ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Survey on External Security Threat with Defense Mechanism for Wireless Sensor Network

Prof.Sagar Thakare[1], Manjusha Nimbalkar[2], Richa Nabar[3]

Assistant Professor, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[1]

PG Student, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[2]

PG Student, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[3]

ABSTRACT: Developing effective security solution for wireless sensor networks (WSN) is not easy due to limited resources of WSNs and the hazardous nature of wireless medium.WSNs are used in large application from civilian to military so security is very important in WSN. Sensor node use wireless communication that is why it is easy for attacker to inject malicious message into the network. In this paper, we have provided security solution for information which transfer or communicate between sensor node and base station using Asymmetric Key Cryptography Algorithm (RSA).

KEYWORDS: Sensor Node, Base Station, Security, Wireless Sensor Network, Asymmetric Key Cryptography

I.INTRODUCTION

WSNs provide potentially low cost solutions to a variety of real world challenges they are quickly gaining popularity. WSNs are emerging as a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management and security.

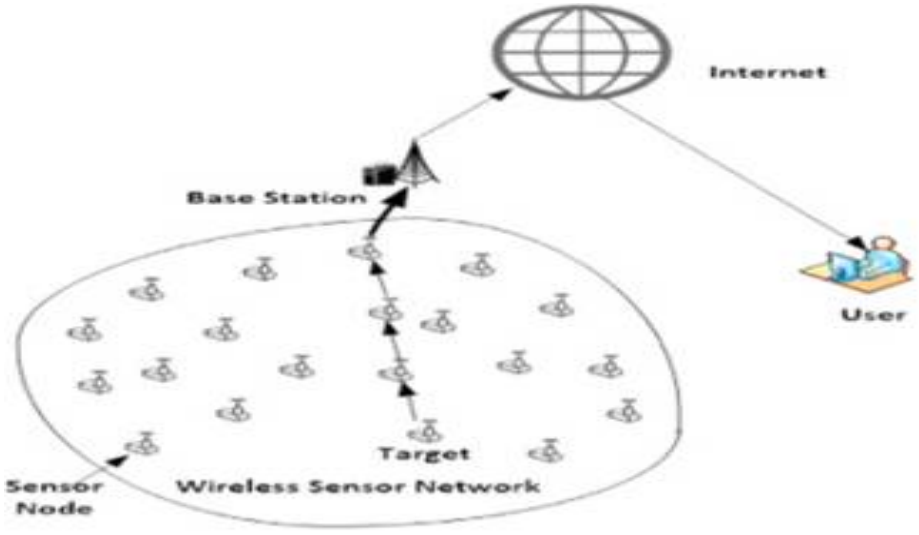

Figure 1: Wireless Sensor Network

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

WSN provide a bridge between the real physical and virtual worlds. Allow the ability to observe the previously unobservable at a fine resolution over large spatio-temporal scales. Have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security. A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

WSN is a wireless network that consists of base stations and numbers of nodes (wireless sensors).Sensors are low powered devices and are capable of observing, measuring and communicating data in the network.These networks are used to monitor physical or environmental conditions like sound, pressure, temperature and co-operatively pass data through the network to a main location as shown in the figure 1.

Limitations of Wireless Sensor Networks:

1. Possess very little storage capacity – a few hundred kilobytes
2. Possess modest processing power-8MHz
3. Works in short communication range – consumes a lot of power
4. Requires minimal energy – constrains protocols
5. Have batteries with a finite life time

Applications of WSN:

- Military applications, such as tracking and environment monitoring surveillance applications use these networks. The sensor nodes from sensor networks are dropped to the field of interest and are remotely controlled by a user. Enemy tracking, security detections are also performed by using these networks.
- Health applications, such as Tracking and monitoring of patients and doctors use these networks.
- The most frequently used wireless sensor networks applications in the field of Transport systems such as monitoring of traffic, dynamic routing management and monitoring of parking lots, etc., use these networks.
- Rapid emergency response, industrial process monitoring, automated building climate control, ecosystem and habitat monitoring, civil structural health monitoring, etc., use these networks.
- Using wireless sensor networks within the agricultural industry are increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pump scan be controlled using wireless I/O devices and water use can be measured.

II.ARCHITECTURE OF SENSOR NODE

A sensor node consisting of five main parts as shown in
Figure 2:

- Sensor
- Memory Storage
- Battery
- Control Unit
- Communication Channel

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

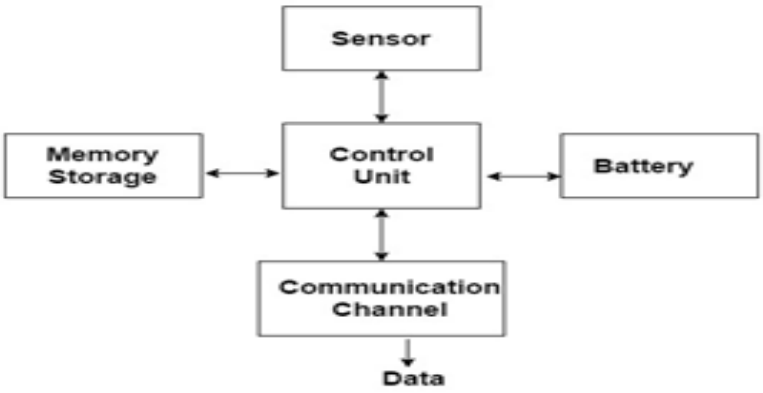

Figure 2: Architecture of Sensor Node

- The task of sensors is to gather information from the environment.
- Battery supplies energy to all parts and the transceiver communicates with the environment.
- The function of control unit which is in the form of microprocessor is to manage the tasks.
- The purpose of memory is to store temporary data or data which is created during processing [1].

III.PROBLEM DEFINITION

Following are some problems regarding security of information in WSN:
Modification: It happens when an unofficial party gains access and mess with the asset. It is a threat to integrity. Example: by amending a value in the packets being broadcast / causing a DOS attack like down pouring the network with sham. It implies some change to the original message and produces an unauthorized effect [2].

Fabrication: It's a threat to integrity and authentication. It happens when an illicit bash pops in forge object into the system. Here an attacker adds wrong data and negotiate the fidelity of the record. Example: adding up of data to a file. WSNs are endangered to security attacks because of the broadcast feature of the communication means and as well as to the assignment of nodes in an unfriendly or dangerous environment [2]

IV.LITERATURE REVIEW

1. AES (Advanced Encryption Standard) algorithm is used as an encryption algorithm to keep the data secure in wireless sensor network. For encryption and decryption of the data during the communication AES -based symmetric key is used that shares the same key. [3]
2. Security mechanism is important in WSN as it provide different levels of security which depends on the resources of sensor network available. Encryption is only way to keep the information secure. Selective encryption of images is an important mechanism to ensure security in network with resource constraint. [4]
3. From this survey we can say that, with the combination of trust factor and fixed path routing to detect malicious activity, simulation results show that proposed method detect malicious nodes efficiently and early, and also with low percentage of false detection.[5]
4. As wireless sensor networks are being used in open field so they need secure communication which involves broadcasting technology. As the hardware technologies are growing rapidly will automatically eliminating the hardware constraint like low processing speed, low memory and battery life time of the sensors may soon be overcome or reduced to facilitate the powerful security measures which are being adopted in this field. [6]
5. Different types of Security attacks, their effects and defense mechanisms in Wireless Sensor Network are vulnerable to security attacks and threats due to its characteristics and limitations. Security attacks are identified and classified from different perspectives based on the attack that occur in network layer. [7]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V.PROPOSED METHODOLOGY

In order to achieve security in wireless sensor network, performing cryptographic operations including encryption, authentication and so on is very important. Due to severe constraints in processing power and supply of energy it becomes difficult to apply data security in some applications because the process of data encryption and decryption consumes a lot of time and power.

Here, Asymmetric Key Cryptography is used to provide security to information which sensor sends to base station. In asymmetric key cryptography, also called public key cryptography, two different keys (which form a key pair) are used. One key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message-not even the original. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties.

RSA is the most widely accepted public-key solution. It solves the problem of key distribution. The approach is that each communicating party processes a key pair, made up of one public key and private key.

To communicate securely over network, all one needs to do is to publish one's public key. All these public keys can then be stored in a database that anyone can consult. However, the private key only remains with the respective individuals.

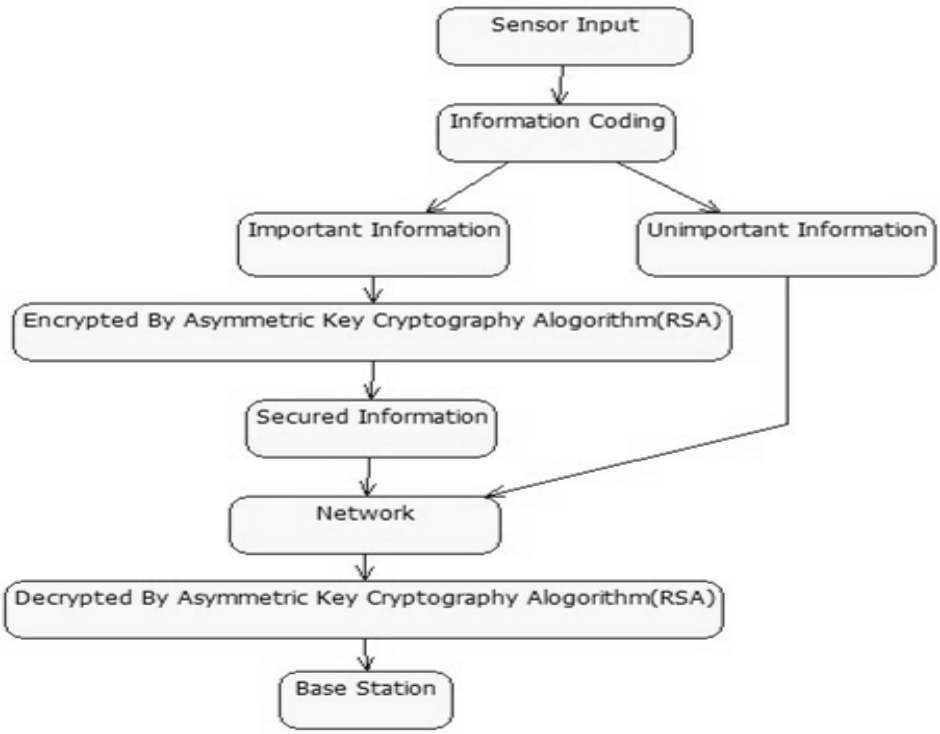

Figure 3: Cryptography Using Asymmetric Key Algorithm (RSA)

Above figure3 shows how the information or message send by the sensor is encrypted and decrypted using Asymmetric Key Cryptography Algorithm (RSA).The working of proposed methodology is described as follows:

i. First, sensor sense the data or information which is the input for the algorithm mentioned above. Then information coding is done.
ii. Input information gets divided into two blocks known as important information and unimportant information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

iii. Only block of important information is encrypted by asymmetric key cryptography algorithm (RSA).Using public key of base station, input block is encrypted.
iv. Now, input block contains secured information. This secured information and block of unimportant information goes to network for transmission.
v. At the side of base station, secured information is decrypted by asymmetric key cryptography algorithm (RSA).Using private key of base station; secured information is decrypted to get original input block of information send by sensor.

VI .LIMITATION

If user loses the private key then received information cannot be decrypted. In the proposed methodology users will have to verify that their public keys truly belong to them.

VII .FUTURE ENHANCEMENT

Although many efforts have been made on key cryptography and defense against attack, some challenges are still need to be addressed. In our proposed methodology future work area is that our technique which is used for securing information should provide authentication for public key.

VIII .CONCLUSION

We have discussed about security problem of information transmitted in wireless sensor network and according to that security solution is provided to do defense against problem. Our security solution does not affect much on processing power and information is also securely transmitted between sensor and base station.

REFERENCES

1. Swati Bartariya,Ashutosh Rastogi"Security in Wireless Sensor Networks: Attacks and Solutions".Vol 5,March 2016
2. Nusrat Fatema ,Remus Brad"Attacks and Counterattacks on Wireless Sensor Networks". Vol. 4,December 2013.
3. Madhumita Panda "Data Security in Wireless Sensor Networks via AES Algorithm", October 2015.
4. Danilo de Oliveira Gonçalves, Daniel G. Costa "A Survey of Image Security in Wireless Sensor Networks", 2015.
5. Prathap U, DeepaShenoy P,Venugopal K R "CMNTS: Catching Malicious Nodes with Trust Support in Wireless Sensor Networks", 2016.
6. P.Brindha, Dr. A.Senthilkumar "Security on Wireless Sensor Networks: A Survey", Vol. 7 (6) , 2016.
7. SuparnaBiswas,SubhajitAdhikari "A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network", Vol.131 , December2015.
8. Atul Kahate"Cryptography and Network Security".

BIOGRAPHY

Prof.Sagar Thakare is a Assistant Professor in Master Of Computer Application Department, College of NCRD's Sterling Institute Of Management Studies,Mumbai University.

Miss.Manjusha Nimbalkar is a Post Graduate student of Master Of Computer Application(MCA), College of NCRD's Sterling Institute Of Management Studies,Mumbai University.

Miss.Richa Nabar is a Post Graduate student of Master Of Computer Application(MCA), College of NCRD's Sterling Institute Of Management Studies,Mumbai University.