ISSN : 2231-0711

Detail and Comparative Study on WSN Security Architectures

[1]E.Parthasarathi,[2]A.R.Bharathidasan,[3]S.Pavithra

[1, 2] M.E Student, [3]Assistant Professor
[1, 2, 3] Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College,
Avadi, Tamilnadu, India

Abstract-Wireless sensor network (WSN) most widely growing technologyin network due to this WSN well known technology among the research community people. WSN having enormous sensing devices to sensing thenecessary information from current environmental scenario and transmit it to particular place or user. In WSN transmitting the obtained data has lot of security constraints i.e.) lot of security issues in transmission.In this paper we are going to analyses the security constraints need for transmission and mechanismsavailable to satisfy the security constraints.

Keywords: Wireless Sensor Networks (WSN),Data security, Survey, Cryptography.

1.INTRODUCTION

Wireless sensor network (WSN) plays major role in industries and patient monitoring systems. WSN currently evolving in military field to detect the enemy troops and in agriculture to collect the details of paddy field, temperature, natural disasters etc.The need for security in WSNs is evident, especially in health care, security, and militaryapplications. Most of the applications relay data that contain private or confidentialinformation.In military scenario the sensor devices are deployed in hostile environment so there is a chance intruder can attack the data. Security is main concern to avoid attacks on confidential data.

Cryptography offers the security to WSN.Cryptography is a method to provide security algorithms to ensure security every point of the network.

Cryptography can be explained in the following aspects:

- ➢ Symmetric,
- ➢ Asymmetric,
- ➢ Hash.

Symmetric Key Cryptography algorithm:

In a Symmetric key algorithm both sender and receiver share the single common secret key for encryption and decryption. Symmetric key mechanisms are simpler and faster. Symmetric key cryptography also called secret key cryptography. Most famous algorithm for symmetric key cryptography is DES(Data Encryption Standard),AES(Advanced Encryption Standard),SPINS,TinySec,LEAP.

Asymmetric Key Cryptography algorithm:

Asymmetric algorithms (public key algorithms) use different keys for encryption and decryption, and the decryption key cannot (practically) be derived from the encryption key. Asymmetric algorithms are important because they can be used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private.

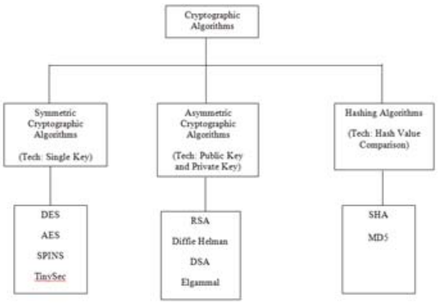
Types of asymmetric algorithms (Public key Algorithm):

RSA,DiffieHelman DSA(Digital Signature Algorithm ,Elgammal XTR.

HASH Function:

Hashes Plays a role in cryptography, they are used to ensure that the messages have not been tampered with. In hash Sender and receiver generates the hash function separately for encryption and decryption later the hash values compared to verify the message is tampered or not.

The most famous hash algorithms are SHA(Secure Hash Algorithm),MD5(Message Digest),etc.


Cryptographic Algorithms
Symmetric Cryptographic Algorithms
(Tech: Single Key)
Asymmetric Cryptographic Algorithms
(Tech: Public Key and Private Key)
Hashing Algorithms
(Tech: Hash Value Comparison)
DES
AES
SPINS
TinySec
RSA
Diffie Helman
DSA
Elgammal
SHA
MD5

The cryptography algorithms are designed based on lower memory and power consumption to increase the network lifetime.So the designer should consider the fore said parameters in their concern before developing algorithms, it is quite complicate to the designer to develop the algorithms with above parameters.

Securing the WSN, the cryptography mechanism must satisfy the following security properties:

- ➢ Confidentiality,
- ➢ Integrity,
- ➢ Authentication and Authorization
- ➢ Availability.

2.SECURITY PROPERTIES

2.1. CONFIDENTIALITY:

The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. In a WSN, the issue of confidentiality should address the following requirements

(i) A sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so,

(ii) Key distribution mechanism should be extremely robust,

(iii) Public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

2.2. INTEGRITY:

The mechanism to ensure that messages are not modified by an entity as it traverses from the sender to the recipient. Different types of mechanisms available for researchers to achieve this goal. While some mechanisms make use of additional communication among nodes, others propose use of a central access control system to ensure successful delivery of every message to its recipient.

2.3.AUTHENTICATION AND AUTHORIZATION:

*Authentication***:**

The process of ensuring the user identity based on the Username and password.

Authorization:

The Process of giving the individuals access to system objects based on their identity

2.4.AVAILABILITY:

This requirements ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service attack (DoS).

3.SECURITY ARCHITECTURE

3.1.TINYSEC :

In 2004 Tinysec introduced by Karlof et al.[8] It is a lightweight, generic security package that developers can easily integrate into sensor network applications. It is the first fully-implemented protocol for link-layer cryptography in sensor networks. The implementation of TinySec is incorporated into the official TinyOS[1] release. Inherently, it provides similar services, including access control, message integrity and confidentiality. Access control and integrity are ensured through authentication, and confidentiality through encryption TinySec allows for two specific variants. The first of these, TinySec-Auth, provides for authentication only, and the second, TinySec-AE, provides both authentication and encryption.

	Encryption	Block Cipher	Freshness (CTR)	Code Requirement	Auth. Provided	Release Year
TINYSEC	CBC Mode	Skipjack	No	7146 Bytes Max	CBC-MAC	2004

TinySec-Auth, the entire packet is authenticated using a MAC, but the payload data is not encrypted; whilst using authenticated encryption, TinySec encrypts the payload and then authenticates the packet with a MAC.

3.2.SECURITY MANAGER:

Heo and Hong proposed a new method of authenticated key agreement [10]. It is based on a Public Key Infrastructure (PKI) and Elliptic Curve Cryptography (ECC). The Security Manager (SM) gives static domain parameters such as the base point and elliptic curve coefficients to prospective network nodes. Devices use these initial parameters to establish are in turn used for securing the network data. After calculating a public key, a node sends this to the SM, which could have a public key list for all nodes in the network. Authenticated key agreement is achieved via the SM, based on the EC-MQV[5] algorithm. This algorithm is more advanced than Diffie-Hellman, eliminating the man-in-the-middle attack. Diffie-Hellman is included in the EC-MQV algorithm as a subset.

	Encryption	Block Cipher	Freshness (CTR)	Code Requirement	Auth. Provided	Release Year
SM	ECC	N/A	No	N/A	EC-MQV	2006

3.3.ZIGBEE:

As previously stated, the ZigBee specification outlines the design of the NWK[5] layer that operates just above the PHY and MAC layers specified by the IEEE802.15.4 standard. The concept of a “Trust Center” is introduced in the specification. Generally, the ZigBee coordinator performs this duty. The coordinator allows other devices to join the network and distributes the appropriate keying information. There are three roles played by the “Trust Center”.

- Trust manager, whereby authentication of devices requesting to join the network is carried out.
- Network manager, maintaining and distributing network keys, and
- Configuration manager, enabling end-to-end security between devices .

There are two modes of operation:

- Residential Mode
- Commercial Mode.

In Residential Mode, the Trust Center will allow devices to join the network, but does not establish keys with the network devices. It therefore cannot periodically update keys and allows for the memory cost to be minimal, as it cannot scale with the size of the network.

In Commercial Mode, it establishes and maintains keys and freshness counters with every device in the network, allowing centralized control and update of keys. This results in a memory cost that could scale with the size of the network. This could be managed through means clustering, for example.

There are three types of keys specified for use in ZigBee security services; the Master Key, the Link Key and the Network Key.

Master keys are installed first, either in the factory or out of band. They are sent from the Trust Center and are the basis for long-term security between two devices.

The Link Key is a basis of security between two devices.

The Network Keys are the basis of security across the entire network.

This operation occurs only in Commercial Mode, as Residential Mode does not allow for authentication.

The ZigBee specification states that CCM*[5] mode of operation is used for security services. CCM*[5] is a generic combined encryption and authentication block cipher mode. This mode of operation is detailed in the ZigBee specification, and is a combination of CTR mode and CBC-MAC mode. It differs only slightly from CCM mode[9], by offering encryption-only and integrity-only capabilities. There are underlying levels of security supported by this architecture, and can be varied depending on the amount and type of security the data is required to maintain

In Zigbee only parties that possess the symmetric key should be able to compute the MAC. The MAC protects packet headers in addition to the data payload. The sender appends the plaintext data with a MAC. The recipient can verify the MAC by computing the MAC and comparing it with the value received in the packet. Initially, CCM*[5] mode applies integrity protection over the header and data payload using CBC-MAC, and then encrypts the data payload and MAC using AES-CTR mode. In this way, AES-CCM includes the fields from both the authentication and encryption operations (a MAC and the frame and key counters), which serve the same functions as described[7].

	Encryption	Block Cipher	Freshness (CTR)	Code Requirement	Auth. Provided	Release Year
ZigBee	AES	AES-128	Yes – CCM*	N/A	CBC-MAC	2005

4.COMPARISON TABLE

	Encryption	Block Cipher	Freshness (CTR)	Code Requirement	Auth. Provided	Release Year
Tinysec	CBC	Skipjack	No	7146 Bytes Max	CBC-MAC	2004
SM	ECC	N/A	No	N/A	WC-MQV	2006
ZigBee	AES	AES-128	Yes – CCM*	N/A	CBC-MAC	2005

5.CONCLUSION

In table the year of release for each of this architecture mentioned. The year is notify progression in the field, and suggests that it will continue for years to come. From a design perspective, scalability of security architectures is a desirable feature. For an authentication purpose, the CBC-MAC algorithm is the most popular method of providing authentication for symmetric key based algorithms. Due to the popularity of the use of CBC-MAC to provide authentication in the security architectures of WSNs. AES algorithm's implementation on different platforms confirmed its superior performance from the small memory of the controller 8-bit to 32-bit processor. In this paper methodologies used in the architecture are analyzed. In WSN all applications will not require the same security, and even in applications that do, different types of messages will require different degrees of security. IEEE 802.15.4/ZigBee security architecture has this salient feature. The security is going to play a major role in wireless sensor networks, and therefore will continue research on security in Wireless Sensor Networks make the sense.

REFERRENCES

[1] Gaurav Sharmaa Suman Balaa, Anil K. Verma," Security Frameworks for Wireless Sensor Networks-Review", 2nd International Conference on Communication, Computing & Security,2012

[2] Qingzhang CHEN, Zhongzhe TANG, Yidong LI, Yibo NIU, Jianhua MO," Research on Encryption Algorithm of Data Security for Wireless Sensor Network", Journal of Computational Information Systems 7:2 (2011) 369-376.

[3] Linciya.T1 and Anandkumar. K.M,"ENHANCED THREE TIER SECURITY ARCHITECTURE FOR WSN AGAINST MOBILE SINK REPLICATION ATTACKS USING MUTUAL AUTHENTICATION SCHEME" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 2, April 2013

[4] INFORMATION PROCESSING AND ROUTING IN WIRELESS SENSOR NETWORKS http://www.worldscibooks.com/compsci/6288.html"

[5] David Boyle, Thomas Newe,"Securing Wireless Sensor Networks: Security Architectures" JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008

[6] ZigBee Alliance (2006) *ZigBee Security Specification Overview* [online], available: http://www.zigbee.org/en/events/documents/december2005_open_house_presentations/zigbee_security_layer_technical_overview.pdf [Accessed 7 Dec 2007].

[7] Hyubgun Lee Kyounghwa Lee Yongtae Shin," AES Implementation and Performance Evaluation on 8-bit Microcontrollers", *International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009.*

[8] Karlof, C., Sastry, N., Wagner, D. (2004) 'TinySec: A Link Layer Security Architecture for Wireless Sensor Networks', Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 03 – 05 November 2004, New York, NY, USA: ACM Press, 162 – 175.

[9] D. Whiting R. Housley and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, Internet Eng. Task Force, Sept. 2003

[10] Heo, J., Hong, C.S. (2006) "Efficient and Authenticated Key Agreement Mechanism in Low-Rate WPAN Environment", *International Symposium on Wireless Pervasive Computing 2006*, Phuket, Thailand 16 – 18 January 2006, IEEE,2006