A Secure Scheme for Wireless Sensor Networks Based on 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; grids; symmetric polynomials.

Abstract. A security scheme for wireless sensor network based grids is given through using the symmetric polynomials. The sensing equilateral hexagon is divided into a number of sections called grids in which both ordinary sensor nodes and powerful sensor nodes are distributed evenly. All sensor nodes including the powerful sensor nodes and the ordinary sensor nodes establish their shared keys through utilizing different symmetric polynomials in each grid. All powerful sensor nodes set up their shared keys through using symmetric polynomials in whole sensing area. At last, all sensor nodes in the sensing area set up their keys directly or indirectly. Analysis demonstrates the wireless sensor network security has been improved.

Introduction

WSNs (Wireless sensor networks) consist of a lot of sensors which have manifold capacities including sensing, computing, communication and can obtain messages from the sensing area and relay the information to another sensors or a sink through a wireless transmission medium[1].

Wireless sensor networks have been researched considerably in resent several decades. Wireless sensor networks have been utilized in many fields and they provide efficient methods to obtain messages such as temperature, humidity, speed, vibration, gas concentration, etc.[2] .

Although wireless sensor networks have numerous applications including industry, agriculture, military, and so on, those sensors have some limitations such as low battery energy, limited calculation capacity, and low communication ability. Additionally, wireless sensor networks sometimes are distributed in unfriendly or even antagonistic environments. Therefore, guaranteeing wireless sensor network security is a challenging issue [3].

The key management scheme is an effective method to ensure wireless sensor network secure. Y.Zhou[4] gave a key management scheme through using the polynomials.

In the paper, we present a key management scheme based on grids for the wireless sensor networks security. This strategy partitions the equilateral hexagon which contains many concentric equilateral hexagons into various grids. All sensors, the powerful sensor nodes and the ordinary sensor nodes, are distributed in the whole sensing area evenly. In each grid, all sensor nodes including powerful sensor nodes and the ordinary sensor nodes set up their shared keys through employing the symmetric polynomials. In the same way, all powerful sensor nodes in the entire sensing area establish their common keys by using symmetric polynomials. Finally, all those sensor nodes in the entire sensing area establish their common keys directly or indirectly. Analysis and comparison demonstrate that this scheme improve the wireless sensor network security and network connectivity.

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

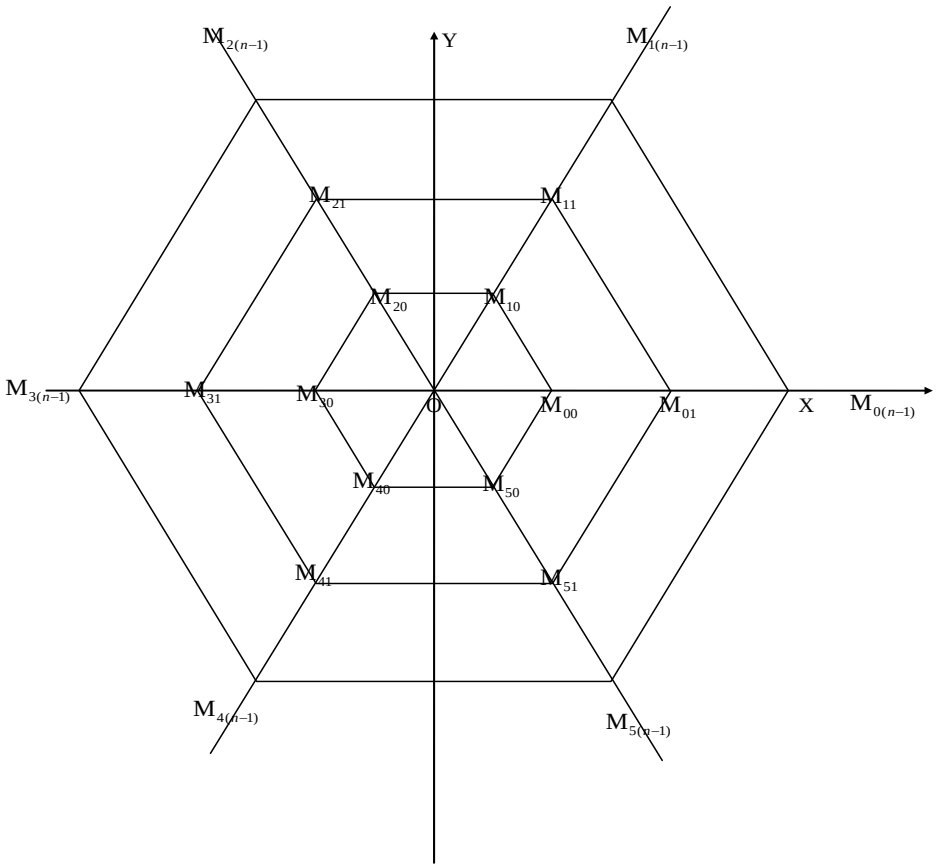

Fig. 1. The sensing equilateral hexagon

Location-based pairwise key establishment

Sensing equliateral hexagon division and sensor distribution.

In this paper, the sensing space is an equilateral hexagon denoted as S and the nodes are equally distributed in S in this scheme. The sensing equilateral hexagon in the wireless sensor networks is divided into $6\times n$ sections. In the Fig.1, there are numerous concentric equilateral hexagon and the side length of the minimum equilateral hexagon is r, the side length of the secondary minimum equilateral hexagon is $2r,\cdots$, the side length of the largest equilateral hexagon is nr. All those concentric equilateral hexagon are divided into 6 sections equally. The section $\mathrm{OM}_{00}\mathrm{M}_{10}$ is denoted as $(0,0)$, the sector $\mathrm{OM}_{10}\mathrm{M}_{20}$ is denoted as $(0,1),\cdots$, the sector $\mathrm{OM}_{50}\mathrm{M}_{00}$ is denoted as $(0,5)$, the section $\mathrm{M}_{00}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{10}$ is denoted as $(1,0)$, the section $\mathrm{M}_{10}\mathrm{M}_{11}\mathrm{M}_{21}\mathrm{M}_{20}$ is denoted as $(1,1),\cdots$, the section $\mathrm{M}_{50}\mathrm{M}_{51}\mathrm{M}_{01}\mathrm{M}_{00}$ is denoted as $(1,5)$, $\cdots$, the section $\mathrm{M}_{5(n-2)}\mathrm{M}_{5(n-1)}\mathrm{M}_{0(n-2)}\mathrm{M}_{0(n-1)}$ is denoted as $(n-1,5)$. Generally, sections are denoted as (p,q). Suppose the area of the section $\mathrm{OM}_{00}\mathrm{M}_{10}$ is $S_{0,0}$. The area $S_{1,0}$ of the $\mathrm{M}_{00}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{10}$ is $3S_{0,0}$, the area $S_{2,0}$ of the $\mathrm{M}_{01}\mathrm{M}_{02}\mathrm{M}_{12}\mathrm{M}_{11}$ is $5S_{0,0},\cdots$, the area $S_{(n-1),0}$ of the $\mathrm{M}_{0(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{1(n-2)}$ is $2(n-1)S_{0,0}$. In the same way, we can obtain those areas of other sections. Suppose α ordinary sensor nodes are distributed in section $\mathrm{OM}_{00}\mathrm{M}_{10}$. Then, 3α ordinary sensor nodes are distributed in section $\mathrm{M}_{00}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{10}$, 5α ordinary sensor nodes are distributed in section $\mathrm{M}_{01}\mathrm{M}_{02}\mathrm{M}_{12}\mathrm{M}_{11}$, $2(n-1)\alpha$ ordinary sensor nodes are distributed in section $\mathrm{M}_{0(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{1(n-2)}$.

Suppose heterogeneous sensor nodes called powerful sensor nodes which have more communication capacity, battery energy, storage memory and higher computational ability than

ordinary sensor nodes are distributed in sensing space equally and β powerful sensor nodes are distributed in sector $\mathrm{OM}_{00}\mathrm{M}_{10}$. Then, 3β powerful sensor nodes are distributed in section $\mathrm{M}_{00}\mathrm{M}_{01}\mathrm{M}_{11}\mathrm{M}_{10}$, 5β powerful sensor nodes are distributed in section $\mathrm{M}_{01}\mathrm{M}_{02}\mathrm{M}_{12}\mathrm{M}_{11}, \cdots, 2(n-1)\beta$ powerful sensor nodes are distributed in section $\mathrm{M}_{0(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{1(n-2)}$. Let all sections be grids, and in a certain grid there are ordinary senser nodes and heterogeneous sensor nodes which are denoted by a ID. All ordinary sensor nodes are denoted in the section $\mathrm{OM}_{00}\mathrm{M}_{10}$ as $1, 2, \cdots, \alpha$, next, all heterogeneous sensor nodes are denoted in the section $\mathrm{OM}_{00}\mathrm{M}_{10}$ as $\alpha+1, \alpha+2, \cdots, \alpha+\beta$. In the same way, All ordinary sensor nodes are denoted in the section $\mathrm{OM}_{10}\mathrm{M}_{20}$ as $\alpha+\beta+1, \alpha+\beta+2, \cdots, 2\alpha+\beta$, next, all heterogeneous sensor nodes are denoted in the section $\mathrm{OM}_{10}\mathrm{M}_{20}$ 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 $\mathrm{M}_{0(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{1(n-2)}$ as $(6n^2-2n+1)(\alpha+\beta)+1, (6n^2-2n+1)(\alpha+\beta)+2, \cdots,$ $(6n^2-2n+1)(\alpha+\beta)+(2n-1)\alpha$,next, all heterogeneous sensor nodes are denoted in the section $\mathrm{M}_{0(n-2)}\mathrm{M}_{0(n-1)}\mathrm{M}_{1(n-1)}\mathrm{M}_{1(n-2)}$ as $(6n^2-2n+1)(\alpha+\beta)+(2n-1)\alpha+1, (6n^2-2n+1)(\alpha+\beta)+$ $(2n-1)\alpha+2, \cdots, 6n^2(\alpha+\beta)$.

Pairwise key establishment among sensors in a section.

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[4]

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

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, the $p = I_1, q = I_2, \mathrm{ID} = I_3$, 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 IDs.

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 $f_u(ID_v)$, and 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 in one certain grid can establish their shared keys.

Pairwise key establishment among all sensor nodes in whole sensing area.

Two powerful sensor node α ($p_\alpha, q_\alpha, ID_\alpha$) and β ($p_\beta, q_\beta, ID_\beta$) locate in two different sections. They can set up their pairwise key if $\|q_\alpha - q_\beta\|$ =1 and $p_\alpha = p_\beta$ hold. In this case, let $I_1 = p_\alpha = p_\beta$, $I_2 = q_\alpha (q_\alpha = q_\beta - 1)$ or $I_2 = q_\beta (q_\alpha = q_\beta + 1)$, and, clearly, $ID_\alpha \neq ID_\beta$. Similarly, a t -degree polynomial defined as 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 between powerful sensor node α and powerful sensor β , node α takes ID_β as the input and computes $f_\alpha(ID_\beta)$, and node β takes ID_α as the input and computes $f_\beta(ID_\alpha)$. Due to the polynomial symmetry, both powerful nodes compute the same shared key. In general, two powerful sensors α and β , where $\|q_\alpha - q_\beta\| = 1$, can establish shared key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$.

Similarly, for the other case, two powerful sensor node α ($p_\alpha, q_\alpha, ID_\alpha$) and β ($p_\beta, q_\beta, ID_\beta$) locate in two different sections. They can set up their pairwise key if $\|p_\alpha - p_\beta\|$ =1 and $q_\alpha = q_\beta$ hold. In this case, let $I_1 = q_\alpha = q_\beta$, $I_2 = p_\alpha (p_\alpha = p_\beta - 1)$ or $I_2 = p_\beta (p_\alpha = p_\beta + 1)$, and, clearly, $ID_\alpha \neq ID_\beta$. Similarly, a t -degree 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 between powerful sensor node α and powerful sensor β , node α takes ID_β as the input and computes $f_\alpha(ID_\beta)$, and node β takes ID_α as the input and computes $f_\beta(ID_\alpha)$. Due to the polynomial symmetry, both powerful nodes compute the same shared key. In general, two powerful sensors α and β , where $\|p_\alpha - p_\beta\| = 1$, can establish shared key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$.

A powerful sensor node can establish common keys with those powerful sensor nodes which locate in sections close to the section the powerful sensor node locates in. It is clear that two powerful sensor nodes can set up their common keys by using intermediate powerful sensor nodes. Therfore, a powerful node can establish common keys with all the powerful sensor nodes in whole sensing area directly or indirectly. In a section, a powerful sensor node can set up common keys with all sensor nodes including ordinary sensor nodes and powerful sensor nodes. Therefore, an ordinary sensor node can establish common keys with those powerful sensor nodes which locate in different sections with the help of the powerful sensor nodes which locate in the same section. Next, the ordinary sensor node can set up common keys with those ordinary sensor nodes which locate in different sections with the help of the powerful sensor nodes which locate in the same section and which locate in those different sections. Therefore, all sensor nodes including ordinary sensor nodes and powerful sensor nodes can establish their common keys with other sensor nodes directly or indirectly.

Performance analysis for WSNs

Security analysis for WSNs.

In a section, two sensor nodes share common key $k_{uv} = f_u(ID_v) = f_v(ID_u)$. From the polynomial employed, 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 powerful sensor nodes which locate in two close sections have

common key $k_{\alpha\beta} = f_\alpha(ID_\beta) = f_\beta(ID_\alpha)$. From the polynomial employed, 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 section, and the enemy can not get all keys of the powerful sensor nodes in this section because the powerful 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 powerful 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 powerful sensor nodes in other sections because different keys among sensor nodes in different sections are different. From above discussion, this scheme has improved 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 secure communication keys with its neighbor noders including ordinary sensor nodes and heterogeneous sensor nodes and then it can set up secure 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 which locate between the node $u\ (p_u, q_u, ID_u)$ and those nodes. Therefore, this scheme can ensure all sensor nodes, ordinary sensor nodes and heterogeneous sensor nodes, are connected safely in the whole sensing area. The node can still communicate with other nodes safely even though some or total of its neighbor ordinary nodes are captured by the enemy becouse it set up secure link with the heterogeneous node in the same section directly and it set up secure links with other heterogeneous nodes in the different sections indirectly. 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 $\alpha\ (p_\alpha, q_\alpha, ID_\alpha)$ and $\beta\ (p_\beta, q_\beta, ID_\beta)$ 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 $\beta\ (p_\beta, q_\beta, ID_\beta)$ 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.

Conclusion

The scheme in this paper combines symmetric polynomial key scheme and the key management strategy based on grids. The sensing equilateral hexagon is divided into a number of grids. All sensor nodes including powerful sensor nodes and ordinary sensor nodes are distributed in the whole sensing area evenly. In each grid, all sensor nodes including powerful sensor nodes and ordinary sensor nodes

establish their common keys through using the symmetric polynomial. Similarly, all powerful sensor nodes in the whole sensing area set up their shared keys through using the symmetric polynomial. At last, all sensor nodes including powerful sensor nodes and ordinary sensor nodes establish their shared keys directly or indirectly. Annalysis shows that this scheme improves the wireless sensor network security.

Acknowledgements

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

References

[1] Amir S. Elsafrawey, Emad S. Hassan, Moawad I. Dessouky. Cooperative hybrid self-healing scheme for secure and data reliability in unattended wireless sensor networks. IET Inf. Secur., 2015, Vol.9, Iss. 4, pp.223-233.

[2] Bochao Zhou, Shuo Yang, Tong Sun, and Kenneth T.V.Grattan. A Novel Wireless Mobile Platform to Locate and Gather Data From Optical Fiber Sensors Integrated Into a WSN. IEEE SENSORS JOURNAL, VOL.15,NO.6,JUNE 2015, pp3615-3621.

[3] Swapna Naik, Dr Narendra Shekokar. Conservation of energy in wireless sensor network by preventing denial of sleep attack. International Conference on Advanced Computing Technologies and Applications, 45(2015) 370-379.

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

[5] 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.