SECURING HABITAT MONITORING MODEL THROUGH ASYMMETRIC CRYPTOGRAPHY CONSIDERING ECC ALGORITHM

Avinash Rai[1], Pushpita Shrivastava[2]
[1] Assistant Professor, Dept. Of ECE, Rajiv Gandhi Proudhyogiki Vishwidhwalaya, Bhopal, M.P., India
avinashrai@rgtu.net
[2]M.E. Student, Dept. of ECE, Rajiv Gandhi Proudhyogiki Vishwidhwalaya, Bhopal, M.P., India
pushpita0909@gmail.com

Abstract— Wireless Sensor Network is a network containing enormous amount of independent sensor nodes which observe, sense, collect the data from physical territory and transfer to the sink node for further processing. Wireless sensor network has many applications in the field of habitat monitoring, military, health care etc. As this network is a fast growing network with an open environment and unattended nature it is prone to many security attacks. In this paper a habitat monitoring model is given, to secure this model Asymmetric Cryptography technique is taken into consideration using Elliptical Curve Cryptography Algorithm.

Keywords— WSN: Wireless Sensor Network, Habitat Monitoring Model, SKC: Secret Key Cryptography, PKC: Public key Cryptography, ECC: Elliptical Curve Cryptography.

Introduction

Wireless sensor network has wide range of applications in many different fields; one of the fields is habitat monitoring. In habitat monitoring the sensors sense the environmental components such as carbon monoxide, temperature, moisture and transmit to the base station. This transmission of confidential data is through an insecure medium and is prone to many security attacks because of this security has become a major concern.

As the WSN is unreliable and unattended kind of network therefore it is vulnerable to many kinds of security attacks. These securities are of two types- active attack and passive attack. If the rival only monitors the communication which is going through than it is known as "passive attack" and if the rival modifies or destroy the information than it is known as "active attack". There are many limitations of this network like limited- energy, power, memory and processing capability. Paper [1], [2], [3], [4] describe different security attacks and need of securing the sensor network.

Hence the best way to secure this network is through "Cryptography".

Cryptographic techniques and two types of cryptography technique –SKC and PKC

Asymmetric cryptography is advance and more secured technique when compared to others and hence in this paper this technique is taken into consideration for securing the wireless network using the Elliptical curve Cryptography Algorithm. Paper [5] and [6] describe about the ECC and shows the advantages of ECC over other Asymmetric cryptography algorithms. Paper [7] and [8] gives the ECC algorithm for securing the data while transmitting it through an unsafe medium.

This paper is based on a habitat monitoring application of WSN which is sense environmental parameters and with the help of zigbee transmits it wirelessly through a insecure medium. Therefore it requires an effective security mechanism for saving the data from security attacks. Cryptography is one of the effective security mechanisms and in that Asymmetric cryptography or Public Key Cryptography is widely used when it comes to securing large amount of sensor nodes. In PKC the algorithm which is presented is Elliptical Curve Cryptography algorithm.

I. BASIC

The habitat monitoring model consist of-

1. Three sensors-

a. temperature sensor-DS1820, whose range is -55°C to 125°C

b. carbon monoxide sensor- MQ9, which has higher sensitivity to CO and combustible gas like methane and propane.

c. Moisture sensor- DTH

2. Microcontroller- the microcontroller is ATMEGA 328 microcontroller having 28 pins.

3. Zigbee- S2C zigbee whose frequency is 2.4GHz and indoor range is up to 60m.

Here the three sensors their respective parameters the sensed data through microcontroller goes to the zigbee which wirelessly transmit the data to the receiver end where another zigbee which is paired to the first zigbee receives the data. Here the data from zigbee goes to the microcontroller which is connected to the laptop through usb drive, for generating the graphs.

Using Laboratory Virtual Instrument Engineering Workbench (LABVIEW) the graphical user interface is designed. In this reading from the sensor are tabulated with the interval of 2 seconds. Its reading can also be exported to excel where its graphs are made, these graphs are shown in the result of this paper.

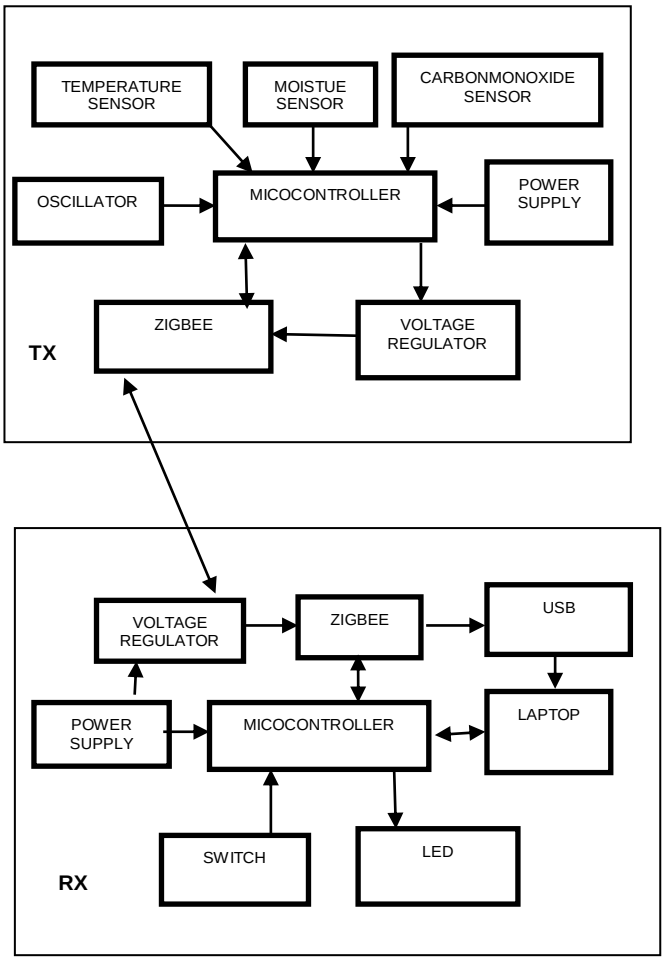


FIGURE: 1 HABITAT MONITORING MODEL

CRYPTOGRAPHY-

This is a technique of converting any message into a code and sends it through an insecure medium so that the only intended recipient can decode the code into meaningful information. This whole process of cryptography takes place into two steps that is encryption and decryption which takes place with the help of a secret key. The two types of cryptography are symmetric cryptography or secret key cryptography which uses same key(symmetric key) for both encoding and decoding purpose and the other is asymmetric key or public key cryptography which uses two keys (public key and private key) for encoding and decoding.

ASYMMETRIC CRYPTOGRAPHY-

In this type of cryptography there are two keys used one is public key which is a shared key and the other is private key which is not shared. That is why this technique is more secured than the other technique. In this the message is encrypted using a public key can be decrypted using the matched private key by applying the same algorithm.

This cryptography technique is more bulky than other techniques, hence an appropriate algorithm should be used as the sensor network has limited memory and energy. That is why Elliptical Curve Cryptography Algorithm is taken into consideration into this paper for securing the sensor network because its key size is comparatively small and hard to break by rivals.

II. PROPOSED METHODOLOGY

Methodology for making a habitat monitoring model involves the following tools and software's. They are-

1. PCB Wizard- PCB WIZARD is a software for designing the printed circuit board, it allows to design both single sided printed circuit board and double sided printed circuit board. Using this software one can design schematic design on which a printed circuit board can constructed.

2. Printed Circuit Board- A printed circuit board (PCB) is a board on which the electrical and electronics components are placed and these components are connected to each other through conductive tracks. Therefore a printed circuit board mechanically braces the components and connects them with the conductive tracks.

3. XCTU- This software is used to configure the zigbees used. As there are two zigbees used one at the transmitter end and another is at the receiver end. Therefore the two zigbees used need to be paired up together as if one transmits other one receives. In the XCTU software firstly the zigbee needs to be placed on the baseboard which is then connected to the system via USB cable. On the main window the communication ports will be shown these ports will be the ports in which the zigbees are connected.

4. ARDUINO Software- This software is used for writing the program in embedded C for both the transmitter and receiver end. This software is used to write and compile the program.

5. LabVIEW- It stands for Laboratory Virtual Instrument Engineering Workbench (LABVIEW). This is software which is system engineering software. This software gives the platform for designing the graphical user interface. In habitat monitoring model the Labview is used for designing the graphical user interface where the readings of the sensors are represented in graphical manner. In this reading from the sensor are tabulated with the interval of 2 seconds. Its reading can also be exported to excel where its graphs are made.

6. UNO Burner- The Uno burner is a hardware which is used to burn the programs from the software to the embedded system. As the programming which is written for the hardware has to be exported to the hardware and this is done through burring the programs in the hardware. Hence the program is burned in the main memory of the whole hardware which is the microcontroller. In this the microcontroller is placed on the base board and that base board is connected to the system from where the program can be burned.

III. IMPLEMENTATION

ELLIPTICAL CURVE CRYPTOGRAPHY (ECC)-

It is an asymmetric cryptography technique which is based on elliptical curve theory. Elliptical curve cryptography is constructed on algebraic structure of elliptical curve. In this technique the key size is very small and because of which it takes less time for computational operation and also consumes less memory and space. It is better option for cryptography than RSA because 256bit ECC public key provide the same security as 3072bit RSA public key.

Elliptical Curve is a plane curve having finite field and the points on the curve satisfying the equation:

$$y2 = x3 + ax + b \quad (1)$$

where a and b are coefficients that define the curve.

ELLIPTICAL CURVE CRYPTOGRAPHY ALGORITHM-

Some parameters-

G: generator point, it is the point on the curve which shows the start of the curve

n: it is order of the generator point such that its scalar multiplication with G gives a point on the curve.

GENERATION OF KEYS:

- Private key- choose any random integer ‘d’

such that

$0 < d < n$

Public key: for getting a public key a

scalar point multiplication has to be done of private key ‘d’ and the generator point ‘G’

$Q = d . G$

In ECC the public key and the private keys are not exchanged. Here the private key is an integer and public key is a point on the curve.

ENCRYPTION: the data is encrypted using a public key ’Q’. The following steps are performed-

- Firstly choose any random number ‘r’ such that the

$0 < r < n$

- Now the next step is to calculate a point R which is the multiplication of secret number ‘r’ and generator point ‘G’

$R = r . G$

- Now calculate the point S which is the shared secret point from where a symmetric key can be derived

$S = R . Q$

DECRYPTION: at the receiver end the encrypted message will be receives in the form of a code. The code can be decoded to the original message by multiplying the publically transmitted point with the private key. This way the shared key S will also be recovered.

$$S = r \cdot d$$

This works-

$$S = R \cdot d$$

$$S = r \cdot G \cdot d$$

$$S = r \cdot Q$$

IV. RESULT

The graphs showing the readings of the three sensors are-

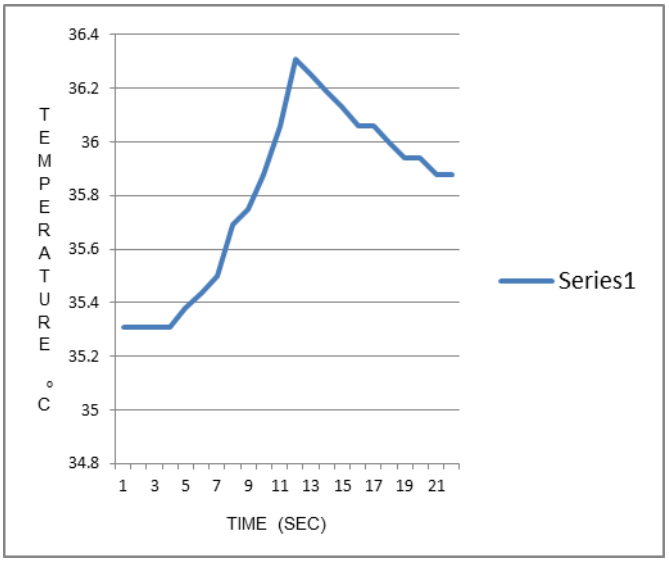
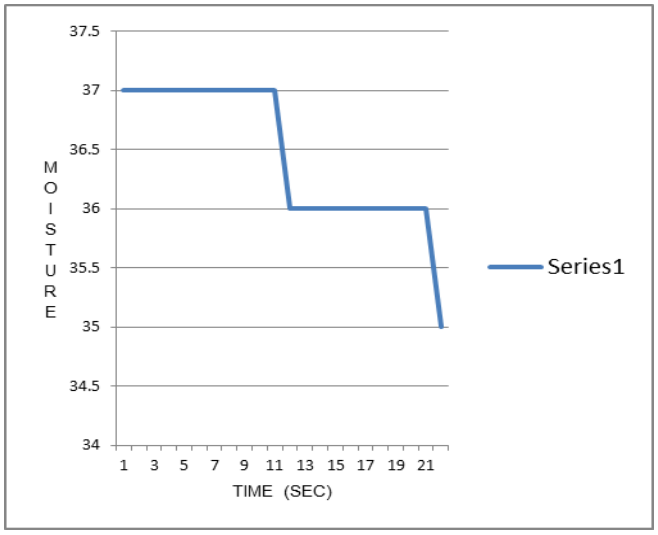
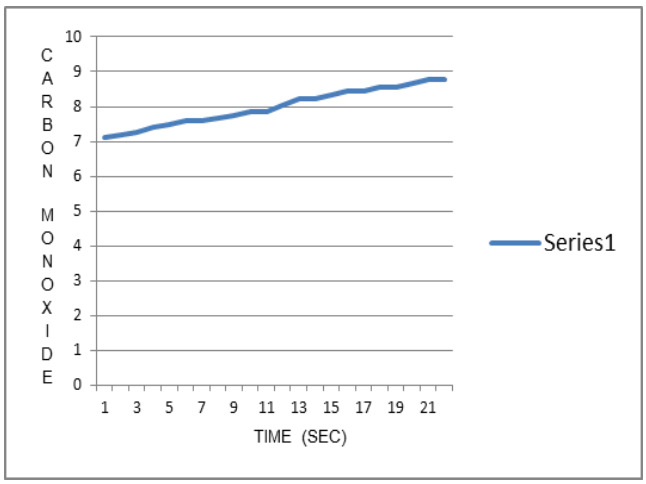


FIGURE: 2 A) READINGS OF TEMPERATURE SENSOR



B) READINGS OF MOISTURE SENSOR



C) READINGS OF CARBON MONOXIDE SENSOR

V. APPLICATIONS

- This model can used for monitoring the pollution level caused by CO and other pollutants in the cities.
- This can be implemented in the forest and by knowing the sudden temperature rise or decrease in moisture level with the help of previous data these scarcities can be eliminated in time.
- By examining the moisture level drought conditions can be predicted in time.
- One of the biggest problem of today is decreasing level of ground water, this can be reduced by monitoring the moisture level inside the ground.

VI. ADVANTAGES

- Due to such large variety of applications less in cost this network can be used in human welfare.
- This network van even be deployed in cruel and hostile environment where wired networks are hard or impossible to deployed.
- WSN is a very flexible network and at any time it can accommodate any amount of devices.
- In ECC algorithms the generation of keys, encryption and decryption process is very fast when compared to other algorithms.

VII. DISADVANTAGES-

- The communication in WSN is through insecure medium therefore it is easy for the hackers to hack it.
- Has limited amount of memory, energy, processing capability.
- There are many challenges associated with WSN such as time synchronization, security, localization, scalability, limited resources etc.
- The major setback of WSN is security attack cause due to this attack the data which can be confidential data can be hacked and altered and also can be used for unfair means.

VIII. CONCLUSION

Habitat monitoring is one of the applications of wireless sensor network which monitors the different parameters of and through zigbee sends it to the base station. This model can be used in many applications and its data can further be saved for eliminating lots of risk factors. As the transmission is through an insecure medium it is prone to many attacks in which someone can monitor it or eavesdrop the message. As a solution to which asymmetric cryptography is very useful. The sensor network can be made secure through asymmetric cryptography using elliptical curve cryptography algorithm which consumes less memory and is faster than other asymmetric cryptography algorithms.

IX. REFERENCES

[1]. Yassine Maleh and Abdellah Ezzati , "An advance study on cryptography mechanism for wireless sensor network- sep 17 2016" Mediterranean Telecommunications Journal, Vol. 6, N{\deg} 2, June 2016. Cornell University Library

[2]. Aarti Gautam Dinker and Vidushi Sharma, "Attacks and challenges in wireless sensor network- 2016" 2016 3rd national conference on computing for sustainable global development. IEEE Xplore document -7724828

[3]. Khina Chelli "Security issue in wireless sensor network : attacks and countermeasures- 2015". International Association of Engineers. Proceeding of the world congress on engineering 2015 vol 1 WCE 2015, july 1-3, 2015, London, U.K.

[4]. Vikash Kumar, Anshu Jain, and N P Barwal " Wireless sensor networks- security issues, challenges and solution- 2014" International Journal of Information and ComputationalTechnology. ISSN 0974-2239 Vol 4, Number 8 (2014) @ International Research Publication House.

[5]. Madhumita Panda " Security in wireless sensor network uing cryptography techniques-2014" American Journal of Engineering Research(AJER) volume3, issue-01

[6]. Iskandar Setiadi, Achmad Imam Kistijantoro, Atsuko Miyji "Elliptical Curve Cryptography- algorithms and implementation analysis over coordinate system- 2015" 2nd International conference on Advanced Inforrmatics : Concepts , theory and applications. IEEEXplore document- 7335349

[7]. Elliptical Curve Cryptography Tutorial by Johannes Bauer at Johannes-bauer.com