International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e- ISSN: 2395-5325
Volume 1. Issue 1. April '2015

IDENTIY BASED DIGITAL SIGNATURE SCHEME ON CLUSTER BASED WIRELESS SENSOR NETWORKS

J.Benitha Christinal,
Assistant Professor,
SNS College of engineering,
Coimbatore

ABSTRACT: In a Wireless Sensor Networks (WSNs) secure data transmission is a critical concern. Clustering of wireless sensor networks is a valuable and practical way to enhance the performance of WSNs. This survey proposes a two secure and efficient data transmission (SET) protocols for Cluster based WSNs, 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. In SET-IBS, the security will base on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further decreases the computational overhead for protocol security, which is crucial for WSNs.In SET-IBOOS scheme the security relies on the hardness of the discrete logarithm problem. This survey explains that an identity based protocols have better performance than the existing protocols like LEACH, SEC-LEACH, ROUTING-Leach for CWSNs, in terms of security overhead and energy consumption.

Key Words: - Cluster-based WSNs, ID-based online/offline digital signature, ID-based digital signature, secure data transmission protocol.

I.INTRODUCTION

Network

Based on information technology, a network is a series of points or nodes interconnected by communication paths. Networks can also be interconnect with other networks and may contain sub networks. A group of interconnected computers and peripherals either by using wire like cable and wireless is capable of sharing software and hardware resources between many users. The Internet is a global network of networks. A system that enables users of telephones or data communications lines to exchange information over long distances by connecting with each other through a system of routers, servers, switches, and the like.

Wireless Sensor Network

Wireless Sensor Networks contains a large number of sensor nodes .These nodes may having limited assets for energy, transmission power, network bandwidth, and computation power. This sensor node governs the physical environment from neighborhood nodes, and collects data from these nodes and then processes information. Sensor networks are not just data networks with sensors being the sources of data because the sensor networks are often developed and deployed for a particular application. The entire network operation is accordingly changed towards satisfying the application. In order to increase overall system efficiency, nodes will perform computations on data which is opposed to simply originating or forwarding information.

A wireless sensor network consists of tiny sensing devices, which normally run on battery power and randomly deployed for detecting and monitoring tasks . One of the typical applications in this network, gathering and sending sensed data to the base station

Cluster Based Wireless Sensor Network

CBRP achieves a good performance in terms of lifetime by balancing the energy load among all the nodes. Formation of Cluster done in the network by using new factors and then construct a spanning tree for sending aggregated data to the base station which can better handle the heterogeneous energy capacities.

Cluster Based Wireless Sensor Network.(CBRP)

CBRP is a distributed and energy efficient protocol. CBRP, define new algorithm for cluster head election that can better handle heterogeneous energy circumstances than existing clustering algorithms which elect the cluster head only based on a node's own residual energy. After the cluster formation phase, CBRP constructs a spanning tree over all of the cluster heads. Only the root node of this tree can communicate with the sink node by single-hop communication.

Identity Based Scheme

The specific goal of the project is to create the secure and efficient data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. The SET-IBS and SET-IBOOS protocols need to be implemented with respect to the security requirements. The proposed SET-IBS and SET-IBOOS protocols need to consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS or IBOOS process. The proposed SET-IBOOS need to achieve a better balance of energy consumption than that of SecLEACH protocol. SET-IBS and SET-IBOOS protocols need to provide Solutions to passive attacks on wireless channel, Solutions to active attacks on wireless channel. Solutions to node compromising attacks.

II.LITERATURE SURVEY- EXISTING SYSTEM

- **Leach Protocol**
- **Leach Like Protocols**
  - **Secleach**
  - **Gsleach**
  - **Rleach**

a) LEACH

In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The low-energy adaptive clustering hierarchy (LEACH) protocol presented is a widely known and effective one to reduce and balance the total energy consumption for CWSNs.To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensors nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime.

b) LEACH LIKE PROTOCOLS

A number of protocols have been presented such as APTEEN and PEACH, which use similar concepts of LEACH called LEACH LIKE PROTOCOLS

c) SECLEACH-(SECURITY LEACH)

[2]This paper investigates the problem of adding security to hierarchical/cluster-based sensor networks where clusters are formed dynamically and periodically, such as LEACH. For this purpose, random key pre distribution, of flat networks, can be used to secure communications in CWNS. The main advantage of this scheme was security is concerned.

d) GSLEACH-(GRID-BASED SECURE LEACH)

[3]The GS-LEACH (grid-based secure LEACH) protocol uses pre deployment key distribution using prior knowledge of the deployment area.The main advantage of this method is The GS-LEACH protocol is more energy efficient than any of the secure flavors of LEACH also GS-LEACH provides a longer network lifetime compared to the other flavors of LEACH.

e) RLEACH-ROUTING LEACH

[4]In this paper, we investigate adding security to cluster-based routing protocols for wireless sensor networks which consisted of sensor nodes with severely limited resources, and introduce a security solution for LEACH, a protocol in which the clusters are formed dynamically and periodically. Our solution uses improved random pair-wise keys (RPK) scheme, an optimized security scheme that relies on symmetric-key methods**.** The main advantage of this method is RLEACH Is Lightweight and Preserves the Core of the Original LEACH and also Security Of RLEACH Has Been Improved. This method consume Less Energy

III.PROBLEM STATEMENT

a) LEACH LIKE PROTOCOLS

Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust Relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs).

b) SYMMETRIC KEY MANAGEMENT

There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH, and RLEACH. Most of them, however, apply the symmetric key management for security, which suffers froma so-called orphan node problem.

c) ORPHAN NODE PROBLEM

- This problem occurs when a node does not share a pair wise 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 pair wise symmetric keys with all of the nodes in a network.
- Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pair wise 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.

d) PAIRWISE KEY SHARING

Even in the case that a sensor node does share a pair wise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

IV.PROPOSED SYSTEM

The feasibility of the asymmetric key management has been used in WSNs recently, which 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. Recently, the concept of IBS has been developed as a key management in WSNs for security.

The IBOOS scheme has been proposed to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced. The IBOOS scheme could be effective for the key management in WSNs. Specifically, the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

ADVANTAGES OF PROPOSED SYSTEM

- The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.
- In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based cryptosystems
- Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.
- SET-IBOOS is proposed to further reduce the computational overhead for security using the IBOOS scheme.
- Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with asymmetric key management.
- The proposed protocols with respect to the security requirements and analysis against three attack models such as active attack, passive attack, compromising attack.

V.CONCLUSION

These surveys introduce the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS.The SET-IBS and SETIBOOS are efficient in communication and applying the IDbased 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.

VI.REFERENCES

1. W. Heinemann, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.
2. L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

3. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks,"Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
4. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
5. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53,1985.
6. J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.

AUTHOR'S PROFILE

J.Benitha Christinal obtained her bachelor's degree in Computer science and Engineering from Karunya University Coimbatore, TamilNadu, India and Masters Degree in Computer science and Engineering from Karunya University Coimbatore, TamilNadu, India. She currently is working as Assistant Professor in Department of Computer Science and Engineering, in SNS College of Engineering, Coimbatore, and TamilNadu. Her research interests include wireless sensor networks, Database management system, Networking and Web designing. She has published 12 papers in reputed international, national level conferences and International journals.