A Scalable Key Scheme for Two-Dimension Wireless Sensor Networks

Yuquan Zhang

Wireless Sensing Institute, College of Information Science and Engineering, Qilu Normal University, China

zyczyq@126.com

Keywords: Wireless sensor network; security; clusters

Abstract. A scheme for wireless sensor network security is given by mainly utilizing unital-based strategy in this paper. The two-dimension sensing square is divided into numerous small squares called cells, and one cluster consists of four small squares. All sensors are same and distributed in the sensing square equally. The common cipher between any two sensor nodes is established through using the unital-based scheme in one certain grid. Analysis demonstrates the strategy requires a lower storage, improves WSN security, has good network connectivity, and has a flexible scalability.

1. Introduction

Recently, the development of micro-electro-mechanical system (MEMS) has facilitated the evolution of small and autonomous wireless device, namely sensor node, which has multiple capabilities, including sensing, computing, and communication[1].

Wireless sensor networks consist of numerous sensor nodes linked by a wireless transmission medium. The unique characters of sensor nodes are low wireless communication capacity, limited energy, limited storage memory and low computational ability.

Wireless sensor networks (WSN) have been proposed for a variety of applications including observing animals in a nature park, assistance in rescue operations, in-home entertainment systems, monitoring person health, management of traffic information, building management.

Due to the hardware resource limitations, the wireless medium of WSN, and, in some cases, the hostile environments in which WSNs are deployed, wireless sensor networks are vulnerable to various malicious attacks[2-6] including eavesdropping, masquerading, traffic-analysis, node capture, and so on.

Assuring the security for WSN is a challenging issue. The key management that thwarts the activities of malicious sensor nodes through generating secret keys in a secure way is an efficient method to guarantee wireless sensor networks secure.

A. Perrig et al.[7] proposed a strategy called SPINS, in which a base station participated. In this scheme, each sensor shares a key with the base station. If two sensors need to establish a pairwise key, the base station sends the pairwise key encrypted with the two shared keys respectively. Although this scheme has good resilience, it has poor scalability because the base station has to send keys to the related sensors. It is expensive and complex for wireless sensor networks to add and delete nodes or re-key for nodes as keying messages are broadcasted to all nodes. To solve those shortages, L. Eschenauer and V. D. Gligor[8] proposed a probabilistic key pre-distribution scheme, which is a basic strategy in many papers, to establish pairwise keys between two nodes. In this scheme, communication keys are set up through three steps: key predistribution, shared-key discovery, and path-key establishment. In the key predistribution phase, a large key pool is generated, and some distinct keys are drown out of the pool and stored into sensor memory. In the shared-key discovery phase, each sensor in WSNs finds its neighbors with its shared keys in its wireless communication range. In the last phase, those sensors that do not share common keys are connected by two or more links at the end of the second step. The strategy has further been improved by Chan et al[9], namely, a q-composite key pre-distribution scheme a random pairwise key scheme. The q-composite key pre-distribution also uses a key pool but requires two nodes compute a pairwise key from at least q pre-distributed keys that they share. The random pairwise key scheme randomly picks pairs of sensor

nodes and assigns each pair a unique random key. S. Hussain et al.[10] proposed a key distribution scheme. It enhance the security for WSNs, but it arouses computing complexness and energy consumption. Liu D and Ning P[11] presented a general framework for polynomial pool-based pairwise key predistribution in sensor networks and two possible instantiations key predistribution schemes: random subset assignment and grid-based schemes. This strategy is secure and resists collusion. The disadvantage is that it will be more vulnerable to be compromised when the sensor network becomes larger. To deal with the drawback in [11], [12], which is an extensive version of the [11], utilized a pool of multiple random bivariate polynomials. Compared with [11], [12] improved the security and the scalability for 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 symmetric to generate keys. Analysis and comparison show that this scheme enhances the resilience of WSNs, and has good network connection.

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. The structure of this strategy

The scheme is a one-layer key management strategy which include the base station and ordinary sensor nodes. There is no heterogenous sensor nodes and cluster head nodes.

In this strategy, the sensing area is a two dimension, x and y, square denoted as S and all sensor nodes are distributed in the square equally. There are N sensor nodes in the sensing area. The sensing square is equally divided into $\left(\sqrt{M}+1\right)^2$, denoted as $\mathrm{C}_{00},\mathrm{C}_{01},\cdots,\mathrm{C}_{0j},\cdots,\mathrm{C}_{0\sqrt{M}}$, $\mathrm{C}_{10},\mathrm{C}_{11},\cdots,\mathrm{C}_{1j},\cdots,\mathrm{C}_{1\sqrt{M}},\cdots$, $\mathrm{C}_{k0},\mathrm{C}_{k1},\cdots,\mathrm{C}_{kj},\cdots,\mathrm{C}_{k\sqrt{M}},\cdots$, $\mathrm{C}_{\sqrt{M}0},\mathrm{C}_{\sqrt{M}1},\cdots,\mathrm{C}_{\sqrt{M}j},\cdots,\mathrm{C}_{\sqrt{M}\sqrt{M}}$, where $0\le j\le\sqrt{M}$ and $0\le k\le\sqrt{M}$, small squares called cells. A cluster includes four cells and then there are M clusters including $\mathrm{G}_{00},\mathrm{G}_{01},\cdots,\mathrm{G}_{0j},\cdots,\mathrm{G}_{0\left(\sqrt{M}-1\right)}$, $\mathrm{G}_{10},\mathrm{G}_{11},\cdots,\mathrm{G}_{1j},\cdots,\mathrm{G}_{1\left(\sqrt{M}-1\right)}$, $,\cdots,\mathrm{G}_{k0},\mathrm{G}_{k1},\cdots,\mathrm{G}_{kj},\cdots,\mathrm{G}_{k\left(\sqrt{M}-1\right)}$, $,\cdots,\mathrm{G}_{\left(\sqrt{M}-1\right)0},\mathrm{G}_{\left(\sqrt{M}-1\right)1},\cdots,\mathrm{G}_{\left(\sqrt{M}-1\right)j},\cdots,\mathrm{G}_{\left(\sqrt{M}-1\right)\left(\sqrt{M}-1\right)}$, where $0\le j'\le\sqrt{M}-1$ and $0\le k'\le\sqrt{M}-1$. In Fig.1, for example, cluster G_{00} consists of cell $\mathrm{C}_{00},\mathrm{C}_{01},\mathrm{C}_{10},\mathrm{C}_{11}$.

There are $N\Big/\left(\sqrt{M}+1\right)^2$ sensor nodes in each cell, so there are $4N\Big/\left(\sqrt{M}+1\right)^2$ sensor nodes in each cluster. All those sensor nodes are denoted by their ID. Those nodes in cell C_{00} are denoted as $1,2,3,\cdots,N\Big/\left(\sqrt{M}+1\right)^2$. Those nodes in cell C_{01} are denoted as $1+N\Big/\left(\sqrt{M}+1\right)^2,2+N\Big/\left(\sqrt{M}+1\right)^2,3+N\Big/\left(\sqrt{M}+1\right)^2,\cdots,2N\Big/\left(\sqrt{M}+1\right)^2$. We can deduce from this and obtain those IDs in other cells. For example, those nodes in cell $\mathrm{C}_{\sqrt{M}\sqrt{M}}$ are denoted as $1+\left[\left(\sqrt{M}+1\right)^2-1\right]N\Big/\left(\sqrt{M}+1\right)^2,2+\left[\left(\sqrt{M}+1\right)^2-1\right]N\Big/\left(\sqrt{M}+1\right)^2,3+\left[\left(\sqrt{M}+1\right)^2-1\right]N\Big/\left(\sqrt{M}+1\right)^2,\cdots,N.$

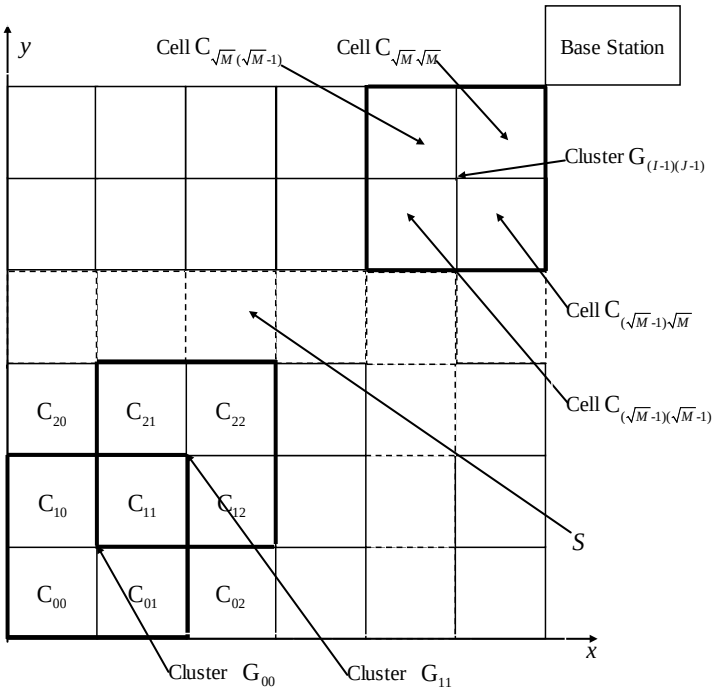

Fig. 1 Location-based cells and clusters

3. The shared keys establishment

The unital design is an Steiner 2-design contains $b = m^2(m^3+1)/(m+1) = m^2(m^2-m+1)$ blocks of a set of $v = m^3+1$ porints[13]Each block comprise of $m+1$points and each point is included in $r = m^2$ blocks. Each pair of points is contained in exactly one block together. Following the idea in the [14] which is obtained based on the unital design, M key groups are generated and each key is denoted by its identifier. There are $m^3_{(0,0)}+1$ keys in the first key group, $m^2_{(0,0)}(m^2_{(0,0)}-m_{(0,0)}+1)$ distinct key rings are constituted based on those keys, $m_{(0,0)}+1$ keys in contained in each key ring, and each key is contained in $m^2_{(0,0)}$ key rings. Similarly, there are $m^3_{(0,1)}+1$ keys in the second key group, $m^2_{(0,1)}(m^2_{(0,1)}-m_{(0,1)}+1)$ key rings are constituted based on those keys, $m_{(0,1)}+1$ keys in contained in each key ring, and each key is contained in $m^2_{(0,1)}$ key rings. By a logical extension of this point, there are $m^3_{(\sqrt{M}-1,\sqrt{M}-1)}+1$ keys in the M th key group, $m^2_{(\sqrt{M}-1,\sqrt{M}-1)}(m^2_{(\sqrt{M}-1,\sqrt{M}-1)}-m_{(\sqrt{M}-1,\sqrt{M}-1)}+1)$ distinct key rings are constituted bsaed on those keys, $m_{(\sqrt{M}-1,\sqrt{M}-1)}+1$ keys in contained in each key ring, and each key is contained in $m^2_{(\sqrt{M}-1,\sqrt{M}-1)}$ key rings.

All those $\sum_{j'=0}^{\sqrt{M}-1}\sum_{k'=0}^{\sqrt{M}-1}\left(m^3_{(j',k')}+1\right)$ keys are different each other. Generally, we let $m_{(0,0)} = m_{(0,1)} =,\cdots,= m_{(0,\sqrt{M}-1)} = m_{(1,0)} = m_{(1,1)} =,\cdots,= m_{(1,\sqrt{M}-1)} =,\cdots, m_{(\sqrt{M}-1,\sqrt{M}-1)}$ because of the equal sensor node distribution.

All those key rings are generated and dispensed to all those clusters respectively, namely, $m^2_{(0,0)}(m^2_{(0,0)}-m_{(0,0)}+1)$ key rings are distributed to all sensors of the cluster G_{00} , $m^2_{(0,1)}(m^2_{(0,1)}-m_{(0,1)}+1)$ key rings are distributed to all sensors of the cluster G_{01}, and so on. In a certain cluster, two neighboring sensors can establish their shared keys directly by exchanging their

keys and their key identifiers through which the two sensors can establish their shared key. It is obvious that each two sensors have only one common key if they can find their common key through using this key management strategy. If two nodes can not establish their shared key, they can finish this task through utlizing their intermetiate nodes with which both of them can establish common keys. If two sensor nodes are in two close clusters respectively and those two clusters have common cell, they can establish their communication keys through using those nodes which are in the common section of the two close clusters. For example, in the Fig.1, two sensor u and v in the cluster G_{00} and G_{01} respectively, they can set up their communication through using those nodes in the cell C_{01} or C_{11}. If two sensor nodes are in two separate clusters respectively or are in two close clusters which have no common cell, they can establish their communication keys through using nodes which are in other cells. For instance, in the Fig.1, two sensor u and v in the cluster G_{00} and $G_{(\sqrt{M}-1,\sqrt{M}-1)}$ respectively, they can set up their communication through using those nodes in the cell $C_{11}, C_{22}, \cdots, C_{(\sqrt{M}-1,\sqrt{M}-1)}$.

4. The scheme performance analysis

4.1 The security analysis

Those sensor nodes that are in the four cells, C_{00}, $C_{(0,\sqrt{M}-1)}$, $C_{(\sqrt{M}-1,0)}$ and $C_{(\sqrt{M}-1,\sqrt{M}-1)}$, are loaded only one key ring. Those sensor nodes that are in the edge cells of the sensing square but not on the corner cells are loaded two key rings. The other sensor nodes are loaded four key rings. So, those sensors not in the corner cells or edge cells will reveal more keys if they are compromised. So, we partition those key rings into two sections or four sections. If a key ring is exposed, other one or three key rings are still secure. According to the above, all keys of key rings in a sensor node are different completely, so, a sensor can reveal any other its key rings, if its one key ring is exposed. A compromised node can damage those nodes which have the same key rings with it. Those nodes are in a certain cluster with the compromised node. So, a compromised node can only damage those nodes which are in the same cluster with it.

4.2 The connectivity analysis

In a certain cluster, all sensor nodes can establish their shared keys and then can cummunicate securely each other. If two nodes are in different clusters and have no common key, they can set up their shared key by using intermetiate nodes and then establish secure communication paths. So, this scheme has a good connectivity.

4.3 The storage analysis

Generally, a node not in the corner cell or edge cell has four key rings and one key ring has $m_{(0,0)} = m_{(0,1)} =, \cdots, = m_{(0,\sqrt{M}-1)} = m_{(1,0)} = m_{(1,1)} =, \cdots, = m_{(1,\sqrt{M}-1)} =, \cdots, m_{(\sqrt{M}-1,\sqrt{M}-1)} = m$ keys. Each pair of nodes only has a shared key. So, a node not in the corner cells or edge cells is loaded $4m$ distinct keys, a node in the corner cell is loaded m keys, and a node in the edge cell is load $2m$ keys.

4.4 The network scalability analysis

In general, a cluster has $4N \big/ \left(\sqrt{M}+1\right)^2$ nodes, and this strategy can generate $m^2_{(j',k')}(m^2_{(j',k')} - m_{(j',k')} + 1)$, where $0 \le j' \le \sqrt{M}-1, 0 \le k' \le \sqrt{M}-1$ key rings for those nodes. If $4N \big/ \left(\sqrt{M}+1\right)^2 < m^2_{(j',k')}(m^2_{(j',k')} - m_{(j',k')} + 1)$, other nodes can added into the cluster. We can let $m_{(j',k')}$ get more value to add more new nodes into the cluster. This scheme has good scalability.

5. Conclusion

This scheme sets up shared keys among all those sensor nodes by using the unital-based strategy after dividing the sensing square into numerous cells and clusters. Analysis for this strategy

demonstrates that this scheme can guarantee the netwok security, has good connectivity, has lower storage, and has good scalability.

Acknowledgements

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

References

[1] J. Ford. "Telecommunications with MEMS devices: an overview", in: Proceedings of the 14th Annual Meeting of the IEEE Lasers and Electro-Optics Society, vol. 2,no.12, November 2001, pp.415-416, (2001).

[2] H. T. Kung, D. Vlah. "Efficient location tracking using sensor networks", in: Proc. the 2003 IEEE Wireless Communications and Networking Conference (WCNC'03), vol. 3, pp. 1954-1961, (2003).

[3] R. Brooks, P. Ramanathan, A. Sayeed,"Distributed target classification and tracking in sensor networks", Proc. IEEE 91 (8) (2003) , pp.1163-1171, (2003).

[4] A. Wood, J. Stankovic,"Denial of service in sensor networks", IEEE Comput. Mag. 35(10), pp. 54-62, (2002).

[5] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", in: Proc. the 1st IEEE International Workshop on Sensor Network Protocols and Applications (SNPA'03),2003, pp.113-127, (2003).

[6] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, "SPINS: security protocols for sensor networks", Wireless Network. pp. 521-534, (2002).

[7] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, J.D. Tygar. "SPINS: security protocols for sensor networks", In: Proceedings of the 7th annual ACM/IEEE international conference on mobile computing and networking, July 2001, pp.189-199, (2001).

[8] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. CCS'02: 9th ACM Conference on Computer and Communications Security. New York: ACM Press, Nov. 2002, pp.41-47, (2002).

[9] H. Chan, A. Perrig, D. Song. "Random key predistribution schemes for sensor networks", Proceedings of the IEEE Syrup. On Research in Security and Privacy, Berkeley, CA, USA, May 11-14 2003, pp.197-213, (2003).

[10] S. Hussain, F. Kausar, A. Masood. "An efficient key distribution scheme for heterogeneous sensor networks", Proceedings of the 2007 international conference on Wireless communications and mobile computing, Honolulu, Hawaii, USA, August 12-16, 2007, pp.388-392, (2007).

[11] 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).

[12] 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).

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

[14] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh, "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.