A new Highly Scalable Key Pre-distribution scheme for WSN

Walid Bechkit, Abdelmadjid Bouabdallah, Yacine Challal

A New Highly Scalable Key Pre-distribution Scheme for WSN

Walid Bechkit *, Abdelmadjid Bouabdallah * and Yacine Challal *
* Compiegne University of Technology , HeuDiaSyc laboratory, UMR CNRS 6599, Compiegne, France

***Abstract*—We propose in this paper a new highly scalable key management scheme for WSN. We make use, for the first time, of the unital design theory for key pre-distribution in WSN. We propose a naive mapping from unitals to key pre-distribution as well as an enhanced unital-based key management scheme. We analyze our solution and compare it to basic approaches; results show that our scheme enhances considerably the network scalability while providing good overall performances.**

***Index Terms*—WSN, security, key management, scalability.**

I. Introduction & main related work

Given the sensitivity of the potential applications of WSN, a large scale deployment of this technology relies on the provided dependability. Particularly, security emerges as a challenging issue in WSN because of the resource limitations and the lack of infrastructure. Key management is one of the required building blocks of many security services. Because of resource limitations, symmetric key establishment is one of the favorite paradigms for securing WSN. Many symmetric key management schemes for WSN were proposed in the literature.

In *probabilistic* schemes, the secure link establishment is conditioned by the existence of shared pre-loaded keys. In the basic Random Key Pre-distribution scheme (RKP) [1], each node is pre-loaded with a key ring of keys randomly selected from a large key pool. After the deployment step, neighboring nodes exchange key identifiers to determine the common keys; one of these common keys is then used as the session secret key. Chan et al. proposed in [2] the q-composite scheme where two neighboring nodes can establish a secure link only if they share at least q keys. The pairwise session key is calculated as the hash of all shared keys concatenated to each other.

Deterministic schemes ensure that each node is able to establish a pairwise key with each of its neighbors. In [3], authors proposed a deterministic pool based key pre-distribution scheme. Instead to randomly select a subset of keys from the global key pool like in RKP, they use the Symmetric Balanced Incomplete Block Design theory (SBIBD) to construct key rings in such a way each two key subsets share exactly one common key. In [4], authors propose a new key management scheme for grid group WSN. Intra-region secure communications are guaranteed using SBIBD theory while inter-region communications are ensured by special nodes called agents.

Existing research works either support a low number a nodes or degrade the other network performances including connectivity, resiliency and storage overhead when the number of nodes is important. Our goal is then to enhance the network scalability without degrading the other performances. For that purpose, we make use of the unital design theory to construct and pre-distribute key rings and we propose an enhanced unital-based solution which increases considerably the network scalability while providing good overall performances.

II. Unital design & Naive Key Establishment

In combinatorics, the design theory deals with the existence and construction of systems of finite sets whose intersections have specified properties. A *unital* design is a Steiner 2-design which consists of a set of $b = m^2(m^3+1)/(m+1)$ subsets called *blocks* of a set of $v = m^3+1$ points. Each block contains $k = m+1$ points and each point is contained in $r = m^2$ blocks. Each pair of points is contained together in exactly one block. We note a unital as a $(m^3+1, m+1, 1)$ design. Without loss of generality, we focus in this work on *Hermitian unitals* which exist for all m a prime power. Construction details can be found in [5] knowing that other constructions for m not necessary a prime power exist in the literature.
A unital may be represented by its $v \times b$ incidence matrix that we call M where rows represent the points P_i and columns represent the blocks B_j. Hence, $M_{ij} = 1$ if $P_i \in B_j$ and 0 otherwise. For instance, we illustrate in figure 1 an incidence matrix of a (9,3,1) hermitian unital.

First, let us use the unital design to pre-distribute keys in a naive way. 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 key ring. We can then generate from a global key pool of $|S| = m^3+1$ keys, $n = m^2(m^3+1)/(m+1)$ key rings of $m+1$ keys each one. Before the deployment step, the unital blocks matching key rings are generated, and each node is pre-loaded with a distinct key ring as well as the key identifiers. After the deployment, nodes exchange their key identifiers to determine the eventual shared key. We proved that each two key rings share at most one common key.

Storage overhead: When using the naive unital-based key pre-distribution (NU-KP) approach, each node is pre-loaded with one key ring corresponding to one block from the unital, hence, each node is pre-loaded with $(m+1)$ disjoint keys and their identifiers.

Network scalability: From construction, the total number of possible key rings when using the naive approach is $n = \frac{m^2 \times (m^3+1)}{(m+1)} = m^2 \times (m^2-m+1)$ which is then the maximum number of supported nodes. The network scalability is then extremely enhanced and tends to $O(m^4)$ which is very high compared to other schemes. For instance, the SBIBD scheme [3] allows to reach a network scalability of $O(m^2)$ at equal design order and then at equal key ring size.

Probability of key sharing: We calculated the key sharing probability when using the NU-KP scheme and found that it is equal to $P_c = \frac{(m+1)^2}{m^3+m+1}$. This probability is low and tends to $O(\frac{1}{m})$ when m is high.

In order to improve the key sharing probability while maintaining high network scalability, we propose in the next section an enhanced unital-based key pre-distribution approach.

$$\begin{pmatrix}
1 & . & . & . & . & 1 & 1 & . & . & . & 1 & . \\
. & . & . & . & . & 1 & . & 1 & 1 & 1 & . & . \\
. & . & 1 & 1 & . & . & 1 & 1 & . & . & . & . \\
1 & . & . & 1 & 1 & . & . & . & 1 & . & . & . \\
. & . & . & . & 1 & . & 1 & . & . & 1 & . & 1 \\
. & . & 1 & . & . & . & . & . & 1 & . & 1 & 1 \\
. & 1 & 1 & . & 1 & 1 & . & . & . & . & . & . \\
1 & 1 & . & . & . & . & . & 1 & . & . & . & 1 \\
. & 1 & . & 1 & . & . & . & . & . & 1 & 1 & .
\end{pmatrix}$$

Fig. 1. Incidence matrix of a (9,3,1) unital

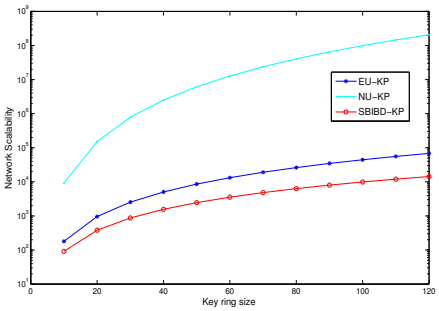

Fig. 2. Netw. scalability at equal key ring size

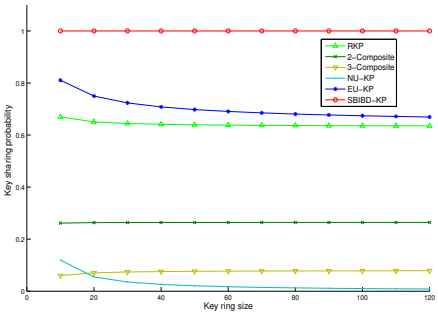

Fig. 3. Key sharing prob. at equal key ring size

III. A NEW SCALABLE UNITAL-BASED KEY MANAGEMENT SCHEME FOR WSN

We propose in what follows a new enhanced unital-based key pre-distribution (EU-KP) scheme for WSN. For the sake of brevity, we give an overview of the construction and the key pre-distribution and we highlight the main results. Without loss of generality, we suppose that the unital order m is a perfect square, if it is not the case, we can refer to the nearest integer greater than the square root of m.

Before the deployment step, we propose to generate blocks of a unital design of order m. We propose then to pre-load each node with $\sqrt{m}$ blocks. The latter are picked in a selective way to be *completely disjoint*. After the deployment step, nodes exchange their key identifiers to determine the common keys. Unlike the basic approach, each two nodes may share between zero and m keys. If two neighboring nodes share one or more keys, we compute the pairwise key as the hash of all their common keys concatenated to each other, this may enhance the network resiliency. Otherwise, neighboring nodes should establish a secure path composed of successive secure links.

Storage overhead: When using the EU-KP approach based on a unital design of order m, each node is pre-loaded with $\sqrt{m}(m+1)$ distinct keys as well as their identifiers.

Network scalability: We calculated the network scalability when using our construction and we found that it is equal to $n = m\sqrt{m}(m^2 - m + 1)$. In figure 2, we compare the scalability of the EU-KP approach to that of the NU-KP and the SBIBD-KP ones at equal key ring size. The figure shows that the naive approach allows to enhance greatly the scalability compared to the SBIBD-KP scheme; the increase factor reaches 10000 when key ring size exceeds 100. Moreover, the figure shows that the EU-KP scheme increases significantly the network scalability compared to SBIBD-KP scheme. For instance, the increase factor reaches five when key ring size is above 100. Otherwise, the obtained results show that at equal network scalability, the key ring size may be reduced over a factor of two when using the EU-KP scheme. Indeed, we reach approximately the same network scalability when using the SBIBD-KP with key ring size equal to 120 and when using the EU-KP with a key ring size of 60.

Probability of key sharing: We calculated the key sharing probability when using the EU-KP approach and we found that is equal to: $P_c = 1 - (1 - \frac{(m+1)^2}{m^3+m+1})^m$. We proved that this ratio tends to $L = 1 - e^{-1} \approx 0.6321$ as m approaches infinity, the probability of key sharing is then always greater than L. We plot in figure 3 the key sharing probability of the different schemes. 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 $O(\frac{1}{m})$. Otherwise, the figure shows that the key sharing probability of the EU-KP scheme remains high even with high value of m and tends to the lower bound L as m approaches infinity. The figure show also that the EU-KP approach provides a better probability of key sharing than the RKP scheme [1] and much better than the q-composite ones [2]. We calculated the key sharing probability of random schemes when the key pool size is equal to the square of key ring size.

In addition to the fact that the EU-KP approach increases significantly the network scalability, it has a good key sharing probability which, however, remains lower than that of the SBIBD-KP scheme. Nevertheless, our scheme allows to reach a total secure connectivity coverage thanks to the secure path establishment. We found that the average secure path length is about 1.33 under realistic deployment conditions. This average value does not exceed 1.39 even the case of a low density.

We compared finally the resiliency of EU-KP scheme to that of the SBIBD-KP one and found that our solution enhances this metric up to 22%. Indeed, using our scheme, neighboring nodes may share many keys which are used to secure links. Attacker need then more overlap keys to break secure links.

IV. CONCLUSION

We proposed a new scalable key management scheme for WSN. We make use of the unital design theory and we proposed a naive mapping to key pre-distribution as well as an enhanced one. We showed that our scheme enhances considerably the scalability while providing good overall performances.

REFERENCES

[1] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In *ACM CCS '02*, pages 41–47, 2002.

[2] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE SP '03*, 2003.

[3] S. A. Çamtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 15:346–358, April 2007.

[4] Sushmita Ruj and Bimal Roy. Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks. *ACM Trans. Sen. Netw.*, 6:4:1–4:28, January 2010.

[5] Jennifer D. Key. Some applications of magma in designs and codes: Oval designs, hermitian unitals and generalized reed-muller codes. *J. Symb. Comput.*, 31(1/2):37–53, 2001.