IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Highly Secure Connectivity Coverage with Scalable Key Management Scheme For Wireless Sensor NetworkS

M.Ayyappan*[1], V.Anitha[2]

*[1]PG Scholar, [2]Professor, Department of Information Technology, Annai Mathammal Sheela Engineering College, Namakkal – 637013, TN, India

ayyappan.hracc@gmail.com

Abstract

The sensitivity of the potential WSN applications and because of resource limitations, key management emerges as a challenging issue for WSNs. One of the main concerns when designing a key management scheme is the network scalability. Indeed, the protocol should support a large number of nodes to enable a large scale deployment of the network. The proposed system is a new scalable key management scheme for WSNs which provides good secure connectivity coverage. For this purpose, make use of the unital design theory. The basic mapping from unitals to key pre-distribution allows us to achieve high network scalability. Nonetheless, this naive mapping does not guarantee a high key sharing probability. Therefore, proposed system is an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability approximately lower bounded by 1 − e-^1   0.632. The approximate analysis and simulations and compare our solution to those of existing methods for different criteria such as storage overhead, network scalability, network connectivity, average secure path length and network resiliency. The proposed approach enhances the network scalability while providing high secure connectivity coverage and overall improved performance. Moreover, for an equal network size, the solution reduces significantly the storage overhead compared to those of existing solutions.

Keywords: Wireless sensor networks, security, key management, network scalability, secure connectivity coverage.

Introduction

Nowadays, Wireless Sensor Networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, usually no trusted third party which can attribute pairwise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes

Problem Statement

Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, usually no trusted third party this can attribute pairwise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution.

In most existing solutions, the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

Wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pair wise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution.

The following drawbacks are identified from the existing system. A host of research work dealt with symmetric key pre-distribution issue for WSNs and many solutions have been proposed. In the existing system many disadvantages occur: the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

Proposed Work

In this proposed system, the aim is to tackle the scalability issue without degrading the other network performance metrics. The main state of the art of symmetric key management schemes for WSNs that classify into two categories: probabilistic schemes and deterministic ones. In further refine the classification into sub-categories with respect to the underlying concepts and techniques used in key exchange and agreement.

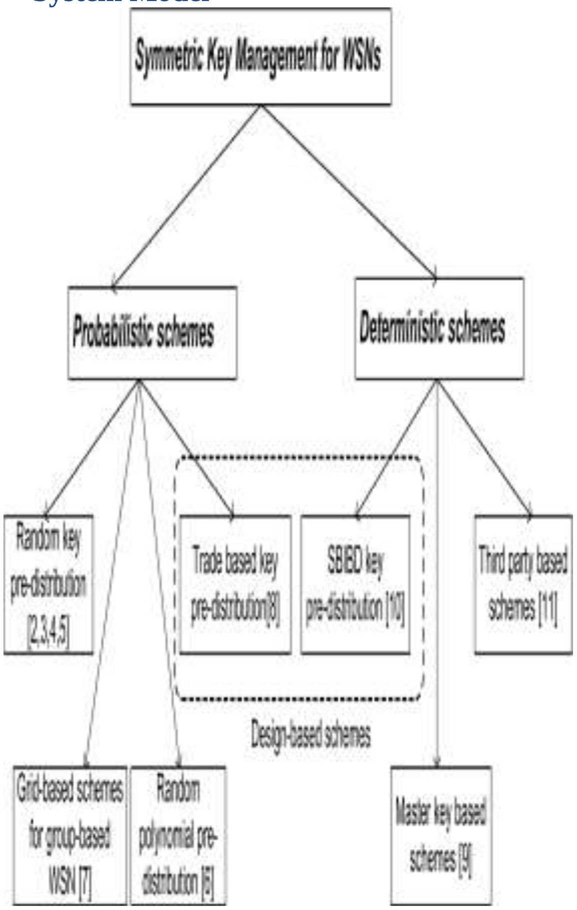
The use of unital design theory in key pre distribution for WSNs. This show that the basic mapping from unitals to key pre-distribution gives birth to highly scalable scheme while providing low probability of sharing common keys. We propose an enhanced unital-based key predistribution scheme in order to increase the network scalability while maintaining a good key sharing probability.

The adequate choice of the solution parameter should guarantee high key sharing probability approximately over bounded by $1-e-1$while ensuring a high network scalability. We analyze and compare our new approach against main existing schemes, with respect to different criteria: storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network resiliency. For this purpose, the target is the design of a scheme which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, the unital design theory for efficient WSN key pre-distribution is used.

The advantages of the proposed system as follows:

- Propose a naive mapping from unital design to key pre-distribution and we show through analytical analysis that it allows to achieve high scalability.
- Propose an enhanced unital based key pre-distribution scheme that maintains a good key sharing probability while enhancing the network scalability.
- Analyze and compare our new approach against main existing schemes, with respect to different criteria: storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network resiliency.

System Model


Symmetric Key Management for WSNs
Probabilistic schemes
Deterministic schemes
Random key pre-distribution [2,3,4,5]
Trade based key pre-distribution[8]
SBIBD key pre-distribution [10]
Third party based schemes [11]
Design-based schemes
Grid-based schemes for group-based WSN [7]
Random polynomial pre-distribution [6]
Master key based schemes [9]

Probabilistic schemes

In probabilistic key management schemes, each two neighboring nodes can establish a secure link with some probability. If two neighboring nodes cannot establish a secure link, they establish a secure path composed of successive secure links. Eschenauer and Gligor proposed in [2] the basic Random Key Predistribution scheme denoted by RKP. In this scheme, each node is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment step, each node i exchanges with each of its neighbor j the list of key identifiers that it maintains. This allows node j to identify the keys that it shares with node i. If two neighbors share at least one key, they establish a secure link and compute their session secret key which is one of the common keys. Otherwise, they should determine a secure path which is composed by successive secure links. The values of the key ring size k and the key pool size |S| are chosen in such a way that the intersection of two key rings is not empty with a high probability. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring. Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool.

Deterministic schemes

Deterministic schemes ensure that each node is able to establish a pair-wise key with all its neighbors. Many solutions were proposed to guarantee determinism. A naive deterministic key pre-distribution scheme can be designed by assigning to each link (i,j) a distinct key Ki,j and pre-loading each node with (n−1) pairwise keys in which it is involved where n is the network size. It is obvious that this solution is not scalable for large WSNs. Choi et al. proposed in [17] an enhanced approach allowing to store only (n+1)/2 keys at each node. For that purpose, they propose to establish an order relation between node identifiers and propose a hash function based key establishment in order to store only half of the node symmetric keys while computing the other half at each node. This approach allows to reduce the required stored keys to the half of network size, however, it is obvious that this scheme remains non scalable enough.

Unital Design for Key Pre-Distribution

In WSNs are highly resource constrained. In particular, they suffer from reduced storage capacity. Therefore, it is essential to design smart techniques to build blocks of keys that will be embedded on the nodes to secure the network links. Nonetheless, in most existing solutions, the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability, or degrade other performance metrics including secure connectivity and storage overhead. This motivates the use of unital design theory that allows a smart building of blocks with unique features that allow tocope with the scalability and connectivity issues.

Background: Unital Design

In combinations, the design theory deals with the existence and construction of systems of finite sets whose intersections have specified numerical properties. Formally, A t-design (v,b,r,k,λ) is defined as follows : Given a finite set X of v points (elements), we construct a family of b subsets of X, called blocks, such that each block has a size k, each point is contained in r blocks and each t points are contained together in exactly λ blocks. For instance, the symmetric Balanced Incomplete Block Design (SBIBD) presented above is a

(ν,b,r,k,λ) design, where $\nu = b = m2+ m + 1$, $r = k = m + 1$ and $\lambda = 1$.

Conclusion

The proposed work is a scalable key management scheme which ensures a good secure coverage of large scale WSN with a low key storage overhead and a good network resiliency, with use of the unital design theory. The basic mapping from unitals to key pre-distribution allows achieving high network scalability while giving allow direct secure connectivity coverage. The proposed is an efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage. The solution parameters are discussed and propose adequate values giving a very good trade-off between network scalability and secure connectivity. The analytical analysis are conducted and simulations to compare the new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances.

References

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

[2] *Amtepe .S and Yener .B, “Key distribution mechanisms for Wireless Sensor Networks: a survey,” Technical Report TR-05-07, Mar. 2005.*

[3] *Betten .A,Betten .D, and Tonchev .V, “Unitals and codes,”” Discrete Mathematics, vol. 267, no. 1-3, pp. 23–33, 2003.*

[4] *Blom .R, “An optimal class of symmetric key generation systems,” in Proc. 1985 Eurocrypt Workshop Advances Cryptology: Theory Appl. Cryptographic Techniques, pp. 335–338.*

[5] *Castelluccia .C and Spognardi .A, “A robust key pre-distribution protocol for multi-phase Wireless Sensor Networks,” in Proc. 2007 IEEE Securecom, pp. 351–360.*

[6] *Chan .H, Perrig .A, and Song .D, “Random key predistribution schemes for sensor networks,” in IEEE SP, pp. 197–213, 2003.*

[7] *Choi .T, Acharya .H, and Gouda .M, “The best keying protocol for sensor networks,” in Proc. 2011 IEEE WOWMOM, pp. 1–6.*

[8] *Du .W, Deng .J, Han .Y, Chen .S, “A key management scheme for Wireless Sensor Networks using deployment knowledge,” in Proc. 2004 IEEE INFOCOM, pp. 586–597.*

[9] *Du .W, Deng .W, Han .J, “A key management scheme for Wireless Sensor Networks using deployment knowledge,” in Proc. 2004 IEEE INFOCOM, pp. 586–597.*

[10] *Eschenauer .L, “A key-management scheme for distributed sensor networks,” in Proc. 2002 ACM CCS, pp. 41–47.*

[11] *Key .D, “Some applications of magma in designs and codes: oval designs, hermitian unitals and generalized Reed-Muller codes,” J. Symbolic Computation, vol. 31, no. 1/2, pp. 37–53, 2001.*

[12] *Liu .D and Ning .P, “Establishing pairwise keys in distributed sensor networks,” in Proc. 2003 ACM CCS, pp. 52–61.*

[13] *Maala .B, Challal .Y, and Bouabdallah .A, “Hero: hierarchcal key management protocol for heterogeneous WSN,” in Proc. 2008 IFIP WSAN, pp. 125–136.*

[14] *Perrig .A, Szewczyk .R, Wen .V,Culler .E, and Tygar .J, “Spins: security protocols for sensor netowrks,” in Proc. 2001 ACM MOBICOM, pp. 189–199.*

[15] *Ruj. S and Roy .B, “Key predistribution using combinatorial designs for grid-group deployment scheme in Wireless Sensor Networks,” ACM Trans. Sensor Netw., vol. 6, no. 4, pp. 1–4:28, Jan. 2010.*

[16] *Ruj. S, Nayak .A, and Stojmenovic .I, “Fully secure pairwise and triple key distribution in Wireless Sensor Networks using combinatorial designs,” in Proc. 2011 IEEE INFOCOM, pp. 326–330.*

[17] *Shakkottai .S, Srikant .R, and Shroff .N, “Unreliable sensor grids: coverage, connectivity and diameter,” in Proc. 2003 IEEE INFOCOM, pp. 1073–1083.*

[18] *Yu .Z and Guan .Y, “A robust group-based key management scheme for Wireless Sensor Networks,” in Proc. 2005 IEEE WCNC, pp. 1915–1920*

[19] *Zhu .S, Setia .S, “Leap: efficient security mechanisms for large-scale distributed sensor networks,” in Proc. 2003 ACM CCS, pp. 62–72.*

[20] *Zhou .Y, Fang .Y, and Zhang .Y, “Securing Wireless Sensor Networks: a survey,” IEEE Commun. Surv. Tuts., vol. 10, no. 1–4, pp. 6–28, 2008*