# A Survey on Cryptographic Schemes used in Wireless Sensor Networks

K.Swaathi
PG Scholar, Department Of CSE
SNS College of Technology
Coimbatore-35,India
swaathik@gmail.com

Prof.B.Vinodhini
Assistant Professor,Department Of CSE,
SNS College of Technology
Coimbatore-35,India
vinodhini.raja@gmail.com

Dr.S.Karthik
Professor and Dean/ CSE
SNS College of Technology
Coimbatore-35,India
profskarthik@gmail.com

**Abstract**— ***Security is considered to be an important issue in wireless sensor networks.Clustering is an effectual and convenient way to enhance performance of the WSN system. Sensor nodes have limited power, computational capabilities and memory. Cryptography is the most offered security service in WSN. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power are needed. For ensuring robust security for the network, the keys are to be managed, revoked, assigned to a new sensor network or renewed. In this paper different cryptographic schemes and their encountered issues are discussed.***

**Keywords- CWSN, Cluster-Head, Key management, Identity based cryptography**

## I. INTRODUCTION

Wireless sensor network is a network consisting of spatially distributed autonomous sensors to monitor physical or environmental conditions like temperature, pressure, sound etc. It is built of sensor nodes. Sensors are inexpensive, low-power devices which have limited resources. Sensors are small in size, and have wireless communication capability within short distances. The sensor nodes vary in size, quantity and cost. A sensor node typically contains a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter / receiver. A wireless sensor network is composed of large number of sensor nodes with limited power, computation, storage and communication capabilities. The topology of WSN varies from a simple star to multi hop wireless mesh network. Security in WSN has six challenges: (i) wireless nature of communication, (ii) resource limitation on sensor nodes, (iii) very large and dense WSN, (iv) lack of fixed infrastructure, (v) unknown network topology prior to deployment, (vi) high risk of physical attacks to unattended sensors.

Sensor nodes are more prone to failures due to frequent environment changes. Security solutions for such applications depend on existence of strong and efficient key distribution mechanisms. It is infeasible, or even impossible in uncontrolled environments, to visit large number of sensor nodes, and change their configuration. Moreover, use of a single shared key in whole WSN is not a good idea because an adversary can easily obtain the key. Thus, sensor nodes have to adapt their environments, and establish a secure network by: (i) using pre-distributed keys or keying materials, (ii) exchanging information with their immediate neighbors, or (iii) exchanging information with computationally robust nodes.

Clustering of sensor nodes improves performance by maximizing the network life span and reducing bandwidth utilization. Thus cluster-based transmission of data in WSNs accomplish the network scalability and supervision.

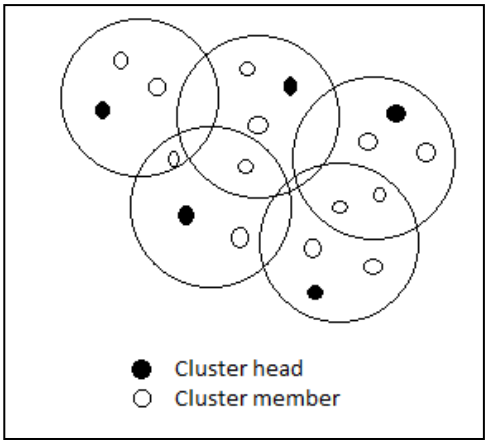


Figure 1. Clustered Wireless Sensor Network

In a cluster-based WSN (CWSN), each cluster has a leader sensor node, known as cluster-head (CH). A CH collects the data gathered by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the aggregated data to the base station (BS).The probability of the asymmetric key management has been revealed in WSNs in recent times, which compensates the deficiency from relating the symmetric key management for security. Digital signature is one of the most significant security services presented by cryptography in asymmetric key management systems, where the binding between the public key and the recognition of the signer is acquired via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the complexity of factoring integers from Identity- Based Cryptography (IBC), is to develop an entity's public key from its character information, e.g., from its identification number or its name. This states that security must encompass all the characteristics of availability, authorization, authentication, confidentiality, integrity and non-repudiation. Probable applications comprise monitoring isolated or hostile locations, objective tracking in combat zone, catastrophe liberation networks, premature fire recognition, and environmental supervision.

## II. LITERATURE SURVEY

This section defines the various asymmetric-key cryptographic methods employed in wireless sensor networks and their issues related to power and energy consumption.

### *A. Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks*

Huang Lu *et.al* proposed a new secure routing protocol with ID-based signature scheme for cluster-based WSNs within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. The formation of clusters is done periodically and dynamically in a cluster-based sensor networks. The disadvantage in using the symmetric key cryptography is pointed out. The orphan node problem arising due to the use of symmetric key is solved here. Two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively are proposed. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, while its security relies on the hardness of the discrete logarithm problem. SET-IBS and SET-IBOOS are efficient in communication and applying the ID based cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. The SET-IBS and SET-IBOOS protocols consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS or IBOOS process as in [1].

### *B. An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures*

In Wireless Sensor Networks (WSNs), authentication is a crucial security necessity to avoid attacks against secure communication. Sensors have resource constraints which pose a serious demerit in applying strong public key cryptographic based mechanisms in WSNs. To deal with the problem of authentication in WSNs, Yasmin, R *et.al* have proposed secure and efficient framework for authenticated broadcast/multicast by sensor nodes and for outside user authentication, which uses identity based cryptography and online/offline signature schemes. The most important objectives of this framework are to allow all sensor nodes in the network, initially, to broadcast and/or multicast an authenticated message rapidly; secondly, to confirm the broadcast/multicast message sender and the message contents; and lastly, to confirm the authenticity of an outside user. In offline phase, the most

time consuming computations are performed and once the message becomes available the online signature is computed within seconds. The projected framework is also evaluated by means of the most secure and efficient identity-based signature (IBS) schemes as in [2].

*C. IKM -- An Identity based Key Management Scheme for Heterogeneous Sensor Networks*

ManelBoujelben et.al proposed IKM, an identity based key management scheme designed for heterogeneous sensor networks. This scheme provides a high level of security as it is based on pairing identity based cryptography. The IKM scheme supports the establishment of two types of keys, pair-wise key to enable point to point communication between pairs of neighboring nodes, and cluster key to make in-network processing feasible in each cluster of nodes. IKM also supports the addition of new nodes and rekeying mechanism. The pairing key management scheme provides low storage cost compared to other key management schemes. An overhead analysis of the proposed scheme is performed in terms of storage, communication, and computation requirements. It can be deployed efficiently in resource-constrained sensor networks that need a high level of security. It can be efficiently implemented in real sensor networks, running security critical applications as in [3].

*D. Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network*

Joseph K. Liu et.al presented an online/offline identity-based signature scheme for the wireless sensor network (WSN). One of the interesting features of this scheme is that it provides multi-time usage of the offline storage, which allows the signer to re-use the offline pre-computed information in polynomial time, in contrast to onetime usage in all previous online/offline signature schemes.Earlier, the only existing ID-based online/offline signature scheme was designed by Xu, Mu and Susilo (this scheme will be referred to as the "XMS" scheme hereafter). In XMS scheme, the signer needs to execute the offline phase every time when he wants to produce a signature. It is called "*one-time*" meaning the offline signature part can be used only *once* and hence, it cannot be re-used. If this one-time scheme is applied into WSN, it becomes impractical since, assuming the offline phase is done at the base station, non-reusability of the storage implies that sensors need to go back to the base station every time for obtaining the next offline signature part. Moreover, the verification of the XMS scheme requires a *pairing* operation, which is a costly computation process for a sensor node.The new technique allows the offline information to be reusable. This way, the signer is not required to execute the offline algorithm every time when he wants to sign a new message. Furthermore, unlike most of the existing (non ID-based) online/offline signatures, our offline signing algorithm does not require any secret information from the signer. Hence, it can be generated by any trusted third party including the PKG. This is particularly useful for a WSN node as the base station, acting as a PKG, can generate the offline information and the node does not need to return to the base station for the renewal of the offline information every time signing is performed. Even this offline information can be hardcoded into the node in the manufacturing stage. This can save a lot communication bandwidth, which is considered to be an expensive cost in the WSN environment as in [4].

*E. An Efficient ID-based Digital Signature with Message Recovery Based on Pairing*

Raylin Tso et.al proposed a new ID-based signature scheme with message recovery. In this scheme (as well as other signature schemes with message recovery), the message itself is not required to be transmitted together with the signature, it turns out to have the least data size of communication cost comparing with generic (not short) signature schemes. Although the communication overhead is still larger than Boneh et al. 's short signature (which is not ID based), the computational cost of our scheme is more efficient than Boneh et al. 's scheme in the verification phase. The concept of identity-based (ID-based) cryptosystem was firstly introduced by Shamir in 1984 which can simplify key management procedures of traditional certificate-based cryptography. Many ID-based cryptosystems have been proposed since that but no IDbased signature scheme with message recovery goes out into the world until the scheme proposed by Zhang et al. in 2005. Zhang et al. proposed two schemes in the paper: an ID-based message recovery signature scheme for messages of fixed length, and an ID-based partial message recovery signature scheme for messages of arbitrary length. Zhang et al.'s idea gives a new concept to shorten ID-based signatures in contrast to proposing a short signature scheme. Our scheme improves the computational cost by one scalar multiplication in the signing phase and almost one pairing computation in the verify/message-recovery phase comparing to Zhang et al. 's scheme. It inherits the efficiency of their scheme on one side and also reduce the total length of the original message and the appended signature on the other side as in [5].

*F. Security in wireless sensor networks: key management module in SOOAWSN*

Mohammed A. Abhuhelale et.al have proposed three methods that represent a complete key management solution that can be applied to LEACH or any similar protocol: Key pre-distribution(KP) method, Public and Private keys method, Multi-generations key method. The aim of KP method method is to have different levels of security on the network communication for the first generation of the network deployment.Their solution adopted the pair-wise key pre-distribution to provide WSN with different level of security. In public and private key method, each sensor use two keys for communication with other sensors, Public key and Private Key; the idea is similar to the traditional use of public and private keys in asymmetric key cryptography in traditional networks. The use of public and private keys provides WSN with higher security level and provides the sensors an alternative way to exchange new keys. The Multi-generations key method relates to the first method. The idea is to reuse the keys that produced from the key pool in KD technique to support key refreshes and to support the expansion of the current sensor network. Finally, the technique that is applied on renewing the key pool provides WSN with an ability to support multi-generations of sensors. The solution is found out by applying it on LEACH as in [6].

*G. IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks*

SriramSankaran et.al presented an identity based key management scheme using Identity-Based Encryption (IBE). IBE facilitates faster key set-up in addition to being lightweight and energy-efficient. This scheme uses IBE to set up pair-wise symmetric keys to preserve data confidentiality and integrity. Publisher-Subscriber driven Body Area Networks enable publishers (medical sensors attached to patients) to disseminate medical data to numerous mobile heterogeneous subscribers (doctors or caregivers) through a subscription mechanism. Such an environment raises serious security concerns due to the privacy critical medical data coupled with the resource constraints of individual body sensors. IBE is based on Identity based cryptography, initially introduced by Adi Shamir in 1984. IBE is used only to exchange pair-wise symmetric keys between publishers and subscribers. The symmetric keys are used in subsequent communications thus reducing the computational overhead on the publishers. IDKEYMAN consists of four phases: Pre-operational phase, Operational phase, Post-operational phase and Destroyed phase. In first phase, each subscriber is pre-distributed with the private key Ks and public key Ksub in addition to a function that takes the ID of the publisher and outputs its corresponding public key. In second phase, the patient identification number (PID) is obtained from the RFID tag and once the patient's information PID is obtained, the mote collects PID, its id MoteID, generates a nonce n1, encrypts message using public key of the subscriber Ksub and sends it securely to the subscriber. Then the subscriber decrypts the received message using its private key Ks and verifies the authenticity of this patient using PID and MoteID. After decrypting the message using Kp and obtaining the pair-wise secret keys, publisher sends a message containing its ID and subscriber's ID encrypted using the pair-wise secret key Kp,s, which is decrypted by subscriber and confirmed. The pair-wise secret keys are used as session keys for future communications. In the last phase, if the public key of the subscriber is compromised, we need to re-initialize the expensive pre-operational phase but there exists no other way to fix this issue. On the other hand, if the pair-wise or session key is compromised, initiating the key agreement process will help solve the problem. IDKEYMAN addresses the real-time and stringent resource requirements of individual body sensors while also being robust to attacks as in [7].

## III. CONCLUSION

The current state of the art of research in sensor networks dealing with security related problems is discussed. The Protocols like LEACH which are cluster based data transmission protocols suffer from variety of security threats. Adding security to such protocols is little bit tricky since they arbitrarily, occasionally and vigorously rearrange the network's clusters and data links thereby threatening the security and vulnerability of the CWSNs. The survey has also revealed some possible future research directions. These include developing security protocols based on asymmetric key cryptography for achieving better efficiency and reduced energy consumption.

## REFERENCES

[1] Huang Lu and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, March 2014.

[2] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures", Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[3] M. Boujelben, H. Youssef, R. Mzid and M. Abid, "IKM -- An Identity based Key Management Scheme for Heterogeneous Sensor Networks", Journal of Communications, vol. 6, no. 2, April 2011.

[4] J.K. Liu, J. Baek, J. Zhou, Y. Yang," Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network", in Lecture Notes. Computer Science, - Appl. Cryptography Network Security, 2009.
[5] R. Tso, C. Gu, T. Okamoto. "An Efficient ID-based Digital Signature with Message Recovery Based on Pairing", Journal of Cryptology, 13(3), pp.361–396, 2006.
[6] M.A. Abuhelaleh and K.M. Elleithy," Security in wireless sensor networks: key management module in SOOAWSN", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.
[7] S. Sankaran, M. Husain, and R. Sridhar,"IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks", Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2010.
[8] H. Lu, J. Li, and H. Kameda," A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature", CONFERENCE PAPER, Report Version, DOI: 10.6084/m9.figshare.761472
[9] J.K. Liu, J. Baek, J. Zhou, "Online/offine identity-based signcryption re-visited", Cryptology ePrint Archive, Report 2010/274, 2010.
[10] M. Rohbanian, M. Kharazmi, A. Keshavarz-Haddad, M. Keshtgary," Watchdog-LEACH: A new method based on LEACH protocol to Secure Clustered Wireless Sensor Networks", cmc, vol. 1, pp.142-146, International Conference on Communications and Mobile Computing, 2010.
[11] Aftab Ali and Farrukh Aslam Khan," Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications", EURASIP Journal on Wireless Communications and Networking SpringerOpen journal, 2013.
[12] Shu Yun Lim a , Meng-Hui Lim, "Energy-Efficient and Scalable Group Key Management for Hierarchical Sensor Network" Journal of Ubiquitous Systems & Pervasive Networks Volume 2, No. 1 (2011) pp. 39-47.
[13] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2,pp. 2-23, Second Quarter 2006.
[14] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2826-2841, 2007.
[15] W. Diffie and M. Hellman, "New Directions in Cryptography,"IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.