ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Unital Design Based Key Pre-Distribution Scheme for Wireless Sensor Networks

Suba.s, R.Jasmine Sugitha
Infant Jesus College of Engineering, Thoothukudi, Tamilnadu, India.

ABSTRACT-Given the sensitivity of the potential applications of wireless sensor networks, security emerges as a challenging issue in these networks. Because of the resource limitations, symmetric key establishment is one favorite paradigm for securing WSN. One of the main concerns when designing a key management scheme for WSN is the network scalability. In this paper, new highly scalable key establishment scheme was proposed for WSN. For that purpose, we make use, for the first time, of the unital design theory. The basic mapping from unitals to pair wise key establishment allows to achieve an extremely high network scalability while degrading, however, the key sharing probability. An enhanced unital-based pre-distribution approach was proposed which provides high network scalability and good key sharing probability. The obtained results show that our approach enhances considerably the network scalability while providing good overall performances. Our solutions reduce significantly the storage overhead at equal network size compared to existing solutions.

INDEX TERMS—Wireless sensor networks, security, key management, network scalability, resource optimization.

I. Introduction

Nowadays, wireless sensor networks (WSN) are increasingly used in numerous fields such as military, medical and industrial sectors; they are more and more involved in several sensitive applications which require sophisticated security services [1]. Due to the resource limitations, existing security solutions for conventional networks could not be used in WSN. So, the security issues became then one of the main challenges for the resource constrained environment of WSN.

The establishment of secure links between nodes is then a challenging problem in WSN. The public key based solutions, which provide efficient key management services in conventional are unsuitable for WSN because of resource limitations. Some public key schemes have been implemented on real sensors [2][3][4], however most researchers believe that these techniques are still too heavyweight over actual sensors'
technology because they induce an important communication and computation overhead [5]. Symmetric key establishment is then one of the most suitable paradigms for securing exchanges in WSN.

In this Paper we are interested in particular in the scalability of symmetric key pre-distribution schemes. Existing research works either allow supporting a low number a nodes or degrading the other network performances including resiliency, connectivity and storage overhead when the number of nodes is important. In contrast to these solutions, our goal is to enhance the scalability of WSN key management schemes without degrading significantly the other network performances. To achieve this goal, we propose to use, for the first time, the unital design to construct and pre-distribute key rings. First, we explain the unital design and we propose a basic mapping from unitals to key pre-distribution for WSN.

Analytic calculations that the resulting basic scheme allows to achieve extremely high network scalability while degrading, however, the key sharing probability.

For this, we propose an enhanced unital-based construction in order to maintain a good key sharing probability while enhancing the network scalability. We carried out analytic calculations and simulations to compare the efficiency of the enhanced proposed approach against basic schemes with respect to important performance criteria: storage overhead, network scalability, session key sharing probability and average secure path length. The obtained results show that at equal key ring size, our approach enhances considerably the network scalability while providing good overall performances. Moreover, we show that given a network size, our solutions reduce significantly the key ring size and then the storage overhead compared to existing solutions.

The remainder of this paper is organized as follows We define in section 2 the metrics used to evaluate and compare key pre-distribution schemes and we summarize the used symbols. Section 3 presents some related works. We give in section 4 a background on unital design while we present, in section 5, the basic mapping to key pre distribution and analyze the performances of the resulting scheme. In section 6, we present the enhanced unital-based construction. In section 7, we evaluate the performances of the enhanced scheme and compare it to the existing ones with respect to various performance criteria; we provide and discuss theoretical and simulation results. Finally, section 8 ends up this paper with some conclusions and future works.

II. RELATED WORKS

Key management problem in WSN has been extensively studied in the literature and several solutions have been proposed. Many classifications of existing symmetric key management schemes can be found in [6][7][8]. Eschenauer and Gligor proposed in [9] 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 exchanges with each of its neighbors the list of key identifiers that it maintains in order to identify the common keys. 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, if neighboring nodes do not have common keys, they should determine secure paths which are composed of successive secure links. 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 [10] the Q-composite scheme which enhances the resilience of RKP. In this solution, two neighboring nodes can establish a secure link only if they share at least Q keys. The pair wise session key is calculated as the hash of all shared keys concatenated to each other. This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link. However, this approach degrades the probability of session key sharing neighboring nodes must have at least Q common keys to establish a secure link.

Chan et al. proposed also in [10] a perfect secure pair wise key pre-distribution scheme where they assign to each possible link between two nodes i and j a distinct key ki,j. Prior to deployment, each node is pre-loaded with p*n keys, where n is the network size and p is the desired secure coverage probability. Hence, the probability that the key ki,j belongs to the key set of the node i is p. Since we use distinct keys to secure each pair wise link, the resiliency against node capture is perfect and any node. that is captured reveals no information about links that are not directly connected to it. The main drawback of this scheme is the non scalability because the number of the stored keys depends linearly on the network size. In addition, this solution does not allow the node post-deployment because existing nodes do not have the new nodes' keys.

Du et al. proposed in an enhanced random scheme assuming the node deployment knowledge. Nodes are organized in regional groups to which is assigned different key pools and each node selects its k keys from the corresponding key pool. The key pools are constructed in such a way that neighboring ones share more keys while pools far away from each other share fewer keys. This approach allows to enhance the probability of sharing common keys because the key pools become smaller. Moreover, the network resiliency is improved since if some nodes of a given region are captured, the attacker could discover only a part of the corresponding group key pool. However, the application of this scheme is restrictive since the deployment knowledge of a WSN is not always possible.

Liu and Ning proposed a new pool based polynomial pre-distribution scheme for WSN. This approach can be considered as an extension of the basic RKP scheme where nodes are pre-loaded with bivariate polynomials instead of keys. A global pool of symmetric bivariate polynomials is generated off-line and each node is preloaded with a subset of polynomials. If two neighboring nodes share a common polynomial, they establish a direct secure by computing the polynomial value at the neighbor identifier; else, they try to find a multi-hop secure path. This approach allows computing distinct secret keys, so the resilience against node capture is enhanced. However, it requires more memory to store the polynomials and induces more computational overhead. Yu and Guan [14] used the Blom's scheme to key pre-distribution in group-based WSN.

Liu et al. proposed in SBK, a self-configuring key establishment scheme for WSN. SBK distinguishes two kinds of nodes: service nodes and worker ones. After the deployment, sensor nodes differentiate their role thanks to a pre-loaded bootsrap program. Service nodes generate a key space using a polynomial-based or the matrix-based model. Then, they distribute the corresponding keying shares to at most worker nodes. Authors propose for that to use a computationally asymmetric channel based on Rabins public key cryptosystem while shifting the large amount of computation overhead to the service nodes. This induces a high load on service nodes which are sacrificed. SBK assumes that all nodes are deployed at the same time and that they are coarsely time synchronized to to start the bootstrapping procedure simultaneously. it assumes also that the network is secured and no active attacks can be launched during the bootstrapping procedure. SBK gives good performances including scalability, resilience and connectivity between worker nodes as far as the assumptions are verified.Deterministic key pre-distribution schemes ensure that each node is able to establish a pair-wise key with all its neighbors.

LEAP makes use of a common transitory key which is preloaded into all nodes prior to deployment of the WSN. The transitory key is used to generate pairwise session keys and 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.

In new key management scheme for grid group WSN. Intra-region secure communications are guaranteed thanks to a SBIBD key pre-distribution while inter-region communications are ensured by special nodes called agents. Furthermore, authors propose to enhance the Camtepe scheme in order to avoid key identifier exchanges. For that, they index all nodes and keys and propose a mapping between node indexes and key indexes.

The main strength of the proposed scheme is the establishment of unique secret pairwise keys between connected nodes. However, this does not ensure a perfect network resilience. Indeed, the attacker may construct a part of the global set of keys and then compute pairwise secret keys used to secure external links where the compromised node are not involved. Moreover, the proposed scheme provides a low session key sharing probability which does not exceed 0.25 in the best case as we prove later. Another drawback of this solution is the network scalability which reaches only 2q2 = O(k2) where k is the key ring size.

We focus in this work on the scalability of key management schemes for WSN. Basic schemes giving a perfect network resilience [10] achieve a network scalability of O(k) where k is the key ring size. Design based schemes as the SBIBD and the trade based ones allow to achieve a network scalability of O(k2). So, large scale networks cannot be supported because the key ring size may be increased which is not suitable due to memory constraints in WSN. In this work we propose new solutions achieving a network scalability of O(k4) when providing good overall performances. For this purpose, we make use, for the first time, of the unital design in order to predistribute keys. We show that the basic use of unital design enhances considerably the scalability of key pre-distribution while decreasing the probability of sharing common keys. we propose a solution which ensures high network scalability while maintaining a good probability of sharing common keys.

.

III. A BASIC MAPPING FROM UNITALS TO KEY PRE-DISTRIBUTION FOR WIRELESS SENSOR NETWORK

At the best of our knowledge, we are the first who propose the use of unital design for pre-distribution in WSN. This scheme may also be generalized to all resource constrained wireless networks where key pre-distribution should be useful. In this section, develop a naive and scalable key pre-distribution scheme based on unital design. 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, $n = b = m^2 (m^3 + 1)/(m+ 1)$ key rings of $k = m + 1$ keys each one.

TABLE I
MAPPING FROM UNITAL DESIGN TO KEY DISTRIBUTION

UNITAL DESIGN	KEY DISTRIBUTION
X: Point Set	S : Key Pool
Blocks	Key Rings(<KR_i>)
Size of the Object Set X : $V=m^3+1$	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 : $n=m^2(m^2-m+1)$

After the deployment step, each two neighboring nodes exchange their key identifiers in order to determine 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 keys 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. 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 × (m + 1) where l is the key size.

B. Network Scalability

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

C. Session Key Sharing Probability

When using the basic unital mapping, we know that each key is used in exactly m2 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 preloaded with a key ring KRu of m+1 different keys. Each of them is contained in $m^2 - 1$ other key rings. Knowing that each two keys occur together in exactly one block, we find that the blocks containing two different keys of KRu 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 Pc of sharing a common key is of them is contained in $m^2 - 1$ other key rings. Knowing that each two keys occur together in exactly one block, we find that the blocks containing two different keys of KRu 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 Pc of sharing a common key is :

$$P_c = \frac{(m+1)^2}{m^3+m+1}$$

D. Summary and Discussion

The evaluation of this naive solution shows clearly that the basic mapping from unitals to key pre-distribution improves greatly the network scalability which reaches O(k4) compared to other schemes like SBIBD and trade ones having a scalability of O(k2) where k is the key ring size. Moreover, given a network size n this naive scheme allows to reduce the key ring size up to$\sqrt[4]{n}$. However, this naïve solution degrades the key sharing probability which tends to O(1/k). In order to improve the key sharing probability of the naive unital based scheme while maintaining a good scalability improvement, we propose in the next section an enhanced construction for key management schemes based on unital design.

IV. A NEW SCALABLE UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME FOR WSN

In this section, we present a new enhanced unital-based key pre-distribution scheme for WSN. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build blocks using unital design and to pre-load each node with a number of blocks picked in a selective way. Before the deployment step, we propose to generate blocks of a m order unital design, each block matches a key set. We propose then to pre-load each node with t completely disjoint blocks, t is then a protocol parameter that we will discuss later. The aim of our construction is to enhance the key sharing probability between neighboring nodes and then decrease the average secure path length as we show later. We propose in algorithm 1 a random block distribution allowing to pre-load t disjoint blocks in each sensor node.

```
Step 1: Generate B = <$B_q$>, Key Sets
        corresponding to Blocks of a Unital
        Design of order m
Step 2: for each $Node_i$ do
Step 3: $KR_i = \{\}$
Step 4: while ($KR_i \leq t(m+1)$) do
Step 5: pick $B_q$ from B
Step 6: if ($KRi \cap B_q$) = $\varphi$ then
Step 7: $KR_{i\,=} KR_i \cup B_q$
Step 8: $B = B\text{-}B_q$
Step 9: end
```

Algorithm 1: A random approach of unital block pre-distribution in the enhanced unital-based scheme

After the deployment step, each two neighbors exchange their key identifiers in order to determine common keys. Contrary to the basic approach, each two nodes may share more than one key when using the proposed construction. Indeed, each node is pre-loaded with t disjoint blocks which mean that each two nodes share up to t2 keys. If two nodes share one or more keys, we propose to compute the pair wise secret key as the hash of all their common keys concatenated to each other. The used hash function may be *SHA-1* [24] for instance. This approach allows enhancing the network resiliency since the attacker needs 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 enhanced version is the improvement of the key sharing probability. As we will show later, this approach allows to achieve a high secure connectivity coverage since each node is pre-loaded with t disjoint blocks. Moreover, this approach increases resiliency through the composite pairwise secret keys witch reinforce secure links. In addition, we show that we maintain high network scalability compared to existing solutions although it remains lower than that of the naive version.

V. CONCLUSION

In this paper, a new highly scalable key pre-distribution scheme for WSN. We make use, for the first time, of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows to achieve an extremely high network scalability while degrading the key sharing probability. We proposed then an enhanced unital-based construction which gives birth to a new key management scheme providing high network scalability and good key sharing probability. We conducted analytic calculation and intensive simulations to compare our solutions to existing ones which showed that our approach enhances significantly the network scalability when providing good overall performances. As future work, we plan to deepen the analysis of our parameter choice in order to suggest values given the best tradeoff. In addition, we attend to analyze more network performances of our solution like the network resilience against node capture attacks.

REFERENCES

[1] B. Maala, Y. Challal, and A. Bouabdallah, "*Hero: Hierarchcal Key Management Protocol for Heterogeneous WSN*," in Proceedings IFIP WSAN,pp.125-136,2008

[2] 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.

[3] D. Liu and P. Ning, *"Establishing Pair Wise Keys in Distributed Sensor Networks*," in Proc. 2003 ACM CCS, pp. 52–61.

[4] H. Chan, A. Perrig, and D. Song, *"Random Key Predistribution Schemes for Sensor Networks," in IEEE* SP, pp. 197–213, 2003.

[5] 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.

[6] S. Ruj and B. Roy, *"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.

[7] 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.

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

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

[10] 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.