# A Secure and Efficient Routing Protocol for Heterogeneous Wireless Sensor Networks

Yuquan Zhang[1,2,a], Lei Wei[3,b]

[1]Shandong Women University, China

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

[3]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; pairwise key; energy; security; connectivity

**Abstract.** A secure and efficient routing protocol for heterogeneous wireless sensor networks is proposed to deal with some issues in the LEACH arithmetic. The wireless sensor networks have some sensor nodes that have greater power and transmission capability than other nodes have. Both ordinary nodes and heterogeneous nodes are distributed respectively in a sensing area that is divided into a number of same equilateral hexagons. Each hexagon has one heterogeneous node. Heterogeneous nodes act as the cluster heads and ordinary nodes act as those cluster sensors in all clusters. The pairwise keys between nodes are established through utilizing the concept of the overlap key sharing and the random key predistribution 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

The development of sensor technologies has facilitated the development of wireless sensor networks (WSNs). WSNs comprise a mass of sensors which are powered by batteries[1]. Heterogeneous wireless sensor networks (HWSNs) include several different kinds of sensors some of which are more powerful than others. During the last decade, WSNs have been researched considerably. Wireless sensor networks are utilized to sustain various applications[2].

When WSNs are deployed in antagonistic environments, security becomes extremely of importance because they are susceptible to be attacked. Key management protocols are of importance in assuring wireless sensor networks secure. Lai D et al.[3] gave a protocol. The scheme generates a bit-string as the key-string-pool (KP), and at random allocates each sensor a subset of the KP as the key-string. Sensors use the overlap intervals of the key-strings as the shared secret key with their neighbor nodes.

Sensors are powered by the batteries carried with them in WSNs. Nowadays, the battery capacity is impossibly enhanced obviously and replacing depleted battery is impossible too. Therefore, it is essential to save the node battery consumption in WSNs.

LEACH protocol is an adaptive cluster routing protocol which saves energy for WSNs. WSNs employing Leach protocol live longer 15% than those utilizing flat multi-jumping routing protocol or using static cluster arithmetic. However, the LEACH protocol has some problems as follow. Firstly, the WSNs consume much battery energy because of the forming clusters in all rounds. Secondly, the LEACH protocol adopts single-hop manner to transmit data from clusters to the base station. Therefore, those distant cluster heads expend much energy to communicate with the base station in large wireless sensor networks which adopt single-hop manner to transmit data[4][5].

Thirdly, when the LEACH protocol was proposed, the WSNs security was not an important issue, so it is not secure enough.

This paper gives a routing protocol, which can save energy and improve security for heterogeneous wireless sensor networks (HWSNs). Both ordinary nodes and heterogeneous nodes (more powerful nodes) are dispensed evenly in a sensing area. The sensing area comprises a number of equilateral hexagons, each of which has one heterogeneous node. The heterogeneous nodes function as cluster heads in all clusters and ordinary nodes function as cluster sensor nodes. The messages are transmitted to the base station through utilizing a multi-jumping manner along a routing path consisting of heterogeneous nodes. The pair-wise keys between nodes are established through utilizing the concept of the overlap key sharing and the random key pre-distribution scheme. The scheme equalizes energy consumption among all the nodes, conserves the node energy, and enlarges the life of wireless sensor networks. In addition, this scheme improves the network security and connectivity.

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

## The Secure and Efficient Routing Protocol for HWSN

### Two-Tier Structure.

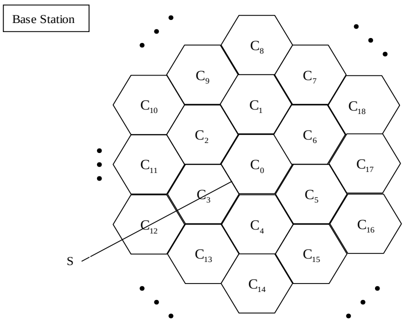

Fig.1 The hexagon sensing area

In Fig.1, the sensing area $S$ in the WSNs is partitioned into $J$ same equilateral hexagon cells, namely $\mathrm{C}_0, \mathrm{C}_1, \cdots, \mathrm{C}_j, \cdots, \mathrm{C}_{J\text{-}2}$ and $\mathrm{C}_{J\text{-}1}$, where $0 \le j \le J-1$, according to their locations.

The LEACH algorithm does not determine the cluster head number and their distribution. Therefore, the unequal energy expense occurs in wireless sensor networks and then the node lifetime distributes in a large extension. In the latter rounds, the blind sensing areas appear, and then the WSN performance reduces.

To solve those problems, this protocol divides the whole sensing area into grids, which are the same and do not change in all rounds and choose all class 1 nodes as the cluster heads. A class 1 node locates in each grid center or close to the center. Each class 1 sensor can only communicate with those class 0 sensors in the same grid and other class 1 nodes. Therefore, this strategy has a two-tier structure including the upper tier that comprises all class 1 nodes and the lower tier that comprises all class 0 nodes.

### Distributed Key Management Scheme.

1) Key Generation and Distribution

Class 0 nodes and class 1 nodes are distributed in the sensing space. The class 0 nodes are normal nodes and the class 1 nodes have more power. Suppose that the links of between sensors are bi-directional. Let $r_i$ $(0 \le i \le 1)$ express the class $i$ communication range. It is clear that $r_0 < r_1$.

The protocol divides the classes of sensor nodes into $J$ groups, where a unique group identifier $j$ is allocated 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 $\Omega_0$, as the key-string-pool for 0 class sensors, the blend of $S_0$ and $S_1$, expressed as $\Omega_1$, as the key-string-pool for 1 class nodes, etc.

A subaggregate of those key-string-pools, expressed as $\Omega_{ij}$, may be 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 subaggregate of $\Omega_k$.

If $\Omega_{i_1 j}(k_1) \bigcap \Omega_{i_2 j}(k_2) \neq \varnothing$ exists, where $k_1 \leq i_1 < i_2$, $k_2 \leq i_1 < i_2, \Omega_{i_1 j}(k_1) \subset \Omega_{k_1}$, 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 have some common bit-strings in group *j*. For instance, 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 be able to have some common bit-strings.

If $\Omega_{ij_1}(k_1) \bigcap \Omega_{ij_2}(k_2) \neq \varnothing$, where $k_1 \leq i$, $k_2 \leq i$, $\Omega_{ij_1}(k_1) \subset \Omega_{k_1}$, and $\Omega_{ij_2}(k_2) \subset \Omega_{k_2}$, sensors in two different groups $j_1, j_2 (j_1 \neq j_2)$ will be able to have some common bit-strings for the same class $i$. Class 0 nodes in different groups may have 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 in different groups may have 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 subaggregate of key-strings, namely $\Phi_{ij}^n$ ($\Phi_{ij}^n \subseteq \Omega_{ij}$), for a node $n$ in class $i$ and group $j$. Next, it assigns the node the key-string shares of these key-strings.

2) Pair-Wise Key Establishment

Let $S$ be the size of the key-string-pool $\Omega_1$. Let $P_0$ and $P_1$ be the number of subaggregate of key-strings which can be stored in a class 0 node and a class 1 node respectively. The probability $p(\alpha)$ that a class 0 node shares $\alpha$ sub key-strings with a class 1 node is calculated as follows

$$p(\alpha) = \frac{\begin{pmatrix} S \\ \alpha \end{pmatrix} \begin{pmatrix} S-\alpha \\ P_0-\alpha \end{pmatrix} \begin{pmatrix} S-P_0 \\ P_1-\alpha \end{pmatrix}}{\begin{pmatrix} S \\ P_0 \end{pmatrix} \begin{pmatrix} S \\ P_1 \end{pmatrix}}.$$

If a class 0 node and a class 1 node share a key, they can establish secure connection. Therefore, the scheme can ensure the class 0 node and a class 1 node set up secure connection if $\sum_{1}^{P_0} p(\alpha) \geq 1$. This result can be obtained through choosing reasonable $S$, $P_0$ and $P_1$.

Suppose a class 1 node only can establish safe links with those class 1 nodes the closest to it in different groups. For example, in Fig.1, the class 1 node in $\mathrm{C}_0$ only can establish secure links with all those class 1 nodes in $\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3, \mathrm{C}_4, \mathrm{C}_5$ and $\mathrm{C}_6$. The probability $p(\beta)$ that two class 1 nodes in different groups share $\beta$ sub key-strings is calculated as follows

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

The strategy can ensure any two class 1 nodes establish safe links, if $\sum_{1}^{P_1} p(\beta) \geq 1$. This result can be obtained through choosing reasonable $S$ and $P_1$.

From above discussion, the strategy can ensure all nodes establish safe links with any other node, if $\sum_{1}^{p_0} p(\alpha) \geq 1$ and $\sum_{1}^{p_1} p(\beta) \geq 1$, through choosing reasonable $S$ , $P_0$ and $P_1$. It is obvious the network connectivity is enhanced because of the heterogeneous nodes.

3) Data Authentication

There are $N_0$ class 0 nodes and $N_1$ class 1 nodes in $S$ . Those two kinds of nodes are evenly partitioned into $J$ same groups denoted as $\mathrm{C}_0^{'}$, $\mathrm{C}_1^{'}$, $\cdots$, $\mathrm{C}_j^{'}$, $\cdots$, $\mathrm{C}_{J\text{-}2}^{'}$ and $\mathrm{C}_{J\text{-}1}^{'}$, where $0 \leq j \leq J-1$. Those two kinds of nodes in group $\mathrm{C}_j^{'}$ are dispensed in cell $\mathrm{C}_j$ . $\frac{N_0+N_1}{J}$ nodes locate in every cell and the setup server distributes a certain $\mathrm{CID}_j \,||\, \mathrm{SID}_{j^{'}}$ to each of all nodes in $S$ , where $0 \leq j \leq J-1$, $0 \leq j^{'} \leq \frac{N_0+N_1}{J} - 1$. The setup server distributes a distinct node identifier, $\mathrm{CID}_j \,||\, \mathrm{SID}_{j^{'}}$, where $0 \leq j \leq J-1$ and $0 \leq j^{'} \leq \frac{N_1}{J} - 1$, to each class 1 node in the cell $\mathrm{C}_j$ and a distinct node identifier, $\mathrm{CID}_j \,||\, \mathrm{SID}_{j^{'}}$, where $0 \leq j \leq J-1$ and $\frac{N_1}{J} \leq j^{'} \leq \frac{N_0+N_1}{J} - 1$, to each class 0 node in the cell $\mathrm{C}_j$ . For example, the setup server distributes $\mathrm{CID}_0 \,||\, \mathrm{SID}_0, \mathrm{CID}_0 \,||\, \mathrm{SID}_1$, $\cdots$ , $\mathrm{CID}_0 \,||\, \mathrm{SID}_{\frac{N_1}{J}-1}$ to all class 1 nodes in the cell $\mathrm{C}_0$ , and distributes $\mathrm{CID}_0 \,||\, \mathrm{SID}_{\frac{N_1}{J}}$ , $\mathrm{CID}_0 \,||\, \mathrm{SID}_{\frac{N_1}{J}+1}$ , $\cdots$ , $\mathrm{CID}_0 \,||\, \mathrm{SID}_{\frac{N_0+N_1}{J}-1}$ to all class 0 nodes in the cell $\mathrm{C}_0$ respectively. Additionally, it distributes each node in all clusters a management key $\mathrm{Key}_{\mathrm{management}}$ . In this paper, $J = N_1$. In each cluster, the cluster head has all class 0 node identifiers.

The node authentication key $\mathrm{Key}_A$ of node $A$ is generated through utilizing hash function with key parameter as the following

$$\mathrm{Key}_A = \mathrm{hash}(\mathrm{Key}_{\mathrm{management}} \,||\, \mathrm{Node\ ID}_A) .$$

where $\mathrm{Key}_{\mathrm{management}}$ is the key parameter, and the node identifier $\mathrm{ID}_A$ is the input.

$\mathrm{Key}_A$ is shared by the cluster head and node $A$ and it is distributed to the node $A$ before deployment.

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

If the class 0 nodes are densely dispensed in a cluster, every occurrence in the cluster will be detected by a number of class 0 sensors each of which has an authentication key and pairwise keys common with its vicinages. When an occurrence occurs in that cluster, the class 0 node $P$ that detects the occurrence creates a report and then transmits it to the cluster head. In order to forward and receive it securely, a legitimate report must attach $m(m>1)$ distinct MACs received from the sensing class 0 nodes. Each node endorses the event by the MAC on the report which is generated through employing its keys, and the cluster head knows those keys. Therefore, when a real occurrence 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 $Q$ has no common pairwise key with it. Otherwise, $Q$ creates $\mathrm{MAC}_{PQ}$, and encrypts its authentication key $\mathrm{K}_P$ 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 $\mathrm{K}_P$ to its list. If two keys with the same subscripts differ each other, it demonstrates that the key could have been disclosed. After creating $\mathrm{MAC}_{PQ}$, $Q$ 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.

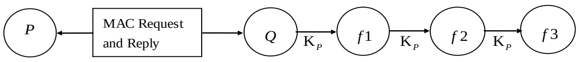

Fig.2 MAC request and key forwarding

**Sending Data from Grids to the Station in This Strategy.**

As mentioned above, in the new routing protocol, the class 1 sensor nodes act as the cluster heads in all clusters. Suppose all clusters have the same number of class 0 nodes. Additionally, suppose the original energy of the same kind of nodes is the same and the data transmitted by each cluster is the same. All the cluster heads communicate with the base station by utilizing the multi-hop manner to save energy. Our scheme guarantees that the same kind of nodes, class 1 nodes and class 0 nodes, spend similar energy.

The cluster routing comprises clusters, which are in the direction from the original cluster to the base station and participate in routing. In Fig. 3, the original cluster head $\mathrm{M}_0$ will relay data to the base station, and a line $\mathrm{L}$ is drawn from the center of cluster $\mathrm{C}_{m_0}$ to the base station. So, the cluster routing includes cluster $\mathrm{C}_{m_0}, \mathrm{C}_{m_1}$ and $\mathrm{C}_{m_2}$, and cluster head $\mathrm{M}_0$, $\mathrm{M}_1$, and $\mathrm{M}_2$ 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 $\mathrm{M}_1$ is compromised, the original routing stops here and the preparing routing is utilized. The new routing clusters contain the cluster $\mathrm{C}_{m_3}$ and a line $\mathrm{L}'$ is drawn from its center to the base station. The new preparing cluster routing consists of clusters, which $\mathrm{L}'$ passes through.

The clusters near to the base station expend more energy because they frequently relay 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 $\mathrm{M}_\mathrm{Y}$ sends data to its next relay cluster head $\mathrm{M}_\mathrm{X}$, the original routing stops, if $E_{\mathrm{M}_\mathrm{X}} < E_{\min}$, where, $E_{\mathrm{M}_\mathrm{X}}$ is the energy of $\mathrm{M}_\mathrm{X}$. Therefore, our strategy can balance the energy consumption in the wireless sensor networks.

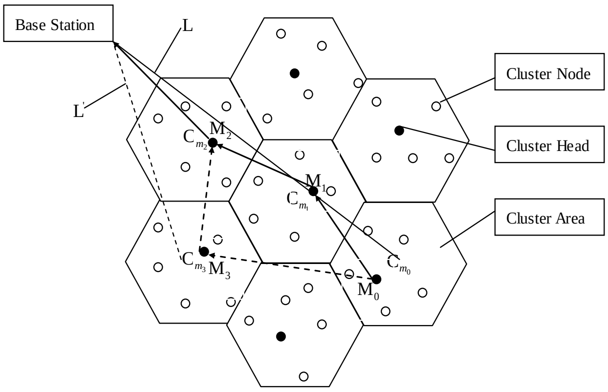

Fig.3 The improved clustering

## The Comparison between the LEACH Protocol and the 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 identifiers. Besides, a malicious node is difficult to obtain those identifiers of class 1 nodes because they are powerful to defend attacks. Therefore, this protocol can defend the Sybil attack.

## Conclusion

In order to save node energy and enhance wireless sensor network security, the LEACH protocol has been improved. The pairwise keys between nodes are established through utilizing the concept of the overlap key sharing and the random key predistribution scheme. All ordinary nodes send their messages to their cluster heads after authenticating those messages. The arithmetic balances energy expense among all the class 1 nodes, saves the node energy, prolongs the WSNs life and improves the security for the wireless sensor network, additionally, it enhance the network connectivity.

## References

[1] Naércio Magaia, Nuno Horta, Rui Neves, Paulo Rogério Pereira, Miguel Correia. A multi-objective routing algorithm for Wireless Multimedia Sensor Networks. Applied Soft Computing 30 (2015) 104-112.

[2] Junyoung Park, Sunggu Lee, Sungjoo Yoo. Time slot assigmnet for convergecast in wireless sensor networks. J. Parallel Distrib. Comput. 83(2015)70-82.

[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.