A Secure Scheme for Cluster-based Wireless Sensor Networks Based on 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: Wireless sensor network; security; clustering; symmetric polynomials

Abstract: A scheme for WSNs(wireless sensor networks) security is given by dividing sensing multi-dimension hypercube into clusters and using the symmetric polynomials in this paper. The multi-dimension sensing hypercube is divided into a number of small same dimension hypercubes called cells, some of which are comprised of a cluster called logical group. The common keys among sensor nodes are established by utilizing symmetric polynomials. Analysis and comparison demonstrate this scheme enhances the WSNs security, and has good network connectivity.

1 Introduction

The wireless sensor network has caught attention for its various application fields, including health monitoring, habitat monitoring, battle field and so on[1]. However, in those applications, WSNs are prone to be attacked for sensors that consist of WSNs have limited communication ability, low calculation, and son on, and they are distributed in hostile environments[2]. Therefore, to assure WSNs secure is an of importance issue.

Yuquan[3] gave a secure strategy in which the sensing hypercube is divided into many cells. Through utilizing symmetric polynomials[4], Ali Fanian et al[5] gave a secure key establishment strategy which ensures WSNs security.

In this paper, we present a dynamic key management strategy. We divide the sensing space into numerous small sections through using the ideas of paper [3], and then set up common keys between each pair of sensors. Analysis demonstrates this strategy improves the WSN resilience and 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.

2 Location-based pairwise key establishment

2.1 Sensing hypercube division and sensor distribution

In this paper, the sensing space is a n_d dimension, $D_1, D_2, \cdots, D_{n_d-1}$, and D_{n_d}, hypercube denoted as V_{hc} and the nodes are equally distributed in V_{hc} in this scheme. The sensing hypercube V_{hc} in the wireless sensor networks is divided into m same hypercube cells, denoted as $C'_{00\cdots00}$, $C'_{00\cdots01}$, $\cdots$, $C'_{00\cdots0D_1}$, $\cdots$, $C'_{00\cdots0(\sqrt[n_d]{m}-2)}$, $C'_{00\cdots0(\sqrt[n_d]{m}-1)}$, $C'_{00\cdots10}$, $C'_{00\cdots11}$, $\cdots$, $C'_{00\cdots1D_1}$, $\cdots$, $C'_{00\cdots1(\sqrt[n_d]{m}-2)}$, $C'_{00\cdots1(\sqrt[n_d]{m}-1)}$, $\cdots$, $C'_{00\cdots D_2 0}$, $C'_{00\cdots D_2 1}$, $\cdots$, $C'_{00\cdots D_2 D_1}$, $\cdots$, $C'_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $C'_{00\cdots D_2(\sqrt[n_d]{m}-1)}$, $\cdots$, $C'_{00\cdots(\sqrt[n_d]{m}-1)0}$, $C'_{00\cdots(\sqrt[n_d]{m}-1)1}$, $\cdots$, $C'_{00\cdots(\sqrt[n_d]{m}-1)D_1}$, $\cdots$, $C'_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-2)}$, $C'_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $C'_{0(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$,

$C'_{(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$. Where, $D_1 = 0,1,\cdots, \left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $\cdots$, $D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$ and $D_{n_d} = 0,1, \cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, according to their geographical locations. All those cells are denoted as $c = 1,2,\cdots 2^{\sqrt[n_d]{m}-1}$ one by one. Prior to the deployment, the key setup server forms the logical groups and then distributes a bit cluster group to each of them.

There are $\left(\sqrt[n_d]{m}-1\right)^{n_d}$ logical groups denoted as $G_{00\cdots00}$, $G_{00\cdots01}$, $\cdots$, $G_{00\cdots0D_1}$, $\cdots$, $G_{00\cdots0(\sqrt[n_d]{m}-3)}$, $G_{00\cdots0(\sqrt[n_d]{m}-2)}$, $G_{00\cdots10}$, $G_{00\cdots11}$, $\cdots$, $G_{00\cdots1D_1}$, $\cdots$, $G_{00\cdots1(\sqrt[n_d]{m}-3)}$, $G_{00\cdots1(\sqrt[n_d]{m}-2)}$, $\cdots$, $G_{00\cdots D_2 0}$, $G_{00\cdots D_2 1}$, $\cdots$, $G_{00\cdots D_2 D_1}$, $\cdots$, $G_{00\cdots D_2(\sqrt[n_d]{m}-3)}$, $G_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $\cdots$, $G_{00\cdots(\sqrt[n_d]{m}-2)0}$, $G_{00\cdots(\sqrt[n_d]{m}-2)1}$, $\cdots$, $G_{00\cdots(\sqrt[n_d]{m}-2)D_1}$, $\cdots$, $G_{00\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-3)}$, $G_{00\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$, $\cdots$, $G_{0(\sqrt[n_d]{m}-2)\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$, $\cdots$, $G_{(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$. Where, $D_1 = 0,1,\cdots, \left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, $\cdots$, $D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right)$, $\left(\sqrt[n_d]{m}-2\right)$ and $D_{n_d} = 0,1, \cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, each of which consists of 2^{n_d} cells. All those logical groups are denoted as $g = 1,2,\cdots 2^{\sqrt[n_d]{m}-2}$ in turn.

There are N sensor nodes in the sensing hypercube V_{hc}. Those nodes are divided into m same groups denoted as $C_{00\cdots00}$, $C_{00\cdots01}$, $\cdots$, $C_{00\cdots0D_1}$, $\cdots$, $C_{00\cdots0(\sqrt[n_d]{m}-2)}$, $C_{00\cdots0(\sqrt[n_d]{m}-1)}$, $C_{00\cdots10}$, $C_{00\cdots11}$, $\cdots$, $C_{00\cdots1D_1}$, $\cdots$, $C_{00\cdots1(\sqrt[n_d]{m}-2)}$, $C_{00\cdots1(\sqrt[n_d]{m}-1)}$, $\cdots$, $C_{00\cdots D_2 0}$, $C_{00\cdots D_2 1}$, $\cdots$, $C_{00\cdots D_2 D_1}$, $\cdots$, $C_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $C_{00\cdots D_2(\sqrt[n_d]{m}-1)}$, $\cdots$, $C_{00\cdots(\sqrt[n_d]{m}-1)0}$, $C_{00\cdots(\sqrt[n_d]{m}-1)1}$, $\cdots$, $C_{00\cdots(\sqrt[n_d]{m}-1)D_1}$, $\cdots$, $C_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-2)}$, $C_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $C_{0(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $C'_{(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$. Where, $D_1 = 0,1,\cdots, \left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $\cdots, D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$ and $D_{n_d} = 0,1, \cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$. The sensor nodes in group $C'_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$ are deployed in cell $C_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$. All those sensor nodes are denoted as $n = 1,2,\cdots N$.

2.2 Key establishment based on symmetric polynomials

Paper [4] set up a polynomial as the following

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

Where all coefficients of $f(x_1,x_2,\cdots,x_{K+1})$ which is a symmetric polynomial are selected from a F_q (where q is a prime integer). Therefore, we get the equation as the following

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

Where ∂ is a permutation. All sensor nodes in WSNs, which employ the protocol based on $f(x_1,x_2,\cdots,x_{K+1})$, get k credentials, $(I_1,I_2,\cdots I_K)$, from the key center, and they are kept in memory. The center calculates the polynomial shares through using the $f(x_1,x_2,\cdots,x_{K+1})$ and $(I_1,I_2,\cdots I_K)$. As the polynomial share, the b_i are kept in sensor memory, and they are figured as the following

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

In this paper, the $c = I_1, g = I_2, n = I_3$, every pair of nodes with only one mismatch in their identities can establish a shared key. Obviously, two sensors in one certain cell have the same values of c and g and they have different values of n. In the same way, two sensors in one certain cell but not in one logical group have the same values of g and they have different values of c and n.

Suppose the identities of nodes u and v in one certain cell $C'_{D_{n_d} D_{n_d-1} \cdots D_2 D_1}$ ($D_1, D_2, \cdots, D_{n_d}, D_{n_{d-1}} = 0,1,\cdots,\left(\sqrt[n_d]{m} - 2\right),\left(\sqrt[n_d]{m} - 1\right)$) are (c_u, g_u, n_u) and (c_v, g_v, n_v) respectively. It is clear that $c_u = c_v, g_u = g_v, n_u \neq n_v$. 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 n_v as the input and computes $f_u^c(n_v)$, and node v takes n_u as the input and computes $f_v^c(n_u)$. Due to the polynomial symmetry, both nodes compute the same shared key. Generally, two sensors u and v in the same cell can establish shared key $k_{uv}^c = f_u^c(n_v) = f_v^c(n_u)$. So, all sensor nodes in one certain cell can establish their shared keys.

Similarly, suppose the identities of nodes u and v not in one certain cell $C'_{D_{n_d} D_{n_d-1} \cdots D_2 D_1}$ ($D_1, D_2, \cdots, D_{n_d}, D_{n_{d-1}} = 0,1,\cdots,\left(\sqrt[n_d]{m} - 2\right),\left(\sqrt[n_d]{m} - 1\right)$) but in one certain logical group $G_{D_{n_d} D_{n_d-1} \cdots D_2 D_1}$ ($D_1, D_2, \cdots, D_{n_d}, D_{n_{d-1}} = 0,1,\cdots,\left(\sqrt[n_d]{m} - 3\right),\left(\sqrt[n_d]{m} - 2\right)$) are (g_u, n_u) and (g_v, n_v) respectively. It is clear that $g_u = g_v, n_u \neq n_v$. In this case, a t-degree (2+1)-variate polynomial defined as follows

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

is utilized. In order to compute a shared key, node u takes n_v as the input and computes $f_u^g(n_v)$, and node v takes n_u as the input and computes $f_v^g(n_u)$. Due to the polynomial symmetry, both nodes compute the same shared key. Generally, two sensors u and v in the same logical group but not in the same cell can establish shared key $k_{uv}^g = f_u^g(n_v) = f_v^g(n_u)$. So, all sensor nodes in the same logical group but not in the same cell can establish their shared keys.

Suppose that sensor node u and v are in different logical groups. From section 2, any two close logical groups have one common cell. In general, there is a sensor node w (c_w, g_w, n_w) which is not only in one logical group with node u but also in the other logical group with node v. So, the shared key between node u and w is $k_{uw}^g = f_u^g(n_w) = f_w^g(n_u)$ and the shared key between node v and w is $k_{vw}^g = f_v^g(n_w) = f_w^g(n_v)$. We can obtain the shared key between node u and v as follows

$$k_{uv} = k_{uw}^g \,||\, k_{vw}^g .$$

3 Security analysis for WSNs

In one certain cell, any two sensor nodes share common key k^c and in one certain logical group any sensor nodes have shared key k^g. From the polynomial employed, it is more difficult to compromise the k^c in this paper than in the paper [4]. Moreover, any two nodes have common key

k^g, so, the scheme in this paper is more secure than that in paper [4]. If k^c of one sensor node is compromised, the enemy only obtains those keys of other nodes in the same cell and it can not get the keys of other nodes in the same logical group. Similarly, if k^g of one sensor node is compromised, the enemy only obtains those keys of other nodes in the same logical group and it can not get the keys of other nodes in the same cell.

4 Conclusion

The scheme in this paper combines symmetric polynomial key scheme and the key management strategy based on cells and logical groups. The sensing hypercube is divided into a number of cells and logical groups with same dimension. The sensor nodes are distributed in the sensing space and establish their pairwise keys by using symmetric polynomial. This scheme is resilient to compromised node attacks, and has good network connectivity.

References

[1] Saru Kumari, et al. User authentication schemes for wireless sensor networks:A review. Ad Hoc Networks 27(2015) 159-194.

[2] Honglong Chen, Wei Lou, Zhi Wang, Junfeng Wu, Zhibo Wang. Securing DV-Hop locatization against wormhole attacks in wireless sensor networks. Pervasive and Mobile Computing 16(2015)22-35.

[3] Yuquan Zhang. A secure based on multi-dimension location for wireless sensor networks. WIT Transaction on Information and Communication Technology, 2014, Vol. 51, pp697-711.

[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, et al. A high performance and intrinsically secure key establishment protocol for wireless sensor networks. Computer networks, 55(2011) 1849-1863.