Quick Spread to Remote Joint Groups Scheme for Wireless Sensor Networks

L.Dhananjaya reddy¹, B.Madhubabu², M.Giri³
M.Tech Scholar¹, Assistant Professor², Head and Professor³
Dept of CSE, SITAMS, Chittoor, A.P, India.

Abstract

We get around these obstacles and close this gap by proposing a novel key management pattern. The new pattern is a hybrid of usual broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any proposed subgroup chosen in an ad hoc way. Following this model, we instantiate a scheme which is confirmed secure in the standard model. Even if all the non-intended members plan, they cannot extract any useful information from the transmitted messages. After the public group encryption key is extracted, both the calculation overhead and the communication cost are independent of the group size. Further, our scheme facilitates simple yet efficient member deletion/addition and flexible rekeying strategies. Its strong security against collusion, its constant overhead, and its implementation friendliness without relying on completely trusted authority render our protocol a very promising solution to many applications. 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 attain 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 superior key sharing probability approximately lower bounded by $1 - e^{-t} \approx 0.632$. We conduct approximate analysis and simulations and compare our solution to those of existing methods for dissimilar criteria such as storage overhead, network scalability, network connectivity, average secure path length and network resiliency. Our consequences 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.

KEY WORDS: Ad hoc networks, cooperative computing, access control, information security, key management. Wireless sensor networks, security, network scalability, secure connectivity coverage.

INTRODUCTION

In many newly rising networks, there is a need to broadcast to remote supportive groups using encrypted transmission. Examples can be found in access control in remote group communication arising in wireless mesh networks (WMNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), etc.

A MANET is a system made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an efficient networking system facilitating data exchange between mobile devices even without fixed
infrastructures. In MANETs, it is important to support group-oriented applications, such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. Nowadays, wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the compassion of these applications, complicated security services are required. Key management is a cornerstone for many security services such as confidentiality and authentication which are required to safe communications in WSNs.

The organization of secure links between nodes is then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most appropriate 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[2][3][4][5][6][7][8][9][10][11][12] Nevertheless, in most existing solutions, the design of key rings (blocks of keys) is strongly connected 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 humiliating the other network performance metrics. For this purpose, we target the design of a scheme which ensures a good quality 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.

Certainly, 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-allocation scheme that maintains a good key sharing probability while enhancing the network scalability. A beginning work and few discussions were presented in [13]. 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 fundamental 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 a background on unital design and we propose a basic mapping from unitals to key pre-distribution for WSNs, we examine the main performances of the resulting scheme. we explain the improved scalable unital-based construction that we propose and we analyze its different performances. we compare our approach to the existing ones concerning different criteria; we give and discuss theoretical and replication results. we end up this paper with some conclusions.

In existing system, In this paper, we circumvent these obstacles and close this gap by proposing a novel key management paradigm. The new paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any proposed subgroup chosen in an ad hoc way. Following this model, we instantiate a scheme which is confirmed secure in the standard model. Even if all the non-intended members plan, they cannot extract any useful information from the transmitted messages.

After the public group encryption key is extracted, both the computation overhead and the statement cost are independent of the group size. Further, our scheme facilitates simple yet efficient member deletion/addition and flexible rekeying strategies. Its strong security against complicity, its constant overhead, and its implementation friendliness without relying on a fully trusted authority provide our protocol a very promising solution to many applications.

PROPOSED MODULE

WSN 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 humiliate 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 to cope with the scalability and connectivity issues.

We propose finally an enhanced

unital-based scheme which achieves an excellent trade-off between scalability and connectivity.
Background: Unital Design

In combinatorics, the design theory deals with the existence and construction of systems of finite sets whose intersections have specified arithmetical properties. Formally, A t-design (ν, b, r, k, λ) is defined as follows: Given a finite set X of ν points (elements), we construct a family of b subsets of X, called blocks, such that each block has a size k, each point is restricted 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 \( ν = b = m^2 + m + 1 \), \( r = k = m + 1 \) and \( λ = 1 \).

A Unital design is an Steiner 2-design which consists of \( b = m^2 + m + 1 \) blocks, of a set of \( ν = m^2(m^2 + 1)/(m+1) = m^2(m^2 + 1) \) points\(^{[19]}\). Each block contains \( m+1 \) points and each point is contained in \( r = m \) blocks. Each pair of points is contained together in exactly one block. We denote the Unital by \( (m^2 + m + 1, m^2 + m + 1, 1) \) or \( (m+1, m+1, 1) \) design for simplicity sake. Without loss of simplification, we focus in this paper on 3 Hermitian unital which exist for all \( m \) a major power. Other construction for \( m \) not necessarily a prime power exists in literature \([19]\). Some Hermitian unital construction approaches were proposed in literature \([20]\), \([21]\).

A unital may be represented by its \( v \times b \) incidence matrix that we call M. In this matrix rows represent the points P and columns represent blocks B. The matrix M is then defined as:

\[
M_{ij} = \begin{cases} 
1 & \text{if } P_i \in B_j \\
0 & \text{otherwise}
\end{cases}
\]

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.

B. 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 inexperienced unital-based key pre-distribution scheme. We propose a basic mapping in which we connect to each point of the unital a separate 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 produce 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 to determine eventual common key. Using this basic approach, each two nodes share at most one common key. Certainly, referring to the unital properties, each pair of points is contained together in precisely one block which implies that two blocks cannot share more than one point. Hence, if two neighboring nodes share one ordinary key, the latter is used as a pair wise key to secure the link; otherwise, nodes should decide secure paths which are composed of successive secure links.

C. Theoretical analysis

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

2) Network scalability: From construction, the total number of possible key rings when using the naive unital based scheme is

\[
 n = \frac{n^2 \times (m^2 + 1)}{(m+1)} = m^2 \times (m^2 - m + 1)
\]

is then the maximum number of supported nodes.

3) Direct secure connectivity coverage: When using the essential 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. significant that two pair of keys occurs together in exactly one block, were absolutely disjoint. Hence, each node shares exactly one key 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 \(m2(m2-m+1)-1\) other possible nodes. Then, the probability \(P\) of sharing a common key can be intended as follows:

\[
P_c = \frac{(m + 1) \times (m^2 - 1)}{m^2(m^2 - m + 1) - 1} = \frac{(m + 1)^2}{m^3 + m + 1}
\]

The appraisal of this naive solution shows clearly that the basic mapping from unital to key pre-distribution gives a high network scalability which reaches \(O(k^4)\). Moreover, given a network size \(n\), this naive scheme allows to decrease the key ring size up to \(\sqrt{n}\). However, this naive solution results a low key sharing probability which tends to \(O(\frac{1}{k})\). In order to improve the key sharing probability while maintaining a good scalability improvement, we propose in the next section an better scalable and efficient unital-based key pre-distribution for WSNs.

**PERFORMANCE COMPARISON**

Network scalability at equal key ring size

In this section, we evaluate the proposed unital-based schemes to existing schemes regarding different criteria. We compare in 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 scalability of the Trade-KP scheme as \(2q^{2k}\) where \(q\) is the first prime power greater than the key ring size \(k\), this value allows a attain the best session key sharing probability using the Trade-KP scheme as we proved in [13].

The figure shows that at equal key ring size, the NU-KP scheme allows to improve 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 \(t\)-UKP schemes achieve a high network scalability. We notice that the higher \(t\) is, the lower network scalability is. Nevertheless, 2UKP and 3-UKP give better results than those of the SBIBDKP and the Trade-KP solutions. Even we choose \(t = \sqrt{m}\) as we propose (UKP*), the network scalability is improved.

For instance, compared to SBIBD-KP scheme, the increase factor reaches five when the key ring size equal to 150. We plot in the same results separately with linear scales which illustrate clearly the network
scalability enhancement when using our solutions.

**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 calculate for each network size the design order allowing to attain the desired scalability and we deduce then the key ring size, the obtained results are reported in figure. The figure shows that at equal network size, the NU-KP scheme allows to reduce the key ring size and then the storage overhead. certainly 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 obviously 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.

![Network scalability at equal key ring size.](image)

**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 intend 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 providing 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 study and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure reporting of large scale networks while providing good overall performances.

**REFERENCES**


