A Scalable Key Scheme for Multi-Dimension 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: Wireless sensor network; security; multi-dimension

Abstract: A key management strategy based on cluster is given to guarantee wireless sensor networks secure. The sensing hypercube is divided into numerous the same small hypercubes with the same dimension with the sensing hypercube. Those small hypercubes are called as cells and 2^n cells consist of a cluster, where, n is the dimension. The wireless sensor network is a one-layer structure and consists of a lot of the same sensor nodes. Those sensors establish their shared keys through utilizing the idea of the unital-based scheme, and then all sensors can set up their secure connection and paths. Analysis shows that this strategy can guarantee the WSNs security, improves the network connectivity, has good scalability, and has lower storage requirement.

1 Introduction

Wireless sensor networks have been researched for many years and they are utilized in numerous fields including agriculture, industry, military and so on[1]. However, wireless sensor networks are easily attacked because they are usually dispensed in unfriendly, or even hostile environments and because sensors have limited capacity for communication, computation, storage and so on[2]. Therefore, how to guarantee wireless sensor networks secure is an important and difficult task. Zhang[3] presented a secure scheme in which the sensing hypercube consist of clusters each of which comprises many cells. In paper [4], the unital design is a Steiner 2-design and it contains $b = m^2(m^3+1)/(m+1) = m^2(m^2-m+1)$ blocks of a set of $v = m^3+1$ points. Each one consists of $m+1$ points, which is included in $r = m^2$ blocks. Every pair of points is exactly included in one block simultaneously. Through employing the idea in the [4], Walid Bechkit et al[5] gave a key management strategy to guarantee a safe coverage for large WSNs.

In the paper, we present a dynamic key management strategy based on n_d-dimension sensing hypercube for the wireless sensor networks security. This scheme divides sensing multi-dimension hypercube into the same dimension small hypercubes called cells, 2^{n_d} cells of which consist of a n_d-dimension cluster called logical group and uses the unital-based scheme to generate keys. Each pair of sensors can set up their shared keys directly or indirectly and then can communicate securely through utilizing the ideas of paper [4] and [5]. Analysis and comparison show that this scheme enhances the resilience of WSNs, and has good network connectivity.

The first section is the introduction. The structure of this scheme is in the second section. In the third section, the shared keys establishment is given. The scheme performance analysis is presented in the section four. The conclusion is in the last section.

2 The structure of this strategy

A n_d dimension, D_1 , D_2 , $\cdots$, D_{n_d-1} , and D_{n_d} , hypercube, denoted as V , is the sensing multi-dimension space. N sensors and M clusters locate in V which is divided into the same

$(\sqrt[n_d]{M}+1)^{n_d}$ hypercubes with n_d dimension equally. Those small hypercubes are cells which are expressed as $\mathrm{C}_{00\cdots00}$, $\mathrm{C}_{00\cdots01}$, $\cdots$, $\mathrm{C}_{00\cdots0d_1}$, $\cdots$, $\mathrm{C}_{00\cdots0\sqrt[n_d]{M}}$, $\cdots$, $\mathrm{C}_{00\cdots d_2\sqrt[n_d]{M}}$, $\cdots$, $\mathrm{C}_{00\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, $\cdots$, $\mathrm{C}_{0d_{n_d-1}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, $\cdots$, $\mathrm{C}_{0\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, $\cdots$, $\mathrm{C}_{\sqrt[n_d]{M}\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, where, $0\le d_1\le\sqrt[d_n]{M}$, $0\le d_2\le\sqrt[d_n]{M}$, $\cdots$, $0\le d_{n_d-1}\le\sqrt[d_n]{M}$ and $0\le d_{n_d}\le\sqrt[d_n]{M}$. 2^{n_d} cells consist of a cluster. All M clusters are expressed as $\mathrm{G}_{00\cdots00}$, $\mathrm{G}_{00\cdots01}$, $\cdots$, $\mathrm{G}_{00\cdots0d_1^{'}}$, $\cdots$, $\mathrm{G}_{00\cdots0(\sqrt[n_d]{M}-1)}$, $\cdots$, $\mathrm{G}_{00\cdots d_2^{'}(\sqrt[n_d]{M}-1)}$, $\cdots$, $\mathrm{G}_{00\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, $\cdots$, $\mathrm{G}_{0d_{n_d-1}^{'}\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, $\cdots$, $\mathrm{G}_{0(\sqrt[n_d]{M}-1)\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, $\cdots$, $\mathrm{G}_{(\sqrt[n_d]{M}-1)\sqrt[n_d]{M}-1)\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, where, $0\le d_1^{'}\le\sqrt[d_n]{M}-1$, $0\le d_2^{'}\le\sqrt[d_n]{M}-1$, $\cdots$, $0\le d_{n_d-1}^{'}\le\sqrt[d_n]{M}-1$ and $0\le d_{n_d}^{'}\le\sqrt[d_n]{M}-1$.

$N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$ sensors are located in each small hypercube, and then $N2^{n_d}\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$ sensors are located in each cluster. Letting IDs express all nodes. We can obtain all sensor IDs. $1,2,3,\cdots,N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$ express those sensor nodes in $\mathrm{C}_{00\cdots00}$ respectively. $1+N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$, $2+N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$, $3+N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$, $\cdots$, $2N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$ express those nodes in $\mathrm{C}_{00\cdots01}$ respectively. We can get the IDs of those sensors in other cells through inducing from above. For example, $1+\left[\left(\sqrt[n_d]{M}+1\right)^{n_d}-1\right]N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$, $2+\left[\left(\sqrt[n_d]{M}+1\right)^{n_d}-1\right]N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$, $3+\left[\left(\sqrt[n_d]{M}+1\right)^{n_d}-1\right]N\big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$, $\cdots,N$ express those nodes in cell $\mathrm{C}_{\sqrt[n_d]{M}\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$ respectively.

3 The shared keys establishment

By a logical extension of the ideas of the paper [4] and [5], the base station generates M key groups and each key has its identifier in this scheme. The first key group consists of $m_{(0,0,\cdots,0,0)}^{3}+1$ keys, $m_{(0,0,\cdots,0,0)}^{2}(m_{(0,0,\cdots,0,0)}^{2}-m_{(0,0,\cdots,0,0)}+1)$ distinct key rings are constituted based on those keys, $m_{(0,0,\cdots,0,0)}+1$ keys are contained in each key ring, and each key is contained in $m_{(0,0,\cdots,0,0)}^{2}$ key rings. Similarly, the second key group consists of $m_{(0,0,\cdots,0,1)}^{3}+1$ keys, $m_{(0,0,\cdots,0,1)}^{2}(m_{(0,0,\cdots,0,1)}^{2}-m_{(0,0,\cdots,0,1)}+1)$ distinct key rings are constituted based on those keys, $m_{(0,0,\cdots,0,1)}+1$ keys are contained in each key ring, and each key is contained in $m_{(0,0,\cdots,0,1)}^{2}$ key rings. By a logical extension of this point, the M th key group consists of $m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1\sqrt[n_d]{M}-1)}^{3}+1$ keys, $m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1\sqrt[n_d]{M}-1)}^{2}$ $(m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1\sqrt[n_d]{M}-1)}^{2}-m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1\sqrt[n_d]{M}-1)}+1)$ distinct key rings are constituted based on those keys, $m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1\sqrt[n_d]{M}-1)}+1$ keys are contained in each key ring, and each key is contained in $m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1\sqrt[n_d]{M}-1)}^{2}$ key rings.

All those $\sum_{d_1^{'}=0}^{\sqrt[d_n]{M}-1}\sum_{d_2^{'}=0}^{\sqrt[d_n]{M}-1},\cdots,\sum_{d_{d_n-1}^{'}=0}^{\sqrt[d_n]{M}-1}\sum_{d_{d_n}^{'}=0}^{\sqrt[d_n]{M}-1}\left(m_{(d_1^{'},d_2^{'},\cdots,d_{d_n-1}^{'},d_{d_n}^{'})}^{3}+1\right)$ keys are distinct each other. In general, let $m_{(0,0,\cdots,0,0)}=m_{(0,0,\cdots,0,1)}=,\cdots,=m_{(0,0,\cdots,0,\sqrt[n_d]{M}-1)}=m_{(0,0,\cdots,1,0)}=m_{(0,0,\cdots,1,1)}=,\cdots,=m_{(0,0,\cdots,1,\sqrt[n_d]{M}-1)}$, $\cdots,=m_{(0,0,\cdots,\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1)},\cdots,=m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1)}$ because of the equal sensor node distribution.

The base station generates all key groups and key rings before sensors are deployed. They are loaded to all multi-dimension clusters respectively. In detail, $m_{(0,0,\cdots,0,0)}^2(m_{(0,0,\cdots,0,0)}^2 - m_{(0,0,\cdots,0,0)} + 1)$ distinct key rings are dispersed in cluster $\mathrm{G}_{0,0,\cdots,0,0}$, $m_{(0,0,\cdots,0,1)}^2(m_{(0,0,\cdots,0,1)}^2 - m_{(0,0,\cdots,0,1)} + 1)$ distinct key rings are dispersed in cluster $\mathrm{G}_{0,0,\cdots,0,1}$, etc. Generally, for two sensors u and v, they can set up their shared keys through exchanging their keys and their identifiers. If they discover their shared key, they have only one shared key based on the unital-based strategy. If they are in the same cell, but can not set up directly, they can set up their common key through using other nodes in this cell. If they are in two different cells, and they are in two different clusters which have common cell, they can establish their shared key through using those sensors located in the common cell. If they are in two separate clusters, they can establish common keys with different sensors, $u^{'}$ and $v^{'}$, which are close and can directly set up common keys with them respectively, where the distance between node u and v is longer than the distance between node $u^{'}$ and $v^{'}$. If u and v still can not establish their common keys through employing sensor $u^{'}$ and $v^{'}$, node $u^{'}$ and $v^{'}$ establish common keys with different sensors, $u^{''}$ and $v^{''}$, which are close with them respectively, and so on. At last, they can set up their shared key by using other sensors between node u and v.

4 The scheme performance analysis

4.1 The security analysis

Those nodes that locate in the 2^n corner cells, $\mathrm{C}_{d_{n_d}d_{n_d-1}\cdots d_2 d_1}$, where, $d_1 = 0$ or $d_1 = \sqrt[d_n]{M}$, $d_2 = 0$, or $d_2 = \sqrt[d_n]{M}$,$\cdots$, $d_{n_d-1} = 0$ or $d_{n_d-1} = \sqrt[d_n]{M}$,$d_{n_d} = 0$ or $d_{n_d} = \sqrt[d_n]{M}$, are loaded one key ring, for each one of them is only included one cluster. Those nodes that locate intersection cells where two two-dimension planes meet are loaded two key rings. Those nodes that locate intersection cells where two three-dimension spaces meet are loaded four key rings. We can deduce the rest from this, those nodes that locate intersection cells where two n_d -dimension spaces meet are loaded 2^{n_d-1} key rings. It will reveal all those sensor keys of the cluster it belongs to, if a node of corner cells is exposed. It will reveal all those sensor keys of two clusters it belongs to, if a node located intersection cells where two two-dimension planes meet. We can deduce the rest from this, it will reveal all those sensor keys of the 2^{n_d-1} clusters it belongs to. Because all $\sum_{d_1^{'}=0}^{\sqrt[d_n]{M}-1}\sum_{d_2^{'}=0}^{\sqrt[d_n]{M}-1},\cdots,\sum_{d_{d_n-1}^{'}=0}^{\sqrt[d_n]{M}-1}\sum_{d_{d_n}^{'}=0}^{\sqrt[d_n]{M}-1}\left(m_{(d_1^{'},d_2^{'},\cdots,d_{d_n-1}^{'},d_{d_n}^{'})}^3 + 1\right)$ keys are different each other, the compromised node can only damage those nodes of the clusters it belongs to in all those cases. Therefore, this scheme improves the WSNs security.

4.2 The connectivity analysis

All nodes of a cluster can establish their common keys directly or indirectly, and then they can cummunicate safely. They can set up their shared keys and then communicate securely through using intermediate sensors for two sensors not in the same cluster. Therefore, this scheme improves WSNs connectivity.

4.3 The storage analysis

From the security analysis, those nodes that locate in the 2^n corner cells are loaded one key rings, those nodes that locate intersection cells where two two-dimension planes meet are loaded two key rings, those nodes that locate intersection cells where two three-dimension spaces meet are loaded four key rings, and so on. We can deduce the rest from this, those nodes that locate intersection cells where two n_d -dimension spaces meet are loaded 2^{n_d-1} key rings. One key ring has $m_{(0,0,\cdots,0,0)} = m_{(0,0,\cdots,0,1)} =,\cdots,= m_{(0,0,\cdots,0,\sqrt[n_d]{M}-1)} = m_{(0,0,\cdots,1,0)} = m_{(0,0,\cdots,1,1)} =,\cdots,= m_{(0,0,\cdots,1,\sqrt[n_d]{M}-1)},\cdots,$ $= m_{(0,0,\cdots,\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1)},\cdots,= m_{(\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1,\cdots,\sqrt[n_d]{M}-1,\sqrt[n_d]{M}-1)}$ keys. Each pair of nodes has a only shared key.

Therefore, a sensor is loaded $2^{n_d-1}m$ keys at most. We can show that this scheme requires lower sensor storage.

4.4 The network scalability analysis

The base station generates $m^2_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}(m^2_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}-m_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}+1)$, where, $0\le d'_1\le \sqrt[d_n]{M}-1$, $0\le d'_2\le \sqrt[d_n]{M}-1$, $\cdots$, $0\le d'_{n_d-1}\le \sqrt[d_n]{M}-1$ and $0\le d'_{n_d}\le \sqrt[d_n]{M}-1$, key rings for those nodes of cluster $\mathrm{G}_{d'_{n_d}d'_{n_d-1}\cdots d'_2d'_1}$. A cluster has $N2^{n_d}\Big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$ nodes. If $N2^{n_d}\Big/\left(\sqrt[n_d]{M}+1\right)^{n_d}$ $< m^2_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}(m^2_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}-m_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}+1)$, other nodes can be added into this cluster. Through letting $m_{(d'_{n_d},d'_{n_d-1},\cdots,d'_2,d'_1)}$ get more values, more new nodes can be added into the cluster in this scheme. Therefore, this strategy has good scalability.

5 Conclusion

The n_d-dimension sensing hypercube is divided into numerous the same small n_d-dimension hypercubes. The scheme sets up shared keys between two nodes by using the unital-based strategy and the ideas of paper [4] and [5]. Analysis shows that this strategy enhances security for wireless sensor networks, improves WSNs connectivity, and has lower storage requirement and good scalability.

References

[1] Omar Rafik Merad Boudia, et al. A novel secure affregation scheme for wireless sensor networks using stateful public key cryptography. Ad Hoc Networks, 32(2015) 98-113.

[2] Sheetal Kalra, Sandeep K. Sood. Advanced password based anthentication scheme for wireless sensor networks. Journal of information security and applications, 20(2015)37-46.

[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] E. F. Assmus and J. D. Key. Designs and their codes. Cambridge Tracts in Mathematics, Cambridge University Press, 1992.

[5] Walid Bechkit, et al. A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL.12, NO.2, FEBRUARY 2013, pp 948-959.