International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 8, November 2014, PP 18-23
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks

Koduri Kavya[1], M .V. Dilip Kumar[2]

P.G.scholar, Dept.of CSE, Krishnaveni Engineering College for Women, Narasaraopet, Andhra Pradesh, India[1], *koduri.kavya@gmail.com*

Asst Professor, Krishnaveni Engineering College for Women, Narasaraopet, Andhra Pradesh, India [2] *saidilipmutala@gmail.com*

Abstract: *Given 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. In this paper, we propose a new scalable key management scheme for WSNs which provides 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 achieve 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 good key sharing probability approximately lower bounded by* $1 - e^{-1} \approx 0.632$*. We 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.*

Keywords: *Wireless sensor networks (WSNs),Micro-Electro-Mechanical Systems (MEMS) technology.*

1. INTRODUCTION

Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has acilitated the development of smart sensors.

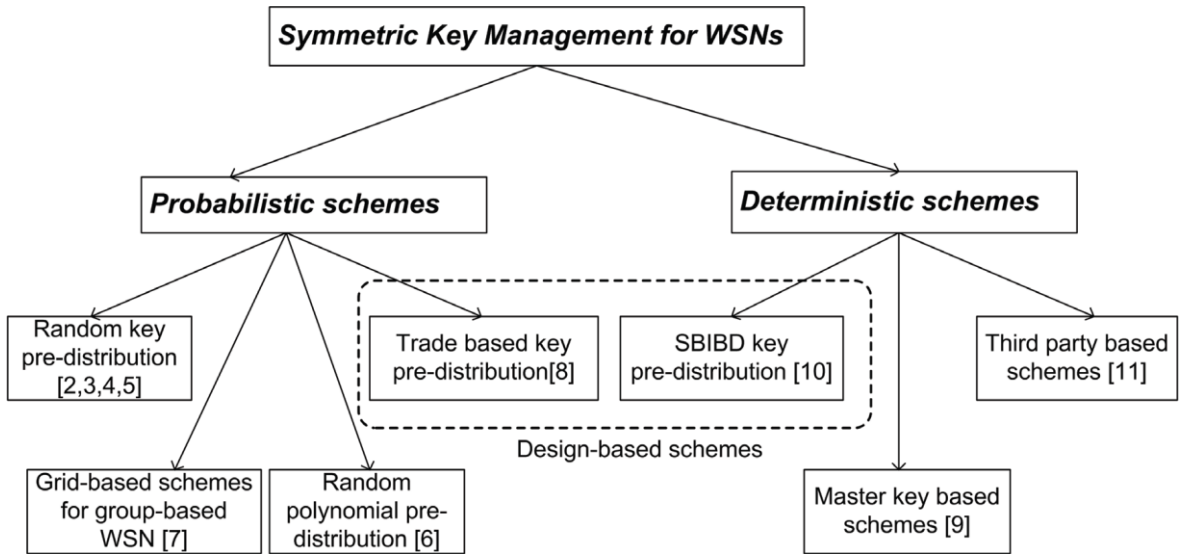


Fig. *Wireless Sensor Network Architecture*

These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user. Smart sensor nodes are low power devices equipped with one or more sensors, a processor,

memory, a power supply, a radio, and an actuator.1 A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment. Since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is implemented for wireless communication to transfer the data to a base station (e.g., a laptop, a personal handheld device, or an access point to a fixed infrastructure). Battery is the main power source in a sensor node. Secondary power supply that harvests power from the environment such as solar panels may be added to the node depending on the appropriateness of the environment where the sensor will be deployed. Depending on the applicationand the type of sensors used, actuators may be incorporated in the sensors.

A WSN typically has little or no infrastructure. It consists of a number of sensor nodes (few tens to thousands) working together to monitor a region to obtain data about the environment. There are two types of WSNs: structured and unstructured. An unstructured WSN is one that contains a dense collection of sensor nodes. Sensor nodes may be deployed in an ad hoc manner2 into the field. Once deployed, the network is left unattended to perform monitoring and reporting functions. In an unstructured WSN, network maintenance such as managing connectivity and detecting failures is difficult since there are so many nodes. In a structured WSN, all or some of the sensor nodes are deployed in a pre-planned manner.3 The advantage of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions. WSNs have great potential for many applications in scenarios such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring, and hazardous environment exploration and seismic sensing entification. Specific examples include spatially-correlated and coordinated troop and tank movements. With natural disasters, sensor nodes can sense and detect the environment to forecast disasters before they occur. In biomedical applications, surgical implants of sensors can help monitor a patient's health. For seismic sensing, ad hoc deployment of sensors along the volcanic area can detect the development of earthquakes and eruptions. Research in WSNs aims to meet the above constraints by introducing new design concepts, creating or improving existing protocols, building new applications, and developingnewalgorithms. In this study,wepresent a top-down approach to survey different protocols and algorithms

2. UNITAL DESIGN FOR KEY PRE-DISTRIBUTION IN WSNS

WSNs 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 n 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 degrade 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.

3. A NEW SCALABLE UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME FOR WSNS

In this section, we present a new unital-based key predistribution scheme for WSNs. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build the unital design blocks and pre-load each node with a number of blocks picked in a selective way.

3.1. Key Pre-Distribution

Before the deployment step, we generate blocks of m order unital design, where each block corresponds to a key set. We pre-load then each node with t completely disjoint blocks where t is a protocol parameter that we will discuss later in this section. In lemma 1, we demonstrate the condition of existence of such t completely disjoint blocks among the unital blocks. In the basic approach each node is pre-loaded with only one unital block and we proved that each two nodes share at most one key. Contrary to this, pre-loading each two nodes with t disjoint unital blocks means that each two nodes share between zero and $t2$ keys since each two unitals blocks share at most one element.

3.2. Theoretical Analysis

We denote in what follows by t-UKP the unital-based key pre-distribution scheme of parameter t (t is the number of preloaded blocks at each node). We note that the 1-UKP scheme matches the basic mapping presented.

Storage Overhead

When using the t-UKP scheme of order m, we pre-loaded each node with $t(m+1)$ distinct keys.

Indeed, from the construction, we can see that t blocks preloaded in a given node are completely disjoint. So, each two blocks within a key ring do not intersect at any key. So, the memory required to store keys is then equal to $l \times t \times (m+1)$, where l is the key size.

4. PERFORMANCE COMPARISON

In this section, we compare the proposed unital-based schemes to existing schemes regarding different criteria

4.1. Network Scalability at Equal Key Ring Size

We compare 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 $m2 + m + 1$ where m s the SBIBD design order and $m + 1$ is the key ring size. We compute the salability of the Trade-KP scheme as $2q2$ where q is the first prime power greater than the key ring size k, this value allows a achieve the best session key sharing probability using the Trade-KP scheme as we proved in. The figure shows that at equal key ring size, the NU-KP scheme allows to enhance 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 figure shows that the t-UKP schemes achieve a high network scalability. We notice that the higher t is, the lower network scalability is. Nevertheless, 2- UKP 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 enhanced. For instance, compared to SBIBD-KP scheme, the increase factor reaches five when the key ring size equal to 150. We plot in Figure 4 the same results separately with linear scales which illustrate clearly the network scalability enhancement when using our solutions

4.2. 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 compute for each network size the design order allowing to achieve the desired scalability and we deduce then the key ring size, the obtained results. The figure shows that at equal network size, the NU-KP scheme allows to reduce the key ring size and then the storage overhead. Indeed 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 clearly 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.

4.3. Energy Consumption at Equal Network Size

In this subsection, we compare the energy consumption induced by the direct secure link establishment phase. Since each node broadcasts its list of key identifiers to its neighbors, the energy consumption can be computed as :$E = Etx \cdot k \cdot log2(|S|) + \eta \cdot Erx \cdot k \cdot log2(|S|)$

Where Etx (resp. Erx) is the average energy consumed by the transmission (resp. reception) of one bit, k is the key ring size, η is the average number of neighbors and $log2(|S|)$ represents the size of a key identifier in bits that we round up to the nearest byte size.

4.4. Network Connectivity at Equal Key Ring Size

We compare in this subsection, the network secure connectivity coverage of the different schemes. First, we plot in Figure 7 (a) the key sharing probability when using the unital based schemes (NU-KP, t-UKP and UKP*). 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 $O(1\ k)$ as k tends to infinity. Otherwise, the obtained results show that the higher t is, the better the direct secure connectivity coverage is. Indeed, loading nodes

with many blocks from unital design allows to increase significantly the key sharing probability. Moreover that the UKP* scheme gives very good connectivity results. For instance, the direct secure connectivity coverage remains between 0.82 and 0.66 when the key ring size is between 10 and 150. As the key ring size is high, the direct secure connectivity of UKP* approaches $1 - e{-}1 \approx 0.632$, which we proved to be an approximate lower bound.

4.5. Network Resiliency at Equal Key Ring Size

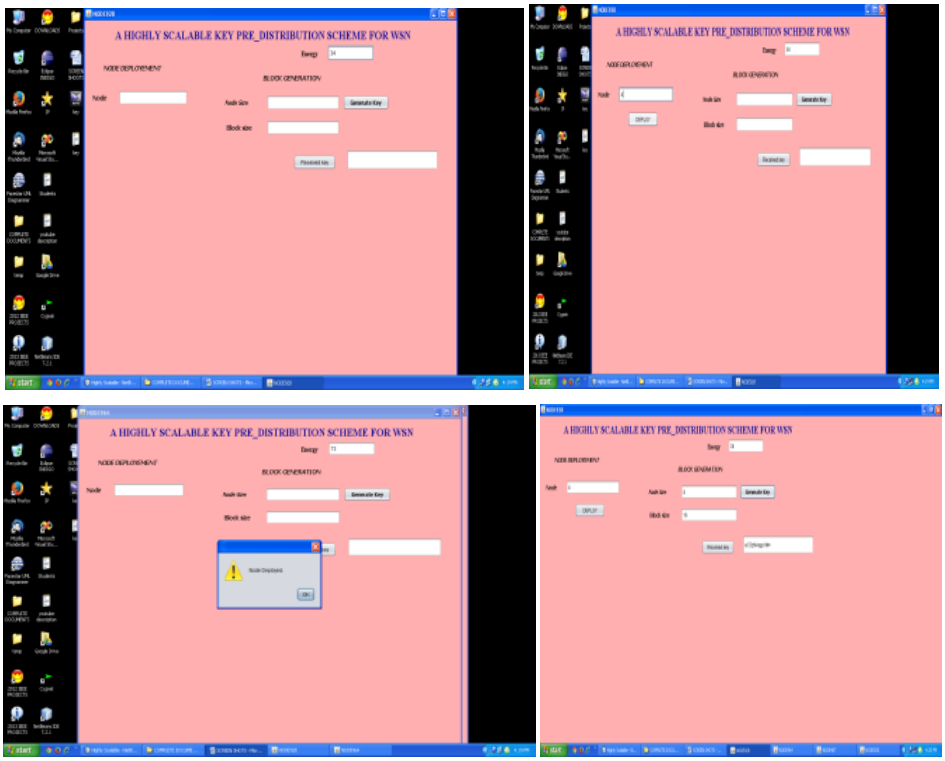
We compare in this subsection, the network resiliency of the vunital-based schemes to those of the Trade-KP and the SBIBDKP ones. We notice that the proposed trade based construction given in [8] allows to have a unique pairwise key per secure link, this key is computed as the hash of a unique pair of initial keys. However the overall network resiliency is not perfect because the compromise of some key rings may reveal other vpairwise secret keys used to secure external links in which the compromised nodes are not involved. We proved that the resiliency of the Trade-KP scheme.

We compare in Figure 8 the network resiliency at equal number of compromised nodes for $|KR| = 68$. The figure shows that the NU-KP scheme provides a good resiliency compared to other schemes. Using the t-UKP, the higher t is, the lower network resiliency is at equal number of compromised nodes. This is due to the number of compromised unital blocks which is multiplied by t. On the other hand, the figure shows that the UKP* scheme improves the network resiliency over the SBIBD-KP scheme by 20%. It also gives a better network resiliency then the Trade-KP scheme when the number of compromised nodes exceeds 60.

4.6. Numerical Results

We provide in table IV numerical results comparing network scalability, direct secure connectivity coverage, and average secure path length of the three schemes (SBIBD-KP, Trade-KP and UKP*) at equal key ring size. We notice that we provide the average network scalability (number of nodes) when using UKP* scheme. On the other hand, we compute the average secure path length based on simulations. We refer in these simulations to the results given in [23] in order to construct a grid deployment model which ensures the network physical connectivity and coverage. Numerical results show that the unital-based key pre-distribution scheme UKP* increases the network scalability over the SBIBD-KP and the Trade-KP scheme while maintaining high secure connectivity coverage. For instance, the network maximum size is increased by a factor of 3 and 4.8 when the key ring size is equal to 68 and 140 respectively compared to the SBIBD-KP scheme. In addition, we maintain a high connectivity over 0.63 which ensures a low average secure path length which does not exceed 1.37.

Screen Shots



5. 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 design 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 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] 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.

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

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

[4] 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.

[5] 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.

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

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

[8] 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, pp. 326–330.

[9] 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.

[10] 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.

[11] M. Rahimi, H. Shah, G.S. Sukhatme, J. Heideman, D. Estrin, Studying the feasibility of energy harvesting in mobile sensor network, in: Proceedings of the IEEE ICRA, 2003, pp. 19–24.

[12] A. Kansai, M.B. Srivastava, An environmental energy harvesting framework for sensor networks, in: Proceedings of the International Symposiumon LowPower Electronics andDesign, 2003, pp. 481–486.

[13] S. Toumpis, T. Tassiulas, Optimal deployment of large wireless sensor networks, IEEE Transactions on Information Theory 52 (2006) 2935–2953.

[14] J. Yick, G. Pasternack, B. Mukherjee, D. Ghosal, Placement of network services in sensor networks, Self-Organization Routing and Information, Integration in Wireless Sensor Networks (Special Issue) in International Journal of Wireless and Mobile Computing (IJWMC) 1 (2006) 101–112.

[15] D. Pompili, T. Melodia, I.F. Akyildiz, Deployment analysis in underwater acoustic wireless sensor networks, in: WUWNet, Los Angeles, CA, 2006.

[16] I.F. Akyildiz, E.P. Stuntebeck, Wireless underground sensor networks: research challenges, Ad-Hoc Networks 4 (2006) 669–686.

[17] M. Li, Y. Liu, Underground structure monitoring with wireless sensor networks, in: Proceedings of the IPSN, Cambridge, MA, 2007.

[18] I.F. Akyildiz, D. Pompili, T. Melodia, Challenges for efficient communication in underwater acoustic sensor networks, ACM Sigbed Review 1 (2) (2004) 3–8.

[19] J. Heidemann, Y. Li, A. Syed, J. Wills, W. Ye, Underwater sensor networking: research challenges and potential applications, in: Proceedings of the Technical Report ISI-TR-2005-603, USC/ Information Sciences Institute, 2005.

[20] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks Elsevier 51 (2007) 921–960.

AUTHORS' BIOGRAPHY

Koduri Kavya received the B.Tech degree in Computer Science and Engineering in the year 2012 and pursuing M.Tech degree in Computer Science and Engineering from Krishnaveni Engineering College for Women.

M.V.Dilip received his M.Tech degree in Computer Science and Engineering and MCA degree. He is currently working as an Asst Professor in Krishnaveni Engineering College for Women.