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

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: Security; grids; symmetric polynomials.

Abstract: A scheme for WSNs(wireless sensor networks) security is given by dividing sensing circle into sections and using the symmetric polynomials in this paper. Ordinary sensor nodes and heterogeneous sensor nodes are distributed in the circle equally. The keys among sensor nodes are established by utilizing symmetric polynomials. Analysis and comparison demonstrate this scheme enhances the WSN security.

Introduction

A lot of sensors that are connected through a wireless transmission medium compose wireless sensor networks. In wireless sensor networks, sensors have limited resources, including limited memory, limited calculating capacity, lower communication power, and so on. Even so, wireless sensor networks have various applications in industry, agriculture, traffic, buildings and so on. In many cases, wireless sensor networks are distributed in unfriendly, even antagonistic surroundings. Therefore, wireless sensor networks are easily exposed to various malicious attacks, and in the same time, wireless sensor networks are limited ability to defense those assaults [1].

Ensuring the wireless sensor networks secure is a valuable and difficult issue. Liu D and Ning[2] gave a common frame for polynomial pool-based pairwise key predistribution and two possible key predistribution schemes, namely, random subset assignment and grid-based schemes. [3], which is an improved version of the [2], employed a pool consisting of multiple random bivariate polynomials. [3] enhanced the scalability and security of WSNs compared with [2].

This paper presents a key management strategy based on symmetric polynomials. Analysis and comparison show that this scheme enhances the resilience of WSNs. The rest of this paper is organized as follows. In section two, pairwise key establishment is given. Performance analysis for WSNs is given in the section three. The conclusion of this paper is in section four.

Location-based pairwise key establishment

Sensing circle division and sensor distribution

In this paper, the sensing area is a circle denoted as S and the nodes are equally distributed in S. The sensing circle in the wireless sensor networks is divided into $m\times n$ sections. In the Fig.1, there are numerous concentric circles and the radius of the minimum circle is r, the radius of the secondary minimum circle is $2r$, $\llcorner$, the radius of the largest circle is nr. All those concentric circles are divided into m sectors equally. The sector $OM_{00}M_{10}$ is denoted as $(0,0)$, the sector $OM_{10}M_{20}$ is denoted as $(0,1)$, $\llcorner$, the sector $OM_{(m-1)0}M_{00}$ is denoted as $(0,m-1)$, the section $M_{00}M_{01}M_{11}M_{10}$ is denoted as $(1,0)$, the section $M_{10}M_{11}M_{21}M_{20}$ is denoted as $(1,1)$, $\llcorner$, the section $M_{(m-1)0}M_{(m-1)1}M_{01}M_{00}$ is denoted as $(1,m-1)$, $\llcorner$, and the section $M_{(m-1)(n-2)}M_{(m-1)(n-1)}M_{0(n-2)}M_{0(n-1)}$ is denoted as $(n-1,m-1)$. Generally, sections are denoted as (p,q). Suppose the area of the sector $OM_{00}M_{10}$ is $S_{0,0}$. The area $S_{1,0}$ of the $M_{00}M_{01}M_{11}M_{10}$ is $3S_{0,0}$, the area $S_{2,0}$ of the $M_{01}M_{02}M_{12}M_{11}$ is

$5S_{0,0}$, ⋯, the area $S_{(n-1),0}$ of the $M_{0(n-2)}M_{0(n-1)}M_{1(n-1)}M_{1(n-2)}$ is $(2n-1)S_{0,0}$. In the same way, we can obtain those areas of other sectors and sections.

Suppose a ordinary sensor nodes are distributed in sector $OM_{00}M_{10}$. Then, $3a$ ordinary sensor nodes are distributed in section $M_{00}M_{01}M_{11}M_{10}$, $5a$ ordinary sensor nodes are distributed in section $M_{01}M_{02}M_{12}M_{11}$, ⋯, and $(2n-1)a$ ordinary sensor nodes are distributed in section $M_{0(n-2)}M_{0(n-1)}M_{1(n-1)}M_{1(n-2)}$. Suppose heterogeneous 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 suppose b heterogeneous sensor nodes are distributed in sector $OM_{00}M_{10}$. Then, $3b$ heterogeneous sensor nodes are distributed in section $M_{00}M_{01}M_{11}M_{10}$, $5b$ heterogeneous sensor nodes are distributed in section $M_{01}M_{02}M_{12}M_{11}$, $(2n-1)b$ heterogeneous sensor nodes are distributed in section $M_{0(n-2)}M_{0(n-1)}M_{1(n-1)}M_{1(n-2)}$. Let all sectors and 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 sector $OM_{00}M_{10}$ as $1, 2, \cdots, a$, next, all heterogeneous sensor nodes are

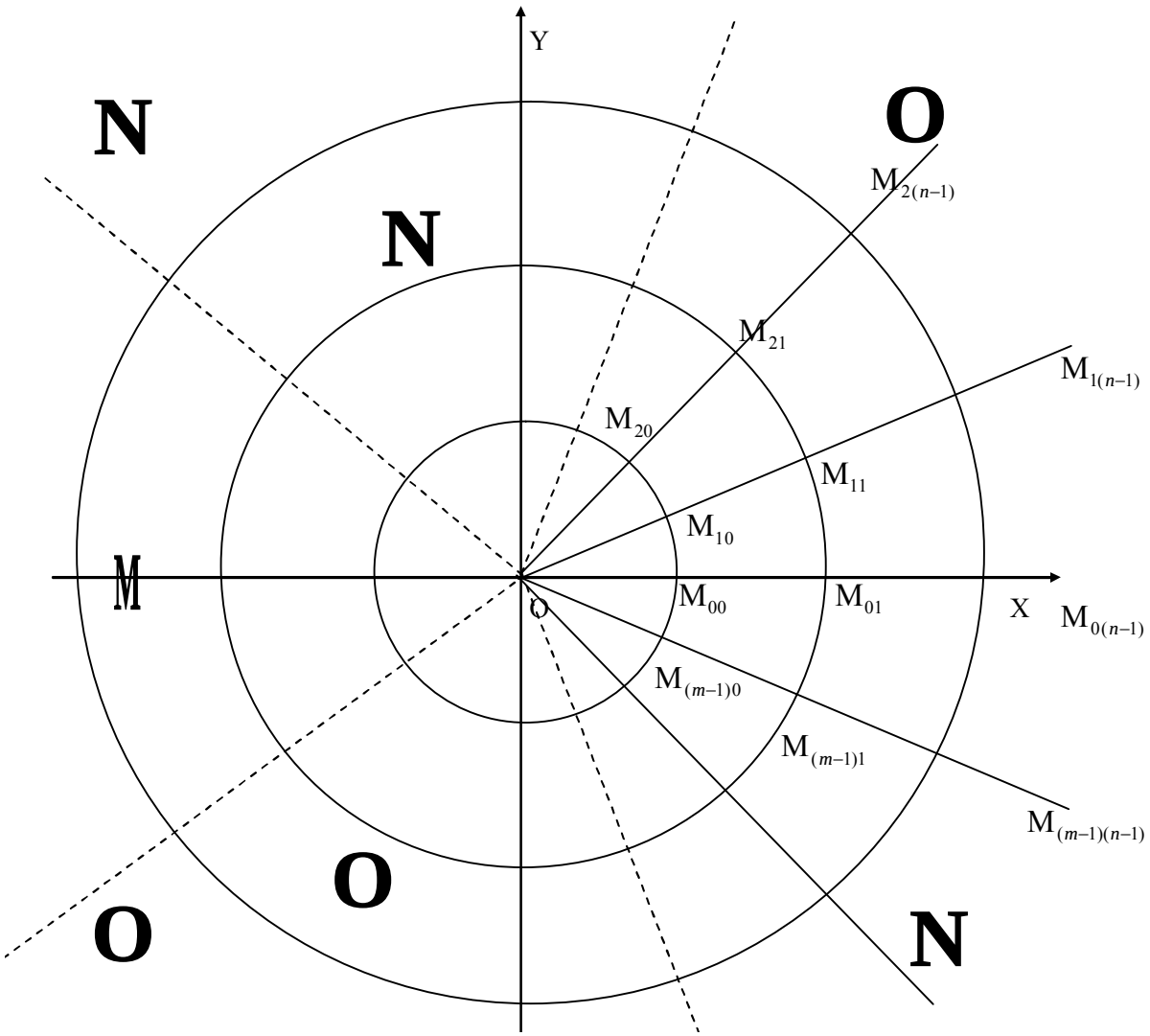

Fig. 1 The sensing circle

denoted in the sector $OM_{00}M_{10}$ as $a+1, a+2, \mathbf{L}, a+b$. In the same way, all ordinary sensor nodes are denoted in the sector $OM_{10}M_{20}$ as $a+b+1, a+b+2, \mathbf{L}, 2a+b$, next, all heterogeneous sensor nodes are denoted in the sector $OM_{10}M_{20}$ as $2a+b+1, 2a+b+2, \mathbf{L}, 2a+2b$. At last, all ordinary sensor nodes are denoted in the section $M_{0(n-2)}M_{0(n-1)}M_{(m-1)(n-1)}M_{(m-1)(n-2)}$ as $(mn^2-2n+1)(a+b)+1, (mn^2-2n+1)(a+b)+2, \mathbf{L}, (mn^2-2n+1)(a+b)+(2n-1)a$, next, all heterogeneous sensor nodes are denoted in the section $M_{0(n-2)}M_{0(n-1)}M_{(m-1)(n-1)}M_{(m-1)(n-2)}$ as $(mn^2-2n+1)(a+b)+(2n-1)a+1, (mn^2-2n+1)(a+b)+(2n-1)a+2, \mathbf{L}, mn^2(a+b)$.

Pairwise key establishment

A polynomial[4] is established as the following

$$f(x_1, x_2, \mathbf{L}, x_{K+1}) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\mathbf{L}\sum_{i_{K+1}=0}^{t} a_{i_1,i_2,\mathbf{L}i_K,i_{K+1}} \times x_1^{i_1} x_2^{i_2} \mathbf{L}\, x_K^{i_K} x_{K+1}^{i_{K+1}} \tag{1}$$

Where $f(x_1, x_2, \mathbf{L}, x_{K+1})$ is a symmetric polynomial and all coefficients of $f(x_1, x_2, \mathbf{L}, x_{K+1})$ are selected from a F_q(where q is a prime integer) which is a finite field. Therefore, we can obtain the equation as follows

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

where ∂ means a permutation. All sensors, that utilize the protocol based on $f(x_1, x_2, \mathbf{L}, x_{K+1})$ protocol, get k credentials , $(I_1, I_2, \mathbf{L}\, I_K)$, from the key management centre, and these credentials are stored in memory. Through utilizing the polynomial $f(x_1, x_2, \mathbf{L}, x_{K+1})$ and those credentials, $(I_1, I_2, \mathbf{L}\, I_K)$, The centre can calculate the polynomial shares. As the polynomial share, the coefficients b_i are stored in sensor memory, and those b_i are calculated as the following

$$f_u(x_{K+1}) = f(I_1, I_2, \mathbf{L}, I_K, x_{K+1}) = \sum_{i=0}^{t} b_i x_{K+1}^i \tag{3}$$

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 ID values.

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-variate polynomial is defined as follows

$$f(x_1, x_2, x_3) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\sum_{i_3=0}^{t} a_{i_1,i_2,i_3} \times x_1^{i_1} x_2^{i_2} x_3^{i_3} \tag{4}$$

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 $f_v(ID_u)$ through utilizing equation (4). 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 $k_{uv} = f_u(ID_v) = f_v(ID_u)$. Therefore, all sensor nodes both ordinary sensor nodes and heterogeneous sensor nodes in one certain grid can establish their shared keys.

Let $OM_{00}M_{10}$ be denoted as $M_{0(-1)}M_{00}M_{10}M_{1(-1)}$, ⊥ , $OM_{(m-2)0}M_{(m-1)0}$ be denoted as $M_{(m-2)(-1)}M_{(m-2)0}M_{(m-1)0}M_{(m-1)(-1)}$, $OM_{(m-1)0}M_{00}$ be denoted as $M_{(m-1)(-1)}M_{(m-1)0}M_{00}M_{0(-1)}$. Without loss of generality, heterogeneous nodes not in the same grid but in the same concentric ring, for example, section $M_{m_1(n'-1)}M_{m_1n'}M_{(m_1+1)n'}M_{(m_1+1)(n'-1)}$ ($0 \le m_1 \le m-1$, $0 \le n' \le n-1$)and section $M_{m_2(n'-1)}M_{m_2n'}M_{(m_2+1)n'}M_{(m_2+1)(n'-1)}$ ($0 \le m_2 \le m-1$, $0 \le n' \le n-1$), can establish their shared key. If $m_2 - m_1 = 1$, those sections are close and mod $(2n'+1)(a+b)$ is utilized,where $0 \le n' \le n-1$. A certain heterogeneous sensor node h in section $M_{m_1(n'-1)}M_{m_1n'}M_{(m_1+1)n'}M_{(m_1+1)(n'-1)}$ can find the unique heterogeneous sensor node m in the section $M_{m_2(n'-1)}M_{m_2n'}M_{(m_2+1)n'}M_{(m_2+1)(n'-1)}$ whose IDs are equal. Then , the identities of nodes h and m are (p_h, q_h, ID_h) and (p_m, q_m, ID_m) respectively , where $p_h = p_m, q_h \ne q_m, ID_h = ID_m$. In this case, a t-degree 3-variate polynomial is defined as follows

$$f(x_1, x_2, x_3) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\sum_{i_3=0}^{t} a_{i_1,i_2,i_3} \times x_1^{i_1} x_2^{i_2} x_3^{i_3} \tag{5}$$

In order to compute a shared key, node h takes q_m as the input and computes $f_h(q_m)$ and node m takes q_h as the input and computes $f_m(q_h)$ through using the equation (5). Due to the polynomial symmetry, both nodes compute the same shared key. Generally, two heterogeneous sensors h and m in the same ring can establish shared key $k_{hm} = f_h(q_m) = f_m(q_h)$.

In the same way, if $m_2 - m_1 = g (2 \le g \le m-1)$, those sections are not close and mod $g(2n'+1)(a+b)$ are utilized, where $0 \le n' \le n-1$, A cetain heterogeneous sensor nodes in section $M_{m_1(n'-1)}M_{m_1n'}M_{(m_1+1)n'}M_{(m_1+1)(n'-1)}$ can establish shared key with an unique heterogeneous sensor node in section $M_{m_2(n'-1)}M_{m_2n'}M_{(m_2+1)n'}M_{(m_2+1)(n'-1)}$.

So, we can obtain that all hetereogeneous sensor nodes not in the same grid but in the same concentric ring can establish their shared keys.

Without loss of generality, heterogeneous nodes not in the same grid but in the same sector, section $M_{m'(n_1-1)}M_{m'n_1}M_{(m'+1)n_1}M_{(m'+1)(n_1-1)}$ ($0 \le n_1 \le n-2$, $0 \le m' \le m-1$)and section $M_{m'(n_2-1)}M_{m'n_2}M_{(m'+1)n_2}M_{(m'+1)(n_2-1)}$ ($1 \le n_2 \le n-1$, $0 \le m' \le m-1$), can establish their shared key. If $n_2 - n_1 = 1$, those sections are close and mod $m(2n_1+1)(a+b)$ is utilized, where $0 \le n_1 \le n-2$. A certain heterogeneous sensor node h in section $M_{m'(n_1-1)}M_{m'n_1}M_{(m'+1)n_1}M_{(m'+1)(n_1-1)}$ can find the unique heterogeneous sensor node m in the section $M_{m'(n_2-1)}M_{m'n_2}M_{(m'+1)n_2}M_{(m'+1)(n_2-1)}$ whose IDs are equal. Then , the identities of nodes h and m are (p_h, q_h, ID_h) and (p_m, q_m, ID_m) respectively , where $p_h \ne p_m, q_h = q_m, ID_h = ID_m$. In this case, a t-degree 3-variate polynomial is defined as follows

$$f(x_1, x_2, x_3) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\sum_{i_3=0}^{t} a_{i_1,i_2,i_3} \times x_1^{i_1} x_2^{i_2} x_3^{i_3} \tag{6}$$

In order to compute a shared key, node h takes p_m as the input and computes $f_h(p_m)$ and node m takes p_h as the input and computes $f_m(p_h)$ through employing the equation (6). Due to the polynomial symmetry, both nodes compute the same shared key. Generally, two sensors h and m not in the same grid but in the same sector can establish shared key $k_{hm} = f_h(p_m) = f_m(p_h)$.

In the same way, if $n_2 - n_1 = g\,(2 \le g \le n-1)$, those sections are not close and mod $m(a+b)\{[2(n_1+0)+1]+[2(n_1+1)+1]+\mathbf{L}+2[n_1+(g-1)]+1\}$ is utilized, A cetain heterogeneous sensor nodes in section $\mathrm{M}_{m_1(n'-1)}\mathrm{M}_{m_1n'}\mathrm{M}_{(m_1+1)n'}\mathrm{M}_{(m_1+1)(n'-1)}$ can establish shared key with an unique heterogeneous sensor node in section $\mathrm{M}_{m_2(n'-1)}\mathrm{M}_{m_2n'}\mathrm{M}_{(m_2+1)n'}\mathrm{M}_{(m_2+1)(n'-1)}$.

Therefore, we can obtain that all hetereogeneous sensor nodes not in the same grid but in the same sector or in the same concentric circles can establish their shared keys. Additionaly, all ordinary sensors and hetereogeneous sensors in a certain grid can set up secure keys. So, all ordinary sensor nodes and hetereogenous sensor nodes in whole sensing circle can establish their shared keys.

Security analysis for WSNs

In one certain cell, any two sensor nodes, including ordinary sensors and hetereogenous sensors, share common key. From the polynomial employed, it is more difficult to compromise the key in this paper than in the paper [5]. Moreover, if a sensor is compromised in a certain grid, it can not reveal any information of sensors in other grids. Therefore, this scheme is more secure than those which do not employ grid methods. Those hetereogeneous sensors have more than one keys by which they establish secure connection. So, in order to enhance the WSNs security, through using those keys this strategy can obtain more complex keys. Those hetereogeneous sensors set up their secure connection by utilizing those more complex keys.

Conclusion

The sensing circle consists of a number of sections. The ordinary sensor nodes and hetereogeneous sensor nodes are distributed and establish their pairwise keys by using symmetric polynomial. This scheme is resilient to compromised node attack, and has good 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] Yuquan Zhang. A Secure Scheme for Heterogeneous Wireless Sensor Networks[J], Journal of Theoretical and Applied Information Technology, 2013(48):570-576.

[2] D. Liu, P. Ning. “Establishing pairwise keys in distributed sensor networks”, In: Proceedings of 10th ACM conference on computer and communications security (CCS03). Washington, DC: ACM Press, pp.41-47, (2003).

[3] Liu D, Ning P. “Improving key pre-distribution with deployment knowledge in static sensor networks”, ACM Transactions on Sensor Networks 2005, 1(2):204-239, (200).

[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] R. Blundo, D. Suntisa, A. Herzbeg, et al. Perfectly secure key distrbution for dynamic conferences, Proc. of the 12th Annual International Cryptology Conference on Advances in Cryptology, Springer-Verlag,1992:471-486.