TELKOMNIKA, Vol.11, No.11, November 2013, pp. 6794~6801
e-ISSN: 2087-278X

A New Routing Protocol for Efficient and Secure Wireless Sensor Networks

Zhang Yu-Quan*, Wei Lei
School of Information Technology, Shandong Women's University, Jinan 250300
*Corresponding author, e-mail:zyczyq@126.com

Abstract

This paper presents an improved LEACH protocol to save energy and enhance network security for wireless sensor networks. All nodes are distributed evenly in sensing area. The sensing area is divided into a number of small squares called cells, and a cluster consists of four cells. The cluster structure does not change in whole network lifetime. A cell head is chosen in each cell and a cluster head is selected from four cell heads in each cluster. The data are transmitted from clusters to the base station by employing the multi-hop manner. All nodes that communicate each other establish pairwise keys. Analysis demonstrates that the new routing protocol saves more node energy, distributes energy consumption to all nodes more evenly, prolongs more lifetime for WSNs than the LEACH protocol dose. Moreover, it enhances the security for WSNs.

Keywords: *wireless sensor network, routing protocol, energy, security*

1. Introduction

Wireless sensor networks have become one of the most interesting and promising research and development fields over the past few years. WSNs have been widely used in many fields [1-3] due to many advantages of WSNs, such as flexibility, fault tolerance, high sensing, self-organization, low-cost and rapid deployment [4].

The sensor nodes can be distributed both in controlled environments, including home, office, warehouse, habitat, forest, etc, and in uncontrolled and dangerous, even hostile, environments, including toxic region, battlefield, etc.

Wireless sensor networks usually contain thousands or millions of sensors, which are randomly and widely deployed. Sensors are powered by battery, which is impossible to be recharged after deployment. Therefore, energy efficiency is an important issue in sensor networks. Moreover, when wireless sensor networks are deployed in an adverse area, they are vulnerable to secure attacks. An adversary can capture and compromise a sensor node, alter the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resource.

Since routing consumes a lot of energy, and security was not a focus in the design of some routing protocol, an efficient and secure routing scheme in sensor networks is of importance [5]. Routing protocols for wireless sensor networks are categorized as data-centric (flat) protocols, hierarchical (cluster-based) protocols and location-based protocols. A typical clustering protocol is called low-energy adaptive clustering hierarchy (LEACH) [6]. It uses the technique of randomly rotating the role of a cluster head among all the nodes in the network. Each cluster selects a cluster head, which is responsible for aggregating collected data and sending data to base station. The LEACH provides a good model that helps to reduce information overload and provides a reliable data to the end user.

This paper proposes an improved LEACH protocol for securely and efficiently gathering, aggregating, and transmitting data in wireless sensor networks. Conventional LEACH includes distributed cluster formation, local processing to reduce global communication, and randomized rotation of cluster-heads, additionally, in conventional LEACH, clusters send data to the base station directly. The new protocol forms clusters only once to save more energy, chooses cell heads and cluster heads in each round, uses multi-hop routing to send data to the base station,

Received April 28, 2013; Revised July 16, 2013; Accepted July 31, 2013

and establishes pairwise keys among nodes. Therefore, the new routing protocol improves the LEACH protocol in prolonging WSNs lifetime and enhancing WSNs security.

The remainder of this paper is organized as following. The secure routing protocol for WSNs is given in section 2. We present the comparison between the LEACH protocol and our scheme in section 3. Conclusion is in the section 4.

2. The New Routing Protocol for WSNs

The LEACH protocol is improved by reducing WSNs energy consumption, prolonging network lifetime, and enhancing network security.

2.1. Location-based Grids

The LEACH protocol is a low-consumption adaptive cluster routing protocol for wireless sensor networks. However, there are a number of rounds in the LEACH algorithm and the cluster structure changes in every round; therefore, it expends much energy to form clusters. In the new routing protocol, the cluster structure is formed in the first round and does not change again in the latter rounds.

The whole sensor area is divided into grids called cells, which are the same and do not change in all rounds. Cell head nodes only communicate with those nodes in the same grid during the selecting period. It is clear the wireless sensor networks save energy because they form and initialize clusters only once and cell heads save energy because they only communicate in their grids.

Suppose that all nodes in WSNs are distributed evenly. In:

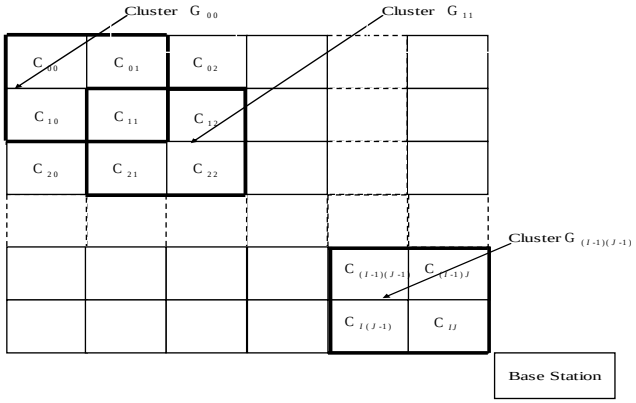

Figure 1. Location-based Cells and Clusters

Figure 1, the sensor area S is divided into $(I+1)(J+1)$ same cells, denoted as C_{00}, $C_{01},\cdots,C_{0j},\cdots,C_{0(J-1)}$, $C_{0J},C_{10},C_{11},\cdots C_{1j},\cdots,C_{1(J-1)},C_{1J},\cdots,C_{i0},C_{i1},\cdots,$ $C_{ij},\cdots,C_{i(J-1)},C_{iJ},\cdots,C_{I0},C_{I1},\cdots,C_{Ij},\cdots,C_{I(J-1)}$, C_{IJ}, where $0\le i\le I$ and $0\le j\le J$, according to their geographical locations. Suppose that there are N sensor nodes in the sensor area S. Those nodes are divided into $(I+1)(J+1)$ same groups denoted as $C'_{00},C'_{01},\cdots,C'_{0j},\cdots,$ $C'_{0(J-1)},C'_{0J},C'_{10},C'_{11},\cdots,C'_{1j},\cdots,C'_{1(J-1)},C'_{1J},\cdots,C'_{i0},C'_{i1},\cdots,C'_{ij},\cdots,C'_{i(J-1)},C'_{iJ},\cdots,C'_{I0},$ $C'_{I1},\cdots,C'_{Ij},\cdots,C'_{I(J-1)},C'_{IJ}$, where $0\le i\le I$ and $0\le j\le J$. The sensor nodes in group C'_{ij} are deployed in cell C_{ij}. There are $\frac{N}{(I+1)(J+1)}$ nodes in every grid. A cluster consists of four cells. For example, in Figure 1, cluster $G_{(I-1)(J-1)}$ consists of cell $C_{IJ},C_{I(J-1)},C_{(I-1)J}$ and

$C_{(I\text{-}1)(J\text{-}1)}$. Therefore, there are $\frac{4N}{(I+1)(J+1)}$ nodes in every cluster. If $I = J$, there are $(I-1)^2 = (J-1)^2$ clusters.

2.2. Two-tier Structure

Although the LEACH protocol evidently prolongs the WSN lifetime by saving more node energy and apportioning energy consumption more evenly than some other routing protocols do, it cannot decide what are selected as the cluster heads, the cluster head number and their distribution. Therefore, the LEACH protocol may cause uneven energy consumption in WSNs and then the node lifetime distributes in a large extension. The blind sensing area appears soon in WSNs and WSN performance deteriorates. In order to solve those problems, we adopt two-tier structure in WSNs.

As in the LEACH protocol, a cell head is chosen in each round in each cell according to the method in the LEACH protocol. However, after all cell heads are chosen, a cluster head is chosen from those cell heads in a cluster.

In our scheme, as in the LEACH algorithm, all nodes in a certain cell decide what are selected as the cell heads by generating and comparing those random numbers. Each node generates a random number and sends it to all other nodes in the network. After all nodes compare their random numbers, a cell head is selected in a cell. Each cell head broadcasts its data packet including its energy, all the distances between it and all other cell heads. Then the cluster heads are selected by comparing the threshold volume $T_{(n)cluster}$.

There are four cell heads in a certain cluster, and suppose that node n is one of them and node n' is one of them too. The average energy of all the first heads is calculated as:

$$E_{average} = \sum_{n=1}^{4} \frac{E_n}{4} \tag{1}$$

Where, $E_{average}$ is the average energy of all the cell heads and E_n is the energy of the cell head n.

The sum of the distance between the cell head n and all other cell heads is calculated as:

$$D_n = \sum_{n=1}^{4} D_{nn'} \qquad n \neq n' \tag{2}$$

Where, D_n is sum of the distance between the cell head n and all other cell heads and $D_{nn'}$ is the distance between the cell head n and the cell head n'.

The $T_{(n)cluster}$ is defined as following:

$$T_{(n)cluster} = \Omega\Psi \tag{3}$$

Where, $\Omega = [W_1 \quad W_2]$, $\Psi = \begin{bmatrix} \frac{E_n}{E_{average}} \\ D_n \end{bmatrix}$, W_1 is positive weight coefficients , and W_2 is negative coefficient.

Generally, a cell head n compares its $T_{(n)cluster}$ with received three $T_{(n')cluster}$ of other cell cluster head n', where $1 \leq n \leq 4$, and $n \neq n'$. If the cluster head n is the maximal and is not compromised, it is selected as the cluster head. In other word, if the cluster head n is the maximal and is not compromised, it is chosen as the cluster head.

2.3. The Pairwise Key Establishment in a Grid

The setup server distributes a node identification ID, $CID_{ij} \| SID_k$, where $0 \le i \le I$, $0 \le j \le J$, and $0 \le k \le \frac{N}{(I+1)(J+1)} - 1$, to each node in the cell C_{ij}. For example, the setup server distributes $CID_{00} \| SID_0$, $CID_{00} \| SID_1$, $\cdots$, $CID_{00} \| SID_{\frac{N}{(I+1)(J+1)}-1}$ to all nodes in the cell C_{00} respectively. Additionally, it distributes each node in all clusters a management key $Key_{management}$.

The node key Key_A of node A is generated by utilizing hash function with key parameter as following.

$$Key_A = hash(Key_{manage} \| Node\ ID_A) \quad (4)$$

Where Key_{manage} is the key parameter, and the node identification ID_A is the input.

Key_A is shared by the base station and node A and it is distributed to the node A before deployment.

Before nodes are distributed, the management key Key_{manage} is set to all nodes and the node function is activated. After a period of time T_{secure}, the management key Key_{manage} is deleted from all nodes in WSN. Therefore, the network security is not compromised after a period of time T_{secure}, even if some nodes are captured.

Neighbor nodes establish common pairwise keys as following.

Generally, node u and node v are neighbor nodes in cell C_{ij}, where $0 \le i \le I$, $0 \le j \le J$. Node u broadcasts message including a secure connection request and its $CID_{ij} \| SID_{k_{(u)}}$ to its neighbors. After one of its neighbors v receives the message sent from the node u, node v calculates $Key_{vu} = hash(Key_v \| CID_{ij} \| SID_{k_{(u)}} \| CID_{ij} \| SID_{k_{(v)}})$ and then sends a message including the result Key_{vu} and its $CID_{ij} \| SID_{k_{(v)}}$ to the node u. In the secure period T_{secure} the node u has the management key Key_{manage}, so node u can calculate the Key_v of node v and then know whether the message is sent from node v. In the same way, node v can calculate node u key Key_u and obtain node u identification $CID_{ij} \| SID_{k_{(u)}}$. Therefore, both node u and node v can calculate their common keys and then establish their secure connection.

$$Key_{u\text{-}v} = Key_{v\text{-}u} = hash(CID_{ij} \| SID_{k_{(u)}} \| CID_{ij} \| SID_{k_{(v)}} \| Key_u \| Key_v) \quad (5)$$

After a period of time T_{secure}, the management key:

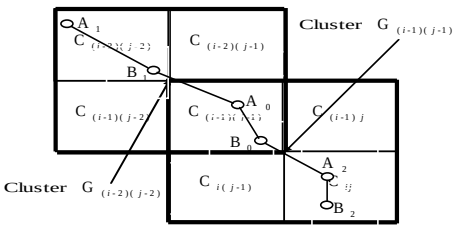

Figure 2. The Secure Connection among Non-neighbor Nodes

$\mathrm{Key}_{\mathrm{manage}}$ is deleted from all nodes in WSN. Therefore, establishing secure connection among nodes is finished.

Next, we discuss how those non-neighbor nodes establish secure connection. In general, in Figure 2, A_1 and B_1 are neighbor nodes in cell $\mathrm{C}_{(i\text{-}2)(j\text{-}2)}$, A_0 and B_0 are neighbor nodes in cell $\mathrm{G}_{(i\text{-}1)(j\text{-}1)}$, and A_2 and B_2 are neighbor nodes in cell G_{ij}, in the same way, B_1 and A_0 are neighbor nodes in cluster $\mathrm{G}_{(i\text{-}2)(j\text{-}2)}$, and B_0 and A_2 are neighbor nodes in cluster $\mathrm{G}_{(i\text{-}1)(j\text{-}1)}$. Therefore, secure connection can be established between A_1 and B_1, A_0 and B_0, A_2 and B_2, B_1 and A_0, and B_0 and A_2 respectively. A_1 and B_2 are in different clusters and they are not neighbor nodes. However, node A_1 can obtain the node identification and key of node B_2 by employing those secure connections between A_1 and B_1, A_0 and B_0, A_2 and B_2, B_1 and A_0, and B_0 and A_2. In the same way, node B_2 can obtain the node identification and key of node A_1. Non-neighbor node A_1 and B_2 establish common keys as following:

$$\mathrm{Key}_{A_1\text{-}B_2} = \mathrm{Key}_{B_2\text{-}A_1} = \mathrm{hash}(\mathrm{CID}_{ij_{(A_1)}} \| \mathrm{SID}_{k_{(A_1)}} \| \mathrm{CID}_{ij_{(B_2)}} \| \mathrm{SID}_{k_{(B_2)}} \| \mathrm{Key}_{A_1} \| \mathrm{Key}_{B_2}) \quad (6)$$

Therefore, non-neighbor node A_1 and B_2 can establish secure connection by employing their common key.

In this scheme, nodes need not save too much keys and they only save management key $\mathrm{Key}_{\mathrm{manage}}$ in the secure period T_{secure}. After a period of time T_{secure}, all nodes only maintain those keys shared with their neighbor nodes. In whole WSN lifetime, the base station only maintains the management key $\mathrm{Key}_{\mathrm{manage}}$ and calculates all other keys by utilizing it.

To establish common keys with other nodes, a node need to calculate several hash operations. A node expends less energy to establish common keys than some other routing protocols do.

2.4. Sending Data from Grids to the Station in our Strategy

The cluster heads send data directly after receiving and aggregating that information sent from those ordinary nodes in WSNs utilizing the LEACH protocol. In large wireless sensor networks, the distant cluster heads consume much more energy to transmit data to the base station through using this manner than those close cluster heads do in WSNs using the LEACH protocol. As a result, the distant cluster heads use up their energy rapidly. Therefore, the LEACH protocol cannot guarantee all nodes have similar lifetime. To solve this problem, all the cluster heads communicate with the base station by employing the multi-hop manner. Additionally, suppose that all clusters have the same number of nodes, and the original energy of each node and the information transmitted by each cluster are the same.

The new routing protocol establishes a cluster head routing from clusters to the base station to guarantee that all nodes consume similar battery energy. Cluster heads transmit data to the near cluster head or to the base station directly along the cluster head routing, rather than communicate with the base station directly.

The cluster routing consists of clusters, which are in the direction from the original cluster to the base station and participate in cluster head routing. In Figure 3, the original cluster head M_0 sends data to the base station, and a line L is drawn from the center of cluster $\mathrm{G}_{(i\text{-}3)(j\text{-}3)}$ to the base station. So, the cluster routing includes cluster $\mathrm{G}_{(i\text{-}3)(j\text{-}3)}$, $\mathrm{G}_{(i\text{-}2)(j\text{-}2)}$ and $\mathrm{G}_{(i\text{-}1)(j\text{-}1)}$, and cluster head M_0, M_1, and M_2 take part in cluster routing. If some routing cluster heads are attacked by enemy or have been compromised, the new scheme designs two or more cluster head routings in the grids to guarantee data secure. For example, if the cluster

head M_1 is compromised, the original routing stops here and the preparing routing is utilized. The new routing clusters contain the cluster $G_{(i\text{-}2)(j\text{-}3)}$ and a line L' is drawn from its center to the base station. The new preparing cluster routing consists of clusters, which L' passes through.

The clusters near to the base station consume much energy because they frequently transmit data for the distant clusters. As a result, the close clusters use up their energy rapidly. To deal with this issue, the new routing protocol designs a threshold volume $E_{\min}$. When a cluster head M_Y sends data to its next relay cluster head M_X, the origin routing stops, if $E_{M_X} < E_{\min}$, where, E_{M_X} is the energy of M_X. Therefore, the new strategy can balance the energy consumption in the wireless sensor networks.

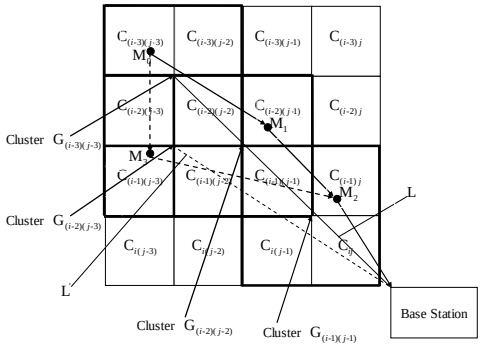

Figure 3. The Multi-hop Cluster Head Routing

3. The Comparison between the LEACH Protocol and the New Protocol

3.1. The Energy Comparison

The LEACH protocol consumes much energy to divide nodes in WSNs into clusters in all rounds. In each round, cluster heads expend considerable energy to broadcast message to all nodes in the network after they are selected as cluster heads. Although the new routing protocol selects cluster heads in each round according to the method in the LEACH arithmetic, clusters are formed in the first round and do not change again in all latter rounds. Therefore, the new scheme saves more energy than the LEACH protocol does.

The LEACH protocol does not decide what are chosen as the cluster heads and their distribution, therefore it induces uneven energy consumption among nodes in WSNs and then the node lifetime distributed in a large extension. The new protocol employs two-tier structure. In a certain cluster, a cell head is selected through using the method in the LEACH protocol, and then a cluster head is chosen from those cell heads by comparing their threshold volume $T_{(n)cluster}$. Therefore, the new protocol efficiently avoids the case in which a node with little energy or a distant node is chosen as the cluster head.

In the LEACH protocol, all cluster heads directly transmit those data to the base station by employing single-hop manner after receiving and aggregating information sent by the ordinary nodes. If those cluster heads are far from the base station, they will spend much battery energy. In the new routing protocol, in a certain cluster, each cell head sends those data to the cluster head after they collect and aggregate information sent by the ordinary nodes and then the cluster heads compress those information sent by cell heads again. All cluster heads transmit those data to the base station by employing multi-hop manner along the routing path consisting of cluster heads. Therefore, the wireless sensor networks can both save the node energy and realize the load balance among them.

3.2. The Security Comparison

Ordinary nodes decide whether they join a certain cluster according to the signal intensity sent by the cluster head, therefore the malicious nodes can easily launch HELLO flooding attack. They broadcast by utilizing high power to attract a number of nodes to join their clusters. After cheating normal nodes to join their clusters, those malicious nodes launch other attacks, such as altered information, selective forwarding and so on, to realize their goals. Additionally, normal nodes are attacked by the Sybil attack. Malicious nodes communicate with different nodes by using different identifications and those identifications change in different rounds to compromise normal nodes.

The new routing protocol forms clusters in the first round, which have same nodes and do not change in all latter rounds. In a certain cluster, a cluster head is selected. Therefore, the HELLO flooding attack is useless in the new routing protocol.

This routing protocol supposes that all nodes in WSNs are secure in the period T_{secure} after all nodes are deployed. In most WSNs, this supposition can be guaranteed. After the secure period, management key $\text{Key}_{\text{manage}}$ is deleted from all nodes in WSNs, and then they only possess node keys and those common keys shared with their neighbor nodes. If a node is captured and compromised, its affection is limited to its neighbor nodes in a certain cell. In this strategy, nodes only receive data from or send data to those secure neighbor nodes, which establish pairwise keys with it. Therefore, the malicious nodes cannot establish communication keys with other normal nodes by utilizing the identification and keys of compromised nodes.

The management key $\text{Key}_{\text{manage}}$ is critical in this protocol. If it is compromised, the enemy nodes can easily get pairwise keys through calculating hash function operation and then harm network security. To deal with this problem, the setup server distributes different management keys in different rounds.

4. Conclusion

Through randomly selecting new cluster heads in all rounds, the LEACH protocol opportions energy consumption to all nodes in wireless sensor network more evenly than some other protocols do. However, LEACH protocol divides clusters by using self-organizing location method, so the result probably is not optimized in every round. Moreover, the wireless sensor networks expend much energy because of the forming clusters in all rounds. Additionally, the LEACH protocol utilizes multi-hop manner to send information from clusters to the base station, the cluster heads expend much energy if they are far from the base station. Besides, the security for WSNs is not a focus when the LEACH protocol was designed, so it is not secure enough.

To solve those problems, the new routing protocol is presented. The sensor area is divided into a number of squares, each of which has equal number nodes. A square is a cluster and all clusters do not change in all rounds. A cluster consists of four cells. A cell head is selected in a cell and a cluster head is chosen from four cell heads in a cluster in each round. Additionally, clusters send data to the base station through utilizing multi-hop manner. Besides, all nodes both neighbor nodes and non-neighbor nodes establish secure connection to guarantee the network security. The new protocol balances energy expense among all the nodes, saves the node energy, and prolongs the life of wireless sensor networks. Additionally, this arithmetic improves the security of the wireless sensor network.

Acknowledgement

This work was supported by the China Postdoctoral Science Foundation under Award Number 20090450298.

References

[1] AM Mainwaring, DE Culler, J Polastre, R Szewczyk, J Anderson. *Wireless sensor networks for habitat monitoring*. Proc. of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSN'02), C.S., Atlanta, Georgia, USA. 2002; 88-97.

[2] R Cardell-Oliver, K Smettem, M Kranz, K Mayer. A reactive soil moisture sensor network: Design and field evaluation. *Journal of Distributed Sensor Networks*. 2006; 1(2): 149-162.
[3] W Xue, Q Luo, L Chen, Y Liu. Contour map matching for event detection in sensor networks. Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD'06), Chicago, Illinois, USA. 2006: 145-156.
[4] T Feilong, G Minyi, L Minglu, Y Yanqin, Z Daqiang, W Yi. *Wireless Mesh Sensor Networks in Pervasive Environment: a Reliable Architecture and Routing Protocol*. International Conference on Parallel Processing Workshops. 2007: 72-72.
[5] LV Hosel, T Nieber, Jian Wu. *Prolonging the Lifetime of Wireless Sensor Networks by Cross-layer Design*. Proceedings IEEE Wireless Communications. 2004; 80-86.
[6] Wendi Rabiner Heinzelman, Anantha Chandrakasan, Hari Balakrishnan. *Energy efficient communication protocol for wireless microsensor networks*. Proceedings of the 33rd Annual Hawaii International Conference On System Sciences. Maui, HI, USA. Los Alamitos CA, USA: IEEE Computer Society. 2000; 1-8.