International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 5 (August '2015)

A STUDY ON SECURE DATA TRANSMISSION IN CLUSTER BASED WIRELESS SENSOR NETWORKS

C.Priya,
M.Phil Scholar,
Department Of Computer Science,
Dr. R.A.N.M. Arts & Science College,
Erode, Tamilnadu, India.

M.Suriya,
Head and Assistant Professor,
Department Of Computer Applications,
Dr. R.A.N.M. Arts & Science College,
Erode, Tamilnadu, India.

Abstract: Secure data transmission is a critical issue for wireless sensor networks. Clustering is an effective and practical way to enhance the system performance of WSNs. A secure data transmission for cluster-based WSNs is studied, where the clusters are formed dynamically and periodically. User propose two Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature scheme and the Identity-Based Online/Offline digital Signature scheme, respectively. In SET-IBS, security relies on the hardness of the Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Keywords: Cluster, Secure, data transmission, Key Management, Wireless sensor Network

I. INTRODUCTION

Recent development in the field of miniaturization led to the development of small tiny sensor nodes which can be deployed on various locations for achieving certain goals. The sensors are capable of self organizing themselves to form a network. Sensors are randomly deployed in the area of interest. As the devices are very small and inexpensive, they can be deployed in large numbers for better accurate sensing. They monitor conditions at different locations such as temperature, humidity, pressure, vehicular movement, soil makeup, lightning condition, noise levels, the presence or absence of certain kind of object etc. The most straight forward application of sensor technology is to monitor remote locations without human interruption [1].

Applications include military, home, Habitat Monitoring, Agriculture etc. For a vast area to be sensed, it is foreseen that even thousands of thousands of sensor nodes are used due to the possibility of damage during deployment. Operating such a huge and complex network requires scalable architecture and management strategies. Scalability in a sensor network can be achieved by a technique known as Clustering where the sensor nodes are grouped in to various clusters and each cluster having a cluster head [2].

The cluster heads may be predesigned by the network designer or elected by the sensors in the network. Clustering algorithms for sensor networks improves network scalability by handling two important problems regarding the size and mobility of the network. Various clustering algorithms have been proposed by the research community. They vary according to the overall network architecture, Node deploying methods and based on the characteristics of the CH node. Number of cluster member will vary according to the application. Usually a cluster head is a node which is very rich in energy resources. Sometimes cluster heads may form a second tier in the network. CH in such architecture acts as relay nodes.

Relay nodes have been proposed in sensor networks for achieving various objectives like data gathering, reduction of transmission range, fault tolerance etc. the communication from the relay nodes and base stations can either be single hop or multi-hop. In a single-hop model CHs send their data directly to the base station[3][4].

Where as in multi-hop CHs send their data through other CHs, thus CHs in such models not only acts as relay nodes for transferring the data to base station, but also collects the data from other relay nodes and transfer the data to the base station. User has presented various design issues and challenges that occur with clustering in wireless sensor networks. Wireless sensor networks (WSNs) are emerging as a technology for monitoring different environments of interest and they find applications ranging from battlefield

reconnaissance to environmental protection. When embedded in critical applications, WSNs are likely to be attacked. Aside from the well known vulnerabilities due to wireless communication, WSNs lack physical protection and are usually deployed in open, unattended environments, which makes them vulnerable to attacks. It is thus crucial to devise security solutions to these networks [2][3].

II. SECURITY IN WIRELESS SENSOR NETWORKS

a) KEY MANAGEMENT MODULE IN SOOA WSN

Due to high restrictions in wireless sensor networks, where the resources are limited, clustering protocols for routing organization have been proposed in much research for increasing system throughput, decreasing system delay and saving energy. Even these algorithms have proposed some levels of security, but because of their dynamic nature of communication, most of their security solutions are not suitable. In this paper we focus on how to achieve the highest possible level of security by applying new key management technique that can be used during wireless sensor networks communications. For our proposal to be more effective and applicable to a large number of wireless sensor networks applications, we work on a special kind of architecture that have been proposed to cluster hierarchy of wireless sensor networks and we pick one of the most interesting protocols that have been proposed for this kind of architecture, which is LEACH. This proposal is a module of a complete solution that we are developing to cover all the aspects of wireless sensor networks communication which is labelled Secure Object Oriented Architecture for Wireless Sensor Networks (SOOAWSN) [4] .

b) SLEACH

SLEACH proposed some additions to LEACH so that it can improve protection for the network. It is suggested that each node has to have two symmetric keys: a pair wise key shared with the BS and the last key chain held by the BS. According to that, it suggested small modifications to LEACH. For the setup phase, the message sent by RNs should consist of an encrypted message that contains the ID of the node that should receive the message and the ID of CH itself as a plain text, and the encryption using the message authentication code (MAC) that is produced using the shred key between CH and the BS. The nodes hold CHs IDs, and at the same time the BS will analyze the messages sent by CHs to authorize them. Any valid CH will then have its ID added to the list of valid nodes IDs. After that, the BS broadcasts the list with the encrypted list for all nodes in the network using µTESLA broadcast authentication scheme. Now the nodes can recognize the authenticated RNs to be connected with, so these nodes send their requests to participate with CHs groups. CHs then broadcasts confirmation messages for approved nodes. Each message will contain the time slot schedule for each node. We can see in this proposed protocol that it does not provide full authentication for node-CH where the messages to be sent from the nodes to CH are not authenticated. Oliveria et.al propose another solution to provide some ways to pre-distribute the keys using random key pre-distribution for securing node-CH communication in LEACH [3].

c) KEY PRE-DISTRIBUTION (KP)

Method In this method we apply the same technique that has been applied by Sec-Leach. The aim of this method is to have different levels of security on the network communication for the first generation of the network deployment. The idea is to create a pool of keys at the B.S. that has specific number of keys generated randomly using a pseudorandom number generator function. At the same time, the B.S. randomly generates key ID for each generated key which is unique for each key. The second step is to provide each sensor with group of keys with equal sizes for each sensor, and these keys has to be picked randomly without removing any key from the key pool. This leads the sensors to have some sharing keys between each other which make node-node communication possible. Meanwhile, the B.S. provides each sensor with at least one unique key which is to be used to communicate between each node and the B.S. LEACH protocol can be securely applied as follows: After each sensor applied the self electing equation on itself and determine its ability to become a CH for the current round, the communication process starts with the setup phase. In this phase, each CH includes the IDs of the keys in its key group, a nonce in its advertising message offering its availability to become a CH. The ordinary nodes then choose an ID (r) that is shared with CH. Then each of these ordinary nodes sends the message to CH requesting to join its group. The message includes the ID of the node, ID of CH, r, join_ request message, and the encryption of node ID, CH ID, r and the nonce sent by CH using MAC that is produced using a symmetric key associated with r. Each CH then sends a confirmation message to approved nodes containing the ID of CH and a group of pairs[7].

d) PUBLIC AND PRIVATE KEYS METHOD

In this 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. Each sensor generates at least one pair of keys that are related mathematically to each other. The sensor keeps one of these keys to itself as a private key and broadcasts to its neighbors

the other key as a Public key. When Sensor A wants to send a message to sensor B, it can follow different procedures. The first one is to send an encrypted message to B using Bs public key. B is the only sensor that is able to decrypt this message using its private key. The other scenario is that A sends an encrypted message to B, encrypted using A's Private key. In this case, a successfully decryption of the message by B, using A's Public key, guarantees that A is the one who sent the message. Another scenario is that A sends an encrypted message to B using B's Public key and send as a part of this message a small part which is encrypted using A's Private key as a signature of A. Another scenario that can be applied is using this technique for key exchanges purpose to exchange keys between sensors; in this scenario, A sends the secret key that need to share with B, this key and a signature of A is encrypted using B's Public Key[7].

e) SECLEACH – A RANDOM KEY DISTRIBUTION SOLUTION FOR SECURING CLUSTERED SENSOR NETWORKS

Clustered sensor networks have been shown to increase system throughput, decrease system delay, and save energy. While those with rotating cluster heads, such as LEACH, have also advantages in terms of security, the dynamic nature of their communication makes most existing security solutions inadequate for them. In this paper, we show how random key predistribution, widely studied in the context of flat networks, can be used to secure communication in hierarchical protocols such as LEACH. To our knowledge, it is the first work that investigates random key predistribution as applied to hierarchical WSNs[9][10].

III. DESIGN AND IMPLEMENTATION ISSUES

Implementing cluster based architecture requires a significant amount of work to be done. Clustering offers a wide range of advantages for a sensor network but still it has its own drawbacks, issues and challenges. In this section we outline several concrete design and implementation issues involved in the development of cluster based network architecture

Node Mobility

Most of the network architectures assume that nodes are stationary. But sometimes it is compulsory to support the mobility of base stations or CHs. Node mobility makes clustering a very challenging task since the node membership will dynamically change, forcing clusters to evolve over time

Traffic Load

Events that are monitored by a sensor network can either be continual or intermittent. Intermittent monitoring generates traffic in the network only when detecting the event of interest, whereas continual monitoring generates traffic at frequent intervals as they continually sense information. Since intermittent events requires only occasional sensing it does not reflect any change in the CH, whereas intermittent events unevenly load CHs relative to the nodes in the cluster and a rotation of CH role may be required if the CH is randomly picked from the sensor population.

Overlapping Clusters

As stated earlier the cluster head CH may be predesigned by the network designer or elected by the sensors in the network. If the later one is opted there is a possibility that a member of one cluster may become the member under another CH. This makes the overlapping clusters also to be considered in the design issues. It is therefore important to establish necessary mechanisms for detecting the existence of overlapped clusters and coordinating between clusters to avoid unfairness, starvation or deadlock during resource competition.

Load Balancing

Load balancing is one of the most pressing issues in sensor networks where CHs are picked from the available sensors. The member sensor nodes needs to be evenly distributed among the different CHs available which if fails will overload a particular CH leading to the failure of that head. So in such cases it is necessary to design equal sized clusters for a fair balancing.

Dynamic Cluster Control

It is necessary to configure a self configuring clustering mechanism with a sensor network. The clustering mechanisms are responsible for the formation of initial clusters which needs to adapt to its location. The clusters are formed based on several metrics like data accessibility, node capacity, network connectivity etc. One of the important design issues in clustering is the cluster head has to dynamically determine the membership of the nodes as the phenomenon moves. It has been noted in, that when the target is beyond the sensing range of the CH, another round of head election is necessary to find a new CH.

Inter-Cluster Coordination

To achieve the desired goal CH" s needed to communicate with each other. They might need to communicate for sharing of information and to achieve coordination. Further data gathered by one cluster can be requested by base station or other CH across the network. So the self configuring clustering mechanism should be capable of handling intercluster communication overheads.

Data Aggregation

The CH needs to perform the task of aggregating and transmitting the data from the nodes in the cluster to the CH

and hence consumes more energy. So there should be a proper care taken while deciding the CH. One way of conserving the energy of the CH‟ s is by rotating the roles between different nodes, at periodic intervals. Another option is to have the powerful node that can handle the additional energy requirement, to act as the CH.

Fault Tolerance

Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures. Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failed node might be a CH or a member of the cluster. Such failures should not affect the overall task and performance of the sensor network. So it is therefore necessary to have a mechanism which will adapt to these types of failures[4-8].

IV.PROBLEM DEFINITION

Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes . In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as clusterhead (CH). A CH aggregates the data collected by the leaf nodes in its cluster, and sends the aggregation to the base station (BS).

To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH , which use similar concepts of LEACH. In this project, for convenience, we call this sort of cluster-based protocols as LEACH-like protocols. Researchers have been widely studying CWSNs in the last decade in the literature. However, the implementation of the cluster-based architecture in the real world is rather complicated. Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links.

V. PROPOSED SYSTEM

In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose 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. It has been proposed in order to reduce the computation and storage costs 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, pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

Advantages:

- Less computation and communication.
- High security.
- 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.
- The proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.
- Reduce the computational overhead for security using the IBOOS scheme.

The proposed system was implemented in .NET Programming , output of sample screens,

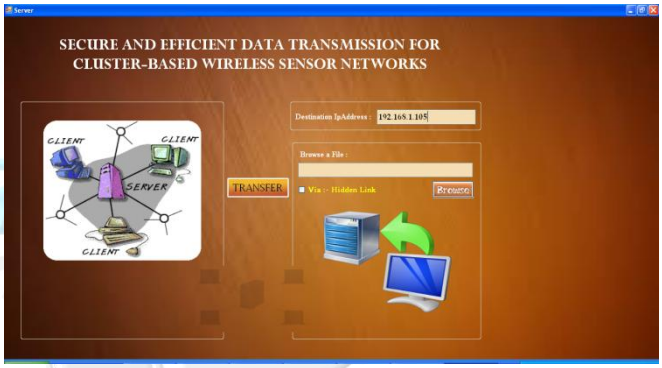

Figure 1: System Selection

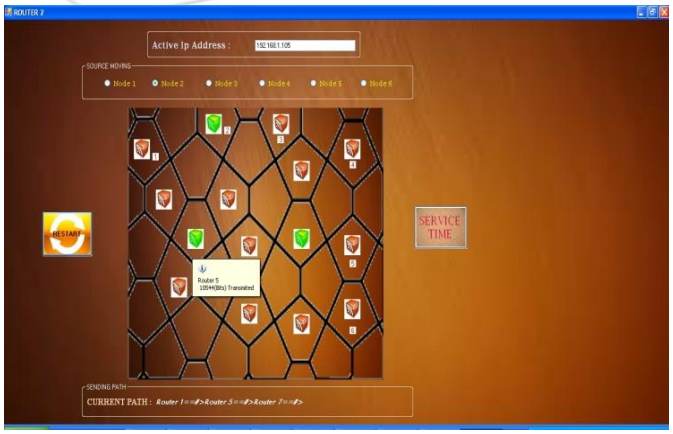

Figure 2: Secure data passing

Set Protocol: Secure and Efficient data Transmission (SET) protocol for CWSNs. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization,

then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

Key Management for Security: Security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verifications.

Key Management: In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security. • Neighborhood authentication In this module, used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, "limited" means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.

Network Scalability: This indicates whether a security protocol is able to scale without compromising the security requirements. Here, "comparative low" means that, compared with SET-IBS and SET-IBOOS. In the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network.

CONCLUSION

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. To overcome the drawback of orphan node problem which is experienced by LEACH, we intend to use the two methods of Identity Based Digital Signature namely the SET-IBS and SET-IBOOS, thus providing efficiency as well as security in the transmission of data among nodes in CWSNs.

In this project, user first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. User then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks.

SET-IBS and SETIBOOS 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. Lastly, the comparison in the calculation and simulation results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

REFERENCES

[1]. T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput.Intell. Springer-Verlag, 2010, vol. 278.

[2]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670,2002.

[3]. L. B. Oliveira, A. Ferreira, M. A. Vilaca *et al.*,"SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.

[4]. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007

[5] Kim, Jinsu1 ; Lee, Junghyun1 ; Rim, Keewook2 3De-Var: Energy-Efficient Cluster-Based Routing Scheme in Wireless Sensor Networks.

[6] Jau-Yang Chang;Pei-Hao Ju An Efficient Cluster-Based Power Saving Scheme for Wireless Sensor Networks.

[7] Po-Jen Chuang;Bo-Yi Li An Efficient Data Dissemination Scheme for Sensor Networks.

[8] Hussain, S. Energy Efficient Data Dissemination in Wireless Sensor Networks.

[9] Jian Chen Yong Guan Pooch, U. An Efficient Data Dissemination Method in Wireless Sensor Networks.

[10] Busse, Marcel Haenselmann, Thomas Effelsberg, Wolfgang Energy-Efficient Data Dissemination for Wireless Sensor Networks.

[11] Ugur Cetintemel Andrew Flinders Ye Sun Power-Efficient Data Dissemination in Wireless Sensor Networks.