INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks

S. Munvar Hussain
MCA, Santhiram Engineering College, Nandyal, JNTU-A, Anantapur, India
P. Bhaskar
M.Tech, Santhiram Engineering College, Nandyal, JNTU-A, Anantapur, India

Abstract:
Given 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. In this paper, we propose a new scalable key management scheme for WSNs which provides a good secure connectivity coverage. For this purpose, we make use of the unital design theory. We show that 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, we propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability approximately lower bounded by $1 - e^{-1} \approx 0.632$. *We conduct 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. Our results show that the proposed approach enhances the network scalability while providing high secure connectivity coverage and overall improved performance. Moreover, for an equal network size, our solution reduces significantly the storage overhead compared to those of existing solutions.*

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

1. 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, 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. Over the last decade, a host of research work dealt with symmetric key pre-distribution issue for WSNs and many solutions have been proposed in the literature. Nevertheless, 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.

In this work, 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 pre- distribution 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 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. 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.

The remainder of this paper is organized as follows: Section 2 presents related works on key management for WSNs. We give in Section 3 a background on unital design and we propose a basic mapping from unitals to key pre-distribution for WSNs, we analyze the main performances of the resulting scheme. In Section 4, we explain the enhanced scalable unital-based construction that we propose and we analyze its different performances. In Section 5, we compare our approach to the existing ones regarding different criteria; we give and discuss theoretical and simulation results. In Section 6, we end up this paper with some conclusions.

2. Related Works: Key Management Schemes For WSNs

Key Management Schemes in WSNs have been extensively in the literature. The scheme is categories into two types probabilistics and deterministic schemes. In deterministic schemes, each two neighboring nodes are able to establish a direct secure link which ensures a total secure connectivity coverage. In probabilistic schemes, the secure connectivity is not guaranteed because it is conditioned by the existence of shared keys between neighboring nodes. We give in table I the definition of the five considered evaluation metrics, while we summarize in table II the main used symbols.

2.1. Probabilistic schemes

In probabilistic key management schemes, each two neigh- boring 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 Pre-distribution 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. Hence, a great number of links will be compromised.

Chan *et al.* proposed in [3] a protocol called Q-composite scheme that enhances the resilience of RKP. In this solution, two neighboring nodes can establish a secure link only if they share at least Q keys.

2.2. 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 $K_{i,j}$ and pre-loading each node with $(n-1)$ pair wise 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 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.

The Transitory key is used to generate a pair wise session keys is cleared from the memory of nodes by the end of a short time interval after their deployment. LEAP is based on the assumption that a sensor node, after its deployment, is secure during a time T_{min} and cannot be compromised during this period of time. LEAP is then secure as far as this assumption is verified.], Ç amtepe and Yener proposed to use combinato- rial design for key pre-distribution in WSN. They proposed a new deterministic key pre-distribution scheme based on Symmetric Balanced Incomplete Block Design (SBIBD). The proposed mapping from SBIBD to key pre-distribution allows to construct $m^2 + m + 1$ key rings from a key pool S of $m^2 + m + 1$ keys such that each key ring contains $k = m + 1$ keys and each two key rings shares exactly one common key .The main strength of the Ç

amtepe scheme is the total secure connectivity indeed each two nodes share exactly one comman key . However, the SBIBD scheme does not scale to very large networks. Indeed, using key rings of $m+1$ keys we can generate only $m^2 + m + 1$ key rings. SBIBD based key pre-distribution was also to guarantee intra-region secure communications in grid group WSNs.

In this work, we seek to design a scalable key management scheme which ensures a good secure coverage of large scales networks with a low key storage overhead. Basic schemes giving a perfect network resilience achieve a network scalability of $O(k)$ where k is the key ring size. The SBIBD and the trade based ones allow to achieve a network scalability of $O(k^2)$. In this work, we propose new solutions achieving a network scalability up to $O(k^4)$ when providing high secure connectivity coverage and good overall performances. For this purpose, we make use of the unital design theory in order to pre-distribute keys. We propose in what follows a basic mapping from unitals to key pre-distribution as well as an enhanced unital based scheme which achieves a good trade-off between scalability and connectivity.

3. Unital Design for Key Pre-Distribution in WSNs

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 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 B_j. The matrix M is then defined an incidence matrix of a 2-(9, 3, 1) *WSNs.*

In this subsection, we start by developing a simple scalable key pre-distribution scheme based on unital design that we de- note 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, refer- ring 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 pair wise key to secure the link; otherwise, nodes should determine secure paths which are composed of successive secure links.

3.1. Theoretical Analysis

1) storage overhead: When using the proposed naive unital based version matching a unital of order m, each node is pre- loaded with one key ring corresponding to one block from the design, hence, each node is pre-loaded with $(m + 1)$ disjoint keys. The memory required to store keys is then $l \times (m + 1)$ where l is the key size.

2) Network scalability: From construction, the total number of possible key rings when using the naive unital based schemes is n= $m \times (m+1) = m^2 \times (m^2 - m + 1)$, this is then the maximum number of supported nodes.

3) Direct secure connectivity coverage: When using the basic unital mapping, we know that each key is used in exactly m^2 key rings among the $m^2 \times (m^2 - m + 1)$ possible key rings. Let us consider two nodes u and v randomly selected. The node u is pre-loaded with a key ring KR_u of $m + 1$ different keys. Each of them is contained in $m^2 - 1$ other key rings among the possible $m^2 \times (m^2 - m + 1) - 1$ ones. Knowing that two pair of keys occurs together in exactly one block, we find that the blocks containing two different keys of KR_u are completely disjoint. Hence, each node shares exactly one key with $(m + 1) \times (m^2 - 1)$ nodes among the $m^2 (m^2 - m + 1) - 1$ other possible nodes, Then, the probability P_C of sharing a common key can be calculated as follows:

The evaluation of this naive solution shows clearly that:

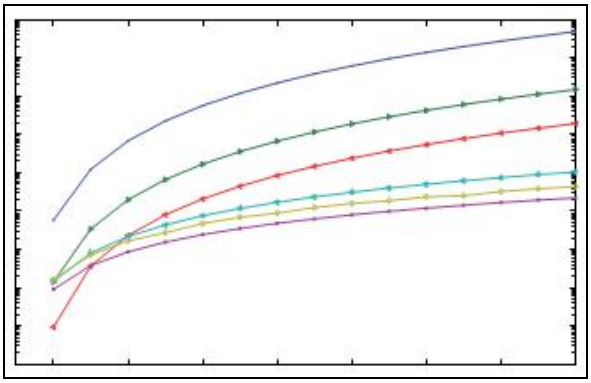

Figure Network scalability at equal key ring size

4. Performance Comparison

In this section, we compare the proposed unital-based schemes to existing schemes regarding different criteria.

4.1. Network scalability at equal key ring size

We compare the scalability of the proposed unital based schemes against that of the SBIBD-KP and the Trade-KP ones. The network scalability of the t-UKP schemes is computed as the average value between the maximum and the minimum scalability. The network scalability of the SBIBD-KP scheme is computed as $m^2 + m + 1$ where m is the SBIBD design order and $m + 1$ is the key ring size. We compute the salability of the Trade-KP scheme as $2q^2$ where q is the first prime power greater than the key ring size k, this value allows a achieve the best session key sharing probability using the Trade-KP scheme as we proved in . The figure shows that at equal key ring size, the NU-KP scheme allows enhancing greatly the scalability compared to the other schemes; for instance the increase factor reaches 10000 compared to the SBIBD-KP scheme when the key ring size exceeds 100. Moreover, the figure shows that the t-UKP schemes achieve high network scalability. We notice that the higher t is, the lower network scalability is. Nevertheless, 2- UKP and 3-UKP give better results than those of the SBIBD KP and the Trade-KP solutions. Even we choose $t = \sqrt{m}$ as we propose (UKP*), the network scalability is enhanced. For instance, compared to SBIBD-KP scheme, the increase factor reaches five when the key ring size equal to 150. W the same results separately with linear scales which illustrate clearly the network scalability enhancement when using our solutions.

The assess the network scalability of random schemes including the RKP and the Q-composite ones regarding to the desired network connectivity and to the net- work capacity to maintain secure links while some nodes are compromised. They defined for that a threshold fm called the *limited global payoff requirement.* The later can be explained as the level of compromise past where the adversary gains an unacceptably information on the other pair wise secret keys. Depending on P_c *and* fm they defined the maximum number supported network size. The authors of [3] present results for $P_c = 0.33$ and $fm = 0.1$ and show that the network scalability with a key ring size of 100 is about 300 for RKP scheme and between 600 and 700 when using Q-composite schemes. The scalability of the same schemes with a key ring size of 400 is respectively of about 1200 and between 2700 and 2800. We can see clearly that our solutions allow to reach much better network scalability than the random schemes under the suggested parameters.

4.2. Key ring size at equal network size

In this subsection, we compare the required key ring size when using the unital-based, the SBIBD-KP and the Trade- KP schemes at equal network size. We compute for each network size the design order allowing achieving the desired scalability and we deduce then the key ring size, the obtained results are reported in Figure 5. The figure shows that at equal network size, the NU-KP scheme allows to reduce the key ring size and then the storage overhead. Indeed the enhancement factor over the SBIBD-KP scheme reaches 20. When using the t-UKP schemes, the results show that the higher t is, the higher required key ring size is. However, this value remains significantly lower than the required key ring size of the SBIBD-KP and the Trade-KP schemes. Moreover, we can see clearly in the figure that at equal network size, the UKP* scheme provides very good key ring size compared the SBIBD-KP and the Trade-KP schemes. For instance, the key ring size may be reduced over a factor greater than two when using the UKP* compared to the SBIBD-KP scheme.

4.3. Energy consumption at equal network size

In this subsection, we compare the energy consumption induced by the direct secure link establishment phase. Since each node broadcasts its list of key identifiers to its neighbors, the energy consumption can be computed as:

$E = E_{tx} \cdot k \cdot log2\,(|S|) + \eta \cdot E_{rx} \cdot k \cdot log2\,(|S|)$

Where E_{tx} (resp. E_{rx}) is the average energy consumed by the transmission (resp. reception) of one bit, k is the key ring size, η is the average number of neighbors and $log_2(|S|)$ represents the size of a key identifier in bits that we round up to the nearest byte size.

We compare the energy consumption of our solutions against SBIBD-KP and Trade-KP the results plotted in equal network size, the NU-KP scheme consumes very small amount of energy to exchange the low number of key identifiers. We also note that the higher t is, the higher the consumed energy is. This is due to the increased number of stored keys and thereby the increased number of exchanged identifiers. Finally, the figure shows clearly that UKP* scheme consumes less energy than the SBIBD-KP and the Trade-KP schemes. This matches our expectation since the energy consumption is strongly correlated to the number of stored keys.

4.4. Network connectivity at equal key ring size

We compare in this subsection, the network secure connectivity coverage of the different schemes. First, we plot the key sharing probability when using the unital based schemes (NU-KP, t-UKP and UKP*). The figure shows that the NU-KP scheme provides a bad direct secure connectivity coverage which decreases significantly when the key ring size increases. Indeed, the key sharing probability is low and tends to $O(1)$ as k *tends* to infinity. Otherwise, they obtained results show that the higher t is, the better the direct secure connectivity coverage is. Indeed, loading nodes with many blocks from unital design allows increasing significantly the key sharing probability. The figure shows moreover that the UKP* scheme gives very good connectivity results. For instance, the direct secure connectivity coverage remains between 0.82 and 0.66 when the key ring size is between 10 and 150. As the key ring size is high, the direct secure connectivity of UKP* approaches $1 - e^{-1} \approx 0.632$ which we proved to be an approximate lower bound Although the unital-based scheme UKP* increases significantly the network scalability and provides a good key sharing probability greater than 0.632, this metric remains lower compared to SBIBD-KP which ensures a perfect key sharing probability equal to one. However, our scheme allows attending a total secure connectivity thanks to the secure path establishment.

We also studied the average secure path length when using different key pre-distribution schemes including our solutions. For this purpose, we conducted simulations while referring to the results given in order to construct a grid deployment model which guarantees the network physical connectivity and coverage. The results showed that the UKP* scheme provides a good average secure path length between 1.18 and 1.36 when the key ring size is between 10 and 150. It does not exceed 1.37 even the key ring size is very high. In others terms, when using the UKP* scheme, two-thirds of possible links in the network will be secured directly while practically all the other third links can establish a 2-hop secure path. We give some numerical results about the average secure path length in the last subsection.

5. Conclusion

We proposed, in this work, 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. We make use of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows to achieve high network scalability while giving a low direct secure connectivity coverage. We proposed then an efficient scalable unital-based key pre-distribution scheme pro- viding high network scalability and good secure connectivity coverage. We discuss the solution parameter and we propose adequate values giving a very good trade-off between network scalability and secure connectivity. We conducted analytical analysis and simulations to compare 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.

6. Acknowledgement

This work is made as part of the Picardie regional project under reference I159C. The authors wish to thank the Picardie regional council in France and the European Regional Development Fund (ERDF) for funding and supporting this project.

7. Network Resiliency of the Trade -Based Key (Pre -Distribution Scheme)

Using the Ruj *et al.* trade construction [8], the two sets T_1 and T_2 contain q^2 key rings each one. Let us assume that x nodes are compromised and let us compute the probability that a given pair of keys K_i and K_j is known (we recall that two nodes can establish a secure session key if they share exactly two common keys).

From construction, we know that each key occurs in exactly q blocks in T_1 and q blocks of T_2, and that each pair of keys occurs in one key ring from T_1 and one key ring from T_2. So, we find that among the $2q^2$ possible key rings, two contains the pair K_i and K_j, $2q-2$ contain only K_i, $2q-2$ contain only K_j and then $2q^2-4q+2$ do not contain any key of K_i and K_j

8. References

1. 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.
2. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 2002 ACM CCS, pp. 41–47.
3. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in IEEE SP, pp. 197–213, 2003.
4. 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.
5. C. Castelluccia and A. Spognardi, "A robust key pre-distribution pro- tocol for multi-phase wireless sensor networks," in Proc. 2007 IEEE Securecom, pp. 351–360.
6. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proc. 2003 ACM CCS, pp. 52–61.
7. Z. Yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in Proc. 2005 IEEE WCNC, pp. 1915–1920.
8. S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs," in Proc. 2011 IEEE INFOCOM, pp. 326–330