SKM: Effective Secure Coverage for Wireless Sensor Networks

G. Mallesham, K. Meena

Christu Jyoti Institute of Technology & Science, Colombonagar,
Yeshwanthapur, Jangaon, Andhra Pradesh ,India

Abstract: In this paper, 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 achieve high network scalability. We propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability. 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.

1. Introduction

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

2. Related Work

Key pre distribution is an important topic that constitutes the basis of security in wireless sensor networks. Many security mechanisms such as encryption and authentication can be provided by accessing to shared keys. Several techniques are previously proposed to address this issue. The Extensive features about key distribution in sensor networks are given by L. Eschenauer and V. Gligor [1], H. Chan. A. Perrig and D. Song [2], D. Liu and P. Ning [3] and Subash.T.D,Divya .C [4]. Eschenauer and Gligor's basic scheme [1] is taken as a framework for many techniques using probabilistic key sharing for key management.These studies compared themselves with the basic scheme as we did in this paper. Eschenauer and Gligor's basic scheme [1] proposed a probabilistic key sharing scheme similar to basic scheme. It provides a secure communication network can be formed with key sharing information between sensor nodes. but it is vulnerable to the node compromise attack. H. Chan. A. Pemg, and D. Song modified E-G scheme by only increasing the number of keys that two random nodes share from at least 1 to at least q. It increased vulnerability in large scale node compromise attack. D. Liu and P. Ning proposed a polynomial pool-based

key pre-distribution scheme where any two sensors can definitely establish a pair-wise key when there are no compromised sensors. It has low resiliency. Subash.T.D,Divya .C used Pairwise key pre distribution scheme to improves the resilience of the network. it is used single hop communication. These above papers are compared which describe information about security issues in wireless sensor network. So in this papers author are given some key management scheme techniques such as probabilistic, q-composite randomize, pair wise and polynomial pool based scheme. Key pre distribution results in high security during adversarial attacks. Key pre distribution algorithms are classified into two groups:

1) Deterministic key pre distribution where the key assignment follows a certain pattern.
2) Randomized key distribution, in which keys are assigned randomly from a large key pool and preloaded in the sensors. On comparisons we concluded that pair wise scheme is better than other scheme because by using this scheme our communication become very secure as compared to other scheme because we are using pairwise keys in this technique so intruder cannot alter data because it contain combination of 2 keys, so if intruder knows all this 2 keys then he/she can only access our data otherwise not.

3. Problem Statement

3.1: Existing System

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.

Disadvantages

A host of research work dealt with symmetric key pre-distribution issue for WSNs and many solutions have been proposed In the existing system many disadvantages occur: the design of key rings (blocks of keys) is strongly related 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.

3.2: Proposed System

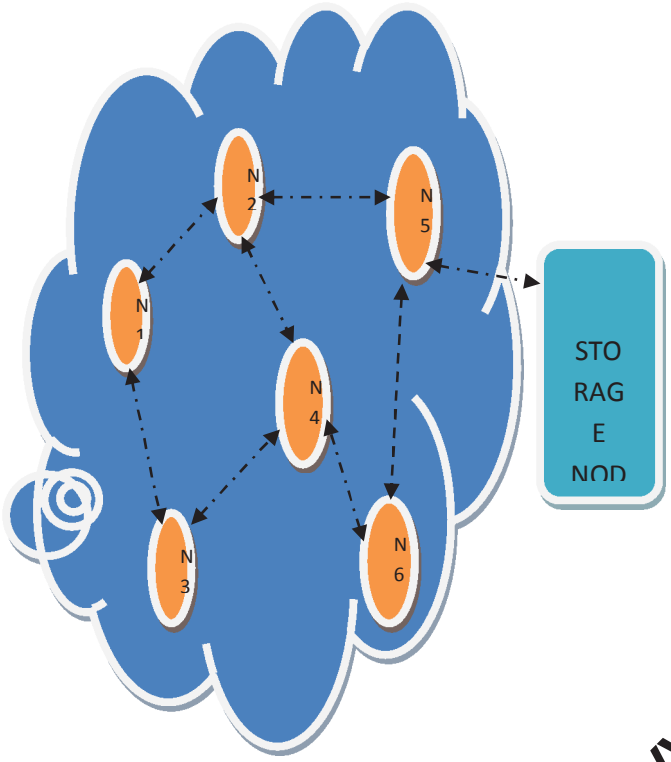
In this proposed system, our aim is to tackle the scalability issue without degrading the other network performance metrics. For this purpose, we target the design of a scheme which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, we make use, of the unital design theory for efficient WSN key pre-distribution.

Advantages

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.

We propose an enhanced unitalbased key pre-distribution scheme that maintains a good key sharing probability while enhancing the network scalability.

4. System Architecture



5. Modules

1. Node Deployment

The first module is Node deployment, where the node can be deployed by specifying the number of nodes in the network. After specifying the number of nodes in the network, the nodes are deployed. The nodes are deployed with unique ID (Identity) number so that each can be differentiated. And also nodes are deployed with their energy levels.

2. Key Generation

After the Node deployment module, the key generation module is developed. Where the number of nodes and number of blocks should be specified, so that the key will be generated. The key is symmetric key and the key is displayed in the text area given in the node.

3. Key Pre-distribution Technique

In this module, we generate blocks of m order initial 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.

4. Secure Transmission with Energy

In this module, the node distance is configured and then the nodes with their neighbor information are displayed. So the nodes which is near by the node, is selected and the energy level is first calculated to

verify the secure transmission. After that the data is uploaded and sent to the destination node. Where in the destination node, the key is verified and then the data is received.

6. Experimental Results

7. Future Enhancement

We will concentrate on probabilistic scheme in future. we will try to increase Local connectivity between nodes by adding XOR operation in efficient key management scheme. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required.

8. 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 achieving 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.

9. References

1. L. Eschenauer and V. D. Gligor. "A key-management scheme for distributed sensor networks", In Proc. of the 9th ACM CCS conference, pp. 41 – 47, 2002.
2. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks".In Proc. of the IEEE Symposium on Security and Privacy, p. 197, 2003.
3. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," In Proc. ofthe 10th ACM CCS Conference, pp. 52 – 61. 2003.
4. Subash.T.D, Divya .C ,"Novel Key Pre-distribution Scheme in Wireless Sensor Network", 978-1-4244-7926-9/11/$26.00 ©2011 IEEE.