A Secure Scheme for Heterogeneous Wireless Sensor Networks Based on Grids and Symmetric Polynomials

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: Wireless sensor network; security; grid; tetrahedron; symmetric polynomials.

Abstract. A scheme for WSNs (wireless sensor networks) security is given by dividing sensing tetrahedron into clusters and using the symmetric polynomials in this paper. The sensing tetrahedron is divided into a number of small grids. All those sensor nodes, both ordinary sensor nodes and heterogeneous sensor nodes are distributed in the sensing tetrahedron. In a grid, all ordinary sensor nodes and heterogeneous sensor nodes establish their shared keys through using the symmetric polynomials. All the heterogeneous sensor nodes establish their shared keys through using the symmetric polynomials. At last, all sensor nodes establish their keys directly or indirectly in the whole sensing tetrahedron. Analysis and comparison demonstrate this scheme enhances the WSN security, has good network connectivity, saves node storage, reduces network computing load, and extends the network lifetime.

Introduction

Wireless sensor networks have various applications and have received considerable attention by researchers all over the world. Wireless sensor networks consist of many small devices called sensor nodes, of course, sometimes, they comprise several kinds of sensor nodes. One kind of sensor nodes are called ordinary sensor nodes, and other kinds of sensor nodes are called heterogeneous sensor nodes which generally have more powerful abilities. We name the wireless sensor networks which consist of ordinary sensor nodes and heterogeneous sensor nodes heterogeneous wireless sensor networks[1][2].

Those sensor nodes in wireless sensor networks are linked by wireless transmission medium. In general, those sensor nodes have some unique characters, including low battery energy, limited communication capacity, low computation ability, etc. Additionally, in order to fulfil their applications, sometimes, wireless sensor networks are distributed in unfriendly or even hostile environment. So, wireless sensor networks are susceptible to various vicious attacks [3].

Guaranteeing the wireless sensor networks secure is an of importance task in order to finish the wireless sensor networks applications. The key management scheme that hinders the activities of malicious sensor nodes is an efficient method to ensure wireless sensor networks security.

Those key management strategies in paper [4] and [5] guarantee the wireless sensor networks secure through using the symmetric polynomials. In the two schemes sensor nodes set up their shared keys through utilizing the symmetric polynomials.

In the paper, we give a key management strategy based on grids for the security of wireless sensor networks. In this scheme, the sensing tetrahedron is divided into a number of grids. All sensor nodes, both ordinary sensor nodes and heterogeneous sensor nodes, are dispensed in the whole sensing tetrahedron. In each grid, two kinds of sensors establish their common keys through using the symmetric polynomials. In the entire sensing tetrahedron, all heterogeneous sensor nodes also set up their shared keys through using the symmetric polynomials. Finally, all sensor nodes in the whole sensing tetrahedron set up their shared keys directly or indirectly. Analysis and comparison show that this scheme enhances the security of WSNs, and has good network connectivity.

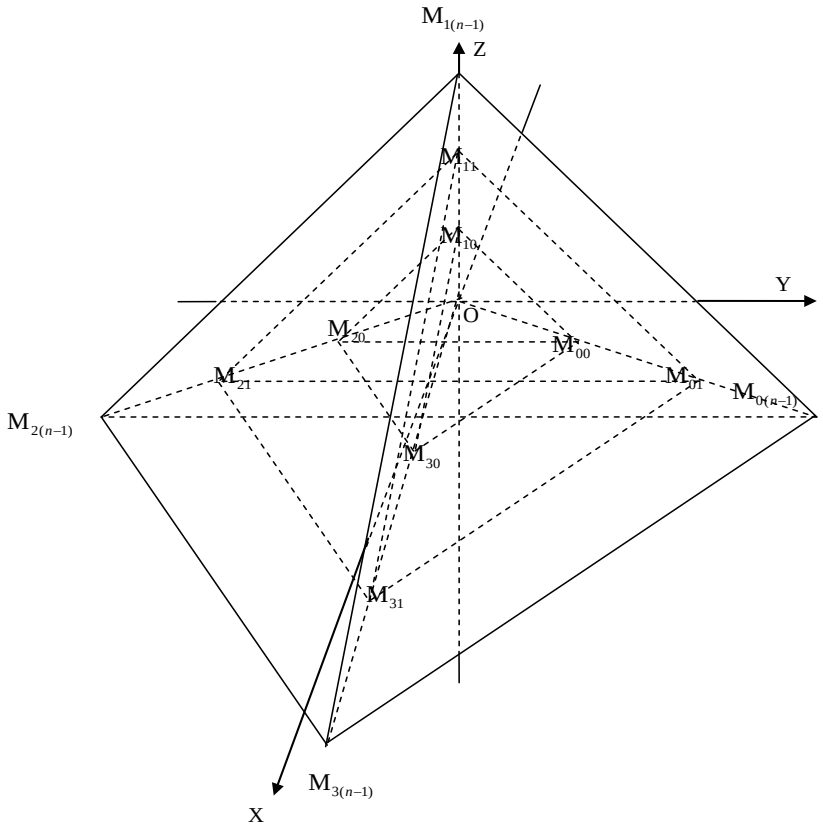

Fig.1. The sensing tetrahedron

The rest of this paper is organized as follows. In section two, the pairwise key establishment is given. Performance analysis for WSNs is given in the section three. The conclusions of this paper are in section four.

The pairwise key establishment

Sensing tetrahedron division and sensor distribution.

In this paper, the sensing space is a regular tetrahedron denoted as V and the nodes are equally distributed in V in this scheme. The sensing regular tetrahedron in the wireless sensor networks is divided into $4\times n$ sections. In the Fig.1, there are numerous concentric regular tetrahedrons whose center is O and the side length of the minimum regular tetrahedron is r, the side length of the secondary minimum regular tetrahedron is $2r,\cdots$, the side length of the largest regular tetrahedron is nr. All those concentric regular tetrahedrons are divided into 4 sections equally. The section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{30}$ is denoted as $(0,0)$, The section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{20}$ is denoted as $(0,1)$, The section $\mathrm{OM}_{10}\mathrm{M}_{20}\mathrm{M}_{30}$ is denoted as $(0,2)$, The section $\mathrm{OM}_{00}\mathrm{M}_{20}\mathrm{M}_{30}$ is denoted as $(0,3)$, The section $\mathrm{M}_{00}\mathrm{M}_{10}\mathrm{M}_{30}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}$ is denoted as $(1,0)$, The section $\mathrm{M}_{00}\mathrm{M}_{10}\mathrm{M}_{20}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{21}$ is denoted as $(1,1)$, The section $\mathrm{M}_{10}\mathrm{M}_{20}\mathrm{M}_{30}\mathrm{M}_{11}\mathrm{M}_{21}\mathrm{M}_{31}$ is denoted as $(1,2)$, The section $\mathrm{M}_{00}\mathrm{M}_{20}\mathrm{M}_{30}\mathrm{M}_{01}\mathrm{M}_{21}\mathrm{M}_{31}$ is denoted as $(1,3),\cdots$, the section $\mathrm{M}_{0(n-2)}\mathrm{M}_{2(n-2)}\mathrm{M}_{3(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{2(n-1)}\mathrm{M}_{3(n-1)}$ is denoted as $(n-1,3)$. Generally, sections are denoted as (p,q). Suppose volume of the section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{30}$ is $V_{0,0}$. The volume $V_{1,0}$ of the $\mathrm{M}_{00}\mathrm{M}_{10}\mathrm{M}_{30}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}$ is $7V_{0,0}$, the volume $V_{2,0}$ of the $\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}\mathrm{M}_{02}\mathrm{M}_{12}\mathrm{M}_{32}$ is $19V_{0,0}$, $\cdots$, the volume $V_{(n-1),0}$ of the $\mathrm{M}_{0(n-2)}\mathrm{M}_{1(n-2)}\mathrm{M}_{3(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{3(n-1)}$ is $6n'V_{00}+V_{(n'-1)0}$ ($n'=0,1,2\cdots n-1, V_{-10}=0$). In the same way, we can obtain those volume of other

sections. Suppose α sensor nodes are distributed in volume $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{30}$. Then, 7α sensor nodes are distributed in section $\mathrm{M}_{00}\mathrm{M}_{10}\mathrm{M}_{30}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}$, 19α sensor nodes are distributed in section $\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}\mathrm{M}_{02}\mathrm{M}_{12}\mathrm{M}_{32}$, $\cdots$, $\frac{(3n^2-3n+1)}{4}\alpha$ sensor nodes are distributed in section $\mathrm{M}_{0(n-2)}\mathrm{M}_{1(n-2)}\mathrm{M}_{3(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{3(n-1)}$.

Suppose heterogeneous sensor nodes which have more communication capacity, battery energy, storage memory and higher computational ability than ordinary sensors are distributed in sensing space equally and β sensor nodes are distributed in section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{30}$. Then, 7β sensor nodes are distributed in section $\mathrm{M}_{00}\mathrm{M}_{10}\mathrm{M}_{30}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}$, 19β sensor nodes are distributed in section $\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{31}\mathrm{M}_{02}\mathrm{M}_{12}\mathrm{M}_{32}$, $\frac{(3n^2-3n+1)}{4}\beta$ sensor nodes are distributed in section $\mathrm{M}_{0(n-2)}\mathrm{M}_{1(n-2)}\mathrm{M}_{3(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{3(n-1)}$. Let all sections be grids, and in a certain grid there are ordinary senser nodes and heterogeneous sensor nodes which are denoted by IDs. All ordinary sensor nodes are denoted in the section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{30}$ as $1,2,\cdots,\alpha$, next, all heterogeneous sensor nodes are denoted in the section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{30}$ as $\alpha+1,\alpha+2,\cdots,\alpha+\beta$. In the same way, All ordinary sensor nodes are denoted in the section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{20}$ as $\alpha+\beta+1,\alpha+\beta+2,\cdots,2\alpha+\beta$, next, all heterogeneous sensor nodes are denoted in the section $\mathrm{OM}_{00}\mathrm{M}_{10}\mathrm{M}_{20}$ as $2\alpha+\beta+1,2\alpha+\beta+2,\cdots,2\alpha+2\beta$. At last, All ordinary sensor nodes are denoted in the section $\mathrm{M}_{0(n-2)}\mathrm{M}_{1(n-2)}\mathrm{M}_{3(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{3(n-1)}$ as $[n^3-\frac{1}{4}(3n^2-3n+1)](\alpha+\beta)+1,[n^3-\frac{1}{4}(3n^2-3n+1)](\alpha+\beta)+2,\cdots,[n^3-\frac{1}{4}(3n^2-3n+1)](\alpha+\beta)+\frac{(3n^2-3n+1)}{4}\alpha$, next, all heterogeneous sensor nodes are denoted in the section $\mathrm{M}_{0(n-2)}\mathrm{M}_{1(n-2)}\mathrm{M}_{3(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{3(n-1)}$ as $[n^3-\frac{1}{4}(3n^2-3n+1)](\alpha+\beta)+\frac{(3n^2-3n+1)}{4}\alpha+1,[n^3-\frac{1}{4}(3n^2-3n+1)](\alpha+\beta)+\frac{(3n^2-3n+1)}{4}\alpha+2,\cdots n^3(\alpha+\beta)$.

Pairwise key establishment among all sensor nodes in each grid.

A symmetric polynomial[4,5] is a t-degree (K+1)-variate polynomial defined as follows

$f(x_1,x_2,\cdots,x_{K+1})=\sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\cdots\sum_{i_{K+1}=0}^{t}a_{i_1,i_2,\cdots i_K,i_{K+1}}\times x_1^{i_1}x_2^{i_2}\cdots x_K^{i_K}x_{K+1}^{i_{K+1}}$. All cofficients of the polynomial are chosen from a finite field F_q, where q is a prime integer. The polynomial f is a symmetric polynomial so that [5]

$f(x_1,x_2,\cdots,x_{K+1})=f(x_{\partial(1)},x_{\partial(2)},\cdots,x_{\partial(K+1)})$

where ∂ denotes a permutation. Every node using the symmetric polynomial based protocol takes K credentials $(I_1,I_2,\cdots I_K)$ from the key management centre, and these are stored in memory. The key management centre must also compute the polynomial shares using the node credentials and the symmetric polynomial. The coefficients b_i stored in node memory as the polynomial share are computed as follows

$$f_u(x_{K+1})=f(I_1,I_2,\cdots,I_K,x_{K+1})=\sum_{i=0}^{t}b_i x_{K+1}^i$$

In this paper, let $p=I_1, q=I_2, \mathrm{ID}=I_3$. Every pair of nodes with only one mismatch in their identities can establish a shared key. Obviously, two sensors in one certain grid have the same values of p and q and they have different values of ID.

Suppose the identities of nodes u and v in one certain grid are (p_u, q_u, ID_u) and (p_v, q_v, ID_v) respectively. It is clear that $p_u = p_v, q_u = q_v, ID_u \neq ID_v$. In this case, a t-degree (3+1)-variate polynomial defined as follows

$f(x_1, x_2, x_3, x_4) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\sum_{i_3=0}^{t}\sum_{i_4=0}^{t} a_{i_1,i_2,i_3,i_4} \times x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}$ is utilized. In order to compute a shared key, node u takes ID_v as the input and computes $f_u(ID_v)$, node v takes ID_u as the input and computes $f_v(ID_u)$, due to the polynomial symmetry, both nodes compute the same shared key. Generally, two sensors u and v in the same grid can establish shared key $k_{uv} = f_u(ID_v) = f_v(ID_u)$. So, all sensor nodes both ordinary sensor nodes and heterogeneous sensor nodes in one certain grid can establish their shared keys.

Pairwise key establishment among all sensor nodes in the whole tetrahedron.

Two heterogeneous sensor node α $(p_\alpha, q_\alpha, ID_\alpha)$ and β $(p_\beta, q_\beta, ID_\beta)$ locate in two different grids. They can establish their pairwise key if $\|q_\alpha - q_\beta\| = 1$ and $p_\alpha = p_\beta$ hold. In this case, assume that $I_1 = p_\alpha = p_\beta$, $I_2 = q_\alpha (q_\alpha = q_\beta - 1)$ or $I_2 = q_\beta (q_\alpha = q_\beta + 1)$, and, clearly, $ID_\alpha \neq ID_\beta$. Similarly, a t -degree polynomial defined as the following

$f(x_1, x_2, x_3, x_4) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\sum_{i_3=0}^{t}\sum_{i_4=0}^{t} a_{i_1,i_2,i_3,i_4} \times x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}$ is utilized.

In order to calculate a shared key between heterogeneous sensor node α and heterogeneous sensor β, sensor node α takes ID_β as the input and computes $f_\alpha(ID_\beta)$, and sensor node β takes ID_α as the input and computes $f_\beta(ID_\alpha)$. Both heterogeneous sensor nodes compute the same shared key because of the symmetry polynomial employed. In general, two heterogeneous sensor nodes α and β, where, $\|q_\alpha - q_\beta\| = 1$ holds, can establish shared key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$.

For the other case, two heterogeneous sensor node α $(p_\alpha, q_\alpha, ID_\alpha)$ and β $(p_\beta, q_\beta, ID_\beta)$ which also locate in two different grids can set up their pairwise key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$, if $\|p_\alpha - p_\beta\| = 1$ and $q_\alpha = q_\beta$ hold. Here, assume that $I_1 = p_\alpha = p_\beta$, $I_2 = q_\alpha (q_\alpha = q_\beta - 1)$ or $I_2 = q_\beta (q_\alpha = q_\beta + 1)$, and, clearly, $ID_\alpha \neq ID_\beta$. Similarly, a t degree polynomial defined as the following

$f(x_1, x_2, x_3, x_4) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\sum_{i_3=0}^{t}\sum_{i_4=0}^{t} a_{i_1,i_2,i_3,i_4} \times x_1^{i_1} x_2^{i_2} x_3^{i_3} x_4^{i_4}$ is utilized.

In order to get a shared key between heterogeneous sensor node α and heterogeneous sensor β, sensor node α takes ID_β as the input and computes $f_\alpha(ID_\beta)$, and sensor node β takes ID_α as the input and computes $f_\beta(ID_\alpha)$. Both heterogeneous sensor nodes compute the same shared key because of the symmetry polynomial employed. In general, two heterogeneous sensor nodes α and β, where, $\|p_\alpha - p_\beta\| = 1$ holds, can establish shared key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$.

A heterogeneous sensor node establishes the common keys with both those heterogeneous sensor nodes which locate in the same grids and those heterogeneous sensor nodes which locate in those grids close to the grid it locates in. It is clear that any pair of two heterogeneous sensor nodes which locate in two different grids not close each other can set up their common keys by using intermediate heterogeneous sensor nodes between them even through the two grids are far away. Therfore, a heterogeneous sensor node establishes common keys with all the heterogeneous sensor nodes in the whole sensing area directly or indirectly. In a grid, a heterogeneous sensor node set up common keys with all sensor nodes including ordinary sensor nodes and heterogeneous sensor nodes. Therefore, an ordinary sensor node establishes common keys with those heterogeneous sensor nodes which locate

in different grids under the help of the heterogeneous sensor nodes which locate in the same grid. Next, the ordinary sensor node can set up common keys with those ordinary sensor nodes which locate in different grids under the help of the heterogeneous sensor nodes which locate in the same grid and which locate in those different grids. Therefore, all sensor nodes including ordinary sensor nodes and heterogeneous sensor nodes establish their common keys with other sensor nodes directly or indirectly.

Performance analysis for WSNs

Security analysis for WSNs.

In a grid, two sensor nodes share common key $k_{uv} = f_u(ID_v) = f_v(ID_u)$. From the polynomial utilized, it is more difficult to compromise the $k_{uv} = f_u(ID_v) = f_v(ID_u)$ in this paper than in the paper [4]. In the same way, two heterogeneous sensor nodes which locate in two close grids have common key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$. From the polynomial utilized, it is more difficult to compromise the key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$ in this paper than in the paper [4]. Moreover, even if the $k_{uv} = f_u(ID_v) = f_v(ID_u)$ in an ordinary sensor node is compromised, the enemy only gets the key of other ordinary sensor nodes in this grid, and the enemy can not get all keys of the heterogeneous heterogeneous sensor nodes in this section because the heterogeneous sensor nodes have the keys $k_{uv} = f_u(ID_v) = f_v(ID_u)$ and $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$. As a result, the enemy can not attack those heterogeneous sensor nodes in this section through using the key $k_{uv} = f_u(ID_v) = f_v(ID_u)$. If an ordinary sensor node is compromised in this section, it is impossible for the enemy gets those keys of those sensor nodes including ordinary sensor nodes and heterogeneous sensor nodes in other grids because different keys among sensor nodes in different grids are different. From above discussion, this scheme improves the WSNs security.

Connectivity analysis for WSNs.

A node u (p_u, q_u, ID_u), of course, that can be ordinary sensor node or heterogeneous sensor node can set up communication keys with its neighbor noders including ordinary sensor nodes and heterogeneous sensor nodes and then it can set uo communication paths with those nodes including ordinary sensor nodes and heterogeneous sensor nodes which are not its neighbor nodes through using those intermediate heterogeneous sensor nodes. Therefore, this scheme can ensure all sensor nodes, ordinary sensor nodes and heterogeneous sensor nodes, are connected safely. The node can still communicate with other nodes safely even though some or total of its neighbor ordinary nodes are captured by the enemy. From discussion from above, an ordinary sensor node set up secure routings with other ordinary sensor nodes which locate in different grids through employing those heterogeneous sensor nodes which locate in its grid or other grids. This scheme can guarantee that it is difficult or impossible to compromise those routings even those heterogeneous sensor nodes are attacked by the enemy because those heterogeneous sensor nodes have more powerful capacities than those ordinary sensor nodes, and then are difficult to be compromised. Therefore, this scheme enahnces the wireless sensor network security.

Storage analysis for WSNs.

For two heterogeneous sensor node α $(p_\alpha, q_\alpha, ID_\alpha)$ and β $(p_\beta, q_\beta, ID_\beta)$ in two different grids, they can establish their pairwise key if $\|q_\alpha - q_\beta\| = 1$ and $p_\alpha = p_\beta$ hold. In this case, we let $I_2 = q_\alpha(q_\alpha = q_\beta - 1)$ or $I_2 = q_\beta(q_\alpha = q_\beta + 1)$ to calculate their shared key to save node storage and reduces the network computing load. In the same way, for two heterogeneous sensor node α $(p_\alpha, q_\alpha, ID_\alpha)$ and β $(p_\beta, q_\beta, ID_\beta)$ also in two different grids, they can set up their pairwise key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$, if $\|p_\alpha - p_\beta\| = 1$ and $q_\alpha = q_\beta$ hold. Here, we let $I_2 = q_\alpha(q_\alpha = q_\beta - 1)$ or $I_2 = q_\beta(q_\alpha = q_\beta + 1)$ to calculate their shared key to save node storage and reduces the network

computing load. Therefore, we can save sensor node storage. reduce the computation load for the sensor nodes and save battery energy. As a result, this scheme enlonges the wireless sensor network lifetime.

Conclusions

The strategy in this paper combines symmetric polynomial key scheme and the key management strategy based on grids. The sensing tetrahedron is divided into a number of grids. All sensor nodes, heterogeneous sensor nodes and ordinary sensor nodes, are dispensed in the whole sensing space evenly. In each grid, all sensor nodes, heterogeneous sensor nodes and ordinary sensor nodes, establish their shared keys through using the symmetric polynomial. Simiarly, all heterogeneous sensor nodes in the whole sensing space set up their shared keys through using the symmetric polynomial. Finally, all sensor nodes, heterogeneous sensor nodes and ordinary sensor nodes, establish their shared keys directly or indirectly. Analysis shows that this scheme enhances the wireless sensor network security and the network connectivity. Moreover, this scheme saves node storage, reduces network computing load, and as a result, this scheme enlarges the wireless sensor networks lifetime.

Acknowledgements

This work was supported by the colleges and universities in Shandong province science and technology plan project number J13LN05.

References

[1] Ravinder Kaur, Kamal Preet Singh. An Efficient Multipath Dynamic Routing Protocol for Mobile WSNs. International Conference on Information and Communication Technologies(ICICT 2014), Procedia Computer Science 46(2015)1032-1040.

[2] J.Szurley, A. Bertrand, M. Moonen. Distributed adaptive node-specific signal estimation in heterogeneous and mixed-topology wireless sensor networks. Signal Processing 117(2015)44-60.

[3] Sergio F. Ochoa, Rodrigo Santos. Human-centric wireless sensor networks to improve information availability during urban search and rescue activities. Information Fusion 22(2015) 71-84.

[4] Ali Fanian, Mehdi Berenjkoub, Hossein Saidi, T. Aaron Gulliver, A high performance and intrinsically secure key establishment protocol for wireless sensor networks, Computer networks 55(2011) 1849-1863.

[5] Y.Zhou, Y. Fang, Scalable link-layer key agreement in sensor networks, in Proc. IEEE Military Commun. Conf. (MILCOM), October 2006, pp.1-6.