Attacks & Cryptographic Measures For Wireless Sensor Network

Pinak Popat[1], Prof. Chirag Gohel[2]
[1]Post Graduate Student, Marwadi Education Foundation Group Of institutions, Rajkot, Gujarat
[2]Assistant Professor, Marwadi Education Foundation Group Of institutions, Rajkot, Gujarat.

Abstract

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Many algorithms are already developed for security in wireless sensor network but with many limitation .For instance key maintenance is a great problem faced in private key encryption methods and less security level is a problem of public key encryption methods even though key maintenance is easy .So by combining both the key exchange method both the problem can be solved.

1. Introduction

All manuscripts must be in English. These guidelines include complete descriptions of the fonts, spacing, and related information for producing your proceedings manuscripts.

Wireless sensor networks are the combinations of micro sensors which communicate with each other using wireless communication. A wireless sensor network is a distributed network of resource-constrained and wireless devices called sensor nodes. Each sensor node monitors some physical phenomenon (e.g., humidity, temperature, pressure, light) inside the area of deployment. The collected measurements are sent to a base station. The communication range of sensor nodes is limited to tens of meters and hence not all of them

***Some basic features of sensor networks are*:**

-Self-organization-Short-range broadcast communication and multi-hop routing
-Dense deployment and cooperative sensors
-Frequently changing topology, due to fading and node failures
-Limitations in computational resources, such as energy and memory[2]

2.Wireless Sensor Networks

Wireless sensor networks(WSN)[2],[3] ,[9]allows monitoring of natural and man-made environments to great level of granularity. This macroscopically view is achieved by placing 100's to 1000's of small wireless sensor nodes or motes, in the target area to sense fields and forces. For this, each sensor node contains sensors, limited data processing capabilities, data and energy storage, and a wireless transceiver enabling them to form a network and work together. In order to deploy in mass the sensor nodes must be expendable ,easy to deploy and use ,inexpensive and maintain.
These features make WSN very flexible and open for wide range of applications. An overview of the history of sensor networks is given in [4]. Wireless sensor networks were started in the military with sensor nodes. The first reported deployments of small, pager sized nodes were [5] for environmental monitoring and [6] for air pollution monitoring. There are also many military applications like target tracking, detecting radiation [7], biological.

3.SECURITY ISSUES IN WSN

3.1Security Requirements

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSNs include:
-Availability:-which ensures that the desired network services are available even in the presence of denial-of-service attacks
-Authorization:-which checks that only authorized sensors can be involved in providing information to network services
-Authentication:-which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network

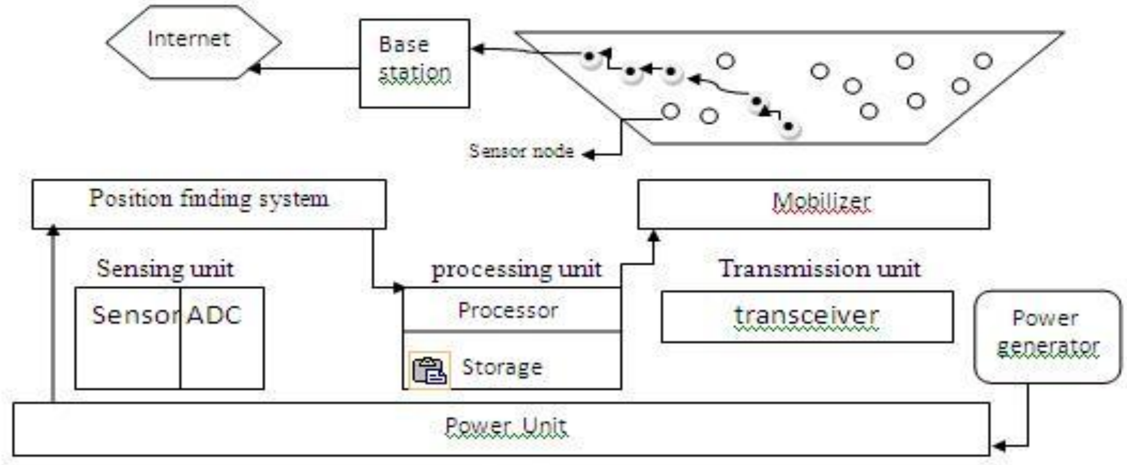


Fig: Architecture of sensor node

-Confidentiality:-which ensures that a given message cannot be understood by anyone other than the desired recipients
-Integrity:-which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
-Nonrepudiation,:-which denotes that a node cannot deny sending a message it has previously sent Freshness, which implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:

-*Forward secrecy*: a sensor should not be able to read any future messages after it leaves the network.
-*Backward secrecy*: a joining sensor should not be able to read any previously transmitted message.

3.2 Security Threats

WSN have unique challenges and because of this traditional security threats that all the other wireless network face cannot assumed for WSN. There are many papers as that presents the significant security problems. Here we will try to summarize all the existing threats and point out the major attacks against a WSN.

4.Attacks on WSNs can be classified from two different levels of views:-

1. Attack against security mechanisms[2]
2. Attack against basic mechanisms (like routing mechanisms).

4.1 Denial of Service (DoS)

It occurs by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents network users from accessing services or resources to which they are registered. DoS attack is meant not only for the hacker's attempt to subvert, disrupt, or destroy a network, but also for any event that destroys a networks capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by flooding and desynchronization.

4.2The Wormhole attack

One node in the network (sender) sends a message to the another node in the network (receiver node).Then the receiving node attempts to send the message to its neighbors. The neighboring nodes think the message was sent from the sender node (which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away. Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighboring information . Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

4.3 The Sybil attack

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network. The incorrect information can be a variety of things, including position of nodes, signal strengths, making up nodes that do not exist. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. An insider will surely participate in the network as it cannot be prevented, but he can only do this by using the identity of compromised node . Public key cryptography is use for preventing such an insider attack, but it is very expensive to be used in the sensor networks.

4.4 Selective Forwarding attack

It is a situation when certain nodes do not forward many of the messages they receive. The sensor networks depend on repeated forwarding by broadcast for messages to propagate throughout the network.

4.5 Sinkhole attacks

In a sinkhole attack, the attacker will try to attract nearly all the traffic from a particular area through a compromised node, creating a allegorical sinkhole by keeping attacker at the Centre. Sinkhole attacks the network by making a compromised node look very attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop-class attacker has a very high frequency power radio transmitter that provide a high-quality route to reach a wide area of the network by transmitting with enough power.

4.6 Passive Information Gathering

An intruder with the help of well-designed antenna and powerful receiver can easily pick off the data stream. Interception of the messages which has the knowledge of the locations of sensor nodes allows an intruder to locate the nodes and destroy them. Besides the locations of sensor nodes, an attacker can observe the application specific content all the messages including message IDs, timestamps and other fields.

4.7 Node Capturing

An adversary captures a node and gets all the information stored in it.

4.8 False or Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network.

4.9 Hello flood attacks

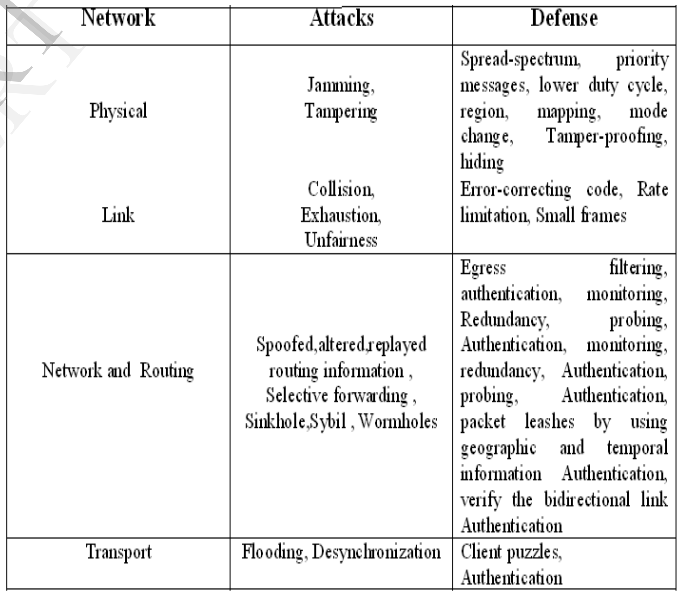
The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent. All messages now need to be routed multi-hop to this parent, which increases delay.

5. Security concern in WSN

Overview of security issues for wireless sensor networks can be found in [9].as shown in table.

6 Defensive mechanisms in WSN

Currently, research on WSNs provides security solutions has focused mainly in three categories:
1) Key management: A lot of work has been done in establishing cryptographic keys between nodes to enable encryption and authentication
2) Authentication and Secure Routing: Some of the protocols are developed for securing information from being hacked by hacker and guarantee its integral delivery to the base station.



Network	Attacks	Defense
Physical	Jamming, Tampering	Spread-spectrum, priority messages, lower duty cycle, region, mapping, mode change, Tamper-proofing, hiding
Link	Collision, Exhaustion, Unfairness	Error-correcting code, Rate limitation, Small frames
Network and Routing	Spoofed,altered,replayed routing information , Selective forwarding , Sinkhole,Sybil , Wormholes	Egress filtering, authentication, monitoring, Redundancy, probing, Authentication, monitoring, redundancy, Authentication, probing, Authentication, packet leashes by using geographic and temporal information Authentication, verify the bidirectional link Authentication
Transport	Flooding, Desynchronization	Client puzzles, Authentication

TABLE: Attacks and Defense

3) Secure services: Certain progress has been made in providing specialized secure services, like secure localization, secure aggregation and secure time synchronization

7. Different cryptographic Algorithm for wireless sensor network

There are various method for cryptography it mainly divided into two parts

1)Symmetric key (private key)
2) Asymmetric key(public key)

7.1 Symmetric key :-

It uses the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption but it requires less computation then public key algorithm[9] .

7.2 Asymmetric key :-

It has two separate keys, one of which is secret and one of which is public. Both key are different but both keys pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions. One of these keys is published or public, while the other is kept private. Here the computation power is more than symmetric key [9].and key management is better than symmetric key

8. Study of symmetric key algorithms [12][13][14]

There are number of asymmetric algorithms but from all of them i have referred few of the basic algorithm like DES/3DES,AES,IDEA,RC5 ,RC6

8.1DES (Data Encryption Standard)

DES is block cipher. A block cipher is a function which helps in doing a bit mapping between plaintext blocks and cipher-text blocks; is called the block length. It consider as a simple substitution cipher with large character size. The function is parameterized by a bit key, taking values from a subset (the key space) of the set of all -bit vectors. It is assumed that the random key is chosen. Use of plaintext and cipher text blocks of equal size avoids data expansion. To allow unique decryption, the encryption function must be one-to-one (i.e., invert- idle).

8.2 3DES

The triple-DES ciphers use three iterations of DES
The three-key variant is defined by
3DES3(K1k2 k K3; M) = DES(K3;DES¡1(K2;DES(K1;M)) ;

DES weakness

-It uses the same key for encryption and decryption so if the key is hacked once all information would to lost and it would not be secure

-Short key length

8.3 Advanced Encryption Standard (AES)

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an hacker knows the plaintext and the cipher text. The AES algorithms are designed to use one of three key sizes (N_k). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secure thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

Strengths:

-AES is extremely fast compared to other block ciphers.
-AES was designed to be used with pipelining.
-The cipher does not use arithmetic operations
-AES is fully self-supporting. Does not use SBoxes of other ciphers, bits from Rand tables, digits of π or any other such jokes. (Their quote, not mine)
-AES is not based on not well understood processes.
-The tight cipher and simple design does not allow to hack.

Limitations:

-The inverse cipher is less suited to smart cards, as it takes more codes and cycles.
-The cipher and inverse cipher make use of different codes and/or tables.
-In hardware, The inverse cipher can only partially re-use circuitry which implements the cipher.

Study of asymmetric algorithms[12][14]

There are number of asymmetric algorithms but from all of them i have referred few of the basic algorithm like RSA and ECC.

9.Study of asymmetric key algorithms

9.1 RSA (Ronald Rivest, Adi Shamir and Leonard Adleman)

For encryption, the sender uses RSA modulus N and the encryption key (or encryption exponent), which is denoted by e. This pair of values is known as the public key pair i.e. (N, e). The receiver uses the private key pair (N, d) which consist of the same RSA modulus N and decryption key (or decryption exponent) d for decrypting the message.

Only the planned recipient would be able to know the value of the private key and can therefore by using that key they can decrypt the message. Public key cryptographic systems have many advantages over private key systems, one of the often advantage is it uses the same encryption key as the decryption key. This means that the sender only have to send key securely to the planned recipient. Often it is also required that two functions are used, one to encrypt and one to decrypt.

9.2 ECC(Elliptic curve cryptography)[1]

This algorithm is mainly depend on the algebraic structure of elliptic curves.The diffuclty in problem is ,the size of the elliptic curve. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements—i.e., that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key—e.g., a 256bit ECC public key should provide comparable security to a 3072bit RSA public key (see #Key sizes).For current cryptographic purposes, an *elliptic curve* is a plane curve which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b,$$

9.3 Hybrid Algorithms for wireless sensor network

Hybrid algorithms are the combination of symmetric key and asymmetric key algorithm. The need to develop this type of algorithm is because of the disadvantage of both algorithm.

Symmetric key algorithm has a disadvantage of key distribution[9] and asymmetric algorithm need much computation so the power of the sensor is wasted in it[9] and it is not feasible to use as power is wasted then sensor will be of no use

Thus the algorithm which combines both the algorithm i.e asymmetric and symmetric so the advantages of both the algorithm can be utilized in it.

Some of the hydrid algorithm like DHA+ECC[16] is described in detail.

10. Conclusion

It has aimed to give an overview of recent progress in wireless sensor network. At first, the working of sensor is described with a sensor architecture and then all the security issue is described in detail with an example. Then I focused on the cryptographic method of sensor network and many methods are described with advantages and disadvantages. Then need of hybrid algorithm is discuss and combination of asymmetric and symmetric method is given by which the advantage of both the algorithm is achieved.

11. References

[1]KRISTIN LAUTER, MICROSOFT CORPORATION , "THE ADVANTAGES OF ELLIPTIC CURVE CRYPTOGRAPHY FOR WIRELESS SECURITY" IEEE Wireless Communications ,Vol 3,pp 22-25, February 2004

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong: "Security in Wireless Sensor Networks: Issues and Challenges" ISBN, 89-5519-129-4,pp 25-32,ICACT2006

[3] Gowrishankar.S 1, T.G.Basavaraju 2, Manjaiah D.H 3, Subir Kumar Sarkar "Issues in Wireless Sensor Networks" Proceedings of the World Congress on Engineering 2008 Vol I
WCE 2008,pp 56-64, July 2 - 4, 2008, London, U.K.

[4] Chee-Yee Chong and P. Kumar, Srikanta."Sensor networks: Evolution,opportunities, and challenges". Proceedings of the IEEE VOL. 91, NO. 8,pp 241-248 AUGUST 2003.

[5] K.Martinez, J.K. Hart, and R. Ong." Environmental sensor networks". World Congress on Engineering 2008 Vol I WCE 2008,pp 56-64 Aug 2004

[6] Kavi K. Khedo1, Rajiv Perseedoss2 and Avinash Mungur" A Wireless sensor network Air pollution monitoring System", International Conference of wireless and mobile network, Vol2,No2,pp 2000-2014,2010

[7] S.M. Brennan, A.M. Mielke, D.C. Torney, and A.B. Maccabe. "Radiation detec-tion with distributed sensor networks".IEEE VOL. 20, NO. 8,pp 57–59, Aug 2004.

[8] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. SPINS: "security protocols for sensor networks". Wireless Networks, 8(5), pp 521–534, Sep 2002.

[9] Yong Wang, Garhan Attebury, Byrav Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials •,pp223-237 2nd Quarter 2006

[10] Adrian Perrig, John Stankovic, and David Wagner. "Security in wireless sensor networks .Commun". ACM, 47(6),pp53–57, Jun 2004.

[11] Fei Hu and Neeraj K. Sharma. "Security considerations in ad hoc sensor networks." Ad Hoc Networks, vol3,pp 69–89, Jan 2005.

[12]http://csrc.nist.gov/publications/fips/fips81/fips81.html

[13]Handbook of Applied Cryptography, by A. Menezes, P. van
Oorschot, and S. Vanstone, CRC Press, 1996.

[14]Lecture Notes on Cryptography by Shafi
Goldwasser1 Mihir Bellare2

[15]KRISTINLAUTER, MICROSOFT
CORPORATION , "THE ADVANTAGES OF
ELLIPTIC CURVE CRYPTOGRAPHY FOR
WIRELESS SECURITY" IEEE Wireless
Communications , Vol 3,pp 22-25, February 2004

[16] Mohd. Rizwan beg1 and Shish Ahmad "ENERGY EFFICIENT PKI SECURE KEY MANAGEMENT TECHNIQUE IN WIRELESS SENSOR NETWORK USING DHA & ECC" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.1, pp 256- 262,February 2012