Review of Asymmetric Key Cryptography in Wireless Sensor Networks

U.SenthilKumaran[1] M.K.Nallakaruppan[2]M.SenthilKumar[3]

[1]Associate Professor, School of Information technology, VitUniversity,Vellore.

[2]Assistant Professor School of Information technology, VitUniversity,Vellore.

[3]Assistant Professor (senior) School of Information technology, VitUniversity,Vellore.

Abstract

In wireless sensor networks (WSN's), our main aim is to ensure the confidentiality of the data which has been sensed , aggregated and communicated to the base node. This will be achieved using key management. Symmetric key management uses only one key for encryption and decryption.Symmetric key management is generally preferred in WSN, because it will consume less battery power, memory and induces less computation overhead. Asymmetric key cryptography uses two separate keys , for encryption and decryption but those two keys are interconnected with complex mathematical algorithm. Since it is using complex mathematical algorithms it will induce huge overhead on power , computation and memory Asymmetric key cryptography is not preferred in WSN. Asymmetrickey cryptography is more secured and efficient when compared to symmetric key cryptography, this paper analyzes various opportunities of implementing asymmetric cryptography in wireless sensor networks.(WSN : Wireless Sensor Networks)

I.Introduction.

A.Key Management.

Key management is systematic process of generating , distributing keys to the various sensor nodes , if the nodes gets compromised we need to revocate the keys to those compromised nodes.

The principal concerns regarding the key management framework are as follows:

- **Key deployment/pre-distribution:** it is process of generating keys and deploying it in the individual nodes.
- **Key establishment:** Here, the methods by which any pair of nodes or a group of nodes establishes a secure session are discussed.
- **Member/node addition:** This process of adding a node to the network, extra node added must be able to establish secure connections with the other nodes.
- **Member/node eviction:** This process eliminates the node from the network such that it will not again be able to establish secure sessions with any of the existing nodes in the network. Moreover, the node will not to decipher future congestion in the network .
- **Key Revocation:** Process of re issuing fresh keys to the compromised nodes.

B.Types of key Management.

1.Symmetric Key Management : Here only one type of key is preferred to authenticate the nodes. Key pre distribution is widely preferred in WSN. Symmetric key cryptography uses relatively simple mathematical operations and hence it demands less computation power , and eventually consumes less battery power. Since its using simpler keys it will give less overhead in terms of memory. Since its consuming fewer resources it is widely preferred in wireless sensor networks.[10]

2.Asymmetric Key Management : it uses two different keys , public key and private key for encryption and decryption. Two keys are mathematically linked with each other, Asymmetric key cryptography incurs huge overhead in terms of memory computation power and battery and hence its generally not preferred in WSN.In the rest of the paper , we discuss more about asymmetric key cryptography and the ways in which it can be implemented in WSN.[10]

Asymmetric Key Cryptography was introduced first by W.Diffie and M. Hellman presents the main idea of a public key cryptosystem.

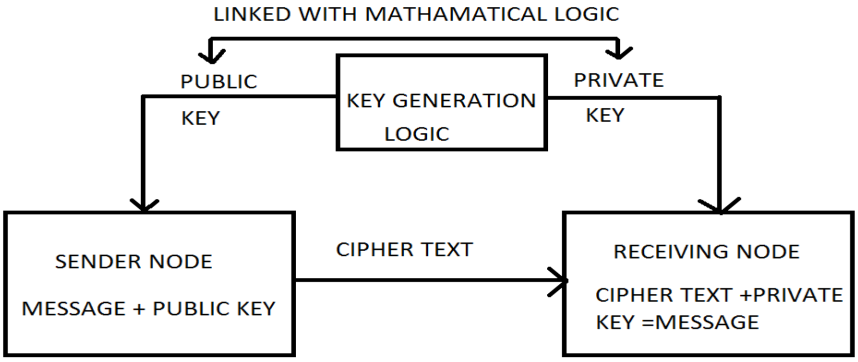

Figure 1: Public-key cryptosystem

Asymmetric key cryptography prefers a pair of keys: a public key and a private key.public key can be broadcasted to all nodes whereas the private key was kept as secret.We use mathematical logic to link public and private keys. Though the public key was broadcasted to every node, hacker will not be able to retrieve private key only with the help of public key. Assume that message*M*was encrypted with the known public key. To decrypt the cipher textC we need private key.occasionally we prefer to encrypt using private key and decrypt using public key.,

We need to simplify this scheme to use it in the wireless scenario .we can replace the trusted third party by the network deployer. Network deployer can act as trusted third party and deploy nodes with an private/public key pair. Every node present in the network can broad cast its public key to its neighbors if requiredto encrypt messages. However, in order to authenticate the public key there is a need for a trusted Certificate Authority which issues appropriate certificates.

Among all public key algorithms, there are three established families of practical relevance. The security of these systems is based on hard mathematic problems:

RSA Is named after its inventorsRivest, Shamir and Adleman [6][8]. This algorithm employs two large prime numbers P and Q .The strength of this scheme is based on the difficulty of finding these large prime numbers which is essential to find the secret key whereas the public key can be distributed freely .this algorithm as variety of applications on the normal conventional network, and is widely used in e commerce. Since we use large prime numbers and factoring as process , it demands high operational requirements in terms of resources. It will take toll on computational power memory, and the longevity of the operation demands power supply as well. All three resources are crucial in wireless sensor networks and hence its very tedious employ this algorithm in wireless sensor network security.

Discrete logarithm : Elgamal proposed another group of asymmetric cryptography algorithm which is widely used in the security of conventional networks.the strength of this scheme relies upon the difficulty in finding the logarithms on the finite field. Resource usage of these algorithm is comparable RSA algorithm, hence it is difficult to implement this algorithm in wireless sensor networks.

Elliptic Curve Cryptography is based on the algebraic structure of elliptic curve used on the finite field , the size the key will depend upon the size of the curve preferred strength of this method relies on the difficulty of the discrete logarithm problem in this setting (ECDLP).it has smaller key size when compared to the non elliptical key methods. Therefore it is considered the most attractive family for embedded devices, however the use of this method in wireless sensor networks is still tedious due to resource constraints.

As we discussed in the abstract, public key cryptography techniques are lot more tedious because of the scarcity of resources in wireless Sensor networks. Few researchers declared that implementation of Public Key Cryptography sensor nodes are not feasible Hence hard-ware support may be needed for public key operations. Researchers concentrated on improving the hardware quality in wireless sensor networks in order to fit asymmetric cryptography in wireless sensor networks.. None of the sensor node platforms currently available on the market provides hardware support for Public Key Cryptography. Any change in the hardware may influence the size of the sensors as well as the cost

There is aserious demand for cost effective Public Key Cryptography hardware solutions for sensor nodes. Meanwhile researchers concentrated more on , software based solutions for asymmetric key management.With respect to wireless sensor networks , asymmetric key cryptography would seem to be the best method for key broadcasting process. It gives necessary security and also provides improved scalability and resilience when compared the symmetric key solutions. Despite all these advantages, the application of public key cryptography protocols in WSNs remains challenging. All three asymmetric cryptography algorithms discussed , require authentication of public keys before key distribution. Implementing this public key cryptography solutions will require presence of a public key infrastructure in which certificate authorities authenticate public keys.

II.Public Key Infrastructure

Security of the Public-key encryption schemes are valid only if the authenticity of the public key is assured. This service is provided with the use of certificate schemes. In cryptography, a public key infrastructure is a methodology that connects public keys with corresponding user identities by means of a Certificate Authority. The main task of a PKI is to create, manage, store, distribute and revoke digital certificates. A typical public key infrastructure consists of:

Certificate Authority (CA) - third party which provides and verifies digital certificate

Registration Authority (RA) –it acts as verifier for (CA)and performs initial authentication before the digital certificates was issued.

Certificate repository - there can be one or more directories where certificates (with their public keys) are stored together with Certificate Revocation Lists (CLRs);

Certificate management system.

In order to participate in a public key infrastructure, user A must first enroll or register with the Registration Authority. The registration authority validates the user'sidentity and forwards his public key to the Certificate Authority. Main aim of the Certificate Authority is to attach the public key and the identifying information and credentials supplied by the Registration Authority. Public key was generated at the end of this process.. The binding is declared when a trusted Certificate Authority digitally signs the public key certificate with its own private key. Certificate authority provides a digital certificate for each user that uniquely identifies each and every user.

When we try to establish the public key infrastructure in wireless sensor networks In the context of wireless sensor networks we have to face many implementation concerns., In addition to the energy , resource , time and transmission constraints WSN also suffers from the lack of trusted infrastructure. Sensor nodes are generally deployed in adverse conditions and hence it is also difficult to deploy certificate authority. Even if we deploy certificate authority protecting it from the attackers is difficult. However certain innovations will help to overcome these constraints.

Network deployer can systematically configure the sensor nodes in the secure environment. Instead of searching for third party trusted entity, network deployer can act as trusted third party and thereby eliminate the need for separate third party.We need high power device to deploy all the keys and other global parameters in to the individual sensor nodes memory. Sensor nodes can be carefully configured in a secure environment which exists before the network deployment phase. Network deployer can act as a trusted entity who can use a high power device (base station) to upload all the global parameters and secret keys into nodes memory. We use the base node as high power device for this uploading process. Base station can also replace the functionality of certificate authority. Base station can be used for creating digital certificates that associate the identity of a node with its public/private key pair. Moreover, the base station can take the role of a Registration Authority, since it is in charge of as-signing identities to all the nodes in the network.

We can apply the same logic and use the base station as a certificate repository, but this idea is not suitable in sensor networks.Sensor nodes mainly prefer multi-hop communication to communicate data to the base station and retrieve the certificates. This communication will drain the crucial battery resources of the network, so it is better to pre- load every node with its own certificate and the Certificate Authority's public key certificates

A.Identity-Based Cryptography (IBC)

In any communication we need sender and receiver, in Identity based cryptography (IBC) we use sender"s identity as public key.In case of wireless sensor networks the sender sensor nodes identity can be taken as public key and private key was derived from mathematical calculations.Adi Shamir formulated this concept in this year 1985.shamir first proposed this concept on theoretical basis without practical implementation.Sakai, Ohgishi and Kasahara Proposed First identity based cryptosystem based on pairings in the year 2000 [4]. Here the key sharing scheme uses identities as public keys and employs the concept ofbilinearity for private key generation.

Soon after the discovery by Sakai, Ohgishi and Kasahara,[5] another application of bi-linear pairings was presented. In 2001 D. Boneh and M. Franklin described an identity-based encryption scheme which was based on the Weil pairing. This scheme fully realized Shamir's vision from 1985 to encrypt messages using only the identity of the recipient. Boneh and Franklin's Identity-Based Encryption scheme remains today as one of the most famous protocols in Identity-Based Cryptography.

Xinxin Fan and Guang Gong [3] proposed an efficient technique to speed up the signature verification in WSNs via cooperation among sensor nodes. The signature verification of a huge sensor nodes was done by enabling some sensor nodes to release the intermediate computation results to their neighbors during signature verification. Kyung-Ah Shim et al [2] proposed an efficient identity-based broadcast authentication scheme, EIBAS, for gaining WSN security .Computation and communication overheads can be minimized with the help of a pairing-optimal identity-based signature scheme with message recovery in which the original signature message is not required to transmit together with the signature, as it can be recovered according to the verification/ message recovery process

Though Identity based cryptography remove the need for public key, we need to generate private keys by means of complex procedures like bilinear pairings and hash tables. This does require lot of resources in terms of computation power, battery and memory. As we discussed earlier WSN has an acute shortage of these three vital resources, we prefer to do the complex operations offline before the deployment of sensor nodes. This can be done with the help of an high powered device like laptop or even a sink node. This operations can be termed as offline operations.Minimal encryption and decryption messages can be performed using the battery power of sensor nodes so that it will preserve the resources. These operations can be termed as online operations.

Fagen Li and Pan Xiong [1] proposed a heterogeneous scheme to secure communication between a internet host and an sensor node. Also it enabled a sensor node in an identity-based cryptography to send a message to an Internet host in a public key infrastructure. It uses two different phases , most of the complex online operations are performed using high power devices before deployment which is generally termed as offline operations. After deployment communicating nodes perform lightweight operations which are termed as online operations.

Senthilkumaran U and IlangoP[9] Here, mutual authentication technique is proposed by allowing sender and recipient to share a common key matrix as an authentication key.Here digital signature and cryptography was performed in asingle logical step. Most of the complex operations are perfomedbeforedeployment using high power device, whiach are termed as offline operations . Rest of the light weight operations are performed by nodes after deployment which are called as online operations.

III.Conclusion

Asymmetric key cryptographic measures are generally ignored in wireless sensor networks because of their heavy usage of resources. Whenever we want to sensor nodes with greater security asymmetric key cryptography is more significant when compared to symmetric key cryptography. Usage of specialized techniques like identity based cryptography , and innovations using pre key deployment , online and offline operations we overcome the issues of asymmetric key cryptography and installed them successfully in WSN. Improvements in hardware and inNovations in security algorithms will further increase the scope ofAsymmetric key cryptography in WSN.

References

[1] Fagen Li and Pan Xiong, “Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things”, IEEE Sensors Journal, Vol. 13, No. 10, October 2013.

[2] Kyung-Ah Shim, Young-Ran Lee and Cheol-Min Park, “EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks”, Ad Hoc Networks 11, 2013, pp. 182–189.

[3] Xinxin Fan and Guang Gong, “Accelerating signature-based broadcast uthentication for wireless sensor networks”, Ad Hoc Networks, 2012, pp.723-736

[4] R. SAKAI AND M. KASAHARA, ID based cryptosystems with pairing on elliptic curve. Cryptology eprint Archive, Report 2003/054, 2003.http://eprint.iacr.org/.

[5] R. SAKAI, K. OHGISHI, AND M. KASAHARA, Cryptosystems based on pairing. The2000 Symposium on Cryptography and Information Security, Okinawa, Japan,2000.

[6] R. L. RIVEST, A. SHAMIR, AND L. ADLEMAN, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21 (1978), pp. 120–126.

[7] T. E. GAMAL, A public key cryptosystem and a signature scheme based on discrete logarithms,

[8] A. SHAMIR, Identity-based cryptosystems and signature schemes, in On Advances in cryptology, proceedings of CRYPTO 84, New York, NY, USA, 1985, Springer-Verlag New York, Inc., pp. 47–53.

[9] U.senthilkumaran. Ilango, P. (2015). Secure authentication and integrity techniques for randomized secured routing in WSN. Wireless Networks, 21(2), 443-451.

[10] U.SenthilKumaranilango ,p Evolution of key management and variations of random key prediddtribution in wireless sensor networks :survey.International journal of Applied engineering and research –volume 9 number(21) (2014) pp 11681 – 11688.