International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Providing Good Coverage and Secure Connectivity Using Key Pre-Distribution Scheme for Wireless Sensor Networks

A. Haritha

MCA Sri Padmavathi College of Computer Science and Technology, Tiruchanoor, Tirupathi, Andhra Pradesh, India

ABSTRACT

Now A Days, wireless device networks (WSNs) are more and more utilized in important applications inside many fields as well as military, medical and industrial sectors. Given the sensitivity of those applications, sophisticated security services square measure needed. Key management may be a corner stone for several security services like confidentiality and authentication that are needed to secure communications in WSNs.In existing system, we discover most Rate Of Networked Computation during a Capacitated Network during this they focused only on network capability they didn't about secure connectivity it means that giving security to that information whereas transfer from source to destination. This is often the massive disadvantage in existing system. To overcome this problem we tend to move to proposed model. we propose a new scalable key management scheme for WSNs that provides a good secure connectivity coverage. For this purpose, we tend to make use of the unital design theory. We tend to show that the basic mapping from unitals to key pre-distribution allows us to attain high network scalability. Nonetheless, this naive mapping doesn't guarantee a high key sharing probability. Therefore, we tend to propose an enhanced unital-based key pre-distribution theme providing high network scalability and good key sharing probability approximately lower bounded by 1 – e–1 ≈ 0.632. we tend to conduct approximate analysis and simulations and compare our solution to those of existing methods for different criteria like storage overhead, network scalability, network connectivity, average secure path length and network resiliency. Our results show that the proposed approach enhances the network scalability whereas providing high secure property coverage and overall improved performance.

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

I. INTRODUCTION

Recent advances in electronic and computer technologies have paved the way for the proliferation of wireless sensor networks (WSN). Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communications. In typical application scenarios, sensor nodes are spread randomly over the deployment region under scrutiny and collect sensor data. Examples of sensor network projects include Smart Dust and WINS. Sensor networks are being deployed for a wide variety of applications, including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes1, or

intentionally provide misleading information to other nodes. To provide security, communication should be encrypted and authenticated. An open research problem is how to bootstrap secure communications among sensor nodes, i.e. how to set up secret keys among communicating nodes? This key agreement problem is a part of the key management problem, which has been widely studied in general network environments. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA, as pointed out in . The third type of key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment. If we know which nodes are more likely to stay in the same neighborhood before deployment, keys can be decided a priori. However, because of the randomness of the deployment, knowing the set of neighbors deterministically might not be feasible. There exist a number of key pre-distribution schemes. Our aim is to tackle the scalability issue without degrading the other network performance metrics. For this purpose, we target 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, we make use, of the unital design theory for efficient WSN key pre-distribution. Indeed, we propose a naive mapping from unital design to key pre-distribution and we show through analytical analysis that it allows to achieve high scalability. Nonetheless, this naive mapping does not guarantee a high key sharing probability. Therefore, we propose an enhanced unital based key pre-distribution scheme that maintains a good key sharing probability while enhancing the network scalability. A preliminary work and few discussions were presented in. The contributions of our work are given next:

- ✓ We review the main state of the art of symmetric key management schemes for WSNs that we classify into two categories: probabilistic schemes and deterministic ones. We further refine the classification into sub-categories with respect to the underlying concepts and techniques used in key exchange and agreement.
- ✓ We introduce the use of unital design theory in key predistribution for WSNs. We 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 pre-distribution scheme in order to increase the network scalability while maintaining a good key sharing probability. We prove that adequate choice of our solution parameter should guarantee high key sharing probability approximately lower bounded by $1-e^{-1}$ while ensuring 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. The obtained results show that our solution enhances the network scalability while providing good overall network performances. Moreover, we show that at equal network size, our solution reduces significantly the storage overhead and thereby the energy consumption.

Scheme

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 coping with the scalability and connectivity issues. In what follows, we start by providing the definition and the features of unital design theory. We explain then the basic mapping from unital to key pre-distribution and evaluate its performance metrics. We propose finally an enhanced unital-based scheme which achieves a good trade-off between scalability and connectivity.

Background: Unital Design

In combinatory, 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 (v, b, r, k, λ) design, where

$v = b = m^2 + m + 1$,

$r = k = m + 1$ and $\lambda = 1$.

A Unital design is an Steiner 2-design which consists of $b = m^2 (m^3+1)/(m+1) = m^2 (m^2-m+1)$ blocks, of a set of $v = m^3 + 1$ points [19]. Each block contains $m+1$ points and each point is contained in $r = m2$ blocks. Each pair of points is contained in exactly one block together. We denote the Unital by $2\text{–}design(m^3+1, m^2 (m^2-m+1)m^2, m+1, 1)$ or by $(m^3 + 1, m+ 1, 1)$ design for simplicity sake. Without loss of generality, we focus in this paper on Hermitian unitals which exist for all m a prime power. Other construction for m not necessarily a prime power exists in literature. Some Hermitian unital construction approaches were proposed in literature. A unital may be represented by its $v \times b$ incidence matrix that we call M. In this matrix rows represent the points p_i and columns represent blocks Bj. The matrix M is then defined as:

Mij =1 if $p_i \in Bj$

0 otherwise

We give in Figure 2 an incidence matrix of a 2-(9,3,1)hermitian unital. It consists of 12 blocks of a set of 9 points. Each block contains 3 points and each point occurs in 4 blocks. Each pair of points is contained together in exactly one block.

A basic mapping from unitals to key pre-distribution for WSNs

In this subsection, we start by developing a simple scalable key pre-distribution scheme based on unital design that we denote by NU-KP for the naive unital-based key pre-distribution scheme. We propose a basic mapping in which we associate to each point of the unital a distinct key, to the global set of points the key pool and to each block a node key ring. We can then generate from a global key pool of

$|S| = m^3 + 1$ keys, n key rings ($n = b = m^2 (m^2 - m + 1)$) of size $k = m+ 1$ keys each one.

Before the deployment phase, we generate the unital blocks corresponding to key rings. Each node is then pre-loaded with a distinct key ring as well as the corresponding key identifiers. After the deployment step, each two neighboring nodes exchange the list of their key identifiers which allows determining eventual common key. Using this basic approach, each two nodes share at most one common key. Indeed, referring to the unital properties, each pair of points is contained together in exactly one block

which implies that two blocks cannot share more than one point. Hence, if two neighboring nodes share one common key, the latter is used as a pairwise key to secure the link; otherwise, nodes should determine secure paths which are composed of successive secure links.

A NEW SCALABLE UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME FOR WSNS

In this section, we present a new unital-based key predistribution scheme for WSNs. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build the unital design blocks and pre-load each node with a number of blocks picked in a selective way.

A. Key Pre-distribution

Before the deployment step, we generate blocks of *m* order unital design, where each block corresponds to a key set. We pre-load then each node with t completely disjoint blocks where *t* is a protocol parameter that we will discuss later in this section. In lemma 1, we demonstrate the condition of existence of such *t* completely disjoint blocks among the unital blocks. In the basic approach each node is pre-loaded with only one unital block and we proved that each two nodes share at most one key. Contrary to this, pre-loading each two nodes with *t* disjoint unital blocks means that each two nodes share between zero and *t*2 keys since each two unitals blocks share at most one element. After the deployment step, each two neighbors exchange the identifiers of their keys in order to determine the common keys. If two neighboring nodes share one or more keys, we propose to compute the pairwise secret key as the hash of all their common keys concatenated to each other. The used hash function may be *SHA-1* for instance. This approach enhances the network resiliency since the attacker has to compromise more overlap keys to break a secure link. Otherwise, when neighbors do not share any key, they should find a secure path composed of successive secure links. The major advantage of this approach is the improvement of the key sharing probability. As we will prove in next subsection, this approach allows achieving high secure connectivity coverage since each node is pre-loaded with *t* disjoint blocks. Moreover, this approach gives good network resiliency through the composite pairwise secret keys which reinforces secure links. In addition, we show that our solution maintains high network scalability compared to existing solutions although it remains lower than that of the naïve version.

Table 1

Unital design	Key pre-distribution
X: Point set	S : Key pool
Blocks	Key rings ($< KR_i >$)
Size of a block ($k = m + 1$)	Size of a key ring ($k = \|KR_i\| = m + 1$)
Size of the object set X: $\nu = m^3 + 1$	Size of the key pool S: $\|S\| = m^3 + 1$
Number of generated blocks: $b = m^2(m^2 - m + 1)$	Number of generated key rings (supported nodes) : $n = m^2(m^2 - m + 1)$
Each point belongs to exactly m^2 blocks	Each key appears in exactly m^2 key rings

II. CONCLUSION

We proposed, in this work, a scalable key management scheme that ensures a good secure coverage of large scales with a low key storage overhead and a good network resiliency. We make use of the unital design theory. we tend to showed that a basic mapping from unitals to key pre-distributional lows to achieve high network scalability whereas giving allow direct secure connectivity coverage. We tend to proposed then an efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage. We tend to discuss the solution parameter and we propose adequate values giving a very good trade-off between network

scalability and secure connectivity. We tend to conducted analytical analysis and simulations to check our 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.

III. REFERENCES

[1]. Prabal Dutta et al., "Design and Evaluation of Versatile and Efficient Receiver-Initiated Link Layer for Low-Power Wireless", SenSys, 2010.

[2]. E.R. Musaloiu, C Liang, A Terzis, "Koala: Ultra-Low Power Data Retrieval in Wireless Sensor Networks", IPSN, 2008.

[3]. E.R. Musaloiu, C Liang, A Terzis, "Koala: Ultra-Low Power Data Retrieval in Wireless Sensor Networks", IPSN, 2008.

[4]. J. Ansari, X. Zhang, P. Mahonen, "Multi-radio Medium Access Control Protocol for Wireless Sensor Networks", DCOSS, 2008.

[5]. Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," IEEE Commun. Surv. Tuts., vol. 10, no. 1–4, pp. 6–28, 2008.

[6]. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 2002 ACM CCS, pp. 41–47.

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

[8]. W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. 2004 IEEE INFOCOM, pp. 586–597.

[9]. C. Castelluccia and A. Spognardi, "A robust key pre-distribution protocol for multi-phase wireless sensor networks," in Proc. 2007 IEEE Securecom, pp. 351–360.

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

[11]. Z. Yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in Proc. 2005 IEEE WCNC, pp. 1915 1920.

[12]. S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial

[13]. designs," in Proc. 2011 IEEE INFOCOM, pp. 326–330.

[14]. S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in Proc. 2003 ACM CCS, pp. 62–72.

[15]. S. A. C¸ amtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 15, pp. 346–358, 2007.

[16]. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "Spins: security protocols for sensor netowrks," in Proc. 2001 ACM MOBICOM, pp. 189–199.

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

[18]. W. Bechkit, Y. Challal, and A. Bouabdallah, "A new scalable key predistribution scheme for WSN," in Proc. 2012 IEEE ICCCN, pp. 1–7.

[19]. J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," J. Netw. Comput. Appl., vol. 33, no. 2, pp. 63–75, 2010.