www.ijiarec.com

ISSN: 2348-2079

FEB-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

ENERGY EFFICIENT DATA TRANSMISSION IN CLUSTERED WIRELESS SENSOR NETWORKS WITH SENSOR SCHEDULING ALGORITHM

[1]K.Swaathi, [2]Prof.B.Vinodhini, [3]Dr.S.Karthik

ABSTRACT

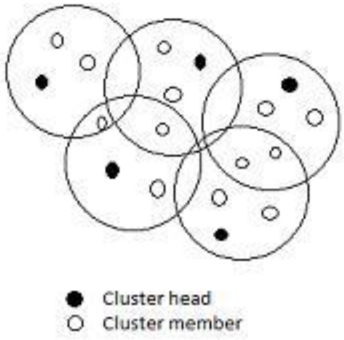
Coverage preservation and prolonging lifetime are the fundamental issues in Clustered Wireless Sensor Networks. Sensor nodes have limited power, computational capabilities and memory. Sensing, transmitting and receiving activities consume battery energy of a sensor, and also limit the network lifetime. Applying the identity based cryptography in CWSN ensures only security and it leads to quick energy drain. To save energy, it should be necessary to schedule the sensor activity such that to allow redundant sensors to enter the sleep mode as often and for as long as possible. The statute of all the deployed sensors should be determined to be either active or sleep based on their capabilities as well as the state durations, such that the network lifetime is maximized. Cluster-based efficient-energy coverage scheme called CSA is proposed to ensure the full coverage of a monitored area while saving energy. CSA uses a sensor scheduling scheme based on the k-density and the remaining energy of each sensor to determine the state of all the deployed sensors as well as the state durations. It aims to provide a better performance in terms of the energy consumption and network lifetime.

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

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

Author for Correspondence:
[1]PG Scholar, Department Of CSE, SNS College of Technology, Coimbatore-35, India, swaathik@gmail.com
[2]Assistant Professor, Department Of CSE, SNS College of Technology, Coimbatore-35, India, vinodhini.raja@gmail.com
[3]Professor and Dean/ CSE, SNS College of Technology, Coimbatore-35, India, profskarthik@gmail.com

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 accomplishes the network scalability and supervision.

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.

RELATED WORK

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].

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].

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].

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 as in [4].

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].

PROBLEM FORMULATION

A new secure routing protocol with ID-based signature scheme for cluster-based WSNs is designed within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. 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 used.

In SET-IBS, the message is encrypted and transmitted to cluster head with the generation of identity based key. SET-IBOOS computes a partial signature even before acquiring a message. Once the message becomes available, it computes the online signature with the help of receiver's identity and transmits the encrypted message. Hence it achieves the security requirements as well as the efficient transmission. The orphan node problem arising due to the use of symmetric key cryptography is solved. SET-IBS and SET-IBOOS are efficient in communication. By applying the ID based cryptosystem, it achieves the security requirements in CWSNs. SET-IBS and SET-IBOOS show better performance than existing security protocols for CWSNs.

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. The network lifetime is reduced due to extra energy consumption by IBS and IBOOS schemes.

SYSTEM MODEL

NODE DEPLOYMENT

Sensors are expected to be remotely deployed in large numbers and to operate autonomously in unattended environments. To support scalability, nodes are often grouped into disjoint and mostly non-overlapping clusters. Every cluster would have a leader, often referred to as the cluster-head (CH). A CH may be elected by the sensors in a cluster or pre-assigned by the network designer. A CH may also be just one of the sensors or a node that is richer in resources. The cluster membership may be fixed or variable. CHs may form a second tier network or may just ship the data to interested parties like a base-station or a command center. It can localize the route set up within the cluster and thus reduce the size of the routing table stored at the individual node. Clustering can also conserve communication bandwidth since it limits the scope of inter-cluster interactions to CHs and avoids redundant exchange of messages among sensor nodes.

The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained. In CWSNs, data sensing, processing, and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node (e.g., a CH) aggregates data and sends it to the BS is preferred than the method that each sensor node directly sends data to the BS. A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the time-division multiple access (TDMA) control used for data transmission.

DATA TRANSMISSION BETWEEN SENSOR NODE AND CLUSTER HEAD

The sensor node sends data to the respective Cluster head. The Cluster Head aggregates the data received and sends to the Base station. The leader is responsible for sending the aggregated information to the sink or base station. The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks. Especially, attacks to CHs in CWSNs could result in serious damage to the network because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending bogus information toward the CHs.

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between leaf nodes and CHs, as well as transmission between CHs and the BS. Most of the existing secure transmission protocols for CWSNs apply the symmetric key management for security, which suffers from the orphan node problem. This problem occurs when a node does not share a pairwise key with others in its preloaded key ring. To mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pairwise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH.

The orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pairwise keys decreases after a long-term operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

This orphan node problem is solved by using the ID based cryptosystem that guarantees security requirements, and designed SET-IBS by using the IBS scheme. SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

The asymmetric key management compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. The identity-based digital signature (IBS) scheme, based on the difficulty of factoring integers from identity-based cryptography (IBC), is to derive an entity’s public key from its identity information, for example, from its name or ID number. The concept of IBS has been developed as a key management in WSNs for security.

SIGNATURE VERIFICATION

The Trusted Authority is responsible for verifying the signature of the sender and it send the data to the Base station only if the signature is valid.

IBS Scheme for CWSNs

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes:

1. Setup:

   The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
2. Extraction:

   Given an ID string, a sensor nod generates a private key sekID associate with the ID using msk.
3. Signature signing:

   Given a message M, time stamp t and a signing key _, the sending node generates a signature SIG.
4. Verification:

   Given the ID, M, and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

IBOOS Scheme for CSWNs

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes

1. Setup:

   The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
2. Extraction:

   Given an ID string, a sensor nod generates a private key sekID associate with the ID using msk.
3. Offline signing:

   Given public parameters and time stamp t, the CH sensor node generates an offline signature SIGoffline, and transmit it to the leaf nodes in its cluster.
4. Online signing:

   From the private key sekID, SIGoffline and message M, a sending node (leaf node) generates an online signature SIGonline.
5. Verification:

   Given ID, M, and SIGonline, the receiving node (CH node) outputs "accept" if SIGonline is valid, and outputs "reject" otherwise.

BOOS PROTOCOL OPERATION

SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. All sensor nodes know the starting and ending time of each round because of the time synchronization. The operation of SET-IBS is divided by rounds. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS.

In each round, the timeline is divided into consecutive time slots by the TDMA control. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly elected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. To elect CHs in a new round, each sensor node determines a random number and compares it with a threshold. If the value is less than the threshold, the sensor node becomes a CH for the current round. In this way, the new CHs are self-elected based by the sensor nodes themselves only on their local decisions. SET-IBS functions without data transmission with each other in the CH rotations. In the setup phase, the time stamp Ts and node IDs are used for the signature generation. In the steady state phase, the time stamp tj is used for the signature generation securing the inner cluster communications, and Ts is used for the signature generation securing the CH-to-BS data transmission.

ATTACK MODELS

To evaluate the security of the proposed protocols, the attack models in WSNs that threaten the proposed protocols are investigated, and the cases when an adversary (attacker) exists in the network. The attack models are grouped into three categories according to their attacking means.

Passive Attack on Wireless Channel

Passive attackers are able to perform eavesdropping at any point of the network, or even the whole communication of the network. Thus, passive attckers can undertake traffic analysis or statistical analysis based on the monitored or eavesdropped messages.

Active Attack on Wireless Channel

Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, the attackers can forge, reply, and modify messages. Especially in WSNs, various types of active attacks can be triggered by attackers, such as bogus and replayed routing information attack, sinkhole and wormhole attack, selective forwarding attack, HELLO flood attack, and Sybil attack.

CONCLUSION

Applying the identity based cryptography in CWSN ensures only security. Security protocols based on identity-based cryptography consumes energy faster than SecLEACH and LEACH protocols. Applying any encryption scheme, a node may require transmission of extra bits. Hence extra processing, memory and battery power are needed. To save energy, it should be necessary to schedule the sensor activity such that to allow redundant sensors to enter the sleep mode as often and for as long as possible. The statute of all the deployed sensors should be determined to be either active or sleep based on their capabilities as well as the state durations, such that the network lifetime is maximized. Cluster-based efficient-energy coverage scheme called CSA is proposed to ensure the full coverage of a monitored area while saving energy. It aims to provide a better performance in terms of the energy consumption and network lifetime.

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.