A Survey of Key Management Schemes in Wireless Sensor Networks

R.Sharmila[#1], P.C.Gopi [#2], Dr.V.Vijayalakshmi[*3]
[#1]Assistant professor, Department of ECE , Rajiv Gandhi College of Engineering & Technology
[#2]Undergraduate student, Rajiv Gandhi College of Engineering & Technology
[#3]Associate professor, Department of ECE , Pondicherry Engineering College, Puducherry, India

Abstract— *In near future, the Wireless Sensor Networks (WSN) is widely used in many applications like military and civil domains. The wireless sensor networks are always deployed in hostile and pervasive environment. Security is major concern in the wireless sensor network. The traditional network security methods are not suitable for wireless sensor networks because of limited resource. Several Key management and establishment schemes have been proposed to provide light weight ciphers. The key management schemes play an important role in wireless sensor networks to achieve security. In this paper a survey of key management schemes in wireless sensor networks has been executed. Each and every key management schemes has some trade off between limited resource and security. Classification of key management schemes based on encryption was done. Further based on key predistribution (with or without deployment knowledge) and rekeying mechanism, the key management schemes have been analysed and their limitations and advantages have been summarized.*

Keyword *- Wireless sensor Networks, Key Management Schemes, Symmetric Key Management Schemes, Asymmetric Key Management Schemes, Dynamic Key Management Schemes.*

I. INTRODUCTION

Recent advances in MEMS technology, WSN play a vital role in an area of communication expressly to sense and report about antagonistic environment. The wireless sensor network consists of large number of tiny sensor nodes; each sensor node is equipped with integrated sensor, low battery powered and the main task of sensor node is sense, process the data and provide short range of communication. The sensor nodes are mainly deployed for military sensing and tracking an object, hostile environmental monitoring, patient monitoring, etc.

When the sensor nodes are deployed in hostile environment the secure communication became extremely important, to survive the various types of malicious attacks. Security is provided by means of encryption and authentication in each communication between two nodes. The traditional cryptographic techniques are not suitable for WSN because of resources constraint. For example, the MICA2 mote consists of an 8 bit AT Mega 128L microcontroller, data rate of 250 Kbits/s, size of flash memory is only 512 Kbyte and on board battery is 3.3 V with 2A-hr capacity [1]. These complications are overcome by means of basic fundamental scheme called key management schemes; it is specially designed for wireless sensor network.

Recently various efficient key management schemes have been proposed to provide secure relation between neighbour sensors during network formation. All these key management schemes have their own advantage and disadvantages. The influential factors are,

- Scalability: Capability to increase the size of wireless sensor network.
- Connectivity: Probability of sensor nodes can find a common secret key to establish secure communication.
- Resilience: Resistance of the WSN against node capture.
- Memory Overhead: Amount of memory unit needed to store security identifications.
- Processing Overhead: Amount of processing cycle required by sensor node to generate a common secret key.
- Communication Overhead: Amount and size of message needed to establish and generate a common key between two sensor nodes.

A. Classification of Key Management Schemes

Generally key management schemes are classified into many types. Depending upon encryption, it is classified into symmetric, asymmetric and hybrid key management scheme. Depending upon key predistribution it is classified into location dependent key predistribution and location independent key Predistribution .Key management Schemes can be further classified into Static and dynamic scheme based on whether rekeying is performed after deployment. In the Static key management scheme once the sensor nodes are deployed in the field, they will not change administrative keys are generated before deployment. In the dynamic key management schemes may change its administrative keys periodically or on demand. The major advantage of dynamic key management scheme is enhanced network survivability and scalability. Depending upon the network model, it is classified into homogeneous or

heterogeneous schemes. Homogeneous schemes commonly a flat network model and all the sensor nodes are having same capabilities.

The key management schemes needs four basic functions, specifically key examinations or key analysis, key assignment, key generation, and key Predistribution. These functions have been tightly coupled with one another and it is carried out by a centralized server or the cooperation of sensor nodes in the network. In this paper, the different key management schemes have been classified based on encryption and it is further classified based on key predistribution (with or without deployment knowledge) and rekeying mechanism.

The rest of the paper is organized as follows: In section 2 details the symmetric key management schemes based on key predistribution and deployment knowledge. In section 3, we explain the Asymmetric key management scheme and its classifications. Finally we conclude this paper in Section 4.

II. SYMMETRIC KEY MANAGEMENT SCHEMES

Most of the traditional key management schemes are not suitable for wireless sensor network due to limited resource and energy constraint of the sensor node. The symmetric key management schemes are suitable for WSN because of limited computation, communication and memory. Based on the key management process (i.e., key analysis, key distribution, key discovery and key establishment) the symmetric key management schemes are introduced in the following subsections.

A. Master Key based pre-distribution Scheme

In the master key management scheme, a single key is preloaded into every sensor node before deployment. Lai et al. (2002) proposed a master key based pre-distribution scheme [2]. The master key is pre distributed into each sensor nodes. Once the sensor nodes are deployed in the field, a pair wise key can be established by using this master key and random number can be exchanged between sensor nodes. The advantage of this scheme is high scalability and memory is efficient but there is a lack of security. It requires a tamper resistant hardware for which the cost is more. It has poor resilience and authentication.

Zhu et al. (2003) proposed an improved scheme called LEAP: Localized Encryption and Authentication Protocol. This scheme offers the better key distribution and node authenticity. It is efficient security mechanism for large scale distributed sensor networks [3]. The basic idea behind the LEAP method is the master key is erased after the pair wise key is established using LEAP method. It increases the resilience but newly added node still has a master key, so more chance for the master key is being compromised.

Perrig et al. (2001) proposed SPINS: Security Protocols for Sensor Networks. In this scheme the base station assign encrypted pairwise key for two sensor nodes using shared keys [4]. This scheme provides perfect resilience but it has poor scalability because the base station needs to send the pairwise keys to sensors node.

Chan and Perrig (2005) proposed PIKE: Peer Intermediaries for Key Establishment in sensor networks [5]. In this scheme the key establishments between two sensor nodes are based on trusted third parties. Major limitation of this scheme was trusted node may be target of attack or possibilities of compromised by adversary.

B. Pairwise Key Establishment

In this scheme establishing pair wise key between each and every pair of nodes in a sensor field. If there are n numbers of nodes in a network every node in the network will have store n-1 keys. This scheme provides good connectivity, confidentiality and authenticity for wireless sensor networks. The major limitation of this scheme is poor scalability and memory. If there are n nodes in the network (the value of n is too large) every node store n-1 keys in its memory, so it need more memory. Also communication between every pair of sensor node is not vital for wireless sensor network.

Chan and perrig (2003) proposed Random pair wise key predistribution scheme .In this scheme, all nodes in a sensor field need not to store n-1 keys for establish the pair wise key [6]. Different pair wise keys are predistributed randomly in sensor nodes before deployment. In this approach, two nodes share a pairwise key with high resilience and authentication. Even if one sensor node is captured, the keys of other nodes are never compromised. The disadvantage is that, it does not allow node addition of sensor node in the network because existing node do not have pairwise keys of newly added sensor nodes. It does not have scalability because each sensor has to store keys as many as the total number of the sensors in the network.

The key predistribution schemes can be further classified into probabilistic and deterministic based on existence of one or more common keys between pair of sensor nodes is not sure in the network.

C. Probabilistic/Random key predistribution schemes

In this scheme the probability of existence of common keys between the intermediate nodes is not sure but it is probabilistically predicted. The basic idea of this scheme is to construct a global key pool and randomly choose the keys (i.e., key ring) from the key pool (i.e., key size) and preload the keys in sensor nodes before deployment (off-line).The major advantage of this scheme is, it improve the network resilience and thwart node compromise.

The basic random key predistribution scheme is EG scheme, Eschenauer and Gligor (2002) proposed a key management scheme for distributed sensor networks [7]. It was the first basic key predistribution scheme for many of the research works. This scheme is especially designed for sensor networks.

There are three phases in the EG scheme: Key predistribution, shared key discovery and path key establishment. In the key predistribution phase, generate a large pool of keys and randomly pick up *n* keys from the pool to establish a key ring, where n << N, where N is the total number of nodes. Each sensor node in the network has unique key ring, it consist of subset of keys.

In the shared key discovery phase, once sensor nodes are deployed in the field, the sensor nodes tries to communicate with the neighbour node by searching common key within the key ring by broadcasting the unique identities of the keys ring that stored in memory. If there is no common between two sensors nodes, path key establishment take place. In this phase the communication take place through intermediate node, which is able to find communications with the both nodes. The path key is unused key of the sensor node and connecting nodes.

This scheme ensures that though the size of the network is large, only a few keys are needed to be stored in each node's memory, thereby saving storage space. These few keys are enough to establish the common key between the nodes based on a selected probability. After deployment, each node tries to discover its neighbour node with which it shares common keys by broadcast their identifiers lists to other nodes. A link establishes between two nodes only if they share a common key .If sensor nodes failed to shares a common key, which make use of path key establishment it provide a link between two nodes when they do not share a common key.

The advantage of EG scheme is, it needs fewer places to store key ring in its memory and scalable because number of keys in the pool and the size of the key ring are adjustable. The disadvantage of this scheme is poor authentication, connectivity and no key refreshing. The key refreshing or key revocation is required if a sensor node is compromised .The EG scheme does not support any clustering operation because every node should guaranteed to have common key with all of its neighbours.

Chan and Perrig (2003) suggested two schemes to improve the resilience of the basic scheme. The first scheme is q-composite scheme and second one is multi path key reinforcement. The q- composite key scheme is extension of EG scheme. The resilience of the network is increased by use of multiple keys instead of single key in basic scheme. In EG scheme, each sensor node is preloaded with a key ring that is randomly chosen from key pool before sensor deployment. After sensor node deployment, the shared key discovery and path key establishment are remain same as basic scheme only difference is instead of sharing single common key ,q common keys in the key rings are shared to construct the shared key. For example: q=2, at least two keys should be shared from key ring. If two keys are not shared from the key rings, they are not connected

D. Matrix based key predistribution Scheme:

Blom.R (1985) proposed an optimal Class of Symmetric key Generation Systems. It is matrix based group key predistribution scheme and not especially designed for wireless sensor networks [8]. In this scheme, generate the symmetric matrix D whose dimension is (λ+1) * (λ+1) .The matrix D works as a secret key and should be kept as secret. The matrix G is publicly known. The symmetric matrix K, where K = $(DG)^T$ G stores all pairwise keys of a group of n nodes. $(DG)^T$ is called secret matrix and must be kept secret to all nodes. The G matrix is given by,

Let K = $(DG)^T$ and A=K.G, anyone can easily compute the symmetric matrix A as follows:

A = K.G = $((DG)^T G) = G^T.D.G = (K.G)^T$.

Each node i stores the i^{th} row of secret matrix D and the i^{th} column of public matrix G. After sensor node deployment, each pair of nodes i and j compute the pairwise key $K_{ij} = K_{ji}$ by only exchanging their columns in plain text because the key is product of their own row and column of others. Here row is always secret. Blom's scheme has λ – secure property, which ensures that as long as no more than λ nodes are compromised the network can be secure. In this scheme, any pair of sensor nodes in a network is able to find a pairwise secret key with neighbors within the communication range. The main limitation of Blom's scheme is, if adversaries compromised more than λ nodes or rows; the entire secret matrix can be obtained by compromiser and the connectivity is poor.

Du W, Han (2004) proposed a key management scheme for wireless sensor networks combined with the Blom's scheme and the basic scheme [9]. The blom's scheme uses one key space for all nodes which guarantees that any pair of nodes can find a pairwise key in the key space. In this scheme using multiple key spaces by first generating ω key spaces using bloms scheme and each sensor nodes carries key information from randomly selected key spaces. If two sensor nodes have common key space, they compute pairwise key from the key information from a common space; when two sensor nodes do not have common key space, they can conduct key agreement via other intermediate nodes which share pairwise keys with them. The main improvement of this scheme is more resilient than blom scheme without increasing the amount of memory. The resilience is further improved by using two hop neighbor key predistribution schemes. The limitation of this scheme is to increase the security, it needs more memory.

Hangyang Dai et al. (2010) proposed new key predistribution scheme using LU matrix method [10]. This method combines LU matrix and polynomial based key predistribution tactic to achieve high resilience and connectivity. First the base station generates a large polynomial pool using Blundo et al. [10] and each polynomial has a unique ID. Each node randomly chooses polynomial from the pool. The LU matrix is formed by randomly choose the group of polynomial from the polynomial pool to form a lower triangular matrix L and the upper triangular matrix

U .The product of L and U matrix is symmetric matrix. Then the polynomials are predistributed to sensor node and randomly distribute the one row and one column to each sensor node. Then the keys are shared by exchanging their row elements of sensor node and compute vector product. If the symmetric condition is satisfied; it shared the key between the sensor nodes and the mutual authentication is achieved.

E. Polynomial Pool based key predistribution Scheme

The basic polynomial key predistribution scheme is proposed by Blundo et al. (1992) [10].The polynomial based scheme is the foundation of pairwise key predistribution schemes. In this scheme, there are three phases: initialization, key discovery and key generalization phase.

In the key generalization phases, key set up server randomly generates a bivariate t-degree polynomial $f(x,y) = \sum_{i,j=0}^{n} a_{ij} x^i y^j$ symmetric polynomial over a finite field Q_p where p is a prime number that is large and it has the property of $f(x, y) = f(y, x)$.In the initialization phase, each node has a unique id and set up server computes a polynomial share of f(x, y).For example: each sensor node i, server computes a polynomial share of f(x,y) that is f(i,y).For any sensor nodes i and node j can compute the common key f(i,j) by calculating f(i, y) at point j and node j can compute the common key with i by calculating f(i,y) at i.

The main limitation of this scheme is each sensor node i needs to store a t-degree polynomial f (i, x) which inhabits (λ+1) log p storage space. The pairwise key is obtained by the two sensor nodes need to evaluate the polynomial for the ID of the other sensor node i.e., f (i, y) and f(x, j).This scheme has more secure and λ-collusion resistant. Suppose the sensor network size is increased, the network is more defenceless to attack. The general polynomial pool based key predistribution scheme greatly reduces the amount of predistributed key information stored in sensor nodes and it allows every pair of sensor nodes to compute a shared key. The main advantage of this scheme is as long as λ or fewer nodes are compromised the rest of the network is remaining secure. So this scheme is λ-Collusion resistant.

III. ASYMMETRIC KEY MANAGEMENT SCHEME

The asymmetric key management or Public key cryptography is one of the cryptographic techniques which consist of private and public key. Existing public key cryptography technique are DES, AES, DSA and RSA provides secure communication. These cryptographic techniques require larger key size to provide higher level of security. So these techniques are not suitable for wireless sensor networks.

It requires more computational power and more processing time for encryption and decryption of data. RSA algorithm was first developed in 1977[12].The key sizes used in the RSA algorithm is 512 to 2048 bits. This modular multiplication can lower the computation time by almost ¾ and complexity by 25%.

Recently Elliptic Curve Cryptography has been proposed for wireless sensor network. It has fast communication time, smaller keys (i.e., need less memory) and bandwidth than RSA [13].A MICA2 mote using ECC can reduce the key size. It provides same secure as Diffie-Hellman scheme.

A. *Key Management using ECC*

ECC was first developed by Koblitz and miller in 1985.ECC is represented using Elliptic curves. It provides same level of security when compared to RSA but with smaller Key Size [14].eg:160 bit for ECC and 1024 bit for RSA. The main advantages of ECC are less number of key sizes, reduced memory and power and low bandwidth. There are three phases in ECC based on hexagonal deployment knowledge.

Phases 1: Key Generation Phase (Generation of seed key)

- Elliptic curve over finite field is given by $y^2 \bmod p = x^3+ax+b \bmod p$ where a,b -Elliptic curve coefficients and p-prime field.

E.g.: Consider N=50, p=53,a=9 and b=17.

- Then elliptic curve equation: $y^2=x^3+9x+17$
- 52 Elliptic curve points have been generated.

Each node is assigned with a unique seed key

Phase: 2 Key predistribution phase

In this phase key ring is generated by point doubling and point multiplication operation over the seed keys and it is pre-distributed into the sensor nodes. The formula used to calculate is $x_{2p}=(\lambda^2-2x_p) \bmod p$ and $y_{2p}=(\lambda(x_p-x_{2p})-y_p) \bmod p$; where, $\lambda=[(3x_p^2+a)/2y_p)] \bmod p$. Once key ring is formed, it is pre-distributed into the sensor nodes before it gets deployed into the terrain.

Phase: 3 Key Agreement Phase (Link Formation)

In this link formation phases, link is created when two nodes shares a common private key. When the size of key ring increases the corresponding link increases and vice versa. The probability of two node sharing a common key is given by $W=1-[(p-r)! / [((p-2r)!)(p^r)]]$, where r is key ring size and p is key pool size. The link increases by increasing the key ring size r. In this scheme the connectivity and resilience analysis is proved that ECC scheme with deployment knowledge achieves a higher connectivity and security with a shorter transmission range and a lower memory requirement.

Du et al. (2009) proposed routing driven ECC based key management scheme for WSN [14] .In this scheme a heterogeneous sensor network is used to provide better performance and security. It establishes shared keys with neighbour sensor nodes that communicate with each other.

Recently the Hyper Elliptic Curve Cryptography (HECC) is one of emerging cryptographic techniques for wireless sensor networks. HECC offers the same level of security when compared to RSA and ECC with smaller Key Size [14].eg:80 bit for HECC, 160 bit for ECC and 1024 bit for RSA.

IV.CONCLUSION

The key Management schemes for wireless sensor networks are still an active research area. It provides fundamental security for wireless sensor network. In this paper, various key management techniques have been surveyed and investigated based on encryption and then divide each classification into several group based on key predistribution and key establishment. Mainly all the key management schemes are designed based on the limited resource of sensor nodes and its security. Key Management scheme for WSNs is still a very fruitful research direction to be more discovered.

REFERENCES

[1] D. Malan, M. Welsh, and M.D. Smith, "A Public- Key Infrastructure for Key Distribution in TinyOs Based on Elliptic Curve Cryptography," in Proc. of 1st IEEE International Conference Communications and Networks(SECON), Santa Clara, CA, Oct. 2004.

[2] Lai B, Kim S, Verb auwhede I, "Scalable session key construction protocol for wireless sensor networks", In: Proceedings of the IEEE workshop on Large Scale Real Time and Embedded Systems LARTES ,December 2002.

[3] S.Zhu, S. Setia, and S.Jajodia,"LEAP: Efficient Security Mechanism for Large Scale Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communication Security (CCS'03), Washington D.C., and October, 2003.

[4] A.Perrig, et. al, "SPINS: Security Protocols for Sensor Networks", Proc. of ACM MOBICOM, 2001.

[5] Chan H, Perrig A, "PIKE: peer intermediaries for key establishment in sensor networks", In: Proceedings of the 24 th annual joint conference of the IEEE computer and communications societies (INFOCOM'05), Miami, FL, USA, March 2005.p.524–35.

[6] Chan H, Perrig A, "Random key predistribution schemes for sensor networks". In: Proceedings of the 2003 IEEE symposium on security and privacy, May 2003.p.197–213.

[7] Eschenauer L, Gligor B D, "A key-management scheme for distributed sensor networks", In: Proceedings of the 9th ACM conference on computer and communication security, Washington, DC, USA, 2002.p.41–7.

[8] Blom R,"Theory and application of cryptographic techniques", In Proceeding of the Eurocrypt 84 workshop on advances in cryptology, Berlin: Springer; 1985. p. 335–8.

[9] Du W, Han Y S, Chen S, Varshney P K, "A key management scheme for wireless sensor networks using deployment knowledge" , In: Proceedings of IEEE INFOCOM 04. Hong Kong: IEEE Press; 2004.p.586–97.

[10] Hang Yan Dai, "Key Predistribution approach in Wireless Sensor Network using LU Matrix,"IEEE sensor journal, Vol.10, no.8, August 2010.

[11] Amar Rasheed, "Key predistribution Scheme for Establishing Pairwise keys with a mobile sink in sensor network," Vol.22, no.1, Jan. 2011.

[12] D. Malan, M. Welsh, and M.D. Smith, "A Public- Key Infrastructure for Key Distribution in TinyOs Based on Elliptic Curve Cryptography," in Proc. of 1st IEEE International Conference Communications and Networks(SECON), Santa Clara, CA, Oct. 2004.

[13] A.S. Wander, N. Gura, H. Eberle et al., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," in Proc. of the 3rd International Conference on Pervasive Computing and Communications(PERCOM),2005.

[14] X. Du, Y. Xiao, M. Guizani, and H.H. Chen, "A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensors Networks." IEEE Transactions on Wireless Communications, accepted and to appear.