ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

A Review on Different Resource Efficient Key Management Schemes for Wireless Sensor Networks

Chidambaram G[#1], Edwin Prem Kumar G[*2]

[#] PG Scholar Dept of Information Technology, Karunya University, Karunya Nagar, Coimbatore, India

[*]Assistant Professor, Dept of Information Technology, Karunya U niversity, Karunya Nagar, Coimbatore, India

Abstract—The wireless sensor networks needs security for transferring the sensed data to the base station. There are many possible ways to attack the transferred data, for reducing the attackssecurity is mostly needed for the network. Key management is the method of using cryptographic keys to provide security. The resources of wireless sensor networks must also be considered for the establishment of keys. This paper explains about the differentmechanisms or protocols that are possible for wireless sensor networks to establish the authentication keys in resource-efficient manner. This paper also presents the different cryptographic methods that are used by the sensor networks for securing its data. This paper does not conclude any specific protocol which is suited for establishing cryptographic keys in resource-efficient manner. But the usage of protocols depends upon the applications of the wireless sensor networks.

Keywords—Wireless Sensor Networks, Resource-efficient, Key Management.

I. INTRODUCTION

Wireless Sensor Networks (WSN) is a group of sensor nodes spatially dispersed for monitoring and recording the physical conditions of the environment and to organize the collected data at a central location. The nodes ofWireless Sensor Networks consists of several parts such as Radio Transceiver (Internal or External Antenna), Microcontroller, Battery, Sensors [1]. The WSNs are used to monitor some of the ambient conditions like temperature, humidity, vehicular movement, lightening condition, pressure, soil makeup etc… The applications of WSN are military, environment monitoring, healthcare monitoring, Home automation, etc…

The Wireless Sensor Networks are broadly classified into two types based on the resource capacities like energy, memory, Sensing range, communication range. The two types of WSN are Heterogeneous wireless sensor networks (HWSN) and Homogeneous wireless sensor networks. The Heterogeneous sensor networks are the networks in which the resources of the nodes are different. In Homogeneous sensor networks the resources of nodes are same. In this paper we consider Heterogeneous Wireless Sensor Networks (HWSN) in which resources of the nodes are different. To balance the resources of sensor nodes in HWSN the nodes are organised into a number of clusters. The node with high resource capacities are cluster head and the node with low resource capacities are cluster members. The factors that influence the design of sensor networks are Fault Tolerance, Scalability, Production cost, Operating environment, Hardware constraints (sensing unit, processing unit, transceiver unit, and power unit), Power consumption [3]. The cluster member of the sensor networks collect the information and transfers it to the cluster head, the cluster head acts as an aggregation point for the cluster members. The cluster head is responsible to transfer the aggregated data to the base station for further processing. In this paper we consider clustered Heterogeneous Wireless Sensor Networks (CHWSN).

A. *Need for security*

The sensor networks are used for tracking enemy vehicles, and also used in many applications like chemical and biological changes. While monitoring these networks has to transmit the gathered information via another node to the head of networks. There are situations like some malicious node are present which may corrupt the data. Some of the other security threats of wireless sensor networks are Radio links are insecure – eavesdropping / injecting faulty information is possible. Sensor nodes are not temper resistant – if it is compromised attacker obtains all security information [2]. To reduce this some security services has to be provided like authenticity, confidentiality, freshness integrity, etc...[4] The need for security in wireless sensor networks is due to unreliable communication and the unattended sensor nodes that are deployed. The security for WSN is based on the Trust Management and Key Management, Trust management is the mechanism that is used to support the decision-making process of the network. In Trust management the data are transferred to the nearby node on the basis of trust that is calculated. Key management is the process of using cryptographic methods for encryption and decryption of the data and also for authentication. One of the major issues of key management is the establishment of keys for authenticating the data within the specified amount of resources.

B. *Key Management*

The key management consists of three different types of keying techniques they are Network keying, Pairwise keying and Group keying [4]. There are three different types cryptographicschemes for key management Symmetric, Asymmetric, and Hybrid [5]. The Symmetric key management is the process of using same key for both encryption and decryption which requires less computation and less energy but it requires more memory space to store the keys. Some of the symmetric key management schemes are Twofish [6], Serpent [7], AES (Advanced Encryption Standard) (aka Rijndael) [8], Blowfish [9], CAST5 [10], RC4 (Rivest Cipher 4) [11], TDES (Triple Data Encryption Standard) [12], RC5 (Rivest Cipher 5) [13] and IDEA (International Data Encryption Standard) [14]. The asymmetric key management scheme uses public key cryptography such as Elliptic Curve Cryptography (ECC) [15], Merkle'spuzzels [16], RSA (Ron Rivest, Adi Shamir and Leonard Adleman) [17], E1Gamal [18], etc… for the shared key establishment and authentication. This mechanism requires high computation and hence it requires more energy but uses less memory to store key. The Hybrid key cryptosystem combines both the symmetric and asymmetric key cryptosystem methods like OpenPGP (Pretty Good Privacy) [19], PKCS(Public-key Cryptography Standards) [20].

There are three different types of key management approaches in sensor networks they are Arbitrated keying protocols, Pre-deployment protocols, and Self-enforcing protocols [3]. The Arbitrated keying protocol is the process of using hierarchical keying based on the identity of the nodes of network. Pre-deployment protocols is the process of deploying the cryptographic keys before deployment of nodes in the area. Self-enforcing protocol is the process of using pairwise keying for their secure transmission of data.

C. *Attacks of Wireless Sensor Networks*

There are different types attacks that are possible in wireless sensor networks some of them areMote-class, Outside/Inside, spoofed, altered, or replayed routing information, selective forwarding, sinkhole attack, sybil attack, wormholes, HELLO flood attacks, acknowledgment spoofing, etc… [2].

- Mote-class: The attacker has access to some of the nodes with similar characteristics.
- Outside/Inside: Attacker compromises some of the nodes in a network.
- Sinkhole attack: A fake sink address is forwarded to all nodes to get the data.
- Sybil attack: A single node acts as another node and pretends in every part of the network.
- Selective forwarding: Nodes are compromised which are responsible for forwarding the data packets.
- Wormholes: A wormhole node is added to the network which blocks the communication of the network.

This paper is organized into following sections, the section 2 consists of the paper that which was proposed to establish the cryptographic keys in resource efficient manner. The section 3 is the different key management strategies in which the detailed explanation of the papers for key management is given, section 4 is the conclusion of the paper and section 5 is the references of the paper that is present.

II. LITERATURE SURVEY

Wireless Sensor Networks has many problems in providing security by using key management techniques, some of them are management of resources for generating key, over storage of keys in the nodes of network, insufficient memory, etc,.. To reduce these problems and to make sensor networks to be secure many authors has proposed different ideas using different cryptographic methods. These different methods provide a way to provide security to the sensor networks using key management. The details of some of the papers that which provides a mechanism to secure the wireless sensor networks data is explained in this section.

In paper [21] it provides a method for generating keys by pairing and identity based encryption properties. The paper [22] explains the usage of hybrid cryptosystems for the encryption and decryption of data instead of symmetric and asymmetric cryptosystems. In [23] it provides the method of sharing the keys using intermediary node of the network.In paper [24] the LEAP (Localized Encryptionand Authentication Protocol)

protocol has been developed which provides multiple types of keys for security of sensor networks in an efficient way. In [25] the scalable session key is developed to reduce the usage of shared secret key which results in less storage of keys in the node. In paper [26] two new protocols SNEP and µTESLA has been developed for providing security to wireless sensor networks in data vice and also for providing security to the broadcasting messages. The following section provides a detailed explanation of different resource efficient key management techniques that has given above. These papers explains about how cryptographic keys can be established efficiently according to the resources of the sensor nodes that are present in the network.

III. KEY MANAGEMENT STRATEGIES FOR WIRELESS SENSOR NETWORKS

This paper is a literature survey paper which does not provide any mechanism for the security of wireless sensor networks, it just provides an explanation about different techniques that has been used previously for generating the cryptographic keys in resource efficient way to make wireless sensor networks secure.

A. Private Key Agreement and Secure Communication for Heterogeneous Wireless Sensor Networks [21]

In this paper a pairing based cryptography over an elliptic curve is used to generate the cryptographic keys. If a node wants to communicate with other node then it can compute the key using the pairing and identity-based encryption properties. This individual generation of keys by the nodes reduces the key storage space of nodes in network. The Base station of the network provides a secret of the key over the elliptic curve which is used by the node to generate key for communicating with other nodes. The Base station also provides the ID and corresponding secret points to all the nodes of the network. After deployment, each nodes of the network knows its ID, secret points and random number. The H-sensor of the network knows ID of all L-nodes of the cluster. The Base station updates random number of L-nodes via its corresponding cluster Head H in a particular interval of time. Since the random number is responsible for providing authentication between L-node and H-node. The L-node and H-node generates a dynamic random number for differentiating each session of the communication between the nodes.

1)Key Establishment and Authentication: The L-node connects with the neighbouring H-node directly or by using other L-node as intermediary. The H-nodes connect with the Base station directly or by using intermediate H-node and all the nodes gets connected to form a hierarchical tree structure. With the Random number, Secret point, ID and Dynamic Random number each node generates its shared secret key for encryption and decryption of data. By the generated shared secret key the authentication for each node is provided. The dynamic random number which is generated by the nodes is used to identify whether the transferred data is different or not. After each communication the dynamic random number is changed by the nodes to reduce attacks. This random number is changed not in a continuous manner after a particular time limit the random number is changed by the Base station of the network.

2) Random number Renewal: The Base station generates a new random number in a particular interval of time, this generated random number is transferred to the L-node by using the corresponding H-node. The Base station encrypts the random number with the shared secret key and sends to the H-nodes. The H-node decrypts and again encrypts the random number with secret key of L-node. If the L-node is not connected directly then a layering encryption method is used, H-node encrypts the random number with original node key and also encrypts with the key of intermediary node. The intermediary L-node decrypts the received number and again transfers it to the original L-node.

B. Efficient Hybrid Security Mechanisms for Heterogeneous Wireless Sensor Networks [22]

This paper presents a method of using probabilistic unbalanced distribution of keys to the nodes of network. The nodes are preloaded with keys before they are deployed. With these keys nodes that are external to the network can securely and efficiently establish the keys for their secure communication. Three steps are followed in this paper they are, Probabilistic Unbalanced key management. The number of keys stored is proportional to the resources of nodes and. A new protocol LIGER is introduced to establish keys between nodes when they are not in connection and also gets the resources when they are available to the network.

The storage of keys in the network is based upon the resources of the nodes. Two levels of keys are stored according to the available resources. These stored keys are generated by using different trust models like Backhaul trust, peer to peer limited trust and peer to peer liberal trust.

*1) Protocol Specification:*There are two different types of protocols that has been used for providing keys to the nodes of the network they are. The protocol used for infrastructureless environment network is referred to as LION and the network which relies upon the Key Distribution Centre is referred to as TIGER. The combination of both LION and TIGER protocol is known as LIGER protocol. All the nodes of network is loaded with random keys that are present in the Key Distribution Centre. If the network is in standalone mode then a new protocol is used for providing the shared key, if the network relies on the Key Distribution Centre then the shared key is chosen from the pool of keys that are present.

In the LION protocol the nodes of the network broadcasts hello messages to other nodes, if the node receives the message then it sends the response message. The node is verified whether it is the node of same network by using the identity. If the node is of same network then a shared key is identified from the key that which are stored before deployment. The TIGER protocol is used when the nodes are available to the Key Distribution Centre. In this an authenticator key is selected from the keys that are stored in the nodes before deployment. The nodes generates a token which consists of a series of included data, a nonce and the authenticator key, with the received token node decides to authenticate or not. If the node is authenticated then it sends a token with its authenticator key and nonce to establish a secure communication.

C. PIKE: Peer Intermediaries for Key Establishment in Sensor Networks [23]

The usage of both Symmetric and Asymmetric cryptosystems provides overhead in either communication cost or memory per node. To reduce this overhead they have proposed a key establishment protocol which uses one or more sensor nodes as intermediate node to establish the keys. This PIKE method is used to establish keys between any two nodes which helps in using for a wider range of network scenarios. The PIKE scheme is mainly developed to reduce the scalability problem of the key distribution to nodes of network.

1) PIKE Protocol: In PIKE method the nodes share their pairwise key with the trusted intermediary node. When the node identifies its intermediary node, then it securely routes the key establishment message to the other node. The nodes are preloaded only with the pairwise key so each node has another node with the same key. Based on the ID of each node the pairwise key is distributed to the node which helps in identifying the node easily after deployment. The nodes are deployed according to the node ID to make the nodes into batches for identifying the nodes that which are not batched. After finding the intermediary node, original node will establish their new key between the neighbouring nodes. This establishment of new key is used to communicate with the other pair of nodes. These generated keys will reduce the security of nodes since those keys are generated using the previous node pairwise key. This PIKE method can be used only when nodes are deployed in a rectangular area.

D. LEAP: Efficient Security Mechanisms for Large-Scale distributed Sensor Networks [24]

LEAP (Localized Encryption and Authentication Protocol) is a key management protocol of sensor networks which is designed to manage the in-network processing and also to restrict the node compromise attacks. This LEAP protocol supports for the establishment of four types of keys to provide a way for secure communication in sensor networks. The four different types of used in the LEAP protocol are the individual key shared with base station, pairwise key for sharing with neighbour or other sensor node, cluster key to share with a group of neighbouring node and group key for sharing with all nodes of the network. The local broadcast authentication protocol present in the network provides source authentication of in-network processing.

1) LEAP Protocol: This LEAP keying mechanism provides confidentiality and authentication to the sensor networks. The data are transferred between nodes as packets. Different packets need different security mechanisms for authentication and confidentiality of the data. This LEAP protocol provides different security mechanisms to different packets of data that are transferred using the establishment of four types of keys. The individual key is the key that every node must have which is to communicate directly with the Base station. This key is used to transmit any sensitive data or to send the information about neighbouring node to the base station when its performance is abnormal. The Group key is the global key that which is shared with all nodes of the network. This group key is used by the base station to broadcast any message to all the nodes of network. Cluster key is the key which is shared by node to all other neighbouring node for transmitting the local messages in secure manner. The Pairwise key is shared between two nodes for identifying the intermediary node to transmit the data, this key is used for securing the communication that which needs privacy or source authentication from all the other node.

*2) Local Authentication:*This authentication is to provide security for every message that are being forwarded or processed from one node to other node. This local broadcast authentication is supported by the cluster key that has been generated, since this cluster key is known only to the local nodes of the network. The Local authentication provides a separate way of security to all the that are being transmitted from one node to the other node.

E. Scalable Session Key Construction Protocol for Wireless Sensor Networks [25]

In this paper a new protocol for building a link-dependent key has been generated by using broadcasting key negotiation messages. To reduce the usage of resources for generating shared secret key this link based key or shared session key method is developed. This link based shared session key is used only to the nodes that which linked each other. The node which is not linked with other nodes is made to be linked with the neighbouring nodes and then the cryptographic keys are established to make the node securely transfer the data to Base Station. The BROadcast Session Key (BROSK) is the protocol that which makes the node to broadcast the key negotiation message. This key negotiation message is broadcasted by the Base station. The node which receives broadcasted message will construct the shared-session keys with nonce. After a particular time period this session keys are regenerated by again negotiating the session keys. These keys are regenerated to reduce the security attacks of the network. When keys are changed the attacker will not be able to know the new key which results in secure transmission of data to the other nodes.

F. SPINS: Security Protocols for Sensor Networks [26]

SPINS is the protocol developed for providing security to Wireless Sensor Networks, it has two building blocks SNEP and µTESLA. The SNEP provides data confidentiality, data authentication, and data freshness. µTESLA provides authentication for broadcast messages. The SNEP protocol provides a counter value to each nodes of the network which is encrypted with the data and is transmitted to other node. With the counter value node identifies that the message received is from the exact node which is connected to the network. To identify the correct and current counter value of the node a nonce is included with the message that is transmitted.

In µTESLA the authentication for broadcasting message is given by using the asymmetry through a delayed disclosure of symmetric keys. The message is sent as packets to other nodes with MAC (Message Authentication Code) key and the secret. This MAC key is generated by public one-way function and it is a chain of key. These proposed protocols has the advantages like low communication cost, weak freshness, replay protection, semantic security, etc,..

TABLE I

Different Methods of Key Management

No.	Protocol used	Cryptographic method	Key Storage(Preloading)	Resources Consumed
1.	Pairing based method [21]	Pairing Based Elliptic-Curve Cryptography[15]	Each nodes knows its ID, Secret Point and Random number, H- node knows IDs of all L-node of its cluster.	Memory is not consumed more but the computation of keys is done by nodes of network,
2.	LIGER=LION(Infrastructureless environment)+TIGER(Based on Key Distribution Centre) [22]	RC5 Symmetric key block-cipher[13]	Yes	Only the shared key is computed by the nodes
3.	PIKE [23]	MAC [27,28]	Yes	The intermediary node

				helps in reducing the usage of energy resources
4.	LEAP [24]	RC5 Symmetric Key block-cipher[13]	Yes	Separate types of keys are preloaded to reduce the usage of same keys by the nodes.
5.	BROSK [25]	MAC [27,28]	No, only the ID and nonce for generating shared session key is stored.	Shared-secret Key is computed by the node.
6.	SPINS 2 Building blocks (SNEP and µTESLA) [26]	RC5 Symmetric Key block-cipher[13]	Yes	Secret Keys are preloaded to reduce the computation energy of the sensor nodes.

IV. CONCLUSION

In this paper different Resource-efficient key management protocols and mechanisms of wireless sensor networks have been surveyed which specifies the generation of cryptographic keys for their secure transaction of data. There are different methods for generating the keys efficiently without wasting the resources of the sensor nodes. In wireless sensor networks resources are the main constraint that has to be considered while performing any of the operations. From the above given paper it is known that while generating the cryptographic keys for sensor networks all the resources of the network must be maintained and also it should not reduce the security of the networks.

REFERENCES

[1] Dargie, W. and Poellabauer,C. ,"Fundamentals of Wireless Sensor Networks: Theory and Practise", John Wiley and sons, 2010.

[2] Vasyl A, Radzevych, and Sunu Mathew, "Security in Wireless Sensor Networks: Key Management Approaches".

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniyam and E.Cayirci "Wireless Sensor Networks: A Survey".

[4] Johnson C.Lee, Victor C.M.Lueng, Kirk H.Wong, Jiannano Cao , Henry C.B. Chan, "Key Management Techniques in Wireless Sensor Networks".

[5] J. Zhang, V. Varadharajan, Wireless sensor network key management survey and taxonomy, Journal of Network and Computer Applications 33 (2) (2010) 63–75.

[6] IrfanLandge, TasneemBharmal and PoojaNarwankar, "Encryption and decryption of data using twofish algorithm", World Journal of Science and Technology 2012, 2(3):157-161.

[7] Tom Moore, Kenneth Ballentine, "Serpent Cipher Design and Analysis", www.cs.rit.edu/kxb3695/csc482/report.pdf

[8] Eric Conrad, "Advanced Encryption Standard", www.giac.org/cissp-papers/ 42.pdf.

[9] Blowfish Encryption Algorithm pocketbrief.net/related/BlowfishEncryption.pdf.

[10] H. M. Heys and S. E. T avares, "On the Security of the CAST Encryption Algorithm" Department of Electrical and Computer Engineering, Queen's University Kingston, Ontario, Canada

[11] William Stallings, "The Rc4 Stream Encryption Algorithm".

[12] Triple Data Encryption Standard (Triple-DES)http://www.vocal.com/cryptography/ tdes/.

[13] Ronald L Rivest, "The RC5 Encryption Algorithm", MIT Laboratory for Computer Science & Technology Square, Cambridge, Mass. 02139, Revised March 1997.

[14] How-Shen Chang, International Data Encryption Algorithm. https://users. cs.jmu.edu/IDEA-by-How-Shen-Chang-2004-FALL.

[15] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig,and Eric Wustrow, "Elliptic Curve Cryptography in Practice", https://eprint.iacr.org/2013/734.pdf.

[16] Merkle's Puzzles http://crypto-it.net /eng/asymmetric/merkle_puzzles.html.

[17] EvgenyMilanov, "The RSA Algorithm", june 3 2009.

[18] The ElGamal Public Key Encryption Algorithm, www.math.uic.edu/leon/ mcs425-s08/handouts/el-gamal.pdf.

[19] Encrypting files with OpenPGP http://blog.linomasoftware.com/2011/04/11/encrypting-files-with-openpgp/.

[20] B. Kaliski, Public-Key Cryptography Standards (PKCS) #8:Private-Key Information Syntax Specification Version 1.2, May 2008.

[21] S.M. Rahman, K. El-Khatib, Private key agreement and secure communication for heterogeneous sensor networks, Journal of Parallel and Distributed Computing 70 (8) (2010) 858–870.

[22] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, T. La Porta, Efficient hybrid security mechanisms for heterogeneous sensor networks, IEEE Transactions on Mobile Computing 6 (6) (2007) 663–677.

[23] H. Chan, A. Perrig, PIKE: peer intermediaries for key establishment in sensor networks, in: Proc. of IEEE INFOCOM05, March 2005, pp. 524–535.

[24] S. Zhu, S. Setia, S. Jajodia, LEAP: efficient security mechanisms for largescale distributed sensor networks, in: Proc. of the 10th ACM Conference on Computer and Communications Security, October 2003, pp. 62–72.

[25] B. Lai, S. Kim, I. Verbauwhede, Scalable session key construction protocol for wireless sensor networks, in: Proc. of the IEEE Workshop on Large Scale Realtime and Embedded Systems, December 2002.

[26] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, J.D. Tygar, SPINS: security protocols for sensor networks, in: Proc. of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking, July 2001, pp. 189–199.

[27] Yuan Xue, "Message Authentication Code",https://tao.truststc.org/Members/yuanxue/network...notes/download.

[28] MarkCC, "Cryptographic Integrity using Message Authentication Codes"http://scientopia.org/blogs/goodmath/2008/10/06/cryptographic-integrity-using-message-authentication-codes, March 2006