ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

A unital design based key distribution scheme for wireless sensor networks

B.Anitha
Assistant professor
Department of Electronics and communication
Bharathiyar Institute of Engineering for Women
Tamilnadu,India
anithajune2@gmail.com

Abstract - **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. A new scalable key management scheme for WSNs which provides good secure connectivity coverage. For this purpose, make use of the unital design theory. It shows 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, propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability. It 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.**

I. 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, 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.

II. METHODOLOGY

At present, agent-based modeling and simulation is the only paradigm which allows the simulation of complex behavior in the environments of wireless sensors (such as flocking). Agent-based simulation of wireless sensor and ad hoc networks is a relatively new paradigm. Agent-based modeling was originally based on social simulation.

A. *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 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.

2. Network scalability: From construction, the total number of possible key rings when using the naive unital based scheme is $n = m^2 \times (m^3+1)(m+1) = m^2 \times (m^2-m+1)$, this is then the maximum number of supported nodes.

3.Direct secure connectivity coverage: When using the basic unital mapping, 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 pre-loaded with a key ring KRuof m + 1 different key. 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, find that the blocks containing two different keys of KRuare 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 can be calculated 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 evaluation of this naive solution shows clearly that the basic mapping from unitals to key pre-distribution gives a high network scalability which reaches O (k4). Moreover, given a network size n, this naive scheme allows to reduce the key ring size up to $4\sqrt{n}$. However, this naive solution results a low key sharing probability

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

which tends to O (1/k). In order to improve the key sharing probability while maintaining a good scalability improvement, propose the next section an enhanced scalable and efficient unital-based key pre-distribution for WSNs

B. *SHA-1 algorithm*

In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. Christo Ananth et al. [10] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results.

SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are named SHA-0, SHA-1, SHA-2, and SHA-3. SHA-0 is the original version of the 160-bit hash function published in 1993 under the name "SHA": it was not adopted by many applications. Published in 1995, SHA-1 is very similar to SHA-0, but alters the original SHA hash specification to correct alleged weaknesses. SHA-2, published in 2001, is significantly different from the SHA-1 hash function. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

C. *Spread spectrum*

Code Division Multiple Access (CDMA) is used as a multiple access technique in telecommunications radio system that can transport multimedia traffic at high data rates. The communications researchers have studied CDMA and are further developing it. This has come out because of the various reasons which contributed to evolution in wireless technology. They include:

- Need for highly reliable telecom network and most important and security against eavesdropping and cryptanalysts.
- Implementation of inexpensive data network.
- End users need new services, like new telephony and internet services.
- Explosive growth of data leading to market growth.
- Introduction of new services imposed by technology changes.

Spread spectrum (SS) techniques are methods in which energy generated at a single frequency is spread over a wide band of frequencies. The basic spread spectrum technique is shown in Fig. 1. This is done to achieve transmission that is robust against channel impairments, and to be able to resist natural interference or jamming and to prevent hostile detection. These techniques were developed by military guidance and communication systems.

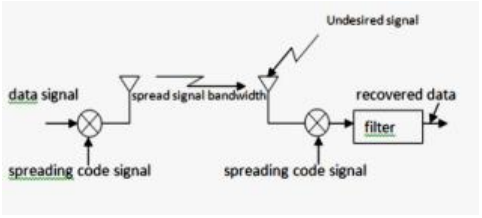


Fig. 1. Model of basic spread spectrum technique

We present now the block diagram of a typical communication system with the difference that the modulator/demodulator has as input the spreading generator. This piece will be explored in following sections.

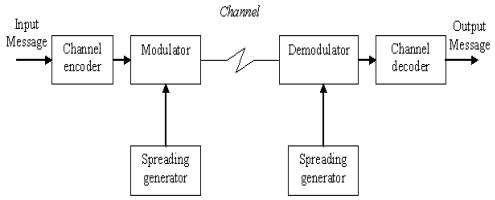


Fig. 2. Block diagram of the spread spectrum communication system

There are two predominant techniques to spread the spectrum:

1. Frequency hoping (FH), which makes the narrow band signal jump in random narrow bands within a larger bandwidth.
2. Direct sequence (DS) which introduces rapid phase transition to the data to make it larger in bandwidth.

We will focus on Direct Sequence Spread Spectrum technique since it is the mostly used in the industry

D. *Walsh-hadamard sequences*

Other common sequences are Walsh-Hadamard sequences currently used in CDMA systems. These sequences are orthogonal (i.e. $\sum b_i b_j = 0$ where b is a row of the matrix), convenient properties for multiple users. The sequences are the rows of the Hadamard matrix H_M defined for $M = 2$ as:

$$H_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

For larger matrices use the recursion:

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

$$H_{2M} = \begin{bmatrix} H_M & H_M \\ H_M & -H_M \end{bmatrix}$$

Example for

$$H_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

Orthogonal codes have perfect properties of cross correlation (if no shift is implemented).

III. SIMULATION RESULTS

For a t-design every set of t points are incident in a constant number, λ, of blocks together and thus for 2-designs, every pair of points occur in λ blocks together. 2-designs are also called balanced incomplete block designs (BIBDs), and are denoted as 2-(v, b, r, γ, λ) or 2-(v, γ, λ) designs. The designs of interest in this thesis are the 2-designs with λ equal to 1, called Steiner 2-designs, in which every pair of points occur together in exactly one block and so each pair of blocks intersect in at most one position.

The parameters of a 2-(v, b, r, γ, λ) design are constrained byvr = bγ (4.1)

asvr and bγ are each the number of non-zero entries in the incidence matrix. Further, any given point P is in a pair with γ − 1 points in each of the r blocks containing it and so there are r(γ −1) pairs involving P. However, P must be paired with each of the v−1 other points exactly λ times and soλ(v − 1) = r(γ − 1) (4.2)

Thus the choice of any three of the parameters completely specifies the design with the remaining two parameters determined by (4.1) and (4.2).

A. *Sensor data waveform*

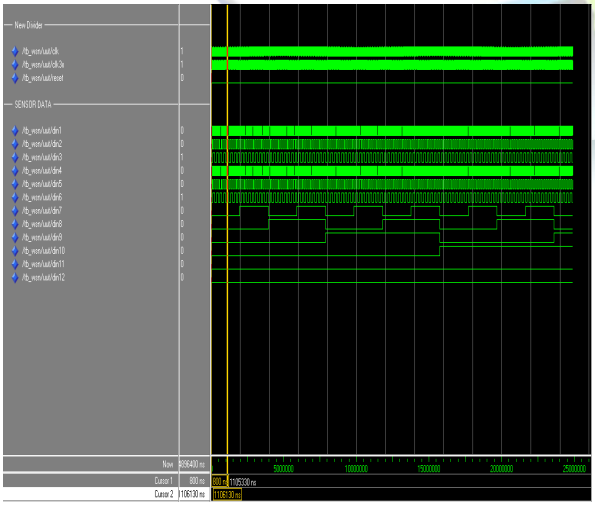


Fig. 3. Sensor data waveform

B. *Walsh code*

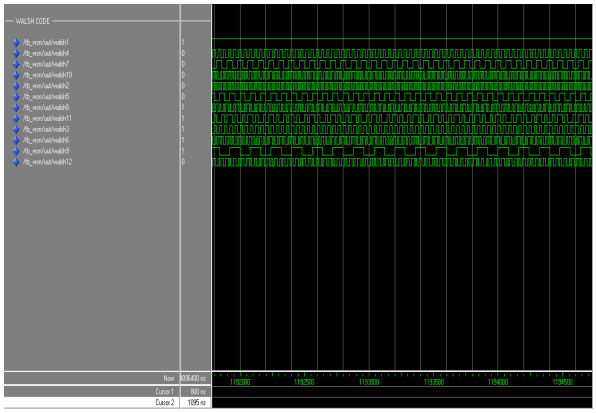


Fig. 4. Walsh code

C. *Sensor node output/encoded data*

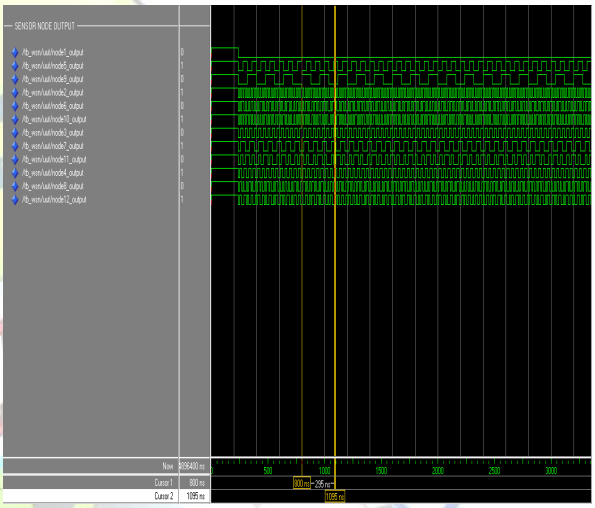
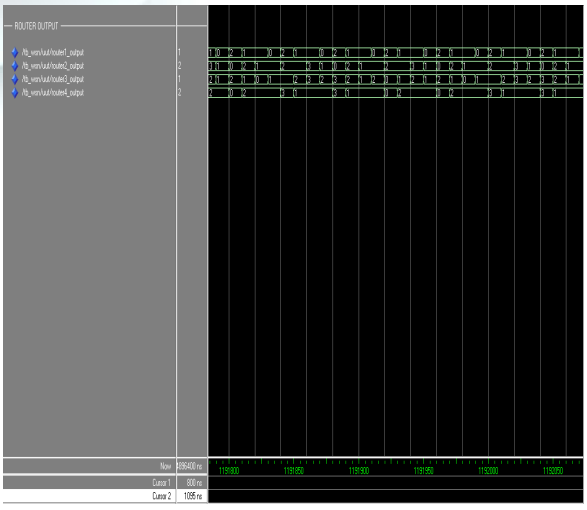


Fig. 5. Sensor node output/encoded data

D. *Router output*



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Fig. 6. Router output

E. *Received sensor data*

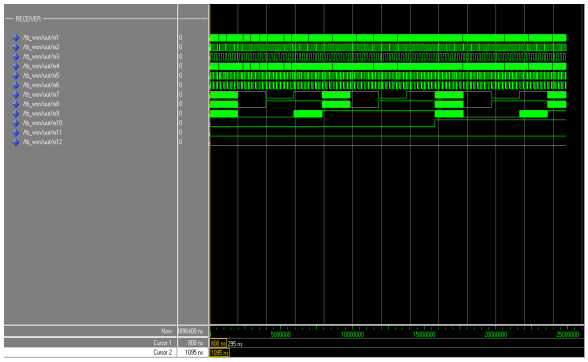


Fig. 7. Received sensor data

IV. Securing Wireless Sensor Networks

Significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that is, a wireless sensor network. WSNs have attracted intensive interest from both academia and industry due to their wide application in civil and military scenarios. In hostile scenarios, it is very important to protect WSNs from malicious attacks. Due to various resource limitations and the salient features of a wireless sensor network, the security design for such networks is significantly challenging. In this article, present a comprehensive survey of WSN security issues that were investigated by researchers in recent years and that shed light on future directions for WSN security.

V. Conclusion

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, use of the unital design theory and spread spectrum methodology. This spread spectrum technique makes this key management a fast and secure system. A basic mapping from unitals to key pre-distribution allows achieving high network scalability while giving low direct secure connectivity coverage. An efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage.The solution parameter and adequate values giving a very good trade-off between network scalability and secure connectivity. An 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.

References

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

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in IEEE SP, pp. 197–213, 2003.

[3] 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.

[4] S. A, Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 15, pp. 346–358, 2007.

[5] S. A, Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Technical Report TR-05-07, Mar. 2005.

[6] 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

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 2002 ACM CCS, pp. 41–47.

[8] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proc. 2003 ACM CCS, pp. 52–61.

[9] B. Maala, Y. Challal, and A. Bouabdallah, "Hero: hierarchcal key management protocol for heterogeneous WSN," in Proc. 2008 IFIP WSAN, pp. 125–136.

[10] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[11] 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

[12] Z. Yu and Y. Guan, "A robust group-based key management scheme for wireless sensor networks," in Proc. 2005 IEEE WCNC, pp. 1915–1920.

[13] 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.

[14] 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.

[15] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," J. Netw.Comput.Appl., vol. 33, no. 2, pp.63–75, 2010.