Secure Communication Using public Key Cryptography in Wireless Sensor Networks

Anushree R
Dept. of Electronics & Communication
SJB Institute of Technology
Bangalore, Karnataka, India
anurgowda@gmail.com

***Abstract*—Wireless sensor network (WSN) is the network of sensor nodes which are capable of sensing the environment for which they are designed and built and are deployed over a large geographical area which communicates through wireless communication channel. These sensor nodes are used in various applications such as monitoring the health of the buildings, aging of bridges, monitoring natural calamities, movements of enemies in the battle field, providing securities to the personnel in the buildings and so on. The information in this kind of application is very important and need to be secured in wireless network environment. Due to the constraints of sensor nodes like limited capabilities, low processing power, limited battery health, low communication range and the use of insecure wireless communication channel makes security in WSN's a challenging task. In this paper the issues that are related to public key cryptography is discussed. First the brief introduction to wireless sensor network and its security issues and challenges are given, and then the proposed method of public key cryptography in detail is discussed.**

Keywords: Wireless Sensor Networks; public key cryptography

I. INTRODUCTION

A wireless sensor network which is the key research area gaining its popularity due to the advancement of technologies in the field of electronics and wireless communication. Wireless sensor networks consist of thousands of tiny sensor nodes that are scattered across large area. These sensor nodes are application specific and are capable of sensing the specific data and send that data to the base station whenever needed.

WSN's provides solutions to many applications such as monitoring environmental pollution, weather forecast, detecting and tracking the enemy movements and any unusual behavior in the battle field, measuring traffic flows, tracking the location of the person in the building. Many of this application have mission critical task and improper use of these information or using forged information leads to unwanted inaccurate result and hence these data needs to the secured.

While there are some limitations In WSN's:

- Sensor nodes are limited in computation, memory and power resources.
- Sensor nodes are deployed in potentially unsecure environment where the intruder can launch many attacks.
- The topology of the networks changes frequently due to the node failures due to energy constraints.
- Sensor nodes do not have global identification.

Providing security in WSN's requires ensuring confidentiality, authentication, data integrity, nonrepudiation and availability. These differences had a great impact on how secure data transfer schemes are implemented in WSN's. For example it is impossible for the sensor networks to meet the requirements of design complexity and the battery backup in advanced anti jamming techniques such as frequency hopping spread spectrum, physical tamper proofing of nodes.

Further due to the limited battery backup and computation power usage of public key cryptography is made impossible but as of recent studies public key cryptography is made feasible in sensor networks. In security scheme of WSN's proper key distribution should be maintained in order to communicate with the neighboring nodes. Along with key distribution, routing protocols is also needed in order to send the messages from one node to the other in a secured way.

However transferring the secured message from one node to the other node or base station needs authenticated broadcast which is a great challenge. In addition to this, the constraint on battery backup lead to the data aggregation. Since the information transferred needs to be confidential, this is achieved through cryptography. The rest of the paper is organized as follows: Background information on WSN's is presented, followed by different attacks on different layers of sensor networks and then we focus on cryptography, followed by public key cryptography and their further studies and conclusion.

II. BACKGROUND

The WSN's is composed of thousands of sensor nodes which are deployed in a sensor field to collect the data and route it back to the base station. This consists of four units namely: sensing unit, processing unit, transceiver unit and power unit [1]. There are some application oriented components such as position finding system, mobilizer and a power generator and is as shown below in figure1.

The sensing unit again consists of two subcomponents namely a sensor and analog to digital onverter [ADC]. The ADC is responsible for converting analog signal to digital signal. The processing unit consists of a small storage unit which is responsible in making procedures to connect the sensor node with the other nodes. A transceiver unit connects the node to the network. The power unit can be of finite i.e it can be a single one for example single battery or it can be connected in a group example solar cells. Since the sensor routing techniques should have the knowledge of locating the things, there is a need for location finding system.

As a result position finding system serves the above purpose in it . Depending on the application mobilizers are used to move the sensor nodes according to the application. The protocol stack compromising of different layers such as application layer, transport layer,network layer, data link layer, physical and they defined as follows:

- Physical layer: is responsible for the selection of frequency, carrier frequency generation, modulation and data encryption.
- Data link layer: responsible for communicating through point to point or through point to multipoint connections, multiplexing of datastreams, detection of data frames.

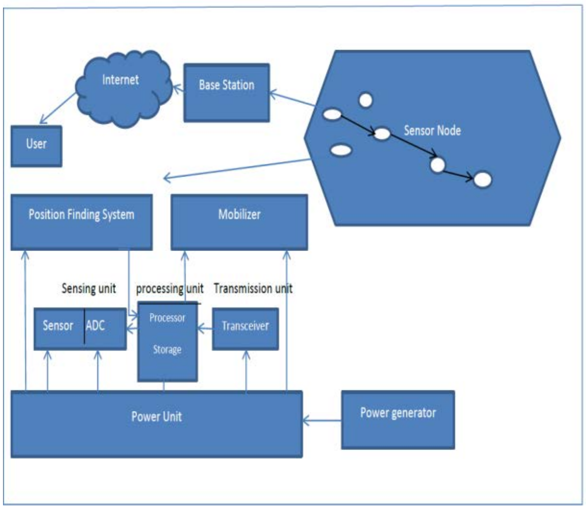

Fig.1: Basic components of Sensor node

- Network layer: is responsible for specifying the packets to their respective addresses.
- Transport layer: is responsible for specifying how packets have to be transported
- Application layer: this is responsible for specifying how the data is requested and provided for the individual sensor nodes and interactions with the end users.

Power management plane manages the power to the sensor node where as the mobility management plane keeps track of the movememt of sensor nodes. The task management balances the task that has been assigned to the sensor to perform particular task[1].

III. CONSTRAINTS IN WSN'S

There some of the few constraints in WSN's they are battery consumption which has again got a subdivision as battery consumption for transducer, battery consumption to communicate between the sensor nodes and the battery consumption for the microprocessor computation. Similarly we have other constraints such as shortage of memory, Transmission range and so on.

A. Security Requirements

Inorder to protect the information or resources from attacks security is required. The security requirements that are included as follows:

- Availabilty, should take care of making the network service available even after the service is denied from it.

- Authorization, which ensures that only the respected sensors should be involved in the particular task .
- Authentication, which ensures the data that is communicated from one node to another node is a valid one.
- Confidentiality, this should ensure that the data communicated should not be undeerstood by the another node.

As a result data or information that has to be communicated through the sensor node has to be secured this is achieved by using a proper cryptographic techniques which will be discussed in detail further.

In WSN's ,if at all a attacker comes to know the security mechanismms that are involved in the sensor network then the there will be hacking of data. Base stations are considered as secured one where routing between the sensor node and the base station needs to be secured.

There are many attacks in sensor networks one among them is the outsider versus insider attacks. The outsider attacks means attack from the nodes that does not belong to that network, where as the insider attack is, the node that belongs to the same network but they behave as if they are unautorised to that. Similarly there are many attacks related to this. Regarding to this there is an denial-of-service [DOS] attacks[2]. This attack usally occurs in any layer of the network. The attacks that are possible in layers are as dicussed below.

B. Physical Layer

As discussed above the physical layer is responsible for the frequency selection, data encryption and so on. Jamming is a kind of attack where the radio frequencies interferes with the nodes of the network that is currently being used. If this attack is strong then this would collapse whole network or else if this is weak attack then, a small subset of the network nodes are affected. However these attacks can be avoided by using a frequency hopping spread spectrum where the signals are transmitted with in the specified frequency bands[3].

Inorder to jam the available frequency the attacker must know the freqency bands used . However if a wide range of frequency band is selected then the attacker can disrupt the entire network nodes. The other attack that is possible with the physical layer is tampering where in which the sensitive data can be tampered as a result the nodes of the network must be tampered proof in order to avoid this attack in the layer.

C. Data Link Layer

The data link layer is responsible for multiplexing of data, frame detection, and so on. There are some categories of of attacks that occur in link layer they are as follows:

a) Collision: it the is suitation where two nodes try communicate at the same frequency range. As a result there will be collision of the two nodes and the data will be mismatched in the packets[1] . Therefore leading to the transmission of invalid data. There are some defense method to over come this collision one is by introducing a error correcting codes whcich the data to be transmitted to longer.

b) Exhaustion: When the collided data is transmitted repeatedly by the attacker causing the data to get exhausted in the link layer. One solution to this attack is by using time division multiplexing , each will be allotted with a specific time slots and the respective nodes are made to transmitt at that time.

D. Networking And Routing Layer

Since these layers are designed mainly for the power efficiency needs. The attacks that are going to occur in these layers are:

a) Spoofed, Altered or Replayed Routing Information: The significant attack in routing layer is spoofying or altering or replaying the information from routing protocols . The attacker directly attacks the routing information which is going to get routed through the neighbouring nodes[4]. This can be overcome by introducing a message authentication code after the message, so that the reciever can receive the data and check whether the data is spoofed or not.

b) Selective Forwarding : In this attack network will route all the messages but the attacker will drop some of the messages in between as a result there will be loss of data. Inorder to avoid this multiple path are created and the data is sent through it[4].

c) Sinkhole: In this type of attack the attacker will make the one of the node as attractive so that the neighbouring node gets attracted to that. As a result the data will flow through this compromised node instead of the actual node[4].

d) Sybil: In this attack one will have more than one identity in a network , as a result there will be mislead of nodes

[5]. However this can be defensed by employing a fault tolerant schemes in the network.

e) Wormholes: A wormhole is a low latency link between the two layers. This link is made by either a single node that is sending messages or by srrounding nodes or either by the non neighbouring nodes[5].

f) Hello Flood Attacks: In this attack the protocols that uses hello packets will be sent this will lead to the assumption that the packet sender is with in the radio range. But the attacker can choose a vast area for transmission by using a high powered transmitter which results in broadcasting a false superior node to the network which may be out of radio range[4].

g) Acknowledgement Spoofing: While routing messages ,some of the nodes require acknowledgement after reciving the packets . But here the attacker will make sure that the acknowledgement will not reach the node there by giving a false assumption to the nodes[4].

E. Transport Layer

This layer is responsible for the end to end connections. The possible attacks that could occur in this layer are flooding and desynchronisation.

Flooding: In this protocol it is required to maintain the state in both end ponit connections which becomes difficult to maintain the memory capacity leading to the exhaustion of the memory called as flooding [4]. There are many solutions to overcome this attack.

Desynchronisation: In this kind of attack , the attacker will lead to the disconnection of the nodes. Consider an example where in which the attacker will repeatedly spoof the messages in to the end point. As a result this will lead to the retransmission of the messages[5]. There exsists a solution to this problem that is by providing authentication to the packets that is communicating between the hosts.

The table1 below gives the brief idea of various possible atacks in the different networks

Layer	**Attacks**	**Solutions**
Physical	Jamming Tampering	Spread spectrum TamperProofing
Link	Collision Exhaustion Unfairness	Error correcting codes Rate limitation Small frames
Network and Routing	Spoofing Selective forwarding Sinkhole Sybil Wormholes Hello Floods spoofing	Authentication Redundancy Monitoring Probing Authentication Authentication Authentication
Transport	Flooding Desynchronisation	Client puzzles Authentication

Table.1 Different attacks and its solutioms related to the respective layer

IV. Cryptography

Cryptography is used for maintaing security of the data that is routed to the sensor networks . These cryptographic techniques should meet all requirements of the WSN's and it should have proper code size, battery consumption and so on. Due to the increased communication of messages through the channels there is a need for maintaing the security of those messages. As a result proper cryptography techniques should be used to ensure secured transmission. Here the communicating parties will be allocated with keys to communicate between them. But however these keys needs to transmitted to them well in prior to the conversation . As a result these keys has to be sent through couriers or mail which results again in the delay[6,7].

There are two approaches to transmitt a key over public channels without compromising the security of the systems. In public key cryptography encryption and decryption are done by using separate keys .The encryption key E can be declared publicly such that each user of that network announces his key in a public directory. As a result any user can send message to any user of the network but the user who knows the decryption key can only receive the message and can decrypt it. Therefore each one sends the message to the recievers by using a encrypted key and the recievers decrypt the message by using a decryption key[6].

The two problems that is probably going to occur in the public key cryptography is authentication and the other is communication of secret encryption key to the communicating party. In order to overcome these problems this paper suggests a method where a authentication and communication of secret key is maintained.

V. Proposed Method

First consider the sensor node network where the sensor nodes are placed in it. Here place the nodes, that have high processing power, high computational power along with high energy in it. Once this nodes are placed ,the nodes that are imparted in to the network will try to form a cluster with the neighbouring nodes. Once this is formed the node that is having the shortest range from the base station will act as a rendezvous point. The following figure2 will demonstrate it.

R = Rendezvous point

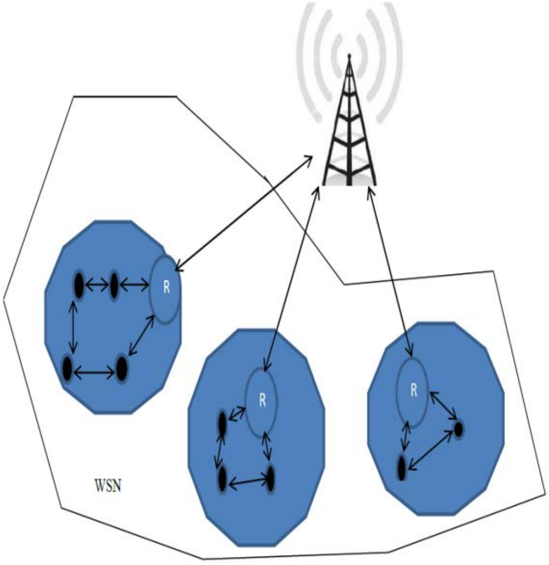

Figure2: illustration of Rendezvous point and base station

This shortest path is found by using a shortest path algorithm. Once the parent node is selected this will be responsible for communicating a secret key between the base station and the communicating node. As a result, problem of communicating a secret key is achieved by using a rendezvous point. This rendevous point will now send a hello message to all the other nodes. Now these nodes will respond by sending their identity to this rendevous point. Once this is done the node say for example node A [N_a]needs to communicate data with the base station, then it will send a message called as base connect [Basecon] to the rendezvous point by using the public key of rendezvous point [P $_u$] to communicate the data. The rendezvous point now will encrypt the data by using the public key of N_a by developing a secret key called as [k_s] which is allocated with a particular time slot using time division spread spectrum. The encryption algorithm that is going to be used is "Elliptic curve cryptography". As a result now the rendezvous point is having the encrypetd data along with the secret key which will be sent to the base station. Now the base station will start decrypting by using its private key [p_b] with in that particular alloted time slot otherwise the data will be lost once the time exceeds no other nodes or base station can access this data. This how the confidentiality and authentication is achieved in this paper . The figure3 will demonstrate it.

P_U = Public key of rendezvous point

P_A = public key of node A

K_S = Secret key

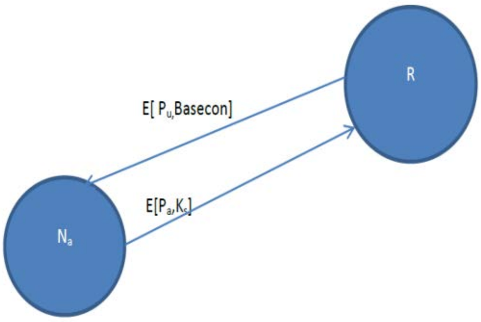

Figure3: Illustration of confidentiality of data transmission

Therefore the authentication function that happens in the proposed system is as shown in figure 4;

M=Message

E= Encryption

//= Concatenate

D= Decryption

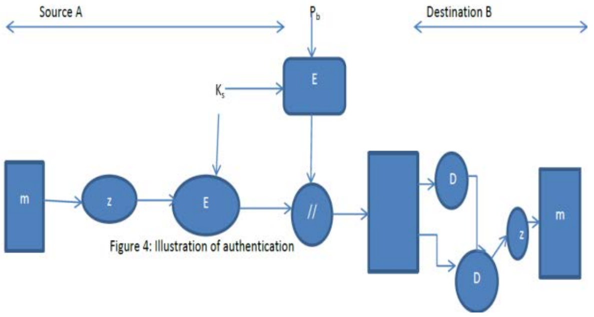

Figure 4: Illustration of authentication

Conclusion

In public key cryptography authentication and maintaing the confidentiality is a challenging task. Various methods are proposed to overcome this problem and they have been achieved to some extent.The proposed system will maintain the confidentiality and authentication of the data that has to be transmitted secertly still better than the exsisting one.But employing this system will take lot of battery life for maintaing the confidentiality of the data . Because first it has to search for the rendezvous point and then it has to communicate a secret key to the requesting node which will consume lot of battery life to that.

References

[1] F. Akyildiz et al., “A Survey on Sensor Setworks,” IEEE Commun. Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.

[2] E. Shi and A. Perrig, “Designing Secure Sensor Networks,” Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.

[3] Hilal Houssain, Mohamad Badra Turki F. Al-Somani, Senior Member, IEEE, “Power Analysis Attacks on ECC: A Major Security Threat”,

[4] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. First IEEE Int'l.

[5] J. Newsome et al., “The Sybil Attack in Sensor Networks: Analysis and Defenses,” IPSN '04: Proc. IEEE Int'l. Conf. Info. Processing in Sensor Networks, Apr. 2004

[6] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Trans. Info. Theory, vol. 22, no. 6, Nov. 1976, pp. 644–54.

[7] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Commun. ACM, vol. 26, no. 1, 1983, pp. 96–99.

[8] “Network Security Essentials applications and standards” William Stallings Fourth edition

[9] G. Gaubatz, J.-P. Kaps, and B. Sunar, “Public Key Cryptography in Sensor Networks-Revisited,” ESAS ’04: 1st European Wksp. Security in Ad-Hoc and Sensor Networks, 2004.

[10] M. O. Rabin, “Digitalized Signatures and Public-Key Functions as Intractable as Factorization,” Tech. Rep., Cambridge, MA, 1979.

[11] J. Hoffstein, J. Pipher, and J. H. Silverman, “Ntru: A Ring- Based Public Key Cryptosystem,” ANTS-III: Proc. 3rd Int'l. Symp. Algorithmic Number Theory, London: Springer-Verlag, 1998, pp. 267–88.

[12] V. S. Miller, “Use of Elliptic Curves in Cryptography,” Lecture notes in computer sciences; 218 on Advances in Cryptology-CRYPTO 85, New York: Springer-Verlag, 1986, pp. 417–26.

[13] N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, vol. 48, 1987, pp. 203–09.