Efficient Key Pre-Distribution Approach for Wireless Sensor Networks

Saurabh Kumar Singh[#1], Dr Harsh K Verma[*2], Ravindra Kumar Singh[#3]

[#]Department Of Computer Science and Engineering, National Institute of Technology Jalandhar
Punjab India

[1]saurabhbans87@gmail.com

[2]vermah@nitj.ac.in

[2] ravindra1987singh@gmail.com

***Abstract*—Wireless sensor network is highly vulnerable to attacks because it consists of various resource-constrained sensor nodes which communicate among themselves via wireless links. Securely distributing keys among sensor nodes is a fundamental challenge for providing security services in WSNs. In the random key pre-distribution approach is suitable for low power and resource constrained sensor nodes, a shared key between a pair of nodes is not guaranteed and thus they may not be able to communicate with each other. Matrix based scheme for key pre-distribution essentially use LU decomposition of matrix which can provide keys between any pair of nodes but are quite vulnerable to attack. This paper proposes an improved and efficient key pre-distribution scheme based on LU composition of matrices. Our scheme, we use integer as elements of symmetric matrices. The existing approach use decomposition of matrices which is compute intensive but our proposed scheme uses composition of matrices. The proposed scheme allows almost 100 % connectivity indifferent of the number of keys and provides resilience against node capture.**

***Keywords*—Wireless sensor network; key pre-distribution; LU matrix; security; matrix decomposition; symmetric matrix.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have potential to provide economical solutions to many problems of practical importance. Some general purpose applications where Sensor Networks can be used are: Emergency Response System, Energy Management, Battlefield Management, Health Monitoring, and Inventory management etc [1]. For example, power load that should be carried over an electrical line depends on the temperature of the wire and the environmental conditions. If the parameters are monitored by remote sensors and transmitted to a base station, it would be possible to meet load requirements optimally. Sensor Networks consist of various resource-constrained devices. Each sensor node has low battery power, less memory and very less computational capability. Same battery is used throughout the life time of a sensor node [1, 8].

However, there are still a lot of unresolved issue in WSN of which security is one of the hottest research issue [1,3,12]. Sensor Networks are deployed in hostile environments. Environmental conditions along with resource-constraints give rise to many type of security threats or attacks. Adversary can physically capture and get the information contained in the sensor node, eavesdrop and inject new messages, modify messages.

Hence there must be some sort of mechanism for node to node data transmission. The message is sent encrypted with a key that is shared by sender and receiver. Keys play a central role in realizing security services like: authenticity, integrity, confidentiality etc. Keys need to be distributed securely among sensor nodes. For the distribution of keys, many ordinary security mechanisms such as public key-based authentication and corresponding key management scheme are impractical and infeasible for WSN.

In this paper, we present a novel scheme for key distribution scheme that is based on polynomial over finite field. This scheme has advantage of both probabilistic and deterministic approaches. It is based on polynomial for a node it guarantees the establishment of key with every node [2,13].

The rest of this paper is organized as follows. Section II describes the existing key distribution scheme for wireless sensor network. Section III gives an overview of the polynomial-based key pre-distribution scheme approach in detail. Section IV presents the key pre distribution scheme with matrix decomposition. Section V deals with the detailed performance analysis. Finally, Section VI concludes this paper.

II. RELATED WORKS

Eschenauer and Gligor [4] propose a probabilistic key pre-distribution scheme for pair wise key establishment. For each sensor node, a set of keys are chosen from a big pool of keys and given to each node before deployment. In order to establish a pair wise key, two sensor nodes only need to identify the common keys they share. Thus every pair of nodes in the network shares a key with certain probability. Since keys are randomly chosen from the key pool, they are not related. Hence it is not possible to calculate other keys by knowing some of the keys from the key pool. Chan et al.[9,10] further extended this idea and developed two key pre-distribution techniques: q-composite key pre-distribution and random pair wise scheme[9]. q-composite key pre-distribution also uses a key pool but requires two sensors to compute a pair wise key from at least q pre-distributed keys they share. In the random pair wise keys scheme, random pairs of sensors are picked and assigned a unique random key. In both the schemes, resilience is improved because probability that a link is compromised, when a sensor node is captured, decreases. But, probability of key sharing also decreases because a pair of sensor nodes has to share q keys instead of one. This scheme achieves good security under small scale attacks, while being vulnerable to large scale attacks.

III. The Polynomial-Based Key Predistribution Scheme

To pre-distribution pair-wise key, the key pre-distribution server first randomly generate a bivariate *t*-degree polynomial over a finite field F_q:

$$f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i$$

Where *q* is a prime number that is large enough to accommodate a cryptographic key, such that it has the property of *f (x, y) = f (y, x)*. Then for each node *i* , the setup server compute a polynomial share of *f (x, y)* , that is *f (i, y)* and store it in sensor node *i*. For any two sensor node *i* , *j* , node *i* can compute the pair-wise key *f (i, j)* by evaluating *f (i, y)* at point *j*, and node *j* can compute the pair-wise key *f (j, i)* by evaluating *f (j, y)* at point *i* . From the property of symmetry of *f (x, y)*, *f (i, j) = f (j, i)* . So the pair-wise key between node *i* and *j* can be established.

In this scheme each sensor node needs to store a bivariate *t*-degree polynomial's coefficients, which would occupy $(t+1)\log_2 q$ storage space. The security proof [3] in ensure that this scheme is unconditionally secure and *t*-collision resistant. In other words the coalition of no more than *t* compromised sensor node know nothing about the pair-wise key between any two non compromised sensor node.

IV. The Proposed Scheme

In this section we briefly describe how the proposed key pre-distribution scheme works in detail. The basic idea can be based on E-G scheme, to remove the drawback of the existing schemes, we proposed a new key pre-distribution scheme with LU matrix for wireless sensor network. The following procedure is executed by base station in order to construct *L*, *U* and *U′* matrices. Which provides full connectivity and better resilience?

A. Preliminaries

We start with a brief description of various concepts and definitions used in this paper.

Definition 1: If a square matrix *M* has the property $M^T = M$, where transpose of matrix *M* is denoted by M^T, we say that *M* is a symmetric matrix. *M* is a symmetric matrix means $M_{ij} = M_{ji}$, where M_{ij} is the element in the i^{th} row and j^{th} column of matrix *M* .

Definition 2: *LU* matrix decomposition of an $n \times n$ matrix *M* decomposes it into two matrices *L* and *U* such that *M = LU* , where *L* is an $n \times n$ lower triangular matrix and *U* is an $n \times n$ upper triangular matrix, respectively.

Definition 3: Let *M* is a square matrix with *M = LU*, and the pivots on the diagonal of *U* are all nonzero. By dividing i^{th} *(1 ≤ I ≤ n)* row of *U* by the nonzero pivot d_i , the matrix *U* is decomposed into a diagonal matrix *D* whose diagonals are just the pivots $d_1,d_2,...,d_n$ and a new upper triangular matrix, denoted by *U'* , whose diagonal elements are all 1. Then *M = LDU'* .

Definition 4: A Circular shift function *(CS)* is a function that defines an operation of rearranging the entries in a tuple, by moving the final entry to the first position. *CS (tuple , n)* indicates that n circular shifts are applied to a given tuple.

Definition 5: A Reverse function(R) is a function that rearranges the entries of a tuple in a reverse order.

B. The proposed key pre-distribution scheme

The proposed key pre-distribution scheme consists of five step

Step 1: Generate a large pool of key and setup server generate randomly a large pool of bivariate *t*-degree polynomial over the finite field.

Step 2: Construct a lower triangular matrix using the randomly selected elements from the key pool. The first condition for selecting elements from the large pool is that all elements present in a column should be multiple of the diagonal element of the same column, some elements should be zero, some elements should be same as diagonal element and all the selected elements should be large.

$$L = \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix}$$

Step 3: Forming an upper triangular matrix using lower triangular matrix: Upper Triangular matrix is formed by taking the simple transpose of lower triangular matrix, i.e., $U = L^T$

$$U = \begin{bmatrix} l_{11} & l_{21} & l_{31} \\ o & l_{22} & l_{32} \\ o & 0 & l_{33} \end{bmatrix}$$

Step 4: Forming a diagonal *D* matrix using *U* matrix: Diagonal matrix *D* is constructed by choosing diagonal elements from matrix *U*.

$$D = \begin{bmatrix} l_{11} & 0 & 0 \\ 0 & l_{22} & 0 \\ 0 & 0 & l_{33} \end{bmatrix} \qquad U' = \begin{bmatrix} 1 & l_{12}/l_{11} & l_{12}/l_{11} \\ 0 & 1 & l_{23}/l_{22} \\ 0 & 0 & 1 \end{bmatrix}$$

Step 5: After computing *L, U, D,* and *U′* matrices, the base station selects one row from lower triangular matrix *L*, i.e., *L* and one column from upper triangular matrix *U* , i.e., *U* for each node and sends both the tuples along with diagonal matrix *D* to each node in the network separately. This is done by using the condition that the row number and column number selected for a particular node should be equal.

IV. Performance Analysis And Comparison

In this section, we present the evaluation of the performances of our schemes, and compare the scheme with Eschenauer and Gligor scheme [4]. Our focus are on analysis of the network connectivity, analysis of resilience against nodes capture and analysis memory usage by each node in the network.

A. Analysis of authentication

The proposed scheme allows node to node mutual

authentication by following the below process:

Step 1: Initially Node A applies Reverse function *(R)* on the selected column elements U'_{ci} and sends it to the Node *B.*

Step 2: Node *B* applies reverse function on the data received from Node A and then applies reverse function to calculate U'_{ci}. Then Node *B* computes the cross product $U = D \times U'_{ci}$. After computing this cross product, Node *B′* generates a key K_{ji} by multiplying L_{rj} with U_{ci} , and apply hash function on key K_{ji} , i.e., $H(K_{ji})$.

Step 3: Now Node *B* applies the same process as done by Node *A* in step 1 own column U'_{cj} and send this value with the generated hash key $H(K_{ji})$ to Node *A* .

Step 4: After receiving data from Node *B*, Node *A* calculates K_{ij} similarly as Node *B* calculated in step 2 and apply the hash function *H* on $K_{ij.}$

Step 5: If $H(K_{ij})$ and $H(K_{ji})$ are equal then Node *A* Yes message along with $H(K_{ij})$ to Node *B* otherwise sends errmsg to Node *B.* If the response is yes then Node *B* verifies $H(K_{ij})$ with $H(K_{ji})$ to establish a secure channel.

B. Analysis of the network connectivity

In this section , we compare the proposed scheme with E & G scheme. Network connectivity, probability p in the proposed scheme sharing at least between any two sensor nodes. We define an event in which a pair of node that does not have a common any one key an[Eve] and pr[eve] is the probability of such event. In proposed scheme, network connectivity p as following.

$$P = 1 - Pr[Eve]$$

$$=1-(1-K/S)^{2S-2K+1}/(1-2K/S)^{S-2K+1/2}$$

Where S is the total number of node in network and K is the number of key in each node

Our scheme show that any two sensor node can always find a shared key between themselves using LU matrix decomposition. In other words, the probability of not sharing a common key between any two network sensor nodes is zero. Figure. 1compares network connectivity p of the proposed scheme with E & G scheme. In the performance analysis, we assume that the size of key pool for each node is 1000, 2000, 5000 and 10000. The result shows that the proposed has 100%.

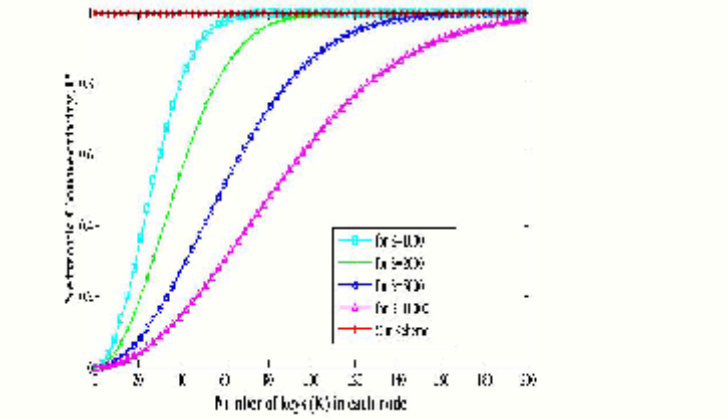

Fig. 1 Analysis of networks connectivity

Connectivity without concern for the number of key per node. In addition key in our scheme occupy less memory space in sensor nodes.

C . Analysis of resilience against node capture

In this section we analyzed resilience to node capture. In wireless sensor networks an adversary can easily calculate the information of compromised nodes, intentionally provide misleading information to the entire network, and break the whole network security. In this section we evaluated that the proposed scheme improves WSN resilience by calculating the fraction of compromised nodes among non-compromised nodes. In addition, we plan to compare our scheme with E & G schemes based on performance. In E & G schemes, the probability of compromising the shared keys between any two non-compromised nodes is following:

$$P_{compromised} = (1 - (1 - k/S)^m)$$

In the proposed scheme, rows from lower triangular matrix L, column from upper triangular matrix U′ , diagonal matrix D, are deleted after the Establishment of the keys. Polynomials which are pre-distributed to each node are randomly selected from the lower triangular matrix L and its degree will be left in each node. For the purpose of addition of new no des in network. When m nodes have been compromised, the probability of compromising the shared keys between any two non-compromised nodes is equal to the probability of compromising the shared polynomials between any two non-compromised nodes But in our scheme if adversary did not get any information from compromised no des about non-compromised nodes, we can say that m is equal to zero. So for our scheme, the probability of compromising the shared keys between any two non-compromised node is following:

$$P_{compromised} = (1 - (1 - k/S)^0)$$

$$P_{compromised} = (1 - 1) = 0$$

C. Memory usage analysis

In this subsection, any two sensor nodes establish the shared key by using polynomial with LU matrix decomposition based key pre-distribution scheme. The network-wide memory usage of our scheme is mostly of polynomial cost. We have

proposed an effcient method to store the row and column information of *L*, and *U* matrices. Our scheme only needs to store each element in the non-zero-element part and one value specifying the maximum number of following zeros in zero-element part of *L* and *U* matrices.

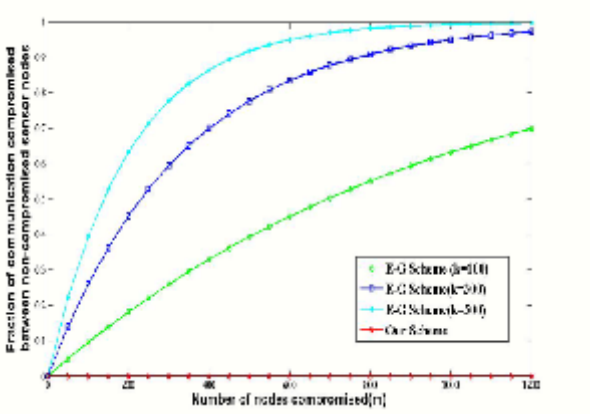

Fig. 2 Resilience comparison E & G scheme and our scheme

This technique is specially suitable for large wireless senor networks. Some notations given below which are used to estimate the storage efficiency:

VI. Conclusion

In recent years key distribution has been one of the hot issues in security research. In This paper, we have proposed a new key pre-distribution scheme based on symmetric matrix with LU decomposition. This scheme guaranteed that any pair of nodes can find a common key between themselves and also it allows more security enhancement on node to node pair-wise key establishment and very good resilience to data exchanged between the nodes and also took very less time to establishment of key between the nodes. This proposed scheme has very less computational overhead to calculate the key in the network.

Acknowledgment

The author would like to thanks the anonymous referess for their valuable comments, which greatly improved the readability of the paper.

Reference

[1] A. Perrig, R. Szewczyk, V. Wen et al.,"SPIN:security protocols for sensor network," Wireless Network,Vol.8.,No.5,pp. 521-534,2002.

[2] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung. Perfectly-secure key distribution for dynamic conferences. In CRYPTO, pages 471–486, 1992.

[3] A. K. Pathan, H. W. Lee, and C. S. Hong, " Security in wireless sensor network: issues and challenges," In proceeding of the 8th ICACT 06,Volume 2, Phoenix Park, Korea, pp. 1043-1048,February, 2006

[4] L. Eschenauer, V. D. Gligor, "A key –managements cheme for distributed sensor network," In proceeding of the 9th ACM conference on Computer and Communication,Washington, DC, USA, pp. 41-47, Nov. 2002.

[5] Taejo on Park and Kang G. Shin. Secure routing based on distributed key sharing in large-scale sensor networks. ACM Trans. Embed. Comput. Syst., 7(2):1–28, 2008.

[6] Hangyang Dai and Hongbing Xu, " Key Predistribution Approach in Wireless Sensor Network Using LU Matrix", IEEE Sensors Journal, Vol, 10. No.8. August 2010.

[7] Ni Chen,Jian Bo Yao and Gang Jun Wen, "An Improved LU Matrix Key Pre-distribution Scheme for Wireless Sensor Networks", International Conference on Advanced Computer Theory and Engineering 2008

[8] Al-Sakib Khan Pathan, Tran Thanh Dai and Choong Seon Hong, "An Efficient LU Decomposition-based Key Pre-distribution Scheme for Ensuring Security in Wireless Sensor Network", Proceeding of The Sixth IEEE International Conference on Computer and Information Technology 2006.

[9] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram Khalili. A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur., 8(2):228–258, 2003.

[10] Chang-Won Park, Sung Jin Choi, and Hee Yong Youn. A noble key pre-distribution scheme with lu matrix for secure wireless sensor networks. In CIS (2), pages 494–499, 2005.

[11] Sung Jin Choi and Hee Yong Youn. Mkps: A multi-level key pre-distribution scheme for secure wireless sensor networks. In HCI (2), pages 808–817, 2007.

[12] Karlof, C. and Wagner, D. "Secure routing in wireless sensor network: Attack and countermeasure", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Application and Protocol, September 2003,pp.293-315.

[13] Sencun Zhu, Shouhuai Xu, Sanjeev Setia, and Sushil Jajodia. Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. In ICNP, pages 326–
335, 2003.

Saurabh Kumar Singh He received B.Tech degree in computer science and engineering in 2009 from Institute of Engineering and Technology Jhansi, India. Currently he is pursuing M.Tech degree,in computer science and engineering from National Institute of Technology Jalandhar India in 2009 and 2011 respectively.
His current research include in wireless sensor network, computer network and information security.

Ravindra Kumar Singh received B.Tech degree in Information Technology in 2009 from Ajay Kumar Garg Engineering College Ghazibad Utter Pradesh Technical University, India. Currently he is pursuing M.Tech degree,in computer science and engineering from National Institute of Technology Jalandhar India in 2009 and 2011 respectively.
His current research include in search engine optimization, wireless sensor network and information security.

Dr. Harsh K Verma He has completed Phd in Numerical Computing from Punjab Technical University Punjab, India.
He **i**s currently a professor and Head of Department of computer science and engineering in National Institute of Technology Jalandhar India.
His research includes in numerical computing, information security and computer networks. He has published various paper in national and international journal and conferences. He has attended various national and international workshop training schools and other technical activity during his academic carrier.