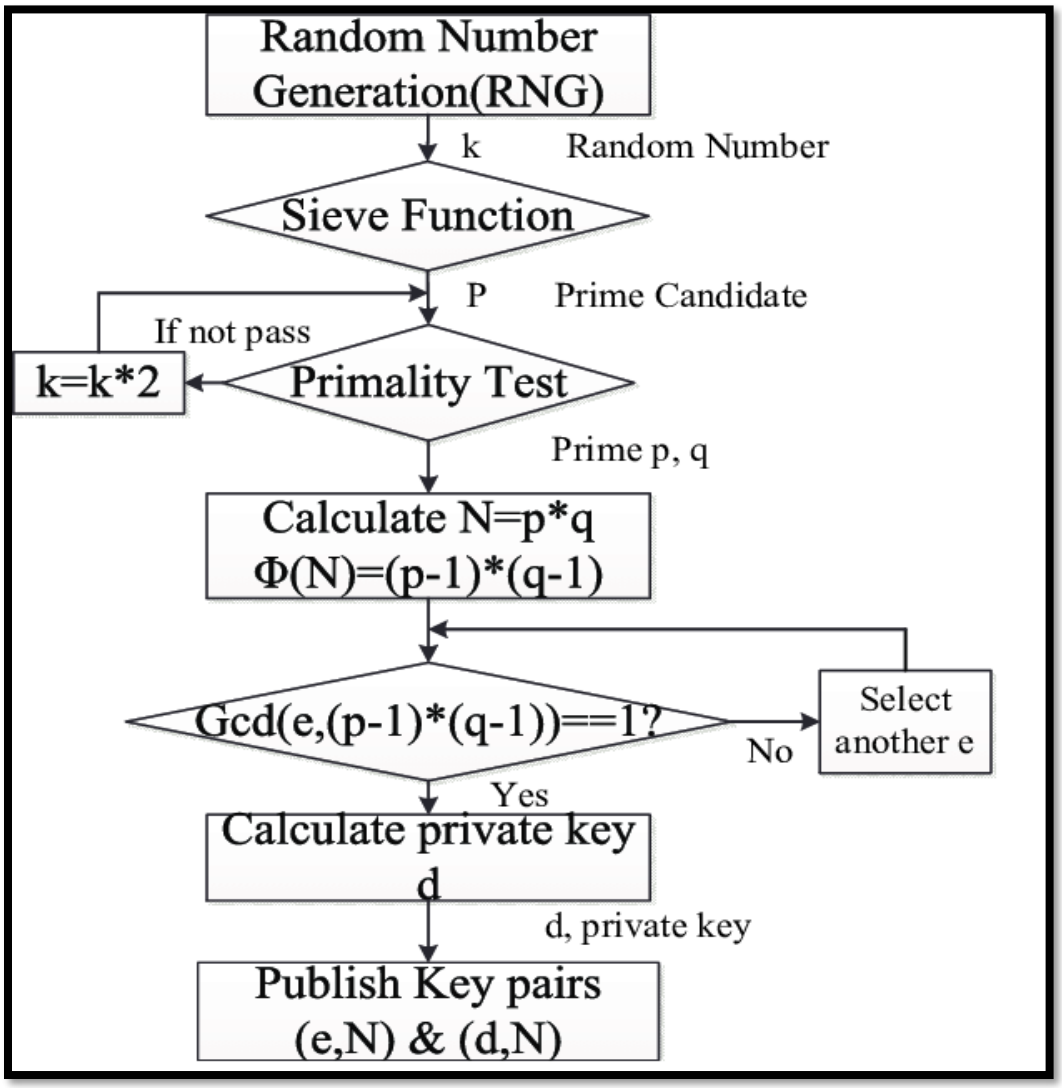


Figure 24: RSA key pair generation

3.3.2 Step 1: initialization and encryption with RSA

This step we will deploy the nodes randomly in 4 regions, and each node with the base station will be deploying RSA public key to all nodes.

3.3.3 Step2: Data advertising and encryption ADV with RSA

This step is consisting of the source nodes sensing the data and then finding a path to send and adv message to the sink, these steps are shown in the figure below:

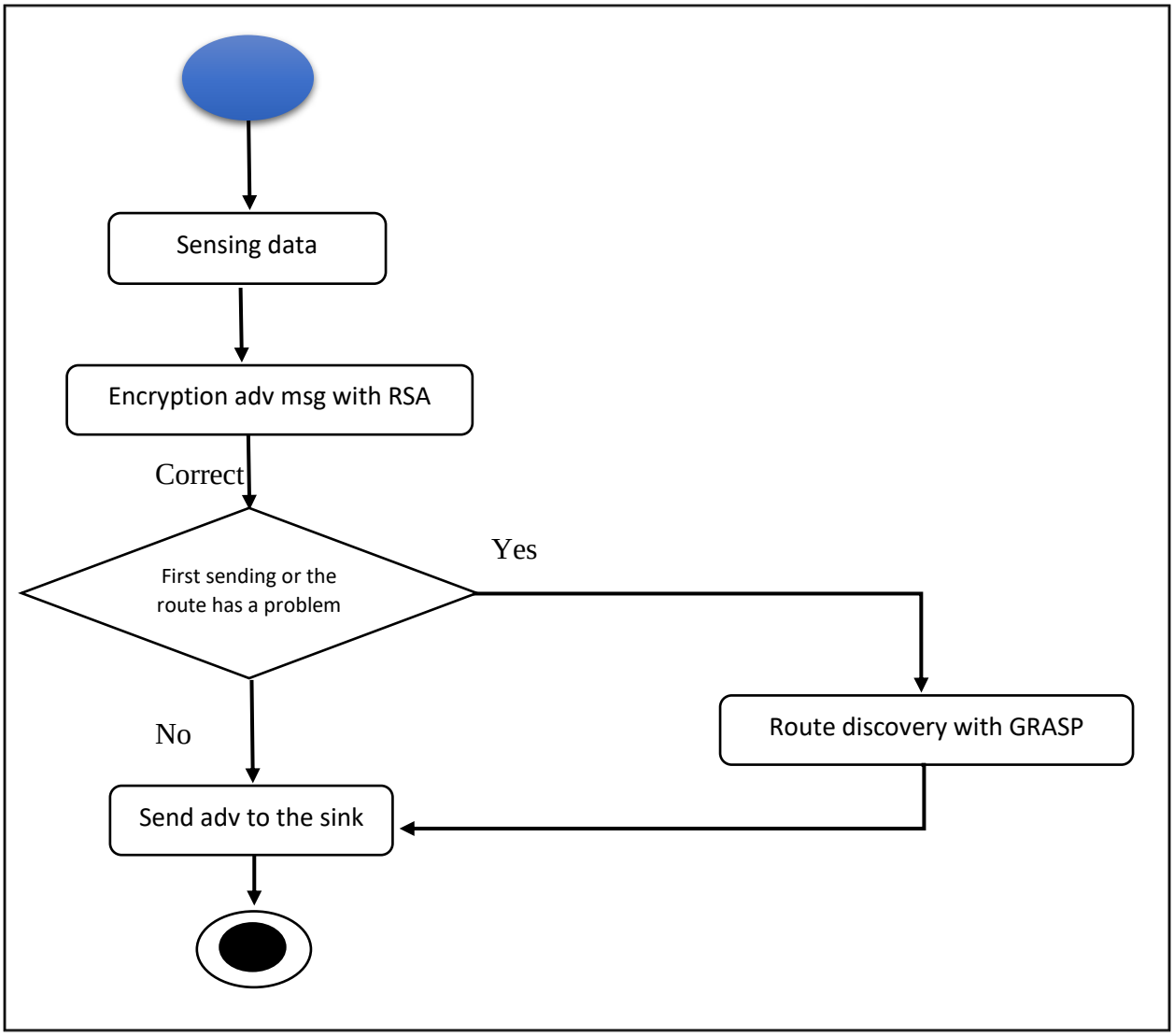


Figure 25: general process of data advertising and decryption with RSA

1. **Sensing data:** for the purpose of sensing data, we have proposed three types of data, temperature data and its value are from -50 to 100 °C, the second one is the light value and it's from 320nm to 730nm. And lastly is humidity from 0 to 100%. Each time the source node chose one data value randomly.

2. **Encrypt adv msg with RSA:** in order to accomplish sending the advertising phase, we need to encrypt the adv message with RSA value to complete sending, to do so the, The RSA encryption simply works by encrypting a value or a plain text, given a plaintext P, represented as a number, the ciphertext C is calculated as: $C = P^e mod\ n$.

3. **Route discovery:** this step is consisting of finding the best optimizing route, by using the GRASP (Greedy Randomized Adaptive Search Procedure), we using it to found in each iteration through a randomized greedy procedure and it consisting of two phases: the phase of construction of a solution which tries to build a circuit according to the semi-greedy algorithm, and the phase of the local search where attempts to improve the rout built in the first strategy by a local search. The final rout will be best solution obtain.

4. **Send adv message:** in the end, the last step a source node knows the path to the sink and it will be verified by the sink that it is secured and it is a part of our local network and not an adversary, it will send and adv message to the sink.

3.3.4 Step 3: Data requesting and decryption adv message with RSA:

To complete this step-in sink, we show that in the figure blow:

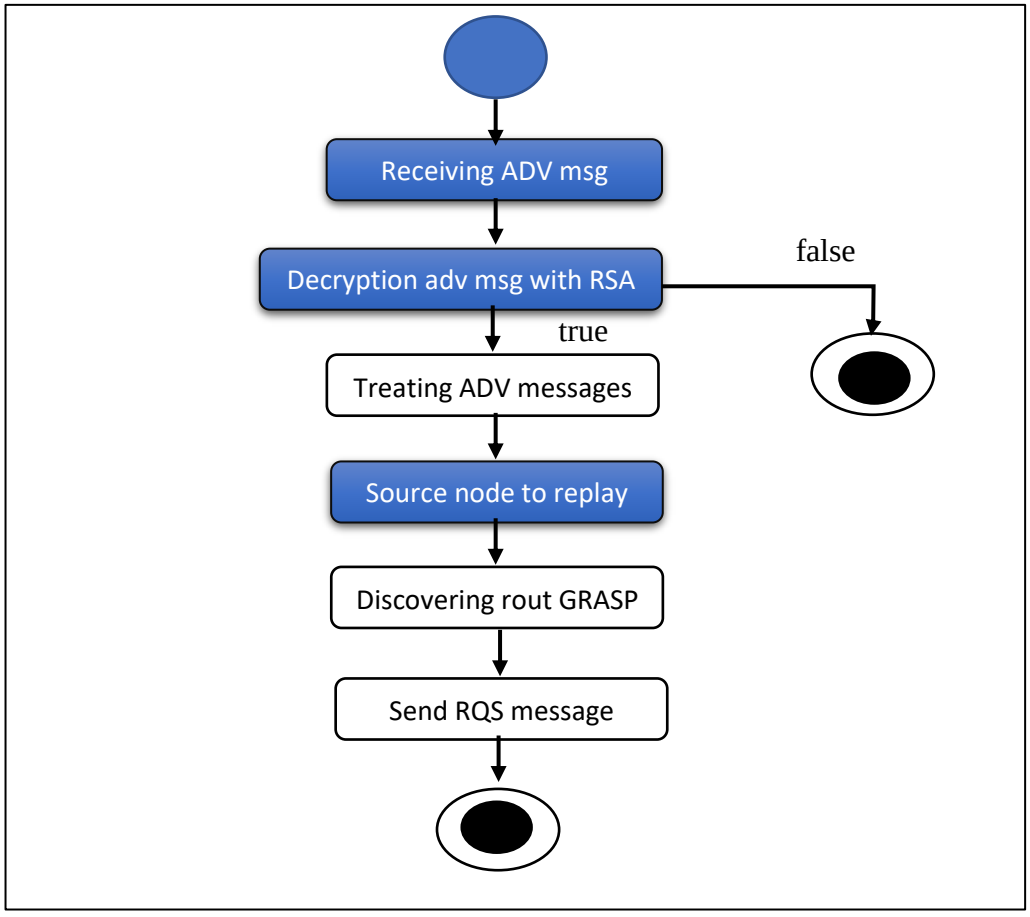


Figure 26: general process of data requesting stage

- **Request message treating:**

5. At the end of receiving all the adv messages from source nodes, the sink now will start decryption of those Adv messages using the private key (n, d), the plaintext can be found using: $P = C^d mod\ n$,those messages contain the source node name and the data he collected and its energy rate. All of those messages need to be treated by the sink, to decide which one it will send the request to.

The sink will class the name and data for the source nodes according to the region and the name of the data, for that we have three possibilities:

- **First possibility:** this possibility no source nodes send any type of data, for that the sink does not send any request.

- **Second possibility:** here just one source node sends one type of data, the sink will check if it needs this data or don't, if he needs that data, it will send request message the source node that send the adv.
- **Third possibility**: for that more then a node sends adv with one type of data, here the sink checks if he needs that data, and checks the energy consumption, and it will choose the highest energy rate and will send request to it**.**

After the possibilities and determining which node to replay

3.3.5 Step 4: Data transmitting and encryption with AES

This process is consisting of the source sound encrypt the data that he senses then after that he send it to sink after receiving a request, as we explain in the following figure:

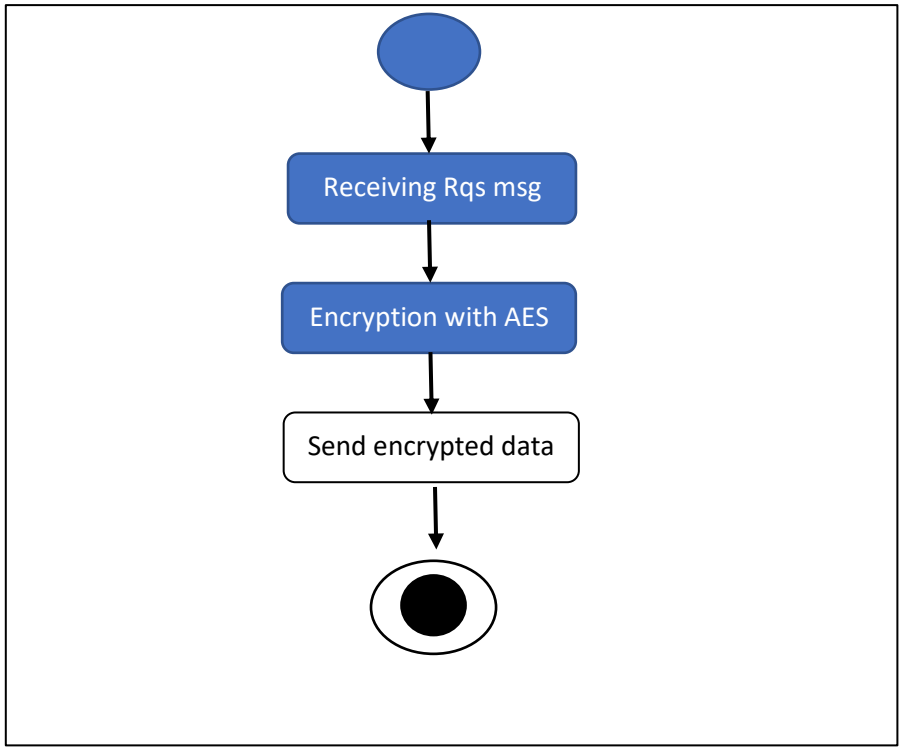


Figure 27: general process of sending and encryption data with AES

Data sending: after we received the request to the sink, any source nodes that receives the request message is able to use the same path without the rote discovery. It will encrypt the data first with AES encryption.

2

AES encryption: or The Advanced Encryption Standard (AES) is a symmetric block cipher, it's implemented in software and hardware to encrypt sensitive data. AES includes three block ciphers: AES-128, AES-192 and AES-256. The steps of this encryption:

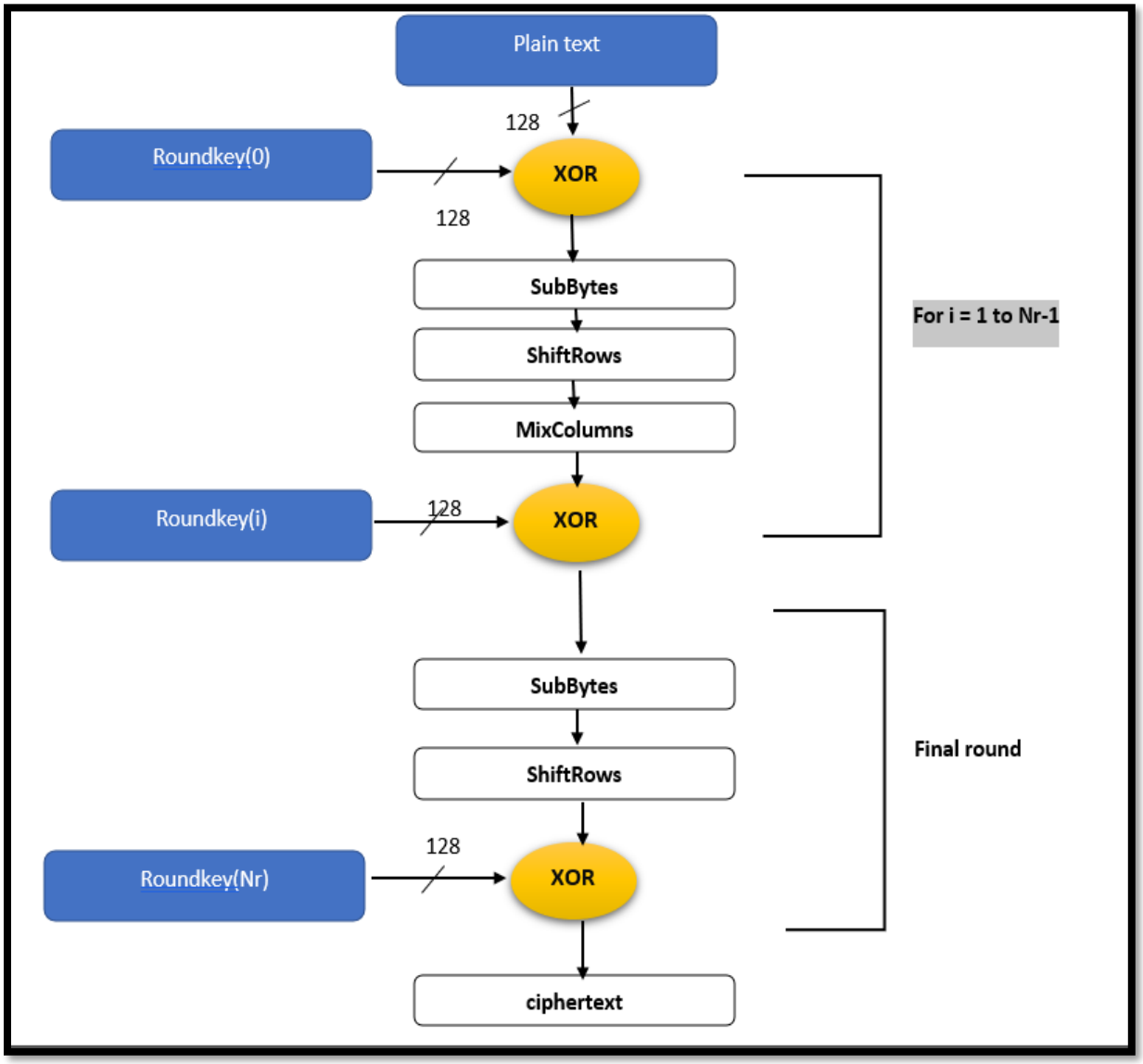


Figure28: AES encryption steps

3.3.6 Step 5: Data saving and decryption: after the sink received the encrypted data by the source nodes and accomplish all steps above, it needs to decrypt that data with AES decryption and show that data above, the following figure show us the decryption phase:

2

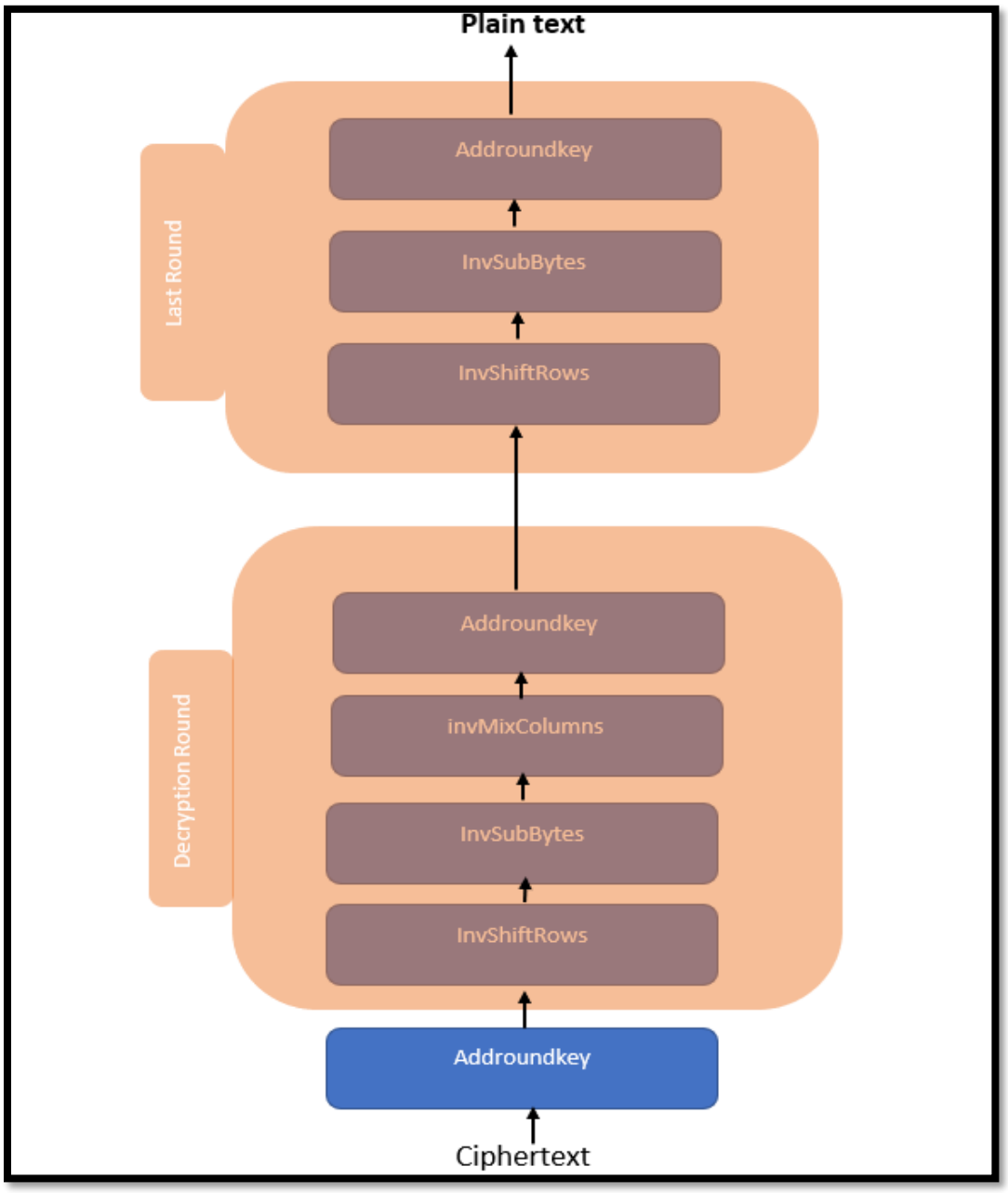


Figure 29: AES decryption

The following figure is showing the general architecture of our application and:

2

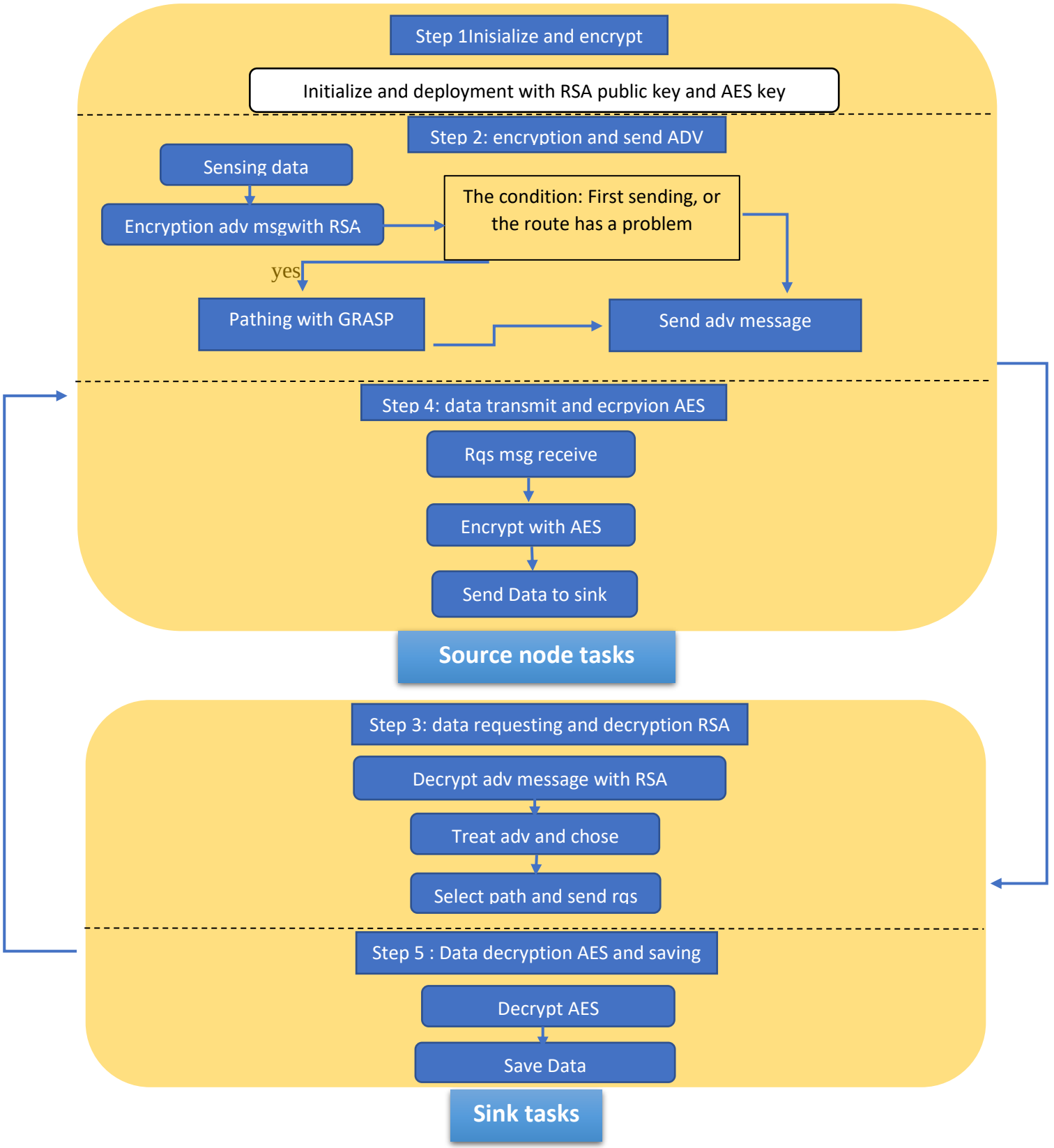


Figure 30: global architecture of our solution

3.4 General operation:

The general operation of our solution will be shown in the figure below:

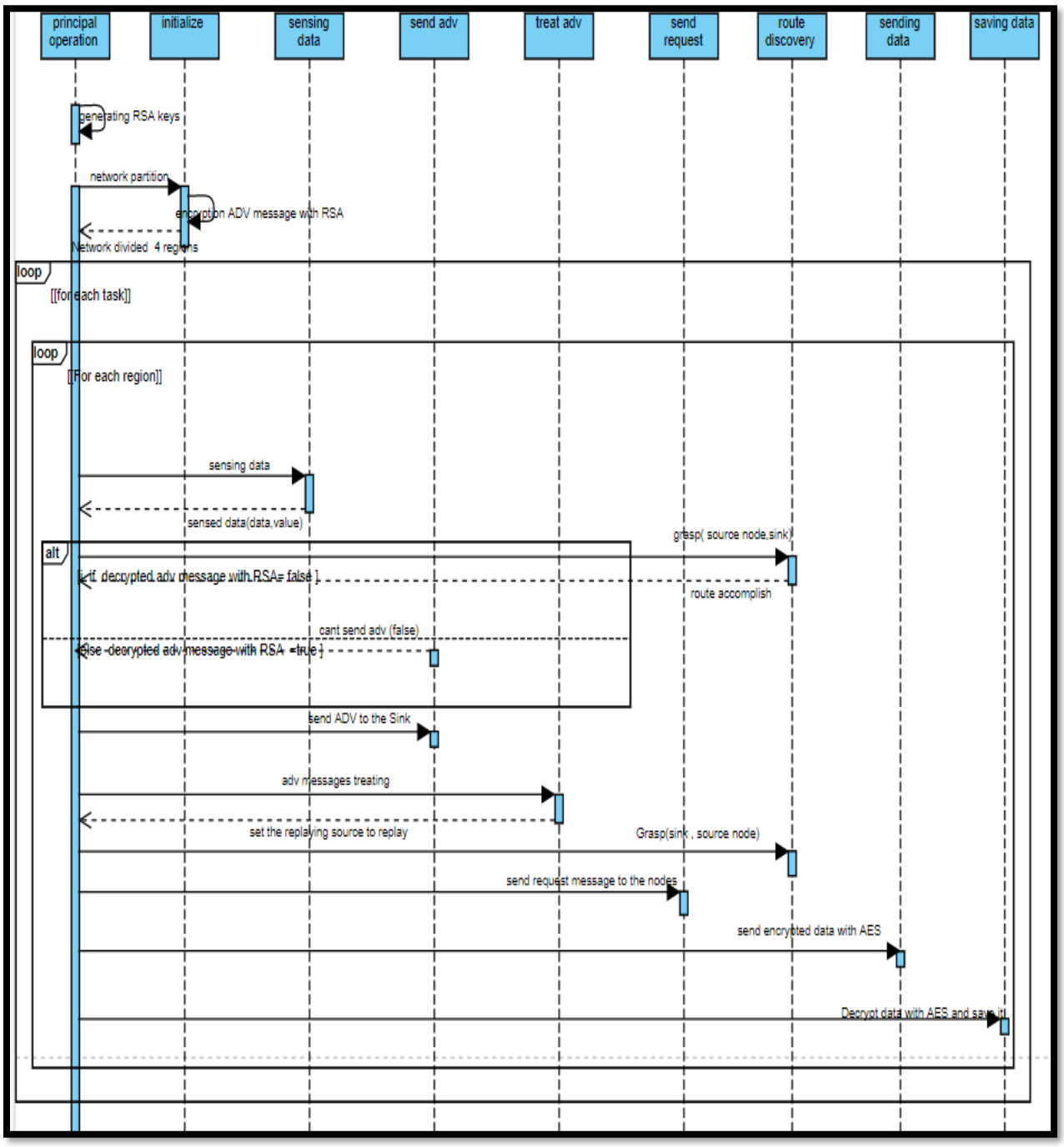


Figure 31: sequence diagram for the solution proposed

- The sink starts the network partitioning into 4 equal regions and encryption phase, by generating the public key and the private key for RSA encryption and deploy the public key with all nodes and also the AES key for encryption and decryption.
- The source nodes sensed the data with its value.
- The source node encrypts its adv message with RSA public key and send to the sink.
- After receiving the adv message the sink decrypted it to check if the node is from our network, if so, it will treat it with other adv messages.
- The sink sends a request to the selected source node asking him to send data to the sink.
- Any source node receives the request will encrypt the data with AES and send it
- The sink receives data and decrypted with AES and save it.

3.5 Conclusion

In this humble chapter we proposed our solution that is based on cryptography and GRASP and we called it secured GR-SPIN, and we talk about its working mechanism and explain them, by talking first about the global details, and detail description and ending with the architecture.

Our solution help keeps network secure from any threats with introducing two level of encryption. Based on modifying SPIN protocol, we see the ways to encrypt and generate keys with RSA encryption and AES encryption also the way to encrypt with it, we also see the benefits of encryption and why it makes hard for imposters to collected and hack our data.

In the next chapter we will talk mainly about the implementation of our security solution or secure GR-SPIN

Chapter 4: implementation

CHAPTER 4: IMPELEMNTATION AND RESULTS

4.1 Introduction:

As we saw in the previous chapter, we spoke about the conception and modeling of a secure modified SPIN routing protocol, with using of GR-GRASP protocol and using encryption for securing the network, and we explain the advantage of symmetric encryption and asymmetric encryption and the benefits of each one, and how they play a huge role.

At the end, in this chapter we present the simulation of our network and obtains results, also we will present the implementation of our system.

We deployed the sensor randomly in the sensing zone and with the deployment we applied the RSA encryption to all sensors, and after sensing we encrypt the information using AES encryption, to find the rout we used Grasp algorithm (Greedy randomized adaptive search procedure), and we will see the result of our security solution.

4.2 Development environment:

4.2.1 Software:

MATLAB: for coding and programing our language we used the MATLAB; MATLAB combines a desktop environment tuned for iterative analysis and design processes with a programming language that expresses matrix and array mathematics directly. It includes the Live Editor for creating scripts that combine code, output, and formatted text in an executable notebook.

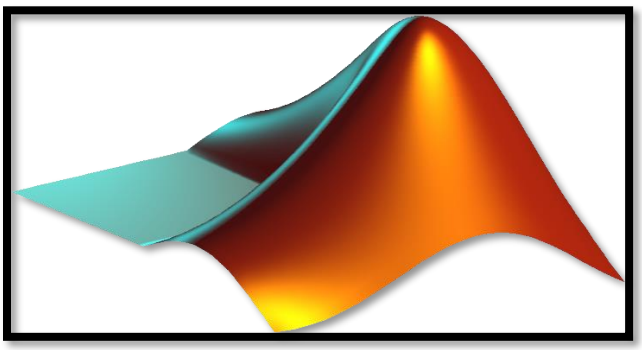


Figure 32: MATLAB icon

Visual studio code: is a code editor redefined and optimized for building and debugging modern web and cloud applications.

Windows 10: s a Microsoft operating system for personal computers, tablets, embedded devices and internet of things devices.

Garuda KDE Dr460nized: garuda Linux is a distro based on archlinux that allows better functionality and easy access to many developments' tools

4.2.2 Hardware: for our hardware we're using a dell laptop with those specs

Dell latitude 3580

Figure 33: Dell latitude 3580

Processor: Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz 2.70 GHz

Ram : 8 Gega DDR4
Storage: 500 gega intel sata SSD.

4.3 Network model

For starter we applied the network with the dimension 150 × 150 and divided by 4 equal regions with a base station (sink) in the middle, the deployment happened randomly in each of the regions, also the nodes who captured the data are 20% from the total number of the nodes and we distributed it by 5% for each regions, for testing and verify the quality of our security solution we have to determined three cases, a small one with just 100 nodes, a medium scale with 200 nodes and finally with 300 nodes, as shown in the figure below:

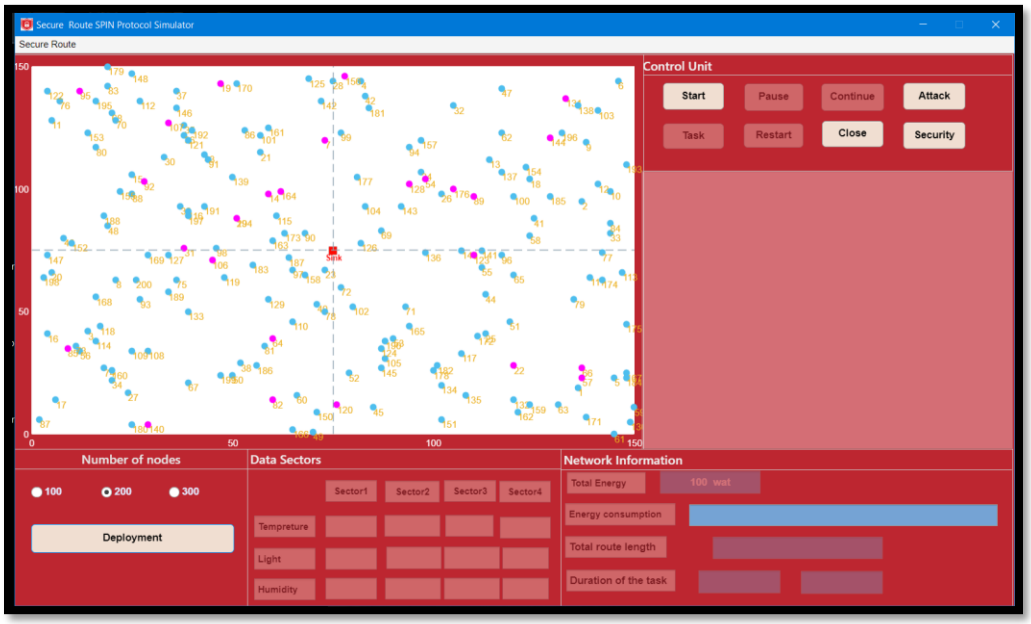


Figure 34: deployment with 200 nodes

4.4 Sensor model

In our network we used the node model we used the IEEE 802.15.4 (Zigbee standard), and the sensor is called TelosB, and the figure below show us the block diagram of this sensor:

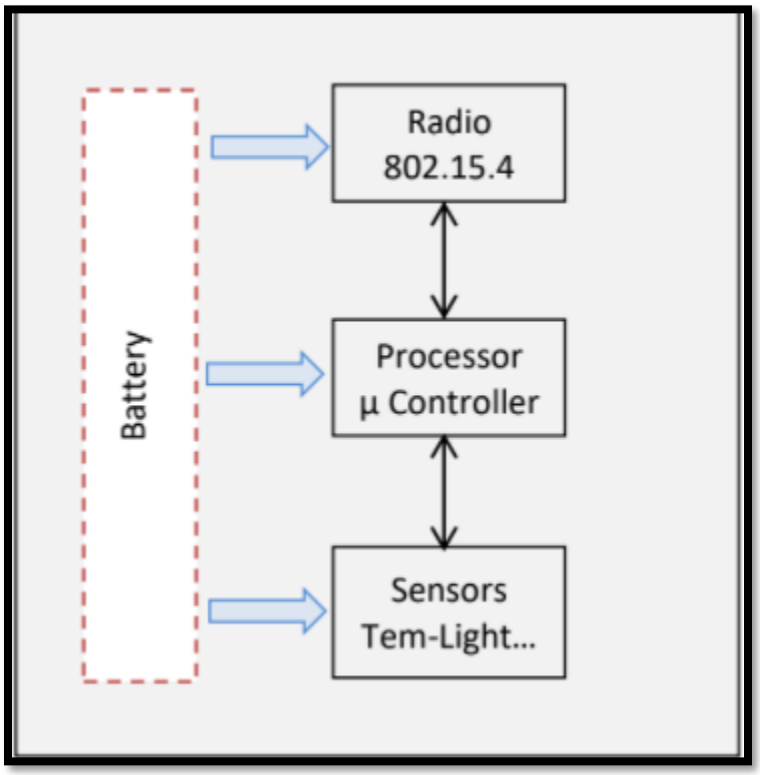


Figure 35: block diagram of TelosB

The sensor is constituting of the component's basic sensor, like a radio devices and processing unit, in this table below we shown some of the parameters of the TelosB sensor:

TelosB settings	
Processor architecture and performance	16-bit RISC architecture
RAM	10l bytes
Frequency band	2400 MHz to 2483.5 MHz
Indoor Range	20m to 30m
Outdoor Range	75m to 100m
Battery	2X AA batteries
Sensors	Temperature-Light-IR-Humidity …etc.
Ui	USB

Table 4: TelosB settings

4.5 Simulation:

The simulation that we applied consists of the following settings as shown in the tables below:

Network settings	
Size	150×150 m
Deployment type	Random
Radio Range	20 m
Packet size	120 bits

Table 5: Network simulation settings

Nodes number			
Cases	Total	Source nodes	Sensor nodes
1	100	20(20%)	80
2	200	40(20%)	160
3	300	60(20%)	240

Table 6: nodes type

4.6 Project structure

The secure rout simulation that we applied, it consists of several structure and levels as shown as below:

4.6.1 Functions

In order to apply our secure routing protocols, we must apply several functions in our project and they are shown in the figure bellow:

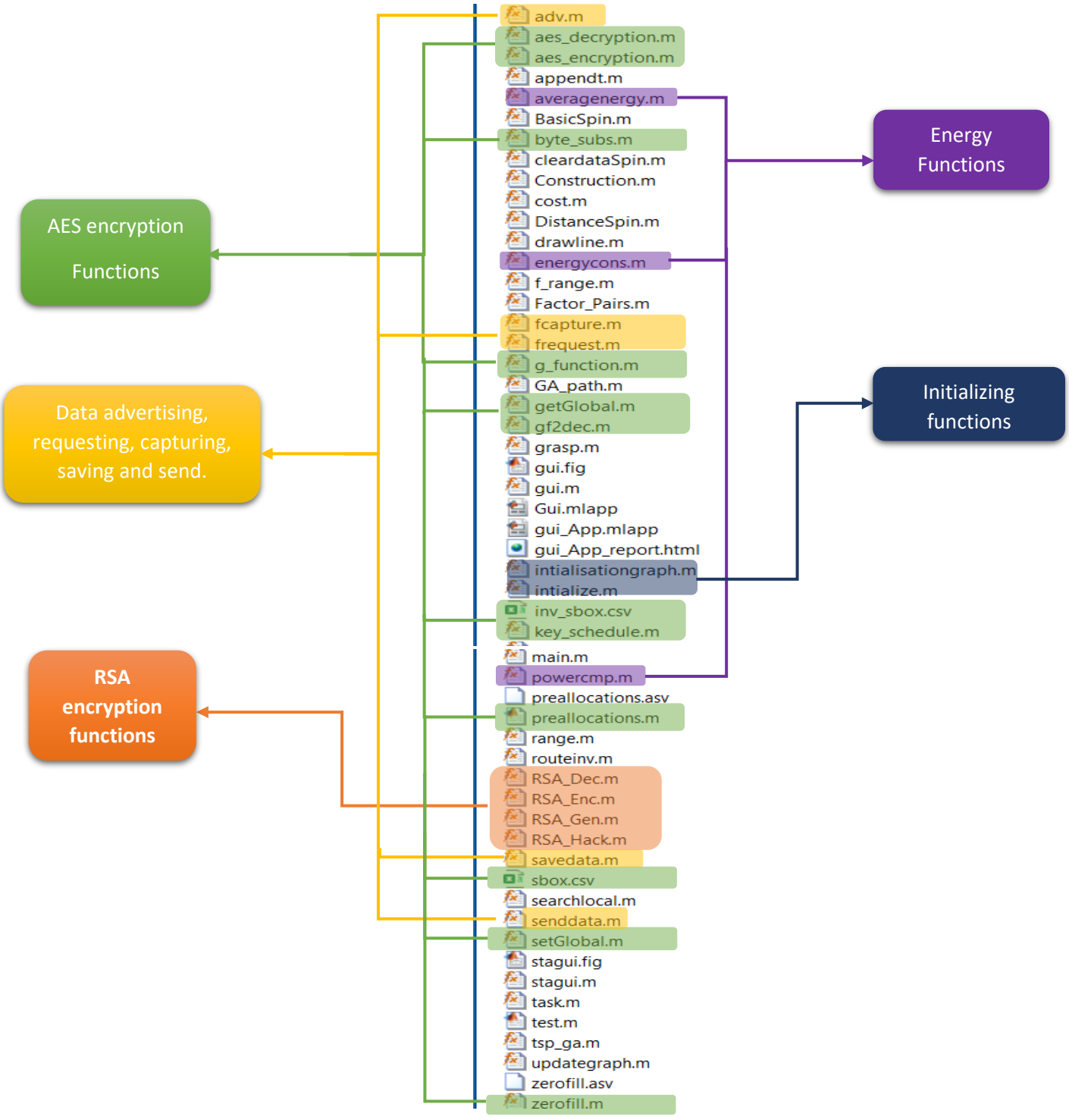


Figure 36: project application structure

4.6.2 Buttons:

The user interface consists of several buttons each one has a purpose that serve an objective, as we shown below each button and the function that he applied and uses:

b- Security button: by pressing this button it will automatically call the RSA_Gen.m and this function will generate a public key and private key for our RSA encryption

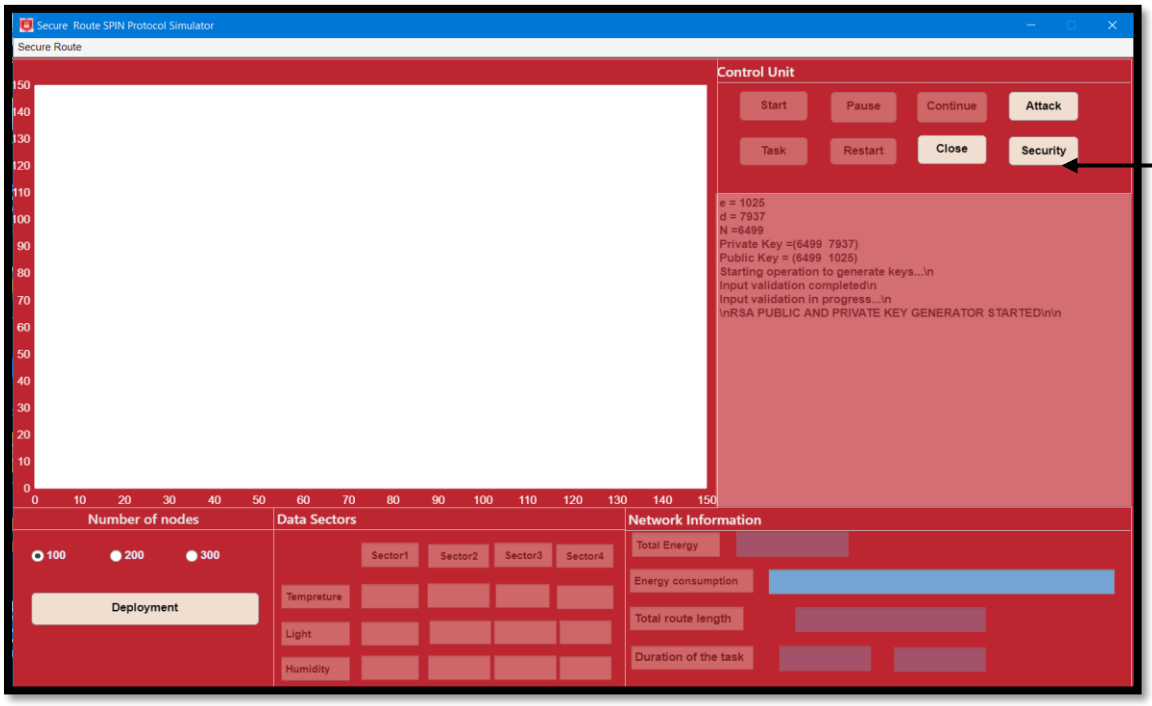


Figure 37: security button function

And this is the RSA_Gen.m function:

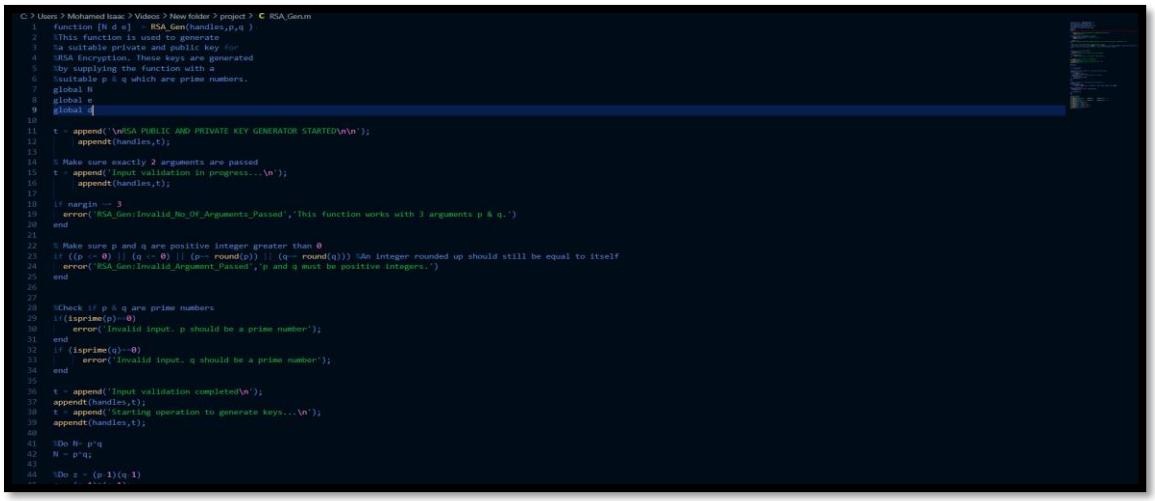


Figure 38: RSA_Gen.m

c- **Deployment button:** the deployment function simply checks each value in the radio button than save it in Nn, after that it will call the function intialize.m, this function will create the sink and the source node and divide the field into 4 regions, for each region there is nodes deployed randomly, this function will call also another function intialisationgraph.m, to determine the Neighbors and their distance for every node, and lastly putting start button in enable mode, and deploy each node with an public key function so no imposter can access the information or data transmitting in our network:

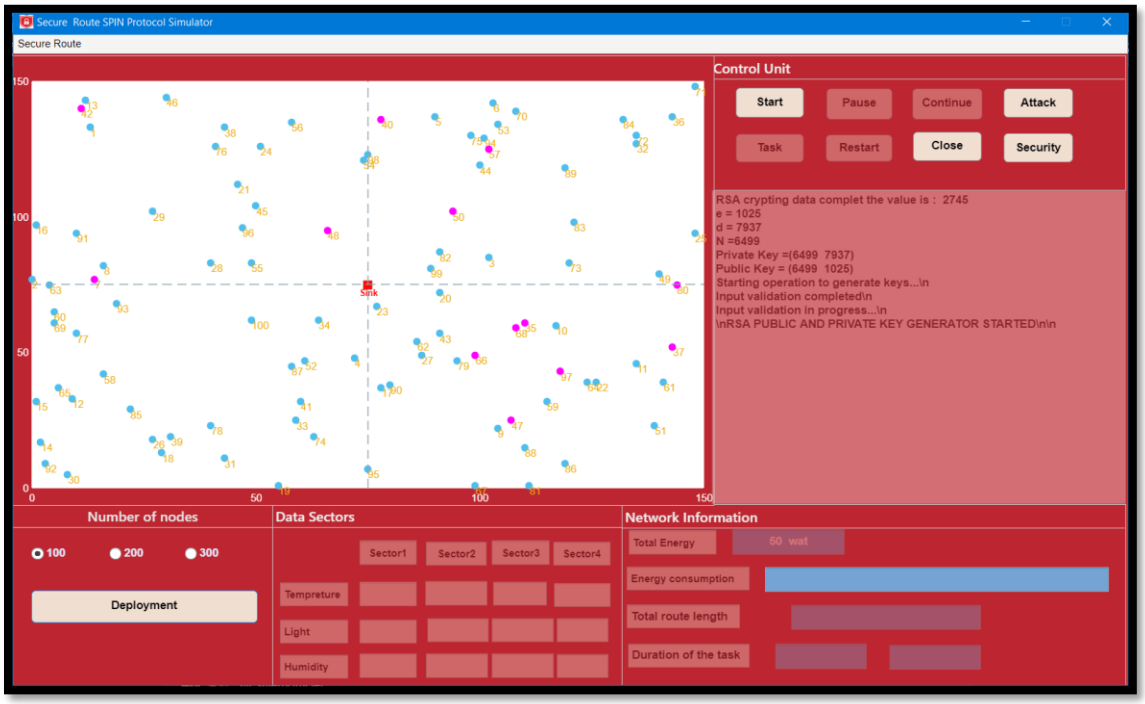


Figure 39: Deployment button

and here it is inisialze.m function:

Figure 40: inisialize.m function source code

The source code for intialisationgraph.m:

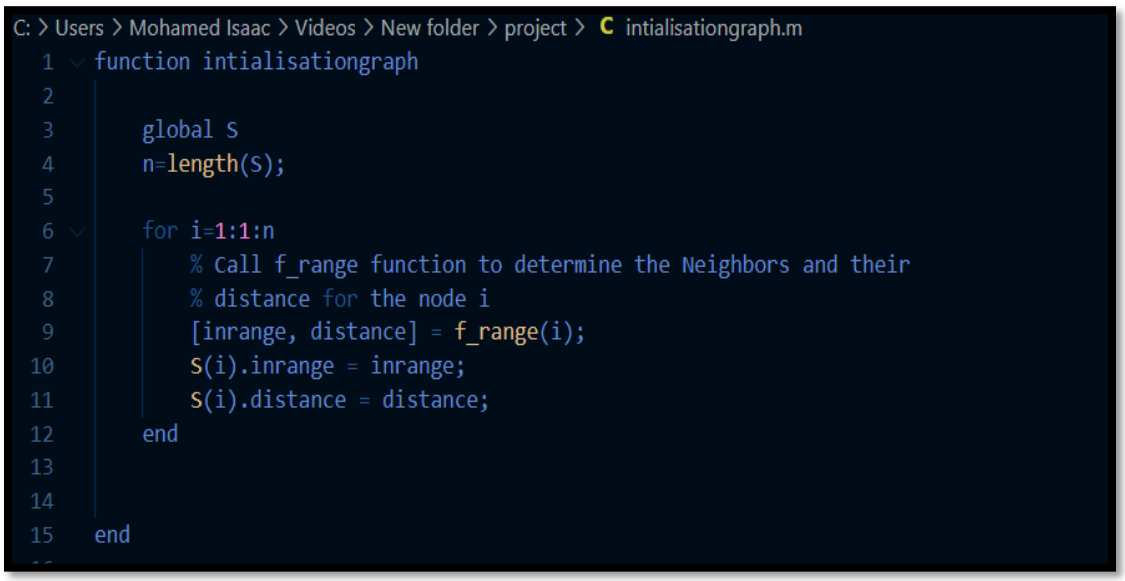


Figure 41: intialisationgraph.m source code

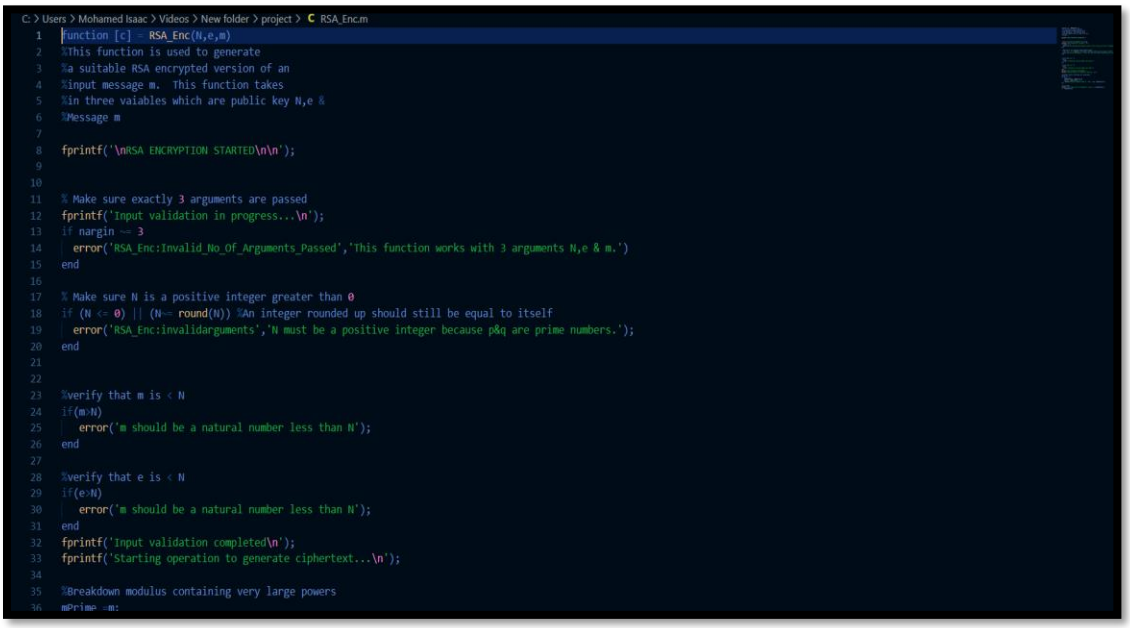


Figure 42: RSA_Enc function

d- **Start button:** by pushing this button we unleashed the full power of our application, first of all the source nodes captured data by the function fcapture.m, this function will randomly capture data for the source node, after capturing the data we will encrypt it by the AES encryption methode by using the aes_decryption.m we also check if the capture data is correct with zerosfill.m and also check the key with same function, after that the source nodes will send and encrypt the advertment to the sink that it collected some data by the function adv.m and RSA_enc.m, if the sink want the data from some node it will simply, the sink will check if the node is not an imposter by decrypting the adv by RSA encrypted message if it's the same as the value that we have (4000) it will accept the adv from the node, then send an request to the source node that he want that data, after all of that the node sends data to the sink by using the function senddata.m and the sink will save this data by the function savedata.m

in the figures bellow we will show a simple run of our application and the use of the function we talk about:

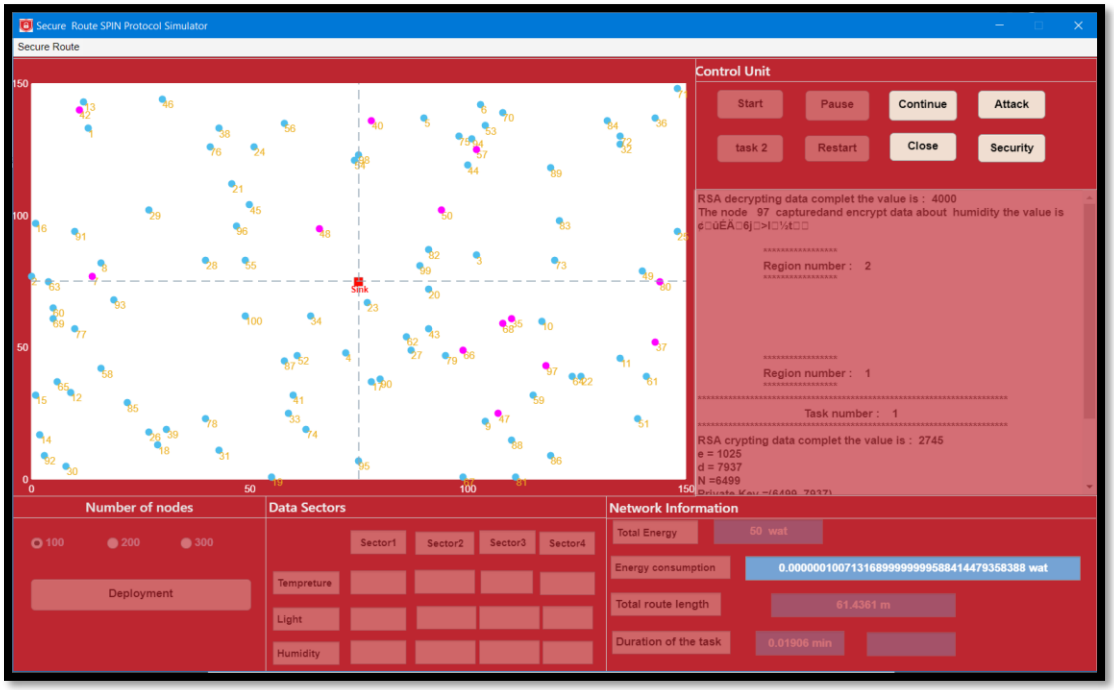


Figure 43: capturing data

And this is the capturing function;

```
C: > Users > Mohamed Isaac > Videos > New folder > project > C fcapture.m
function  fcapture(handles,source,plaintext )
global S
global datakeys
global plaintext
global ciphertext

% Global Variable Declarations
preallocations;

    index = randi([1, length(datakeys)]);
    data = string(datakeys(index));


        if isequal(data,  'tempreture')
          S(source).data = 'tempreture';
          % S(source).datavalue = randi([ 40,123]);
          a=10;
          alpha(a)= randi([ 50,100]);
          plaintext = num2str(alpha(a));
          % plaintext = input('Type in an input message (16 characters or less):\n','s');
           plaintext = zerofill(plaintext);
           key = 'isaac';
          % key = input('Type in a secret key/password (16 characters or less):\n','s');
           key = zerofill(key);

        % Key Schedule
        round_keys = key_schedule(double(key));
        % Message Encryption
         ciphertext = aes_encryption(source,plaintext,round_keys);
         S(source).datavalue=char(ciphertext);

            t = append('The node','   ',num2str(source),'  captured and encrypt data about  tempreture the value is   ','   ',S(source).datavalue );
           appendt(handles, t);
        end
```

Figure 44: fcapture.m function

And after we captured the data, we encrypted it with aes_encryption.m function

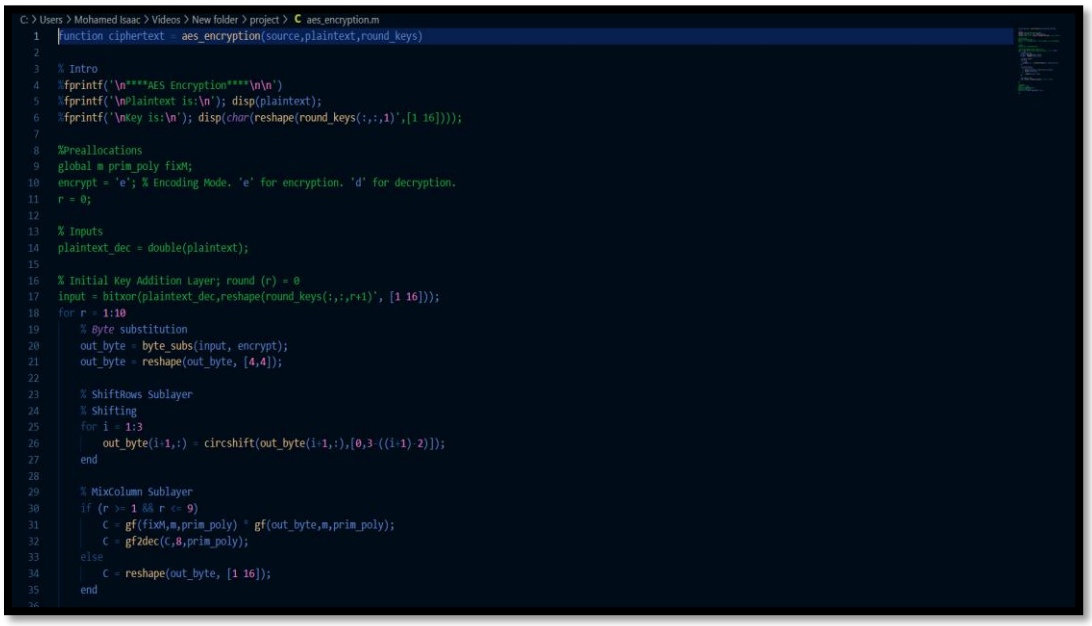


Figure 45: AES encryption function

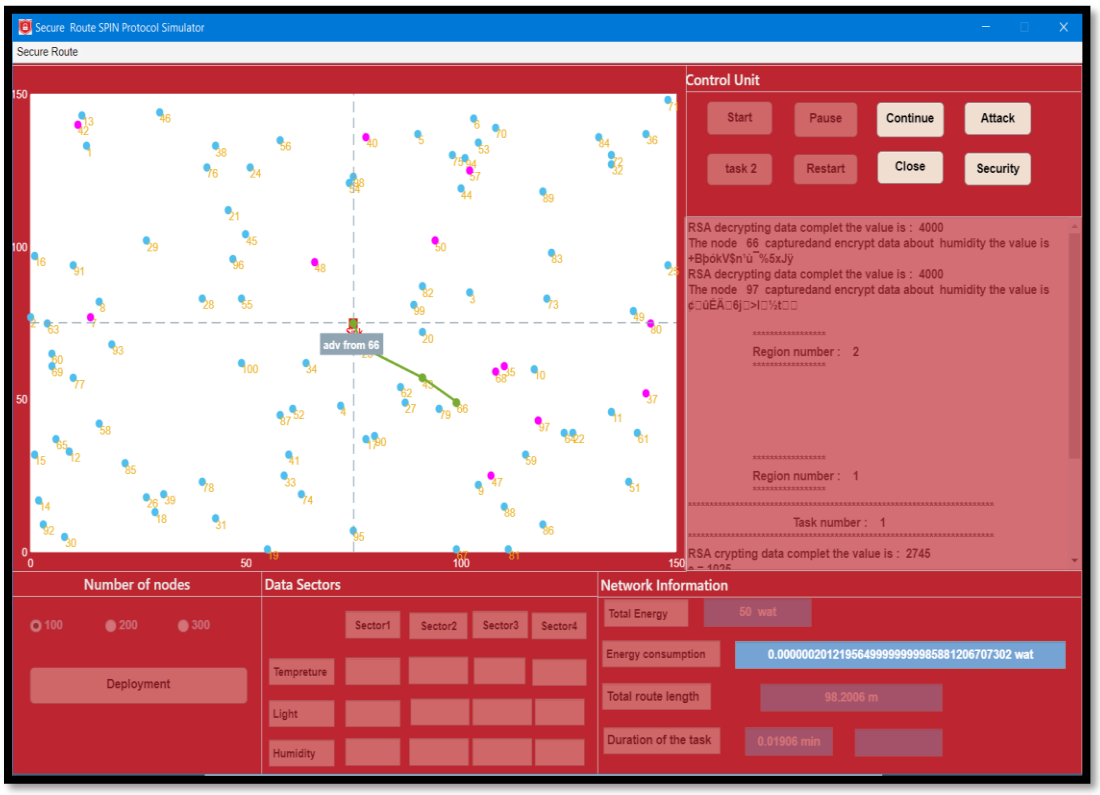
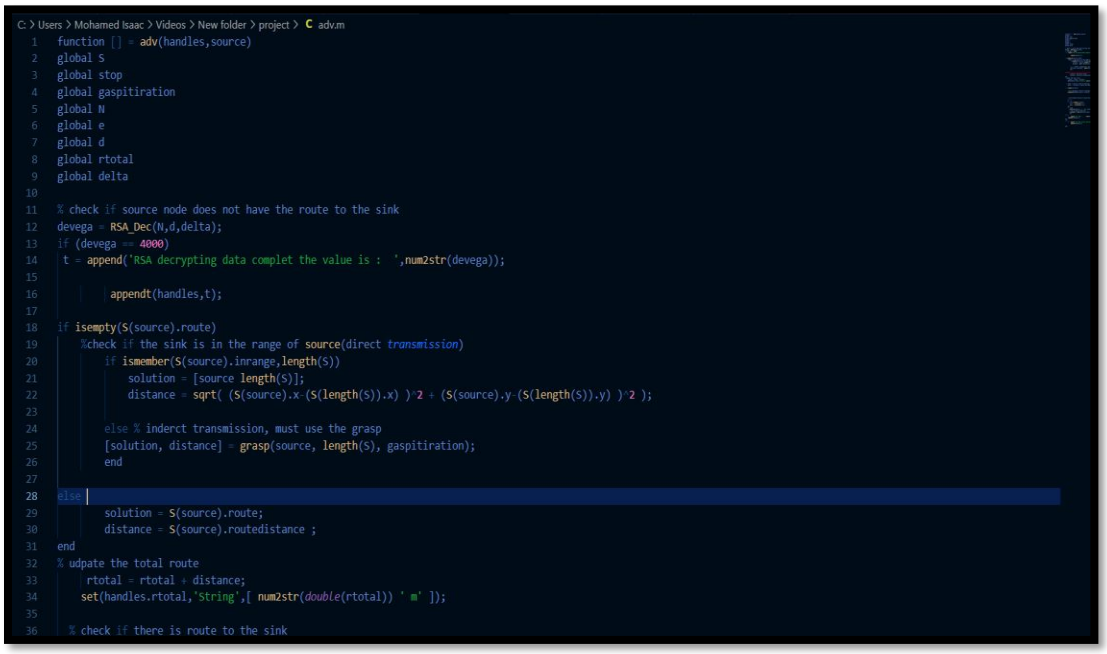


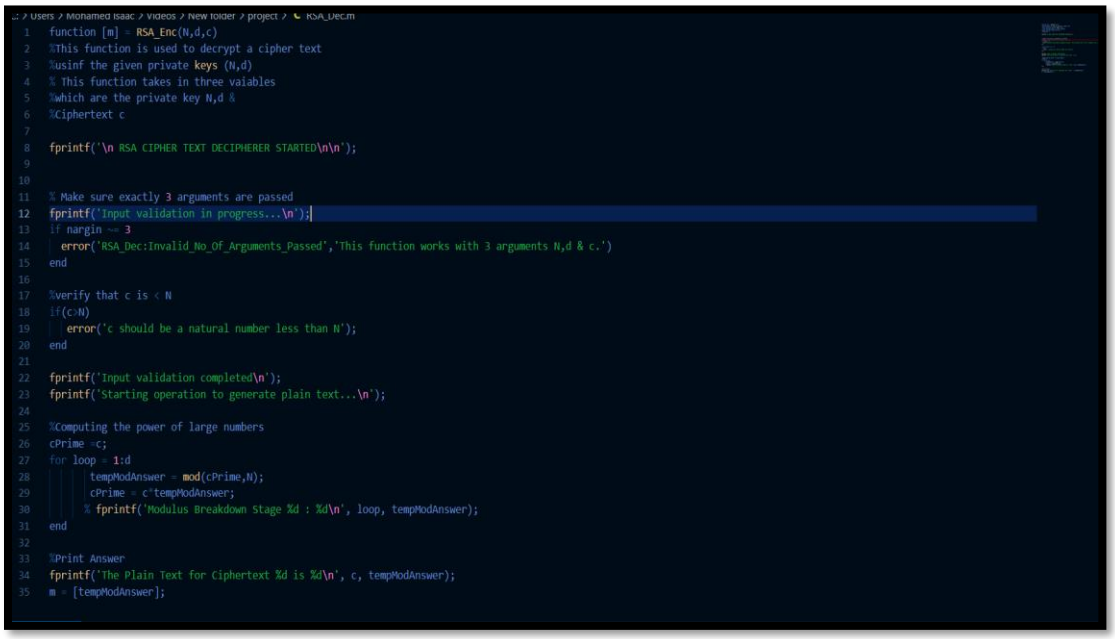
Figure 46: adv from the source node to the sink



```
C: > Users > Mohamed Isaac > Videos > New folder > project > C adv.m
function [] = adv(handles,source)
global S
global stop
global gaspitiration
global N
global e
global d
global rtotal
global delta

% check if source node does not have the route to the sink
devega = RSA_Dec(N,d,delta);
if (devega == 4000)
 t = append('RSA decrypting data complet the value is :  ',num2str(devega));

        appendt(handles,t);

if isempty(S(source).route)
   %check if the sink is in the range of source(direct transmission)
       if ismember(S(source).inrange,length(S))
           solution = [source length(S)];
           distance = sqrt( (S(source).x-(S(length(S)).x) )^2 + (S(source).y-(S(length(S)).y) )^2 );

       else % inderct transmission, must use the grasp
       [solution, distance] = grasp(source, length(S), gaspitiration);
       end

else
       solution = S(source).route;
       distance = S(source).routedistance ;
end
% udpate the total route
    rtotal = rtotal + distance;
   set(handles.rtotal,'String',[ num2str(double(rtotal)) ' m' ]);

 % check if there is route to the sink
```

Figure 47: adv.m function

And decrypting with RSA_Dec.m



```
.: > Users > Mohamed Isaac > Videos > New folder > project > RSA_Dec.m
function [m] = RSA_Enc(N,d,c)
%This function is used to decrypt a cipher text
%usinf the given private keys (N,d)
% This function takes in three vaiables
%which are the private key N,d &
%Ciphertext c

fprintf('\n RSA CIPHER TEXT DECIPHERER STARTED\n\n');


% Make sure exactly 3 arguments are passed
fprintf('Input validation in progress...\n');
if nargin ~= 3
  error('RSA_Dec:Invalid_No_Of_Arguments_Passed','This function works with 3 arguments N,d & c.')
end

%verify that c is < N
if(c>N)
    error('c should be a natural number less than N');
end

fprintf('Input validation completed\n');
fprintf('Starting operation to generate plain text...\n');

%Computing the power of large numbers
cPrime =c;
for loop = 1:d
        tempModAnswer = mod(cPrime,N);
        cPrime = c*tempModAnswer;
      % fprintf('Modulus Breakdown Stage %d : %d\n', loop, tempModAnswer);
end

%Print Answer
fprintf('The Plain Text for Ciphertext %d is %d\n', c, tempModAnswer);
m = [tempModAnswer];
```

Figure 48: RSA_Dec.m function

After we send an adv the sink replay with a request that he want the data from the node:

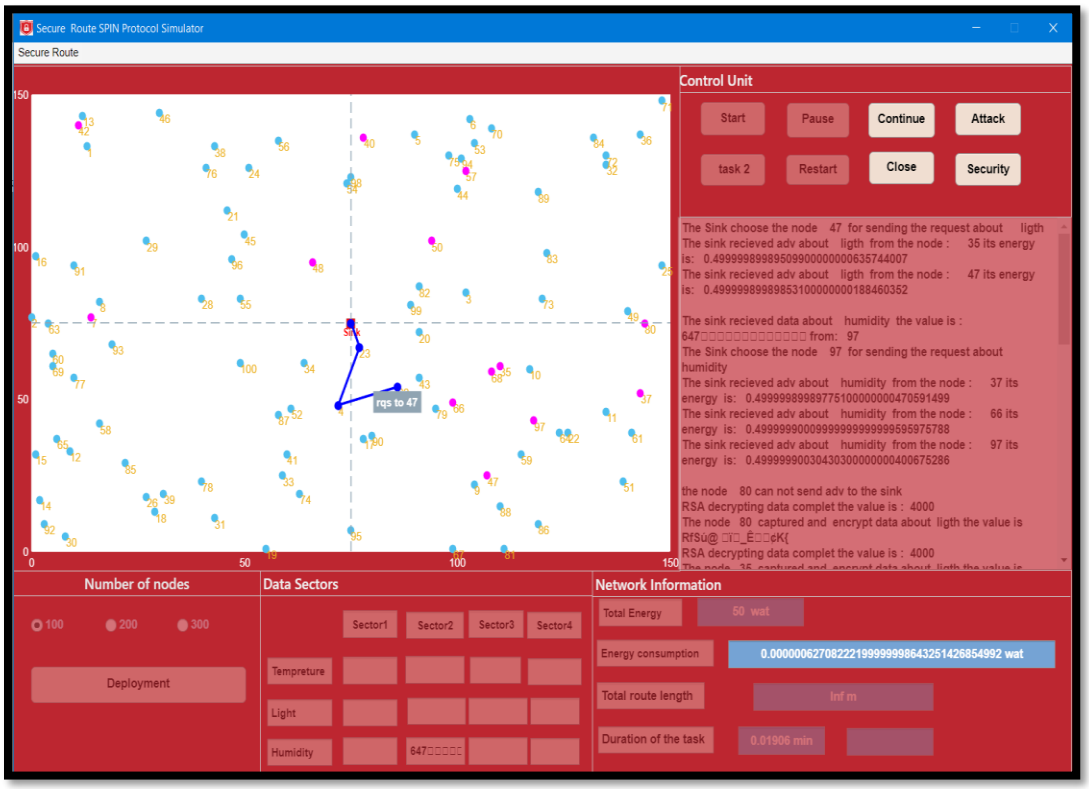


Figure 49: requesting data

```
function [] = frequest(handles,source)
global S
global stop
global gaspitiration

global regionindex;
global rtotal

% get last time saving this type of data
if  regionindex == 1
    time =S(length(S)).r1time(S(source).data);
elseif regionindex == 2
    time =S(length(S)).r2time(S(source).data);
elseif regionindex == 3
    time =S(length(S)).r3time(S(source).data);
elseif regionindex == 4
    time =S(length(S)).r4time(S(source).data);
end

    % the sink check if needs this data or not
if etime(clock , time) > 2.5*60

    % check if direct or inderct transmission
    if ismember(S(source).inrange,length(S))
        solution = [length(S) source ];
        distance = sqrt( (S(source).x-(S(length(S)).x) )^2 + (S(source).y-(S(length(S)).y) )^2 );
    else
    [solution, distance] = grasp(length(S), source,  gaspitiration);
    end

    % send the used route by the sink to source node
    S(source).route = routeinv(solution);
    S(source).routedistance = distance;

    % update total route
    rtotal = rtotal + distance;
```

Figure 50: frequest.m function

The node will send the data to the sink after he send the request and the sink will save the data and display to us:

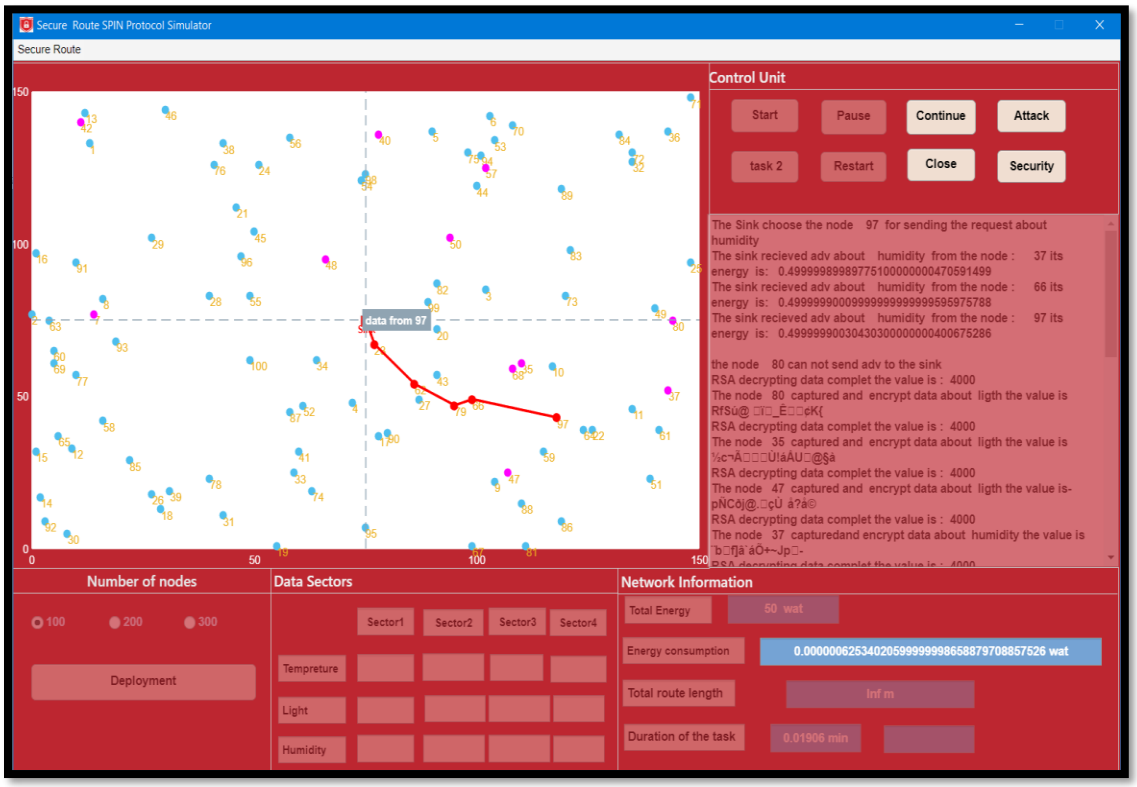


Figure 51: sending data to the sink

```
C: > Users > Mohamed Isaac > Videos > New folder > project > C senddata.m
function [] = senddata(handles,source )
global S;
global stop
global ns
global gaspitiration

global rtotal
ns = ns +1;

% chech if the source node has the route
if isempty(S(source).route)
    % chech if direct or indirect transmission
    if ismember(S(source).inrange,length(S))
        solution = [source length(S)];
        distance = sqrt( (S(source).x-(S(length(S)).x) )^2 + (S(source).y-(S(length(S)).y) )^2 );
    else
    [solution, distance] = grasp(source, length(S), gaspitiration);
    end

else
    solution = S(source).route;
    distance = S(source).routedistance ;
end



    % update total route
    rtotal = rtotal + distance;
    set(handles.rtotal,'String',[ num2str(double(rtotal)) ' m' ]);
    % update energy
    energycons(handles,source, solution,  'data',200);

    x = [];
    y = [];
    for i=1:1:length(solution)
            x(i) = S(solution(i)).x;
```

Figure 52: senddata.m function

The sink also will decrypt the data that the source node send it and then save it and display it

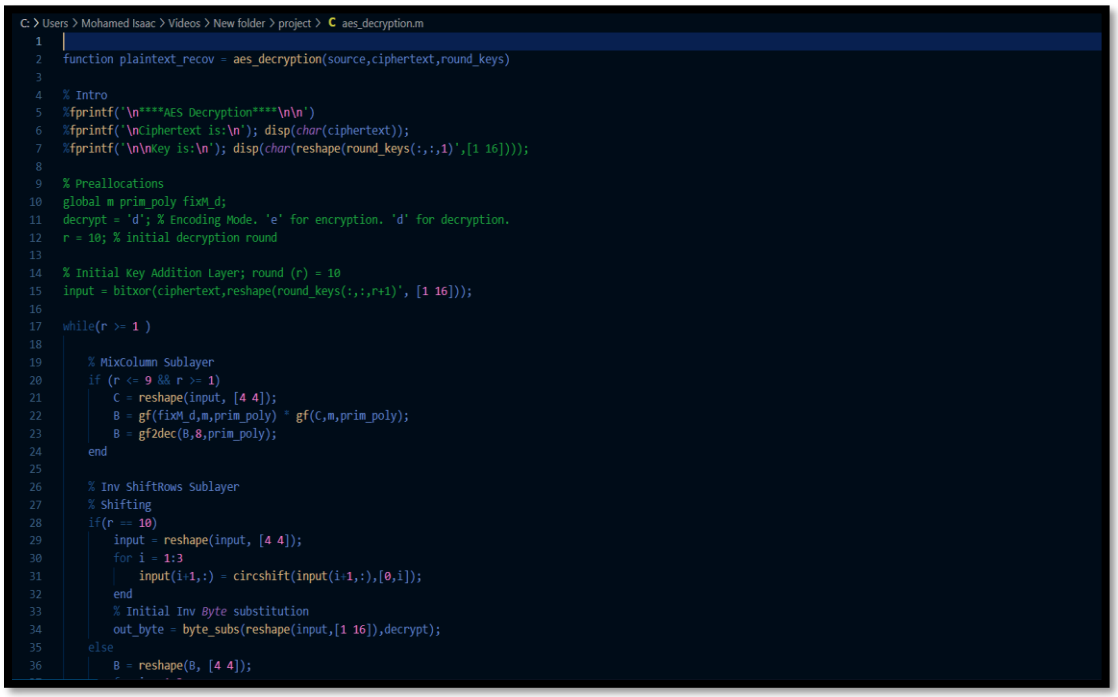


Figure 53: aes_decryption function

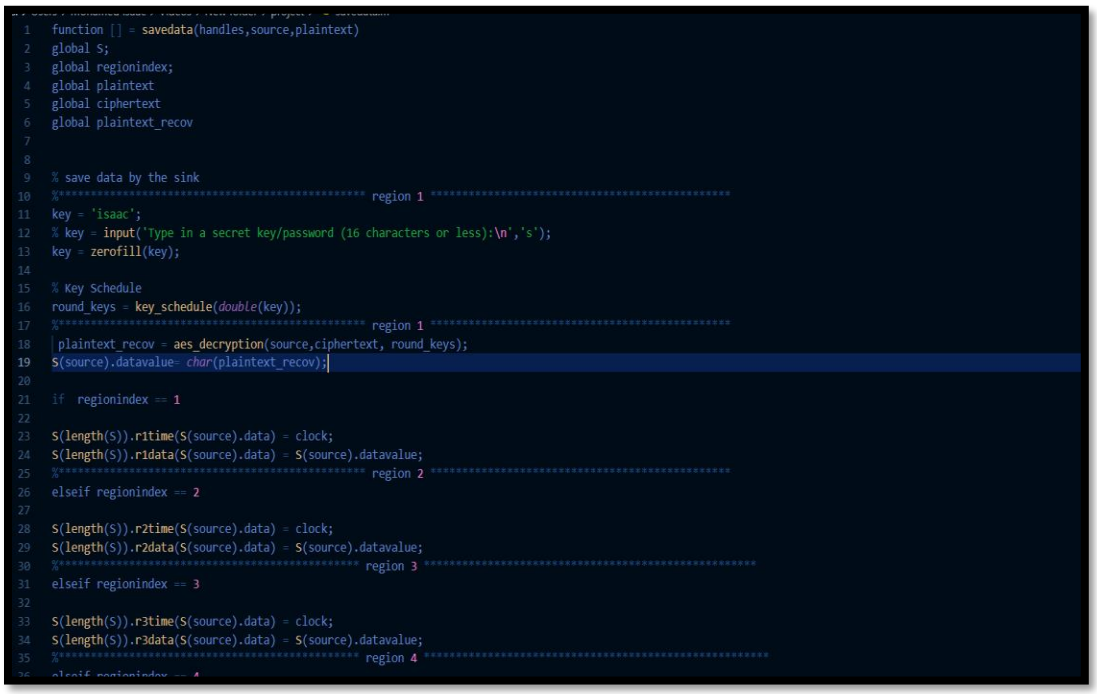


Figure 54: Savedata.m function

The data saved will be displayed in the data sector

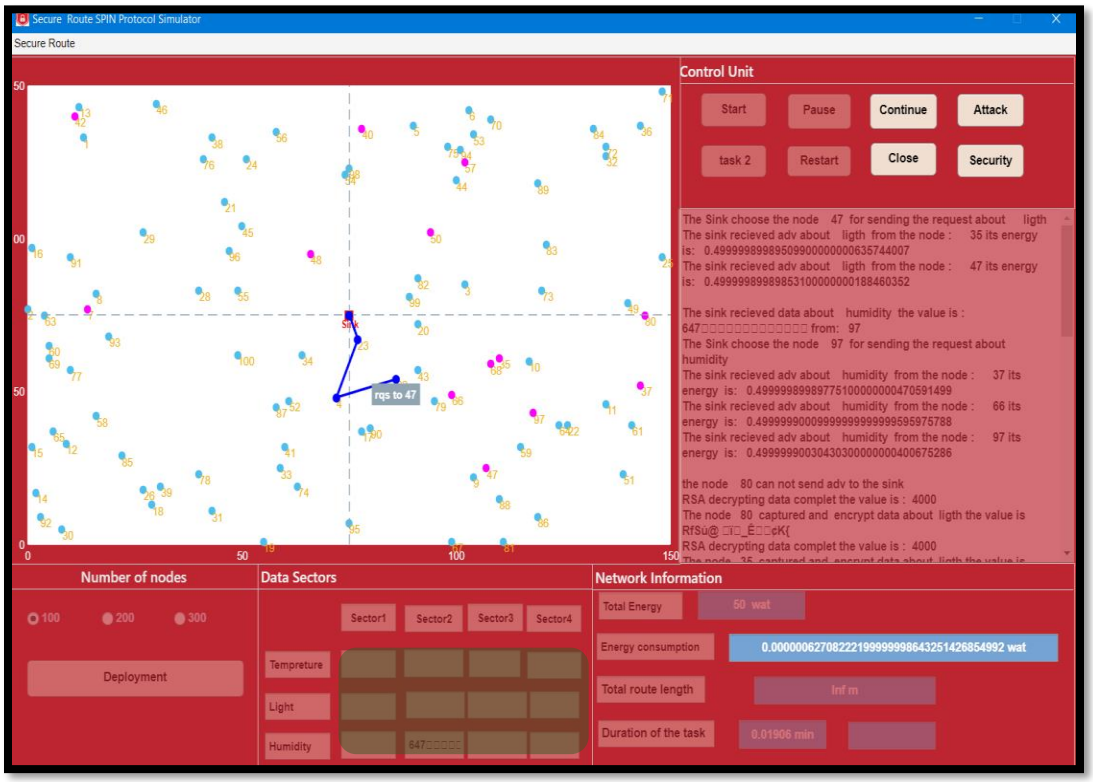


Figure 55: save and display data

Each line that drowns in the simulation it used the function drawline.m

```
function [ ] = drawline(handles,x,y,msg,source)
global S
avdcolor = [0.467,0.675,0.188];
rqscolor = 'b';
datacolor = 'r';
if strcmp(msg, 'adv')
    for i=1:1:5
        plot(handles.axes1,S(source).x,S(source).y,'o','MarkerEdgeColor','w', 'MarkerFaceColor','w');
        hold on;
        pause(0.3);
        plot(handles.axes1,S(source).x,S(source).y,'o','MarkerEdgeColor','m', 'MarkerFaceColor','m');
            pause(0.3);
    end

     plot(handles.axes1,S(source).x,S(source).y,'o','MarkerEdgeColor','m', 'MarkerFaceColor','m');

h = animatedline(handles.axes1,'color',avdcolor, 'linewidth',2,'linestyle','-','marker','o','MarkerEdgeColor',avdcolor,'MarkerFaceColor',avdcolor,'DisplayName','ADV');

end
if strcmp(msg, 'rqs')
h = animatedline(handles.axes1,'color',rqscolor, 'linewidth',2,'linestyle','-','marker','o','MarkerEdgeColor', rqscolor,'MarkerFaceColor', rqscolor,'DisplayName','ADV');
end
if strcmp(msg, 'data')
h = animatedline(handles.axes1,'color',datacolor, 'linewidth',2,'linestyle','-','marker','o','MarkerEdgeColor',datacolor,'MarkerFaceColor',datacolor,'DisplayName','ADV');
end



for i=1:1:length(x)
        addpoints(h,x(i),y(i));
        if i~=1
%           delete(text(x(i-1),y(i-1),'adv'));
            set(k(),'Visible','off');
        end
        if strcmp(msg, 'adv')
       k = text(handles.axes1, x(i)-7,y(i)-7,['adv from ' num2str(source)],'color','w','FontWeight','Bold','BackgroundColor',[0.565 0.643 0.698]);
```

Figure 56: drawline.m function

The total energy consumption is calculated used the function energycons.m and averagenergy.m

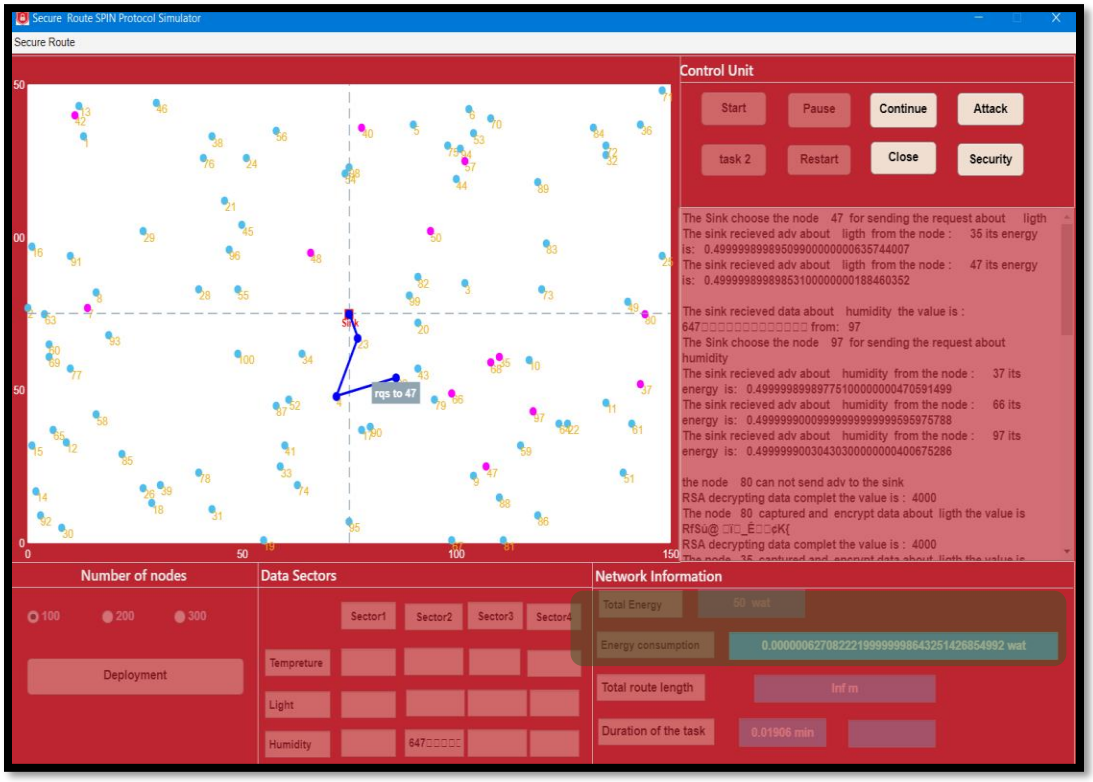


Figure 57: energy consumption and total energy

```
C: > Users > Mohamed Isaac > Videos > New folder > project > C averagenergy.m
1   function result = averagenergy
2   global S
3
4       result = true;
5
6       for i=1:1:length(S)-1
7           if ~isequal(S(i).status , 'active')
8               result = false;
9           end
10
11      end
12
13  end
14
15
```

Figure 58: avergenergy.m function

```
function [] = energycons(handles,source, solution,  msg , K)

global S
global EconsTotal
global kAdvRqs
global datasize
global Eelec
global Eamp

datasize = K;
Esensing = 0.00000005;
Egrasp   = 0.00000005 ;
Eelec    = 10^0.000000000001;
Eamp     = 0.0013^0.000000000001;
kAdvRqs = 10;
        if strcmp(msg, 'adv')

                        d = S(source).distance(solution(2));
                        ETx = Eelec * kAdvRqs + Eamp * kAdvRqs *d.^2;
                        Etotal =  ETx + Esensing + Egrasp;
                        S(source).E = S(source).E - vpa(Etotal);
                        EconsTotal = EconsTotal + vpa(Etotal);

            if length(solution) > 2
                for i=2:1:length(solution)-1
                            d = S(solution(i)).distance(solution(i+1));
                            ETx = Eelec * kAdvRqs + Eamp * kAdvRqs *d.^2;
                            ERx = Eelec * kAdvRqs ;
                            Etotal = ETx + ERx;
                           S(solution(i)).E = S(solution(i)).E + vpa(Etotal) ;
                           EconsTotal = EconsTotal + vpa(Etotal);
                end

            end
        end
```

Figure 59: energycons.m function

e- Pause button: this button simply pauses the simulation from working tell you press the continue button

f- Continue button: this button will continue the task after you press pause button.

g- Restart button: this button will restart the whole simulation.

h- Close button: this button simply closes our application.

i- Task button: the task button will start a new task each time the task completed so it will number of tasks and it uses the task.m function

```
function task(handles)

global S;
global stop;
global regionindex;
global close;
global task
global regions
global tStart

 t = append('*********************************************************************');
 appendt(handles, t);
 t = append('                                ',' Task number : ','   ',num2str(task));
  appendt(handles, t);
 t = append('*********************************************************************');
 appendt(handles, t);

task = task +1;

tStart = tic;

for regionindex=1:1:4
    tStatregion = tic;
        t = append('                    ',' ****************');
     appendt(handles, t);
        t = append('                    ',' Region number : ','   ',num2str(regionindex));
      appendt(handles, t);
        t = append('                    ',' ****************');
     appendt(handles, t);
        t = append(' ');
     appendt(handles, t);
        region = regions(num2str(regionindex));
    for j=1:1:length(region)

        if stop
            break;
```

Figure 60: Task.m function

j- Attack button: attack button will simply generate an attack that will create an imposter node and it will tell other nodes to send the data to it instead of the base station, also it will stop the path between the source nodes and other nodes, it will test our security solution.

4.7 Results

the result we got from this simulation evaluates the performance of our safety mechanism in terms of resistance against type attacks Modification and falsification of data.

As shown in the figure 57,58 and 59, it will show the nodes that are secured and the encrypted data that no adversary can access or accede to it:

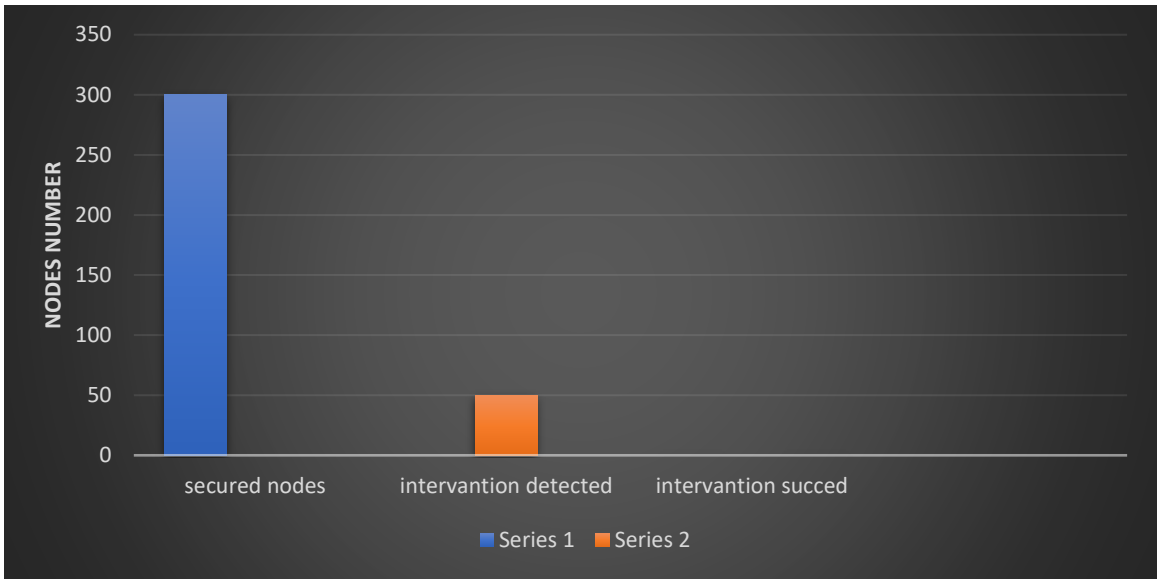


Figure 61: simulation results

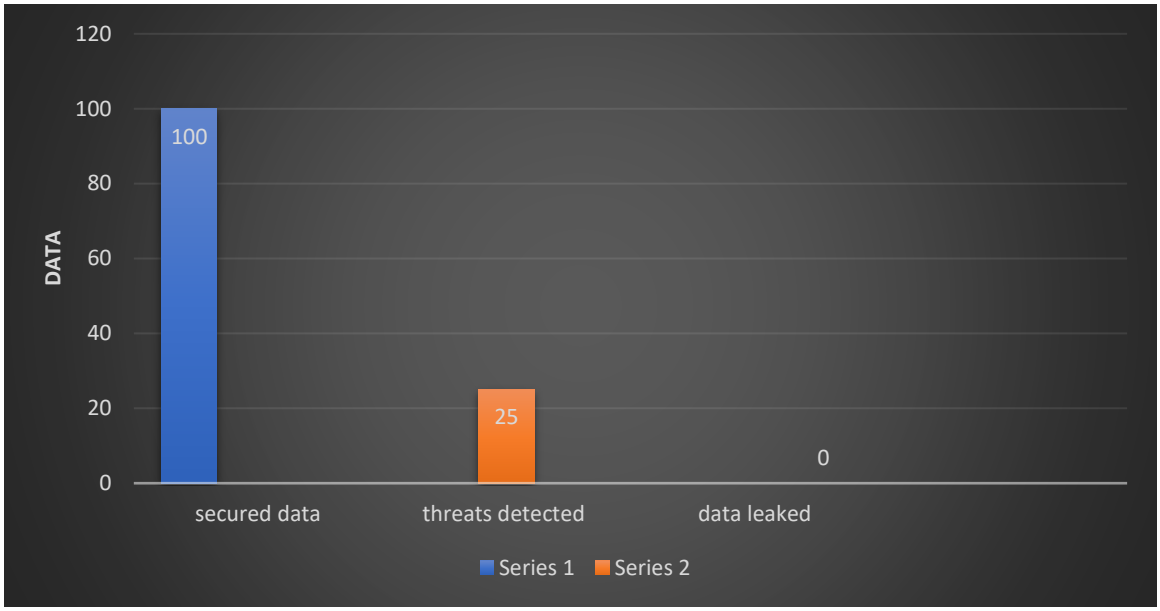


Figure 62: simulation results

Energy: as shown in the figure 59 our security solution doesn't consume as much energy and don't need too much to process all the data in encryption and decryption:

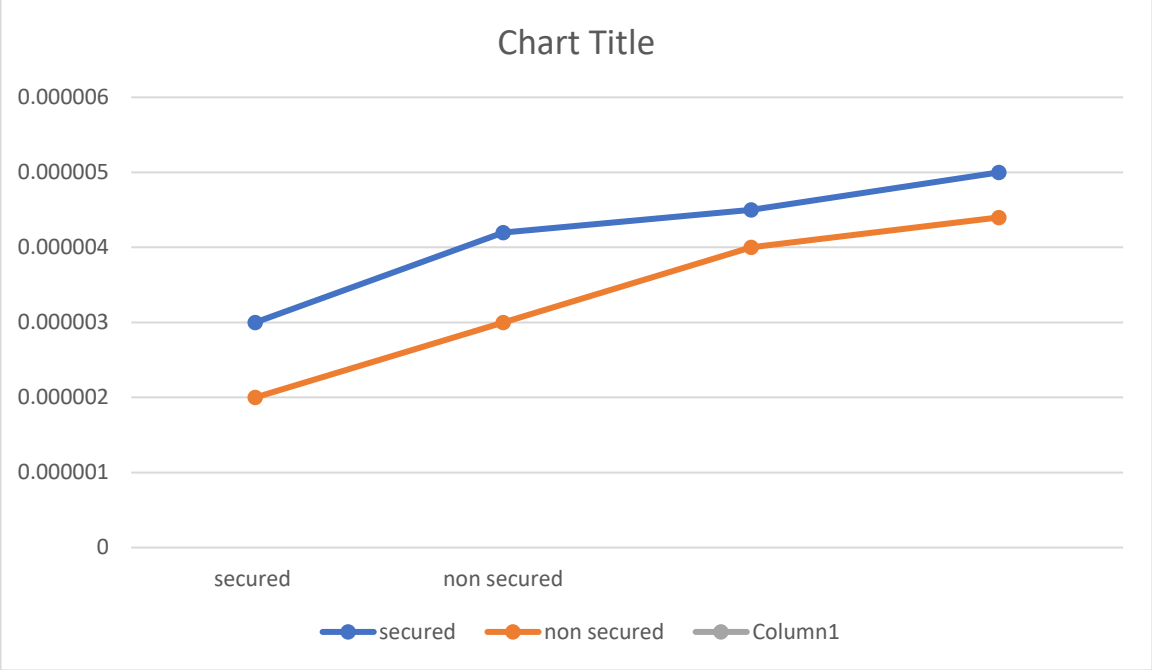


Figure 63: energy consumption

4.8 Conclusion

In this chapter we saw the simulation of our application, and the tools that we used, the network models and also the parameters. We have presented the results obtained to compare the time between non secured and secured solution. and in conclusion our solution makes the network more secured and very hard to attackers to access our information.

General conclusion

In our thesis we discuss security descriptions in WSN, the classification of security and also security protocols in WSN, and also comparison between security protocols. We also discuss the problem of security in wireless sensor network WSN. And propose a solution in Following the 5 steps below to insure a symmetric encryption and asymmetric encryption and stating the benefits of each one in securing the GR-SPIN Protocol.

Step 1: initialization and deployment with RSA public key and AES

In this step we simply divided the network by four equal regions, after deployment finish immediately we will deploy the RSA public key with all the nodes, and also AES key method to the whole network (sink and nodes).

Step 2: Data advertising and decryption with RSA

In order to a source node to advertise its data that he sensed in its sensing zone it must first decrypt the RSA value if it's the same, then it will discover the path that leads to the sink and send and adv message to it.

Step 3: Data requesting and decryption with RSA

Now in the sink, after receiving a list of adv messages, the sink will first decrypt the RSA value first to be able to complete requesting, after the value is correct and decryption is complete the sink will decide who to send the request message to for asking data.

Step 4: Data transmitting and encryption with AES

This phase any source node that receives a request from the sink will firstly encrypt the data with AES encryption and it will send it to the sink.

Step 5: Data saving and decryption

After the sink receives the data, it will decrypt it and save it and show us the results.

Each of these steps are repeated for each region and

The results of this simulation proved that our security solution makes a huge deal compared to non-secured basic protocol.in the future improvements, we may improve our modified secure SPIN by:

- generating the keys in AES encryption.

Bibliographies

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks

2. Muhammad Nadeem Akhtar1 , Arshad Ali2 , Zulfiqar Ali3 , Muhammad Adnan Hashmi 4 and Muhammad Atif . Cluster based Routing Protocols for Wireless Sensor Networks: An Overview

3. e-Health Systems, 2016. A wireless sensor network (WSN) can be defined as a network of small embedded devices, called sensors, which communicate wirelessly following an ad hoc configuration**.**

4. S. Ziane and A. Mellouk. ―A swarm intelligent scheme for routing in mobile ad

networks‖. Systems Communications, IEEE, Aug 2005 5. CHUAN XU 1, ZHENGYING XIONG 2, GUOFENG ZHAO 3, AND SHUI YU 4,‟ An

Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN‟,

September 30, 2019.

6. Action Nechibvute,1 Albert Chawanda,1 and Pearson Luhanga,‟ Piezoelectric Energy

Harvesting Devices: An Alternative Energy Source for Wireless Sensors‟, Hindawi

Publishing Corporation Smart Materials Research, Volume 2012, Article ID 853481

7. Mekki nabil Mohammedi kada -Techniques de conservation d'énergie pour les réseaux de capteur sans fi. Thesis master. Order : acces

8. FEHAM Mohammed. KADRI Benamar. LABRAOUI Nabila - Mise en place d'un Réseau de Capteurs Sans Fil pour la Détection des Feux de Forêt (RCSF-DFF) .access : 35/1/12/2012

9. David Rey . COLLECTE DES DONNÉES D'UN RÉSEAU DE CAPTEURS SANS FILS EN UTILISANT UNE SURCOUCHE RÉSEAU PAIR À PAIR (final thesis avril 2010).

10 . W. Ye, J. Heidemann, and D. Estrin. "An Energy-Effcient MAC Protocol for Wireless Sensor Networks". pp 1567-1576, June 2002.11. Ahmad Alkhatib. Wireless Sensor Network Architecture. Conference: in 2012 International Conference on Computer Networks and Communication Systems (CNCS) 2012Volume: 12

12. endi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan,‟ EnergyEfficient Communication Protocol for Wireless Microsensor Networks ‟, Massachusetts Institute of Technology Cambridge, MA 02139

13. Muhaammad R Ahmed, Xu Huang, Dharmandra Sharma and Hongyan Cui . Wireless Sensor Network Characteristics and Architectures . World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering Vol:6, No:12, 2012

14. LIU Yong-Min , WU Shu-Ci , NIAN Xiao-Hong . The Architecture and Characteristics of Wireless Sensor network. 2009 International Conference on Computer Technology and Development

15. Sensor Networks: The Advantages and Disadvantages You Need To Know. Totalphase. available at: https://www.totalphase.com/blog/2019/04/sensor-networks-the-advantages-and-disadvantages-you-need-to-know/ .access:1/28/2021

16. Prachi Arora. WSN and its Application. M.Tech, Central university of Jharkhand, Ranchi, India

17. Jamal N. Al-Karaki Ahmed E. Kamal. Routing Techniques in Wireless Sensor Networks: A Survey. Dept. of Electrical and Computer Engineering Iowa State University, Ames, Iowa 50011 Email: {jkaraki, kamal}@iastate.edu

18. Alexandria Engineering Journa. Routing protocols for wireless sensor networks: What the literature says?. Volume 55, Issue 4, December 2016, Pages 3173-3183

19. Imene ALOUI,‟ Une Approche Agent Mobile Pour Les Réseaux De Capteurs‟, thesis of doctorat, biskra university 2016.

20. Bazzi, Hiba Sami; Haidar, Ali Masoud; Bilal, Ahmad (2015). [IEEE 2015 International Conference on Computer Vision and Image Analysis Applications (ICCVIA) - Sousse, Tunisia (2015.1.18-2015.1.20)] International Conference on Computer Vision and Image Analysis Applications - Classification of routing protocols in wireless sensor network. , (), 1–5. doi:10.1109/ICCVIA.2015.7351790.

21. Dionisis Kandris , Christos Nakas , Dimitrios Vomva and Grigorios Koulouras, Applications of Wireless Sensor Networks: An Up-to-Date Survey, microSENSES Research Laboratory, Department of Electrical and Electronic Engineering, Faculty of Engineering, University of West Attica, GR-12241 Athens, Greece; mscres-2@uniwa.gr (C.N.); mscee17009@teiath.gr (D.V.)

22. KAZAR Youcef . „Intrusion detection in wireless sensor networks (WSNs)“. Thesis master.

Order N◦ : RTIC 20/M2/2017 [23] Y. Chen, Wei Shen, H. Huo, Youzhi Xu. A Smart Gateway for Health Care System Using Wireless Sensor Network. DOI:10.1109/SENSORCOMM.2010.88Corpus ID: 18724627.

24. Mekki nabil and Mohammedi kada,“ Techniques de conservation d“énergie pour les reseaux de capteur sans fil“, master thesis,university of saida, juin 2018

25. M.A. Matin and M.M. Islam,“ Overview of Wireless Sensor Net“,September 2012,ResearchGate

26. CHUAN XU 1, ZHENGYING XIONG 2, GUOFENG ZHAO 3, AND SHUI YU 4,“ An

Energy-Efficient Region Source Routing Protocol for Lifetime Maximization in WSN“,

September 30, 2019.

27. Mohammed Mehdi Saleh. Wireless sensor network (WSN). University of Anbar.

28. Marc von Boemcken and Conrad Schetter.

29. security-in-computing-5-e

30. Archana Choudary. What is Network Security: An introduction to Network Security

31. Jaydip Sen. Security in Wireless Sensor Networks. Department of Computer Science & Engineering, National Institute of Science & Technology, INDIA

32. Carman, D. W., P. S. Krus, and B. J. Matt. 2000. “Constraints and Approaches for Distributed Sensor Network Security.” Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA.

33. Eschenauer L., and V. D. Gligor. November 2002. “A Key-Management Scheme for Distributed Sensor Networks.” In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS’02), 41-47, Washington DC, USA.

34. C K Marigowda, Manjunath Shingadi : SECURITY VULNERABILITY ISSUES IN WIRELESS SENSOR NETWORKS: A SHORT SURVEY. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013

35. Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim:A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks. 보안공학연구논문지 (Journal of Security Engineering), 제 9권 제 3호 2012년 6월

36. Furrakh Shahzad1 , Maruf Pasha2 , Arslan Ahmad2. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. nternational Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, December 2016

37. Mohamed-Lamine Messai. Classification of Attacks in Wireless Sensor Networks. nternational Congress on Telecommunication and Application’14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014

38. Yacine Challal, « Réseaux de Capteurs Sans Fils », Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17 Novembre 2008.

39. J.N. Al-Karaki, A.E. Kamal, Routing techniques in wireless sensor networks: a survey, Wireless Commun. (IEEE) 11 (2004) 628.

40. Harsh Kupwade Patil. Thomas M. Chen. Wireless Sensor Network Security

41. Monika Bhalla, Nitin Pandey, Brijesh Kumar. Security Protocols for Wireless Sensor Networks

42. Karlof, Chris; Sastry, Naveen; Wagner, David (2004). [ACM Press the 2nd international conference - Baltimore, MD, USA (2004.11.03-2004.11.05)] Proceedings of the 2nd international conference on Embedded networked sensor systems - SenSys '04 - TinySec. , (0), 162–. doi:10.1145/1031495.1031515

43. Murat Dener. Security Analysis in Wireless Sensor Networks. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 303501, 9 pages http://dx.doi.org/10.1155/2014/303501

44. Yu Chengbo Cui Yanzhe Zhang Lian Yang Shuqiang. ZigBee Wireless Sensor Network in Environmental Monitoring Applications. hengbo Cui Yanzhe Zhang Lian Yang Shuqiang Research Institute of Remote Test&Control Chongqing University of Technology Chongqing, China (400050) yuchengbocqut.edu.cn

[45] Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno. Asymmetric Encryption in Wireless Sensor Networks. Additional information is available at the end of the chapter http://dx.doi.org/10.5772/48464.

46. Josh Fruhlinger. What is cryptography? How algorithms keep information secret and safe. Public keys, private keys, and hash functions make the secure internet possible.

47. Peter Loshin, Michael Cobb. Data security guide: Everything you need to know. Data security guide: Everything you need to know

48. Emily Williams. Cryptography 101: Symmetric Encryption. https://medium.com/@emilywilliams_43022/cryptography-101-symmetric-encryption-444aac6bb7a3

49. Ons JALLOULI. Chaos-based security under real-time and energy constraints for the Internet of Things. g. UNIVERSITE DE NANTES, 2017. English.

50 .Samir athmani. Protocole de sécurité Pour les Réseaux de capteurs Sans Fil. These Pour l'obtention du Magistère en Informatique Option : Ingénierie des Systèmes d'Informations

51.Digital signature: 8 frequently asked questions about it.

52 Christof Paar et al. Understanding Cryptography