Short Communication

U-Key: A Secure Unital-Based Wireless Sensor Network

Kochurani Jacob*, Maria Siby, Riya Mathew Mannoor, Tibin Thomas and Elisabeth Thomas
Department of Computer Science and Engineering, Amal Jyothi College of Engineering, Kanjirapally, Kerala, India
kochuranijacob@cs.ajce.in

Available online at: www.isca.in, www.isca.me
Received 18th April 2016, revised 5th August 2016, accepted 14th August 2016

Abstract

Wireless sensor network emerges as the backbone of the next generation technologies. The sensor nodes in the network have limited resources, which arise network scalability and security issues. The symmetric key establishment technique used for establishing connections in WSN limits the network scalability. If we distribute the keys to the nodes in advance the scalability could be increased. The unital design theory could be used for this purpose by mapping the unitals to pair wise keys. Although this could increase the scalability of the network, the key sharing probability decreases. An enhanced unital based technique could be used to increase the scalability without decreasing the key sharing probability. The U-key network is able to achieve good scalability level without compromising the performance and security of the network.

Keywords: WSN, Scalability, Symmetric key, Unital design, Key distribution, Security.

Introduction

There have been multitudes of developments in the field of wireless sensor network. These networks are mainly used to monitor several physical and environmental conditions. Most of the developments of WSN were motivated by military, industrial and consumer applications. Since these networks are widely used in so many critical fields, its security is important. The nodes in the WSN have limited physical resources which in turn limits their network capabilities. This limitation also affects the security that can be implemented in this system.

To secure communications in networks, key management scheme is used. This provides security services such as confidentiality and authentication. Conventional networks use public key based solutions for efficient key management. But the resource limitations in the nodes of WSN hinder the public key based key management scheme. An ideal solution for this is to implement symmetric key establishment technique. Symmetric key establishment requires initial exchange of a shared key which provides integrity. To exchange keys in a private manner between the nodes it will need a trusted third party. This is not feasible in case of WSN due to lack of infrastructure.

Hence the most effective mechanism for key establishment in WSN is to use key pre-distribution. Here the keys are distributed to the nodes before deployment of the network. After deployment the nodes build up the network using the pre-distributed secret keys. Key pre-distribution involves three phases. During the key distribution phase the keys are generated and placed in the sensor nodes. The shared key discovery phase searches for common shared keys between a pair of nodes in the network and communication link is established between these nodes. The path key establishment phase connects these links and establishes paths to create a connected graph. This generates a WSN networks which is based on this pre-distributed keys.

The scalability of network is critical in case of wireless sensor networks. Increasing the scalability decreases the network performance of nodes in WSN.

We need to improve the scalability of network, without considerably decreasing the network performance of nodes. For this we use unital design theory to construct and pre-distribute keys. To maintain a good key sharing probability an enhancement is added to the basic unital design.

Related Work

The most prominent issue related with WSN network is the key management problem. Random Key Pre-distribution (RKP) was one of the earliest solution to this which is a symmetric key management scheme. In this a key ring of *k* keys is selected randomly from a pool of keys and is distributed to each node. But, if any corruption occurs in the network, an attacker can easily get access to a part or the whole key pool.

Further many schemes were proposed to overcome the key management problem of WSN. A prominent scheme among them is Symmetrical Balanced Incomplete Block Designs (SBIBD). BIBD is a set of *k* distinct element subsets of X, called blocks. In SBIBD each block contains *k* elements, each element occurs in exactly *k* blocks, there is an intersection of elements in each pair of blocks .These schemes require an increase in key size to enhance the scalability of network.

But this is not feasible due to memory constraints. A solution is needed which provides good key sharing probability while increasing the network scalability.

Unital Design Overview

The unital design theory involves systems of finite sets which on intersection have numeric properties. The unital set t(v,b,r,k,λ) is a finite set X of v points(elements),b subsets of X, called blocks, each block of size k. The each point of the set is contained together in r blocks and each t points are contained together in λ blocks. 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 consists of blocks $b= m^2(m^3+1)/(m+1)$ contains m+1 points and set of points $v= m^3+1$ where each point is in $r=m^2$ blocks. We note the Unital as a 2-design $(m^3+1,m^2(m^3+1), m^2,m+1,1)$ or as $(m^3+1,m+1,1)$ for simplicity sake. Each pair of the points is contained in one block.

Unitals to Key Pre-Distribution Mapping

For pre-distribution of keys in WSN, unital design theory is used. We could use this theory for any applications which are resource limited or which uses pre –key distribution. It is a scalable pre-distribution scheme based on mapping of unitals to key pre-distribution. Here a distinct key is corresponded to each point of the unital, to the global set of points we associate the key pool and to each block a node key ring. From a global key pool of $|S| = m^2 + 1$ keys we generate $n = b = m^2(m^3 + 1)/(m+ 1)$ key rings of $k = m + 1$ keys. Table 1 shows the mapping from unital design to key-pre distribution.

Table-1
Unitals to Key Pre-Distribution Mapping

Unital design	Key Distribution
X: Point set	S: Key pool
Blocks	Key rings ($< K R_i >$)
Size of a block $(k = m + 1)$	Size of a key ring ($|K Ri| = m + 1$)
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 (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

The unital block corresponding to the key rings is generated before the deployment of the network. Then the distinct key ring and key identifiers are preloaded to each node in the wsn network. Then the neighboring nodes identify the common key by exchanging the key identifiers. At least one common key should be shared by the pair of nodes. In unital design, two blocks cannot share more than one point. The common key could be used to establish a secure communication link between those pair of nodes. If there is no common key between a pair of nodes, we could establish a communication link between these nodes through successive secure links.

To enhance the key sharing probability while maintaining high network scalability a new enhanced scalable unital-based key pre-distribution scheme is introduced for WSN. An algorithm is used to represent the random approach to build blocks and to pre load each node using unital design. Each node with a number of blocks for the network is chosen in a selective way.

Blocks of *m* order unital design is generated before deploying the network, where each block matches a key set. We use *t* completely disjoint blocks to pre-load each node with a number of blocks. Algorithm-1 shows the random block distribution in which each sensor node can pre-load *t* disjoint blocks.

```
Generate $B = < Bq >$, key sets corresponding $t$ blocks of a unital design of order $m$
foreach $Node_i$ do
    $KR_i = \{\}$
    while $( |KR_i| \leq t ( m + 1 ))$ do
        pick $Bq$ from $B$
        if $(( KR_i \cap Bq ) = \emptyset )$ then
            $KR_i = KR_i \cup Bq$
            $B = B - Bq$
        end
    end
```

Algorithm-1
A random approach to build blocks and to pre distribute each node using unital design

This approach helps to decrease the secure path length. Here after deploying the network, each two neighbors can determine their common key by exchanging their key identifiers. This is the basic approach. But there is chance that two neighbors can share more than one key and this result in a contradiction. A hash function could be used as a solution to this which generates a secret key between the pair of nodes by concatenating the common keys by which a secure link is established. This approach helps to improves network resiliency. That is if an attacker want to break the secure link, he needs more overlap keys.

For a highly scalable and secure communication, the proposed system u-key consist of five stages of operation. Figure-1 shows these stages as a block diagram. To deploy a secure network, first deploy nodes using unital design approach. To provide secure communication through these nodes, generate secret keys and distribute them to nodes using mapping function where a mapping is performed from unital to key distribution. The data is transmitted between the nodes after encryption using the generated secret keys. The destination node receives and decrypts the data using its own secret key. Thus communication is made secure through the proposed u-key approach.

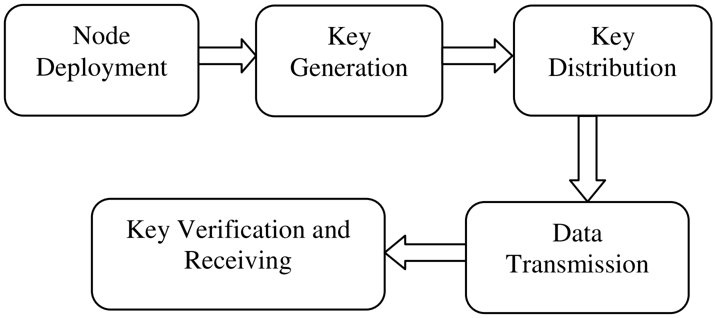

Figure-1
General block diagram of the proposed system

The u-key approach increases the resiliency through the pair wise secret key which reinforces secure paths. The main advantage is that it improves the key sharing probability by maintaining network scalability.

Conclusion

In this paper, we propose a u-key approach to secure Wireless Sensor Networks. For this we use a unital based approach. It is an enhanced highly scalable key distribution mechanism for WSN. Unital design theory is chosen as the base for this. Then a mapping is performed from unital design to pre-key distribution. Thus a new key management scheme is introduced for key distribution. This scheme provides a good key sharing probability and high scalability for WSN. It also provides secure links between nodes for communication and better overall performances.

References

1. Walid Bechkit, Yacine Challal and Abdelmadjid Bouabdallah (2012). A New Scalable Key Pre-distribution Scheme for WSN. IEEE. International Conference on Computer Communication Networks, 2012, Munich, Germany. 1-7, 2012. <hal-00710086>.

2. Eschenauer L. and Gligor V.D. (2002). A key-management scheme for distributed sensor networks. In ACM Conference on Computer and Communications Security (CCS), 41-47.

3. Du W., Deng J., Han Y., Chen S. and Varshney P. (2004). A key management scheme for wireless sensor networks using deployment knowledge. In IEEE INFOCOM, 586-597.

4. Chan H., Perrig A. and Song D. (2003). Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy, 197.

5. Liu D. and Ning P. (2003). Establishing pairwise keys in distributed sensor networks. In ACM Conference on Computer and Communications Security(CCS), 52-61.

6. Zhou Y., Fang Y. and Zhang Y. (2008). Securing wireless sensor networks: A Survey. IEEE Communications Surveys and Tutorials, 10(1-4), 6-28.