Security of Cluster Based Wireless Sensor Routing

Mahendra S. Thakare
Department of Electronics and Communication Engineering
GHRCEM, Pune, Maharashtra, India

Rageshri V. Bakhare
Department of Electronics and Communication Engineering
GHRCEM, Pune, Maharashtra, India

Abstract - New advances in wireless communications and electronics have led to the development of low-cost, low power and multifunctional small smart sensors. These sensors have the ability to sense, process data and communicate with each other via a wireless connection. A collection of a large number of these sensors is known as a wireless sensor network (WSN). In wireless sensor networks nodes are deployed to detect events or environmental phenomena by sensing, processing and forwarding data to an interested user.

Wireless sensor networks, sensor nodes have a limited power resource. The energy consumed to route data from the sensor node to its destination raises as a critical issue in designing wireless sensor network routing protocols. In this paper proposed a routing protocol called MIN-RC to enhance and provide cryptographic security in the hierarchical routing protocol LEACH-C. MIN-RC uses an adaptive method to control the round time considering the current state of the network. The simulation results of proposed protocol using the ns2 simulator will show the improvement of the network efficiency in comparison to existing state-of-the-art protocols and cryptographic security for trusted information from trusted nodes and CH selection process at both ends using RSA algorithm.

Keywords - wireless sensor networks routing; Round time; LEACH-C; Encryption; Decryption; MIN-RC, Sensors.

I. INTRODUCTION

The expansion in technology mean that many wireless sensor nodes are now relatively low cost; however, the cost of deploying them can remain high. There is a requirement to get the longest life out of a network of sensors and the life is generally limited by battery power consumption. A wireless sensor network (WSN) consists of a collection of these nodes that have the ability to sense, process data and communicate with each other via a wireless connection.

Wireless sensor networks (WSN's), the improvement in sensor technology has made it possible to have extremely small, low powered sensing devices equipped with programmable computing, multiple parameter sensing and wireless communication capability. Also, the low cost makes it possible to have a network of hundreds or thousands of these sensors, thereby enhancing the reliability and accuracy of data and the area coverage. Wireless sensor networks offer information about remote structures, wide-spread environmental changes, etc. in unknown and inhospitable terrains. There are a number of advantages of wireless sensor net- works over wired ones such as ease of deployment (reducing installation cost), extended range (network of tiny sensors can be distributed over a wider region).

When embedded in critical applications, WSNs are likely to be attacked [4], [5]. 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. Adding security to LEACH-like protocols is challenging, as its dynamic and periodic rearranging of the network's clustering (and changing links) make security solutions that provide long-lasting node-to-node trust relationships (to be sure, provided by most existing solutions) inadequate. And even though there is previous work on security for LEACH, it does not address all the problems. Existing solutions for conventional and even other wireless ad hoc networks are not applicable here, given the lack of resources in sensor nodes. Public-key-based methods are one such example. In addition, efficient solutions can be achieved only if tailored to particular network organizations.

In TEEN [1] and APTEEN [2] threshold values are used to control data transmission. HEED [3] selects a set of nodes as cluster heads depending on the residual-energy of the node and on a secondary parameter intra-cluster

communication cost for cluster head selection. SecLEACH [4] providing efficient security to pairwise node-to-CH communications in LEACH-like protocols using random key predistribution, SLEACH [7] selects security method using building blocks from SPINS.

In this paper, we described the MIN-RC a routing protocol based on LEACH-C that minimizes the variance of energy consumption caused by unbalanced clustering. MIN-RC uses a variable round time rather than a fixed round time as in LEACH-C, and considers the minimum cluster size to control round time, and this will always minimize the round time according to the current state of the network.

Also investigate the problem of adding security to cluster-based communication protocols for homogeneous WSNs (those in which all nodes in the network, except the BSs, have comparable capabilities) and overcomes the security problem by key distribution of symmetric encryption system in public key encryption using RSA algorithm which uses two keys, which work in pairs for decryption and encryption. So that, one can apply the encrypting transformation first and then the decrypting one, or the decrypting transformation first followed by the encrypting one. Each CH ask for the certificate authority before transmitting the information to avoid any un-trusted node.

II. RELATED WORK

In clustering protocols, there are two kinds of node: CH (cluster head node) and non-CH nodes. Sensors are organized in clusters each having one sensor promoted as CH. All non-CH nodes transmit their data to their CH, which routes it to the remote sink or PN (processing node). LEACH [6], a well-known clustering protocol for WSNs. The operation of

LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, when data transfers to the base station occur. However, in set-up phase, there is no guarantee that nodes selected as cluster head are evenly dispersed throughout the network because procedure to select cluster head is based on the random cluster formation method having local probability. When the number of CH is much less than the expected value, The CH will take too much traffic load and dead quickly. So these nodes in the cluster cannot reporting information to BS, BS will loss these data. This will affect the network. To solve this problem, in this paper, an improved version of LEACH was proposed, named Variable-round LEACH (VR-LEACH for short). In VR-LEACH, When there is less (no) cluster head or cluster head has less energy, we change the time of round.

LEACH is one important well known hierarchical routing protocol [3]. The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, when data transfers to the base station occur. Initially, each node choosing a random number between 0 and 1. If the number is less than a threshold, the node becomes a CH for the current round. Cluster-head for the current round broadcasts an advertisement message to the rest of the nodes. The non-CH nodes must keep their receivers on during this phase of set-up to hear the advertisements of all the CH nodes and decides the cluster to which it will belong for this round. The cluster-head node creates a TDMA schedule telling each node when it can transmit and broadcast back to the nodes in the cluster. Once the clusters are created and the TDMA schedules fixed, data transmission can begin [6].

The LEACH algorithm divides the network life time into a number of rounds, where each round has two phases: Setup phase (Clusters' formation) and Steady State Phase (operating phase).

$$T(n) = \begin{cases} \frac{P}{1-P*(r mod \frac{1}{P})} & \text{if n} \in \text{G} \\ 0 & \text{otherwise} \end{cases}$$

In the Setup phase the clusters are formed by the nodes themselves using equation (1), where N is the number of nodes, k is the number of clusters, r is the current round number, and Ci is a function to be determined. If the node i was selected as a cluster head in the recent round (r mod(N/k)) each node selects a random number between 0 and 1, if this random number is greater than a threshold T then the node will be selected as a cluster head and broadcasts an advertisement message containing its Id. Other nodes (non-cluster head) decide to join a cluster depending on the signal strength of the received advertisements, then the nodes send a Join-Request message to the selected CH. After the CH receives the joining messages from other nodes which decided to join this cluster; the CH head creates a TDMA schedule and broadcasts this schedule to all the cluster members. The TDMA schedule contains a time slot for each node to communicate with the CH.

The Steady State Phase is broken into a number of frames; in each frame the sensor node sends its data to the CH using its time slot in the TDMA schedule, after that it switches its state to the sleep mode. When the CH node receives data from its members, the CH aggregates the received data and sends the aggregated data directly to the BS, and this process is repeated until the end of the round, by the end of each round, nodes enter the setup phase again to select a new set of cluster heads for the next round [2] [3].

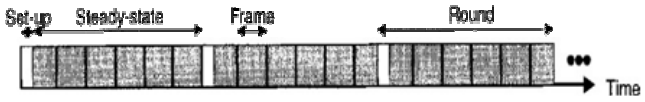

Fig. 1. Time line showing LEACH operation. Adaptive clusters are formed during the set-up phase and data transfers occur during the steady-state phase

The steady-state operation is broken into frames, where nodes send their data to the cluster head at most once per frame during their allocated transmission slot. The duration of each slot in which a node transmits data is constant, so the time to send a frame of data depends on the number of nodes in the cluster.

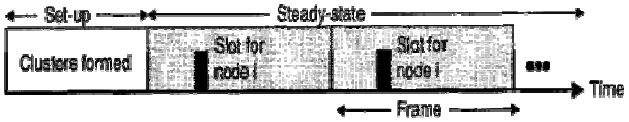

Fig. 2. Time line showing LEACH operation. Data transmissions are explicitly scheduled to avoid collisions and increase the amount of time each non-cluster head node can remain in the sleep state

Fig. 2 shows the time line for one round of LEACH. We assume that the nodes are all time synchronized and start the set-up phase at the same time. This could be achieved, for example, by having the BS send out synchronization pulses to the nodes. Frame of data depends on the number of nodes in the cluster. Fig. 2 shows the time line for one round of LEACH. We assume that the nodes are all time synchronized and start the set-up phase at the same time. This could be achieved, for example, by having the BS send out synchronization pulses to the nodes.

Like most routing protocols for WSNs, LEACH is vulnerable to a number of security attacks [7], including jamming, spoofing, replay, etc. However, because it is a cluster- based protocol, relying fundamentally on the CHs for data aggregation and routing, attacks involving CHs are the most damaging. If an intruder manages to become a CH, it can stage attacks such as sinkhole and selective forwarding, thus disrupting the workings of the network. Of course, the intruder may leave the routing alone, and try to inject bogus sensor data into the network, one way or another. A third type of attack is (passive) eavesdropping. Note that LEACH is more robust against attacks than most other routing protocols [5]. In contrast to more conventional multihop schemes where nodes around the BS are especially attractive for compromise(because they concentrate all network-to-BS communication flows), CHs in LEACH communicate directly with the BS, can be any- where in the network, and change from round to round. All these characteristics make it harder for an adversary to identify and compromise strategically more important nodes.

One of the first steps to be taken to secure a WSN is to prevent illegitimate nodes from participating in the network. This access control can preserve much of a network's operations, unless legitimate nodes have been compromised. (Note that access control does not solve all security problems in WSNs. E.g., it is ineffective against DoS attacks based on jamming wireless channels, or manipulating a node's surrounding environment to induce the reporting of fabricated conditions.) Access control in networks has typically been implemented using cryptographic mechanisms, which rely critically on KD.

III. PROBLEM STATEMENT

A. Network Model

We consider a wireless sensor network model, where a number of sensor nodes N are randomly deployed over the sensing area in a uniform manner, the sensor nodes monitor environmental phenomena and send their data to the BS. We have some preliminary assumptions for our network model. Sensor nodes and BS are immobile after deployment and the BS is located far from all sensors, all nodes are homogeneous and have the same capabilities where each node has a unique identifier (Id), each node is equipped with location detection capability for example GPS, nodes can control their transmission power to send directly to the BS. All nodes start with the same energy

level and the BS has unlimited energy resource, nodes always have data to send to the BS, perfect data aggregation where the CH aggregates the collected data messages into a single message [6].

B. Existing Key Distribution Scheme

There are a number of KD schemes in the security, most of which are ill-suited to WSNs: public key based distribution, because of its processing requirements; global keying, because of its security vulnerabilities; complete pairwise keying, because of its memory requirements; and those based on a key distribution center, because of its inefficiency and energy consumption [4].

Some KD schemes have been specifically designed for WSNs. While they are well- suited for network organizations they were designed for, they are inadequate for others. These schemes typically assume that a node interacts with a quite static set of neighbors and that most of its neighborhood is discovered right after the deployment. However, clusters in LEACH are formed dynamically (at random) and periodically, which changes interactions among the nodes and requires that any node needs to be ready to join any CH at any time.

C. Trusted CH

As, LEACH protocol is divided into clusters so once the malicious node becomes the cluster head then it will impact the complete network and tamper the data. In short we have to make the cluster head secure in order to prevent the network from the attack [5]. In this paper we discussed that each CH ask for the certificate authority which is having the certificate authority first by collecting the private before transmitting the information to avoid any un-trusted node.

IV. MIN-RC PROTOCOL

MIN-RC is based on LEACH-C protocol to balance the energy consumption of sensor nodes in order to solve the overload energy consumption problem. MIN-RC uses a variable length round based on the minimum cluster size. The network life time of MIN-RC is broken down into a number of rounds, and each round starts with the setup phase, where each node sends its Id, location and current level of residual energy to the BS, then the BS partitions the network into k clusters and before sending the cluster information to the nodes the BS calculate the time for the next round T current. In order to solve the problem of overload energy consumption and minimize the diversity of the energy consumption between nodes, MIN-RC uses an adaptive round-control method to balance the energy consumptions.

V. OVERVIEW OF SOLUTION

We propose a cryptographic solution that divides this authenticated broadcast with distribution of public keys to all nodes present in the cluster. After the formation of CH for each cluster, the CH will collect the private keys of all the nodes residing that cluster and outside the cluster and get the certificate authority.

After getting the certificate authority when any node from the same cluster or intermediate node outside the cluster will try to communicate or share information (i.e. while transmitting and receiving) it will first ask for certificate and afterwards only that CH will communicate further. Due to this solution if any un-trusted node tries to communicate then due to certificate failure the information will not be share.

VI. CONCLUSION

In this paper we describe MIN-RC an enhancement of LEACH-C protocol, which is an adaptive round-control method to better utilize the energy consumed during the round time of a sensor network communication protocol. Our proposed method considered the size (number of nodes) of the cluster in each round and the optimal number of frames to define the length of the current round.

We also described cryptographic solution for securing node-to-node communication in LEACH-based networks. This solution bootstraps its security from random key predistribution. Future work show that the energy efficiency, and security level can be each traded off for another, depending on what is most critical in a system.

REFERENCES

[1] Arati Manjeshwar and Dharma P. Agrawal “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks” in 2001.
[2] Arati Manjeshwar and Dharma P. Agrawal “APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks” in the International Parallel and Distributed Processing Symposium (2002).
[3] Ossama Younis and Sonia Fahmy “HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks” in IEEE TRANSACTIONS ON MOBILE COMPUTING (Oct-Dec 2004).
[4] Leonardo B. Oliveira, Hao C. Wong, M.Bern, Ricardo Dahab, A.A.F.Loureiro “SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks” in 2005.
[5] Kun Zhang, Cong Wang and Cuirong Wang “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management” in 2008.
[6] Zhiyong PENG and Xiaojuan LI “The Improvement and Simulation of LEACH Protocol for WSNs” in 2010.
[7] Adrian Carlos Ferreira, Marcos Aurelio Vilaca1, Leonardo B. Oliveira1, Eduardo Habib,Hao Chi Wong, Antonio A.Loureiro “On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks”.
[8] Nauman Israr and Irfan Awan “Multohop clustering algorithm for Load BALANCING IN WSN” in I. J. of Simulation Vol. 8 No.1.