Improving the LEACH Protocol for Heterogeneous Wireless Sensor Networks

Yuquan Zhang[1,a] , Lei Wei [2,b]

[1]Wireless Sensing Institute, College of Information Science and Engineering, Qilu Normal University, China

[2]College of Physics and Electronic Engineering, Qilu Normal University, China

[a]email:zyczyq@126.com; [b]email:weilei76@126.com

Keywords: Heterogeneous wireless sensor network; routing protocol; pairwise key; energy; security; connectivity

Abstract. Routing protocol has been a challenging issue in the design of wireless sensor networks. This paper presents an improving LEACH protocol for heterogeneous wireless sensor networks. The new protocol consists of a number of rounds. The wireless sensor networks have some sensor nodes that have greater power and transmission capability than other nodes. Both ordinary nodes and heterogeneous nodes are distributed respectively in a sensing area that is divided into a number of equilateral hexagons called clusters, each of which consists of six equilateral triangles called cells. After forming the clusters, they do not change in all latter rounds. Each equilateral triangle has the same number nodes, both heterogeneous nodes and ordinary nodes, and then each equilateral hexagon has the same number nodes too. The protocol selects a heterogeneous node that is at the cluster center as the cluster head in all clusters. The pairwise keys between nodes are established through utilizing the concept of the overlap key sharing and the random key pre-distribution scheme. Moreover, all ordinary nodes send their messages to their cluster heads after authenticating those messages. The data are sent to the base station in a manner of multi-jumping along a routing path consisting of cluster heads. The arithmetic balances energy expense among all kinds of nodes, saves the node energy, and prolongs the life of wireless sensor networks. Additionally, analysis demonstrates that the connectivity and security of wireless sensor networks have been improved obviously with some heterogeneous nodes.

Introduction

Wireless sensor networks (WSNs) usually comprise of a number of sensor nodes, with limited storage, computation capability, and communication ability[1]. Recently, they are becoming more and more important. WSNs have been used in various fields[2].

WSNs are some times dispensed in hostile environments to fulfill their applications. Therefore, ensuring the network security is of importance. The security for WSNs is one of issues. Lai D et al[3]described the OKS (Overlap-Key-Sharing) scheme. The protocol generates a bit-string as the key-string-pool (KP) of the sensor network, and at random allocates each sensor a subaggregate of the key-string-pool. Sensors employ the overlap intervals of the key-strings as the shared secret key with their vicinage nodes.

In WSNs, sensors are powered by their batteries. Nowadays, the battery capacity is of difficulty to be improved obviously and depleted battery is impossible to be replaced too. Therefore, saving the node energy consumption is of importance in WSNs.

As an adaptive cluster routing protocol, LEACH protocol saves energy for WSNs. Leach protocol can enlarge WSNs lifetime longer 15% than those utilizing flat multi-jumping routing protocol. However, the LEACH protocol has some weak points as follow. In the first place, the WSNs consume much battery energy because they form clusters in all rounds. Secondly, the LEACH protocol adopts single-hop method to relay data from clusters to the base station. Therefore, those remote cluster heads expend much energy to communicate with the base station in large wireless sensor networks[4], [5]. Thirdly, when the LEACH protocol was propounded, the WSNs security was

not an important topic, so it can not ensure network security.

This paper researches how to save node energy consumption and improve security for WSNs using LEACH protocol. The heterogeneous wireless sensor networks (HWSNs) have some powerful sensor nodes, namely heterogeneous sensor nodes, which have greater power than other nodes have. Ordinary nodes and heterogeneous nodes are dispensed respectively in the sensing area. The sensing area is partitioned into a number of equilateral triangle cells and equal number ordinary nodes locate in each cell. Six cells comprise a cluster, in each of which one heterogeneous node locates. The heterogeneous nodes play the part of cluster heads in all clusters and ordinary nodes play the part of cluster sensors. The data are relayed to the base station through using a multi-jumping method along a routing path consisting of heterogeneous nodes. The pairwise keys are established through utilizing the method of the overlap key sharing and the random key pre-distribution strategy. This scheme balances battery energy expense of all the nodes, saves the node energy, and prolongs the network life. Moreover, it improves the security and connectivity of WSNs.

The rest of this paper is as follow. Section 2 describes the secure routing protocol for HWSNs. Section 3 gives the comparison between the LEACH protocol and this strategy. Conclusion is in the section 4.

The secure and efficient routing protocol for HWSNs

Two-tier structure.

We divide the whole sensor area into grids and presume that all the grids are the same and do not change in all rounds. It is clear the wireless sensor networks save more energy because they form and initialize clusters only once and the cluster heads save energy because they only communicate in their grids.

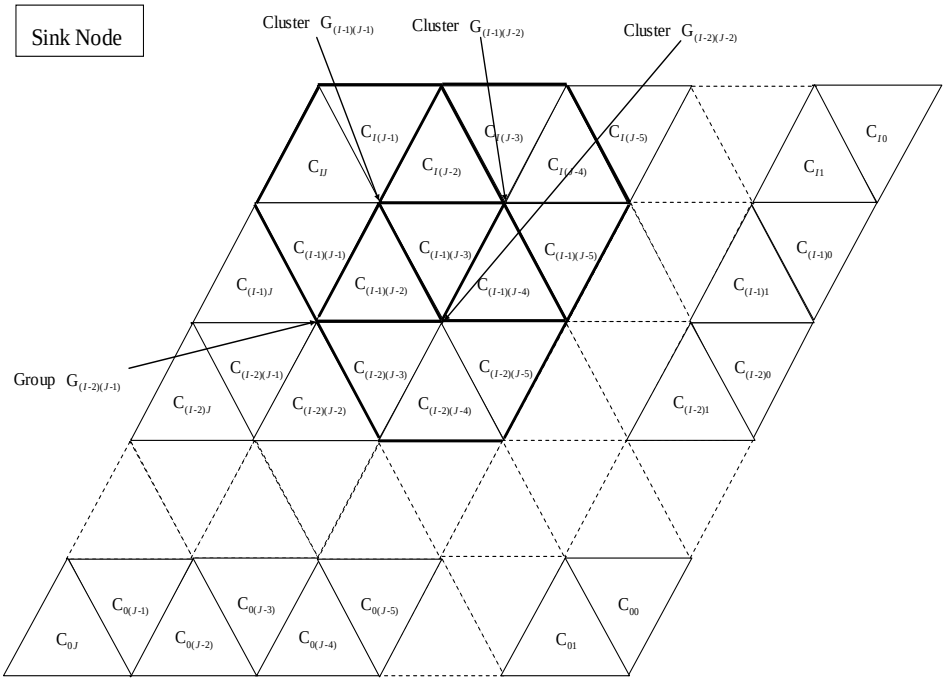

Fig. 1. The hexagon sensing area

In Fig. 1, the sensing area S_{area} in the wireless sensor networks 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.

The LEACH algorithm does not decide the cluster head number and their distribution and the distant nodes with smaller energy also probably become cluster heads. Therefore, it can induce the

unequal energy expense in wireless sensor networks and then the node life distributes in a large extension. In the latter rounds, the blind sensing areas appear in the WSN and then the performance of the WSN decreases.

To deal those problems, the sensing area is divided into a number of equilateral triangle cells and six cells consist of a cluster. All clusters are the same and do not change in all rounds and select all class 1 nodes as the cluster heads. The cluster head, namely a class 1 node, is at the cluster center in each cluster. Each class 1 node only communicates with those class 0 nodes in the same cluster and other class 1 nodes. Therefore, this paper has a two-tier structure including the upper tier that consists of all class 1 nodes and the lower tier that consists of all class 0 nodes.

Distributed Key Management Scheme.

1) Key Generation and Distribution

Class 0 sensors and class 1 sensors are scattered in S_{area}. The class 1 nodes called heterogeneous nodes have more power than the class 0 nodes called normal nodes. Suppose that the node links are bidirectional. Let r_i $(0 \le i \le 1)$ express the class i communication scope.

The protocol divides the classes of sensor nodes into J groups, where a unique group identifier j is assigned to each group.

The key server creates I bit-strings, where a unique identifier i is allocated to each of them, expressed as $S_0, S_1, \cdots, S_{I-2}, S_{I-1}$, and then takes S_0, expressed as Ω_0, as the key-string-pool for 0 class sensors, the blend of S_0 and S_1, expressed as Ω_1, as the key-string-pool for 1 class nodes, etc.

A subset of those key-string-pools, denoted as Ω_{ij}, is created for nodes in class i and group j. Allowing $\Omega_{ij} = \bigcup_{k=0}^{i} \Omega_{ij}(k)$, where $\Omega_{ij}(k)$ is a subset of Ω_k.

If $\Omega_{i_1 j}(k_1) \bigcap \Omega_{i_2 j}(k_2) \neq \varnothing$ holds, where $k_1 \le i_1 < i_2$, $k_2 \le i_1 < i_2$, $\Omega_{i_1 j}(k_1) \subset \Omega_{k_1}$, and $\Omega_{i_2 j}(k_2) \subset \Omega_{k_2}$, one class i_1 node and one class i_2 node $(i_1 < i_2)$ will be able to share some common bit-strings in group *j*. Exempli gratia, if $\Omega_{0j}(0) \bigcap \Omega_{1j}(0) \neq \varnothing$, where, $\Omega_{0j}(0) \subset \Omega_0$ and $\Omega_{1j}(0) \subset \Omega_0$, one class 0 and one class1 node will share some common bit-strings.

If $\Omega_{ij_1}(k_1) \bigcap \Omega_{ij_2}(k_2) \neq \varnothing$, where $k_1 \le i$, $k_2 \le i$, $\Omega_{ij_1}(k_1) \subset \Omega_{k_1}$, and $\Omega_{ij_2}(k_2) \subset \Omega_{k_2}$, sensors in groups $j_1, j_2 (j_1 \neq j_2)$ will share some bit-strings for the same class i. Class 0 nodes locating in different groups may share no common bit-strings, namely, $\Omega_{0j_1}(k_1) \bigcap \Omega_{0j_2}(k_2) = \varnothing$, where $\Omega_{0j_1}(0) \subset \Omega_0$ and $\Omega_{0j_2}(0) \subset \Omega_0$, and class 1 nodes locating in different groups may share no common bit-strings, namely, $\Omega_{1j_1}(k_1) \bigcap \Omega_{1j_2}(k_2) \neq \varnothing$, where $\Omega_{1j_1}(0) \subset \Omega_0$, $\Omega_{1j_1}(1) \subset \Omega_1$, $\Omega_{1j_2}(0) \subset \Omega_0$, and $\Omega_{1j_2}(1) \subset \Omega_1$.

The key server chooses a subset of key-strings, $\Phi_{ij}^n (\Phi_{ij}^n \subseteq \Omega_{ij})$, for a node n locating in class i and group j. Next, it assigns the node the key-string shares of these key-strings.

2) Pair-wise key establishment

The pair-wise key establishment comprises two parts. One is the pair-wise key establishment among all sensors, including class 0 nodes and class 1 nodes, in each cluster and the other one is the pair-wise key establishment among all class 1 nodes in the whole sensing area.

Let S denote the size of the key-string-pool Ω_1. Suppose P_0 and P_1 be the number of subsets of key-strings that can be stored in a class 0 node and a class 1 node respectively. In each cluster, we calculate the probability, $p(\alpha)$, that a class 0 node shares α sub key-strings with a class 1 node as follows

$$p(\alpha)=\frac{\binom{S}{\alpha}\binom{S-\alpha}{P_0-\alpha}\binom{S-P_0}{P_1-\alpha}}{\binom{S}{P_0}\binom{S}{P_1}}.$$

A class 0 node and a class 1 node can establish secure connection if they share a key. Therefore, the scheme can guarantee the class 0 node and a class 1 node establish secure connection if $\sum_{1}^{p_0} p(\alpha)\geq 1$. We can obtain this result through choosing reasonable S, P_0 and P_1.

We calculate the probability, $p(\beta)$, that two class 1 nodes in different groups share β sub key-strings as follows

$$p(\beta)=\frac{\binom{S}{\beta}\binom{S-\beta}{P_1-\beta}\binom{S-P_1}{P_1-\beta}}{\binom{S}{P_1}^2}.$$

The scheme can guarantee that any two class 1 nodes establish secure connection if $\sum_{1}^{p_1} p(\beta)\geq 1$. We can obtain this result through choosing reasonable S and P_1.

To sum up, the scheme can guarantee that all nodes including class 0 nodes and class 1 nodes can establish secure connections with any other node, if $\sum_{1}^{p_0} p(\alpha)\geq 1$ and $\sum_{1}^{p_1} p(\beta)\geq 1$, through selecting reasonable S, P_0 and P_1. It is clear that the network connectivity is enhanced because of the heterogeneous nodes.

Data authentication.

N_0 class 0 sensor nodes locate in S_{area}. Those class 0 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 $0\leq i\leq I$ and $0\leq j\leq J$. The sensor nodes in group C'_{ij} are deployed in cell C_{ij}. $\frac{N_0}{(I+1)(J+1)}$ class 0 nodes locate in every grid. Six cells consist of a cluster, which has a class 1 node as the cluster head. The cluster head locates in the cluster center. For example, in Fig. 1, cluster $G_{(I-1)(J-1)}$ consists of cell C_{IJ}, $C_{I(J-1)}$, $C_{I(J-2)}$, $C_{(I-1)(J-1)}$, $C_{(I-1)(J-2)}$, and $C_{(I-1)(J-3)}$. Therefore, $\frac{6N_0}{(I+1)(J+1)}+1$ nodes locate in every cluster. Let $I=J$ and then there are $(I-1)^2=(J-1)^2$ clusters, where any cluster does not contain cell C_{I0} and C_{0J}. The setup server distributes a $GID_{ij}\|SID_{j'}$ to each of all nodes in the S_{area}, where $0\leq i\leq I-2$ and $0\leq j\leq J-2$, $0\leq j'\leq \frac{6N_0}{(I+1)(J+1)}$. The setup server distributes a distinct node identification, $GID_{ij}\|SID_{j'}$, where $0\leq i\leq I-2$, $0\leq j\leq J-2$ and $j'=0$, to each node class 1 sensor node in the cluster G_{ij} and a distinct node identification, $GID_{ij}\|SID_{j'}$, where $0\leq i\leq I-2$, $0\leq j\leq J-2$ and $1\leq j'\leq \frac{6N_0}{(I+1)(J+1)}$, to each node class 0 sensor node in the cluster G_{ij}. For example, the setup server distributes $GID_{00}\|SID_0$ to the class 1 nodes in the

cluster G_{00}, and distributes $GID_{00} \| SID_1, GID_{00} \| SID_2, \cdots, GID_{00} \| SID_{\frac{6N_0}{(I+1)(J+1)}}$ to all class 0 nodes in the cell C_{00} respectively. Additionally, it distributes each node in all clusters a management key $Key_{management}$. In each cluster, the cluster head, namely the class 1 node, has all class 0 node identifications.

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

$Key_A = \text{hash}(Key_{management} \| \text{Node ID}_A)$

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

Key_A is shared by the cluster head, namely class 1 node, and node A and it is distributed to the node A before deployment.

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

If the class 0 sensor nodes are densely distributed in a certain cluster, every event in that field will be sensed by a number of class 0 sensors each with an authentication key and pairwise keys common with its neighbors. When an event occurs in that cluster, the class 0 sensor node, denoted as node P, which detects the event creates a report and then sends it to the cluster head. To be forwarded and received securely, a legitimate report must attach $m(m>1)$ distinct MACs accepted from the sensing class 0 nodes. Every node endorses the event by employing its keys to generate a MAC on the report and the cluster head knows all the keys. Therefore, when a real event occurs, multiple detecting nodes jointly generate a complete report with the required m MACs and the associated keys. To collect those MACs, P broadcasts a message to its neighbors. It will be ignored if its neighbor node, denoted as Q, have no common pairwise key with it. Otherwise, node Q creates MAC_{PQ}, and encrypts its authentication key K_P with the shared pairwise key and then forwards it downstream to nodes, such as f_1, f_2 and f_3 in Fig. 2 where f_1 has pairwise key with Q and f_2 respectively, similarly, f_2 has pairwise key with f_1 and f_3 respectively. Each node along the forwarding path has an authentication key list. If the node can not find a key match from its list, it will add K_P to its list. If two keys with the same subscripts differ each other, it demonstrates that the key could have been disclosed. After creating MAC_{PQ}, Q transmits it to node P safely, and P attaches it to the report. After P collects up to m MACs, it sends the report to the base station. Each intermediate node in the path will verify if the report has m MACs and if one of the m MACs is the same as the MAC calculated through employing the corresponding key in its authentication key list. The report will be filtered out if the authentication fails.

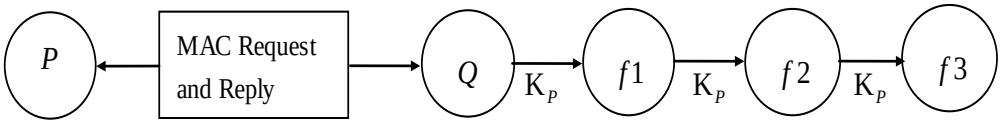

Fig.2. MAC request and key forwarding

Sending data from grids to the station in our strategy.

All cluster heads directly send those messages to the base station after receiving and compressing those data sent by the ordinary nodes of their clusters in the LEACH protocol. In large wireless sensor networks, the cluster heads far from the base station consume much battery energy to send

their data to the base station. In the new routing protocol, the distant cluster heads communicate with the base station through employing the multi-jump manner to save battery energy. Our scheme set up a routing path from clusters to the base station to guarantee that all nodes spend similar energy. Distant cluster heads transmit information to the near one through the cluster routing, rather than communicate with the base station directly.

In the design of the LEACH protocol, the routing security was not a focus, therefore, it do not guarantee the data secure, which are sent to the base station. If a cluster head ID is suspicious of being compromised, routing paths will avoid containing it to assure data secure.

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

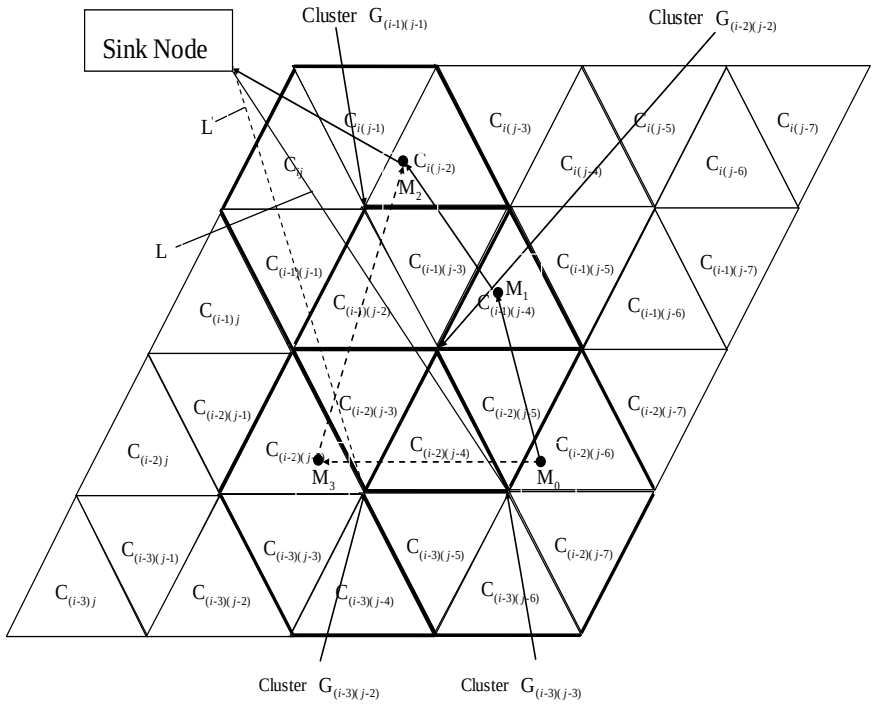

Fig.3. The improved clustering

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

The comparison between the LEACH protocol and new protocol

The energy comparison.

In the initialization of the LEACH protocol in each round, after the cluster heads are selected, they expend much energy to broadcast the message to all the nodes in the network. In our strategy, however, the clusters are formed in the first round and then do not change again in all latter rounds, moreover, in each latter round the class 1 nodes remain cluster heads. Therefore, our scheme saves more energy than the LEACH arithmetic does.

In the LEACH arithmetic, after collecting and aggregating those data sent by the ordinary nodes, all cluster heads directly send those information to the base station through single-hop manner. In large wireless sensor networks, the heads expend much energy to send data to the base station by employing this manner. Our strategy randomly establishes secure data routing consisting of class 1 nodes, which communicate with base station by employing multi-hops manner. Therefore, the new routing protocol spends less energy to send information to the base station than the LEACH protocol does.

As mentioned above, the wireless sensor networks can both save the node energy and realize the load balance among them. Additionally, all clusters have the same number of nodes and we suppose that the original energy of each same kind of nodes and the data transmitted by each cluster are the same, so, the protocol balances energy expense among all the nodes. Therefore, the new scheme extends the network existence.

The secure comparison.

1) The HELLO flooding attack

In the LEACH protocol, ordinary nodes decide whether they join a certain cluster by the signal intensity sent by the cluster head, so the malicious nodes can easily launch HELLO flooding attack. The malicious nodes broadcast by utilizing high power to attract a number of nodes to join their clusters. After cheating normal nodes to join their clusters, the malicious nodes launch other methods, such as altered information, selective forwarding and so on, to realize their goals. The new routing protocol forms clusters in the first round and do not change again, moreover, those nodes in all clusters remain in their clusters in all rounds. Therefore, the HELLO flooding attack is meaningless to the new scheme.

2) The Sybil attack

Normal nodes in the LEACH protocol possibly are compromised by Sybil attack. A malicious node communicates with different normal nodes as different identities in WSNs and its identities change in different rounds. It declares that it has much energy to increase the chance of been selected as the cluster head. In our scheme, those clusters are the same and do not change in all rounds and this protocol selects all class 1 nodes as the cluster heads in the first round and those class 1 nodes remain cluster heads in all latter rounds. If a malicious node captures one class 0 node, it can not obtain any other node’s identity because class 0 nodes only have their own identifications. Besides, a malicious node is difficult to obtain those identifications of class 1 nodes because they are powerful to defend attacks. Therefore, this protocol can defend the Sybil attack.

The conclusion

In order to save node energy and enhance wireless sensor network security, the LEACH protocol has been improved. This paper presents a routing protocol based on clusters in which the sensing area consists of a number of equilateral hexagons called clusters, and each of clusters has six equilateral triangles called cells. The class 1 nodes act as the cluster heads in all clusters. The data are sent to the base station through employing a multi-jumping manner along a routing path consisting of cluster heads, namely class 1 nodes. In a certain grid, the cluster head establishes pairwise keys with all class 0 nodes through employing the concept of the overlap key sharing and the random key pre-distribution scheme. Similarly, in the whole sensing area, all cluster heads, namely all class 1 nodes, establish their pairwise keys through employing the same methods. All

those messages, which class 0 nodes send to the cluster head in a certain cluster, are authenticated. The arithmetic balances energy expense among all the class 1 nodes, saves the node energy, prolongs the life of wireless sensor networks and improves the security for the wireless sensor network, additionally, it enhance the network connectivity.

Acknowledgements

This work was supported by the Project of Shandong Province Higher Educational Science and Technology Program, and the project number is J13LN05.

References

[1] Dnyaneshwar S. Mantri, Neeli Rashmi Prasad, Ramjee Prasad. Bandwidth efficient cluster-based data aggregation for Wireless Sensor Network. Computers and Electrical Engineering 41 (2015) 256-264.

[2] Jose M. Lanza-Gutierrez, Juan A. Gomez-Pulido. Assuming multiobjective metaheuristics to solve a three-objective optimisation problem for Relay Node deployment in Wireless Sensor Networks. Applied Soft Computing 30 (2015) 675-687.

[3] Lai D, Hwang S. Kim, Verbauehrde I. Reducing radio energy consumption of key management protocols for wireless sensor networks. Proceedings of ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED’04), 2004, pp. 351-356.

[4] Andrew Wichmann, Turgay Korkmaz. Smooth path construction and adjustment for multiple mobile sinks in wireless sensor networks. Computer Communications 000 (2015) 1-14.

[5] Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Mat Kiah, Ismail Ahmedy. Survey of secure multipath routing protocol for WSNs. Journal of Network and Computer Applications 55 (2015) 123-153.