Cryptanalysis of LU Decomposition-based Key Pre-distribution Scheme for Wireless Sensor Networks[*]

Bo Zhu[†], Yanfei Zheng, Yaowei Zhou and Kefei Chen

[†]Department of Computer Science and Engineering,
Shanghai Jiaotong University, Shanghai, 200240, China
zhubo03@gmail.com

Abstract

S. J. Choi and H. Y. Youn proposed a key pre-distribution scheme for Wireless Sensor Networks based on LU decomposition of symmetric matrix, and later many researchers did works based on this scheme. Nevertheless, we find a mathematical relationship of L and U matrixes decomposed from symmetric matrix, by using which we can calculate one matrix from another regardless of their product – the key matrix K. This relationship would profoundly harm the secure implementation of this decomposition scheme in the real world. In this paper, we first present and prove the mathematical theorem. Next we give samples to illustrate how to break the networks by using this theorem. Finally, we state the conclusion and some directions for improving the security of the key pre-distribution scheme.

Key words. Wireless Sensor Networks, Key Pre-distribution, Key Management, LU Decomposition, Symmetric Matrix.

1 Introduction

Wireless Sensor Networks (WSNs) are gaining popularity quickly because of their flexibility and low cost to solve a variety of real-world challenges [7, 8]. The nodes in WSNs are equipped with may low power devices, such as environmental sensors, signal processing chips, wireless transceivers, etc. As the information collected by the sensors and processed by the chips can be transmitted node by node, WSNs can be designed for remote locating, target tracking and environmental monitoring, especially in certain critical areas, such as airports and battlefields. Because WSNs are always expected to deal with sensitive data and operate in hostile environments, potential security issues should be considered from the beginning of the system design. But due to nodes' limited storage space and computing ability, the challenges to secure WSNs are much different from the traditional networks. Lots of researchers have begun to discover new methods or develop existing mechanisms to adapt to nodes' resource constraints but not lower the security level of WSNs.

A secure and efficient key pre-distribution scheme for WSNs aims to provide an appropriate plan to generate and store secret keys, and compute common keys for node-to-node secure communication. The key pre-distribution scheme is the foundation to gain authenticity and confidentiality of WSNs. In EUC Workshops 2005, S. J. Choi and H. Y. Youn proposed a key pre-distribution scheme for WSNs [1]. The scheme first describes the way to form the possible keys to a symmetric matrix K, and then decompose it into the product of a lower triangle matrix L and an upper triangle matrix U. The scheme uses the L matrix for secret information of the nodes in WSNs, and the U matrix for public information exchange and building common keys. S. J. Choi and H. Y. Youn's scheme can

[*]This work is supported by 973 Program under Grant No. 2007CB311201 and National Natural Science Foundation of China under grant No. 60703030.

guarantee that any pair of nodes can find a common key between them. After that, C. W. Park *et al.* proposed an approach [2] to compute the U matrix based on the L matrix such that the same property as [1] is preserved but the time overhead of LU decomposition is avoided. A. K. Pathan and many other researchers proposed improved schemes [3, 4, 5] for ensuring the security and resilience of the network by using LU decomposition adopted from [1]. And later S. J. Choi and H. Y. Youn proposed a multi-level key pre-distribution scheme [6] for the security of WSNs based on [1].

Our Contributions. We find a mathematical property of LU decomposition of symmetric matrix. By using this property, we can calculate part of, even all of, the L matrix based on the U matrix and a little information about the L matrix, and vice versa. This would harm the security of actual usage of the LU decomposition scheme. As a result, if one node is broke, a large amount of, even all of the secret information of the L matrix would be easily recovered no matter what their product – the key matrix K – is. Therefore, people should protect every node, or change another decomposition method in order to preserve the merits of bringing symmetric matrix decomposition into key pre-distribution mechanism in WSNs.

Organization. The rest of this paper is organized as follows: section 2 briefly presents the original key pre-distribution scheme proposed by S. J. Choi and H. Y. Youn; section 3 analyzes the properties of the L and U matrixes decomposed from a symmetric matrix, and describes how to use such properties to calculate the secret information contained in nodes; section 4 gives the conclusion.

2 Choi and Youn's Scheme

Definition 1 *A symmetric matrix is a square matrix that is equal to its transpose, e.g. $K = K^T$. The elements of a symmetric matrix are symmetric with respect to the main diagonal (top left to bottom right), $k_{i,j} = k_{j,i}$.*

Definition 2 *LU decomposition is the process to decompose an $m \times m$ matrix K into two matrixes such that $K = LU$, where L is an $m \times m$ lower triangular matrix and U is an $m \times m$ upper matrix.*

The key pre-distribution process contains four steps [1]:

Step 1 : Generat a large pool of keys which are possibly to be used during the communication between nodes.

Step 2 : Form a symmetric matrix K by using the keys in the pool.

Step 3 : Apply LU decomposition to the symmetric key matrix K, then we get L and U.

Step 4 : Assign keys to nodes: every node is randomly assigned the data of one row of the L matrix and one column of the U matrix, where the row and the column have the same position in the matrix. For example, the data of ith row of the L matrix (denoted as L_{r_i}) and the ith column of the U matrix (denoted as U_{c_i}) should be assigned to a same node.

Finding common keys and authentication. If the ith node and the jth node want to build a secure communication, they first exchange the U matrix's column data which they have respectively (in WSNs the data would be broadcasted on the air), e.g. U_{c_i} and U_{c_j}. One thing to keep in mind is that the row data of the L matrix, e.g. L_{r_i} and L_{r_j}, should never be transmitted out of the nodes for the consideration of the security of the whole system. The two nodes compute vector products as follows:

$$\begin{aligned} \text{the } i\text{th node:} \quad & k_{i,j} = L_{r\_i} \times U_{c\_j} \\ \text{the } j\text{th node:} \quad & k_{j,i} = L_{r\_j} \times U_{c\_i} \end{aligned}$$

Because K is a systematic matrix, $k_{i,j} = k_{j,i}$. Then the two nodes use the calculated $k_{i,j}$ as the common secret key to communicate. And we would have varied methods for node-to-node authentication, such as checking whether the computed $k_{i,j}$ is equal to $k_{i,j}$.

3 Cryptanalysis

3.1 Mathematical Property

First let us analyze the property of the L and U matrixes decomposed from a symmetric matrix. Denote $L \times U = K$ as

$$\begin{bmatrix} l_{1,1} & & & & & \\ \vdots & \ddots & & & & \\ & & l_{t,t} & & & \\ & & l_{t,t+1} & \ddots & & \\ \vdots & & \vdots & & \ddots & \\ l_{m,1} & \cdots & l_{m,t} & \cdots & \cdots & l_{m,m} \end{bmatrix} \times \begin{bmatrix} u_{1,1} & \cdots & & & \cdots & u_{1,m} \\ & \ddots & & & & \vdots \\ & & u_{t,t} & u_{t,t+1} & \cdots & u_{t,m} \\ & & & \ddots & & \vdots \\ & & & & \ddots & \vdots \\ & & & & & u_{m,m} \end{bmatrix}$$

$$= \begin{bmatrix} k_{1,1} & \cdots & & & \cdots & k_{1,m} \\ \vdots & \ddots & & & & \vdots \\ & & k_{t,t} & \cdots & k_{t,j} & \\ & & \vdots & \ddots & & \\ \vdots & & k_{j,t} & & \ddots & \vdots \\ k_{m,1} & \cdots & & & \cdots & k_{m,m} \end{bmatrix}$$

We can easily get the following equations:

$$k_{i,j} = \begin{cases} l_{i,1}u_{1,j} + l_{i,2}u_{2,j} + \cdots + l_{i,i}u_{i,j} & (i < j) \\ l_{i,1}u_{1,j} + l_{i,2}u_{2,j} + \cdots + l_{i,i}u_{i,i} & (i = j) \\ l_{i,1}u_{1,j} + l_{i,2}u_{2,j} + \cdots + l_{i,j}u_{j,j} & (i > j) \end{cases}$$

Theorem 1 *If the product of an $m \times m$ lower triangular matrix L and an $m \times m$ upper triangular matrix U is an symmetric matrix, then*

$$l_{i,i} : l_{i+1,i} : \cdots : l_{m,i} = u_{i,i} : u_{i,i+1} : \cdots : u_{i,m}$$

where $1 \leq i < m$.

Proof. Induction.

When $i = 1$, assuming $i < j \leq m$, we have

$$\begin{cases} k_{1,j} = l_{1,1}u_{1,j} \\ k_{j,1} = l_{j,1}u_{1,1} \end{cases}$$

Since $k_{1,j} = k_{j,1}$, we have

$$l_{1,1}u_{1,j} = l_{j,1}u_{1,1}$$

which can also be denoted as

$$l_{1,1} : l_{j,1} = u_{1,1} : u_{1,j}$$

Thus

$$l_{1,1} : l_{2,1} : \cdots : l_{m,1} = u_{1,1} : u_{1,2} : \cdots : u_{1,m} \tag{1}$$

When $i = t > 1$, assume any $i = t' \in [1, t)$ satisfies Theorem 1. $k_{t,j} = k_{j,t}$, where $t < j \leq m$, implies

$$\begin{aligned} & l_{t,1}u_{1,j} + l_{t,2}u_{2,j} + \cdots + l_{t,t-1}u_{t-1,j} + l_{t,t}u_{t,j} \\ = \; & l_{j,1}u_{1,t} + l_{j,2}u_{2,t} + \cdots + l_{j,t-1}u_{t-1,t} + l_{j,t}u_{t,t} \end{aligned} \tag{2}$$

Since

$$l_{1,1} : l_{2,1} : \cdots : l_{m,1} = u_{1,1} : u_{1,2} : \cdots : u_{1,m}$$

we have

$$l_{t,1} : l_{j,1} = u_{1,t} : u_{1,j}.$$

that is

$$l_{t,1}u_{1,j} = l_{j,1}u_{1,t} \tag{3}$$

Similarly, we can prove

$$l_{t,2}u_{2,j} = l_{j,2}u_{2,t}\ ,\ \cdots\ ,\ l_{t,t}u_{t,j} = l_{j,t}u_{t,t} \tag{4}$$

Substituting (3) and (4) into (2) and simplifying gives

$$l_{t,t}u_{t,j} = l_{j,t}u_{t,t}$$

and so

$$l_{t,t} : l_{j,t} = u_{t,t} : u_{t,j}$$

Thus

$$l_{t,t} : l_{t+1,t} : \cdots : l_{m,t} = u_{t,t} : u_{t,t+1} : \cdots : u_{t,m} \tag{5}$$

Finally, from (1) and (5), we know that Theorem 1 holds for any $1 \leq t < m$.

The proof is complete. □

We take the sample matrixes in S. J. Choi and H. Y. Youn's paper [1] to illustrate Theorem 1:

$$L = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -1 & -6/7 & 1 \end{bmatrix} \text{ and } U = \begin{bmatrix} 2 & 4 & -2 \\ 0 & -7 & 6 \\ 0 & 0 & 29/7 \end{bmatrix} \tag{6}$$

The ratio of the column data of the L matrix is the same as the ratio of the U matrix's row data:

$$1 : 2 : -1 = 2 : 4 : -2$$

$$1 : -6/7 = -7 : 6$$

3.2 Paradigms

Recall that the nodes in WSNs should exchange the column vector U_{c_i} and U_{c_j} of the matrix U before they calculate a common secret key to communicate. The U_{c_i} and U_{c_j} are transmitted in plaintext, so potential adversaries eavesdrop on the air and will get almost all of the data of the U matrix in the worst case. Then by using Theorem 1, the adversaries will get the ratio of the elements in the column vectors of the L matrix as well. As a result, if the row vector contained in one node is gotten – the adversaries may need to break only one node – all of the L matrix's data with related positions would be calculated. One broken node would harm the security of the whole wireless network.

For example, if adversaries break the node containing L_{r_j} and get the all the data of the U matrix by eavesdropping, the rest of data of the matrix L which can be calculated is shown as the following figure. All of the data of L_{r_i}, where $i < j$, would be calculated, and part of the data of L_{r_i}, which $i > j$, would be calculated as well. More information L_{r_j} have – less zeroes are contained in the L_{r_j} – more data of the L matrix would be made out.

Especially, because of the publicity of the U matrix, we can know which node contains more information. This would be a great convenience for adversaries to choose their targets to break. We still take the above L and U matrixes (see (6)) for example. If we only know

$$L_{r\_2} = [2, 1, 0] \text{ and } U = \begin{bmatrix} 2 & 4 & -2 \\ 0 & -7 & 6 \\ 0 & 0 & 29/7 \end{bmatrix}$$

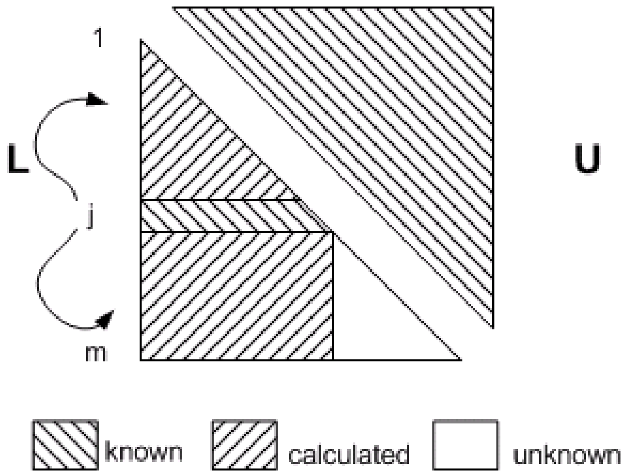

Figure 1: The coverage of the data which can be calculated when the jth node is broke.

By using Theorem 1 we can calculate as follows:

$$\begin{cases} l_{1,1} = \frac{u_{1,1}}{u_{1,2}} l_{2,1} = \frac{2}{4} 2 = 1 \\ l_{3,1} = \frac{u_{1,3}}{u_{1,2}} l_{2,1} = \frac{-2}{4} 2 = -1 \\ l_{3,2} = \frac{u_{2,3}}{u_{2,2}} l_{2,2} = \frac{6}{-7} 1 = -\frac{6}{7} \end{cases}$$

Thus we get

$$L' = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -1 & -6/7 & * \end{bmatrix}$$

part of which we computed is same as the data of the original sample matrix L.

Even if the adversaries are hard to get the full U matrix, they could still calculate certain row vector L_{r_i} which they are interested in within the following three steps:

Step 1 : Break one of the nodes, which contains L_{r_j} where $i < j$. In this step, people can choose the possible weak node to break, such as the one lacking enough hardware protection or whose protection is partially broken with age. Then we will get L_{r_j} and U_{c_j}.

Step 2 : Eavesdrop the communication of the node which is to be attacked, and get the information about U_{c_i}. If the target node is working, this step would also be easy.

Step 3 : Finally, by using Theorem 1 and the information about U_{c_i}, L_{r_j} and U_{c_j}, we can calculate L_{r_j}:

$$l_{i,t} = \frac{u_{t,i}}{u_{t,j}} l_{j,t}$$

The whole process is described as Figure 2 to show the differences with above process with Figure 1.

4 Conclusion

From the foregoing discussions, we can safely draw the conclusion that although the key pre-distribution scheme proposed by S. J. Choi and H. Y. Youn has convenience and merits in many aspects, the scheme has certain problems

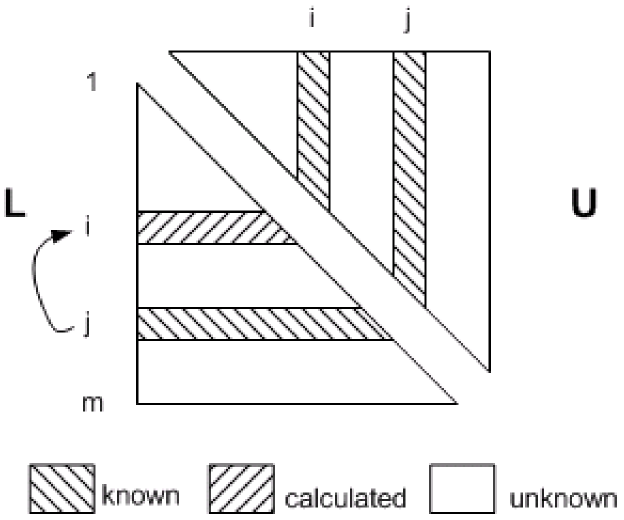

Figure 2: Calculate the ith node's secret information by first breaking the jth node.

which would harm the security of the whole wireless network. Because of the ratio relationship between the L and U matrixes decomposed from a symmetric matrix, people can calculate all of, or part of, the secret information contained in one node via the information of another node in the same wireless network. Consequently, people should fully protect every node to secure the entire network, especially the nodes carrying the most amount of information.

The basic mind of S. J. Choi and H. Y. Youn that using symmetric matrix is still a good idea, since it guarantees each pair of nodes can calculate a secret common key for communication and perform mutual authentication but do not increase overloads of calculation and storage for each node. Because Theorem 1's proof uses induction method and the structure characteristics of the lower and upper matrixes, the matrixes decomposed from an symmetric matrix by using another method - not the LU decomposition - may not satisfy the Theorem 1. Thus we might be able to use other methods to decompose the key matrix K for the key pre-distribution of the wireless sensor networks to preserve the convenience and avoid the shortages of LU decomposition scheme.

References

[1] S. J. Choi and H. Y. Youn, *An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Networks*, EUC Workshops 2005, LNCS 3823, pp. 1088-1097, 2005.

[2] C. W. Park, S. J. Choi, and H. Y. Youn, *A Noble Key Pre-distribution Scheme with LU Matrix for Secure Wireless Sensor Networks*, CIS 2005, Part II, LNAI 3802, pp. 494-499, 2005.

[3] A. K. Pathan, T. T. Dai, and C. S. Hong, *A Key Management Scheme with Encoding and Improved Security for Wireless Sensor Networks*, ICDCIT 2006, LNCS 4317, pp. 102-115, 2006.

[4] T. T. Dai, A. K. Pathan, and C. S. Hong, *A Resource-Optimal Key Pre-distribution Scheme with Enhanced Security for Wireless Sensor Networks*, APNOMS 2006, LNCS 4238, pp. 546-549, 2006.

[5] A. K. Pathan, T. T. Dai, and C. S. Hong, *An Efficient LU Decomposition-based Key Pre-distribution Scheme for Ensuring Security in Wireless Sensor Networks*, CIT'06, Proceedings of The Sixth IEEE International Conference on Computer and Information Technology, p. 227, 2006.

[6] S. J. Choi and H. Y. Youn, *MKPS: A Multi-level Key Pre-distribution Scheme for Secure Wireless Sensor Networks*, Human-Computer Interaction, Part II, HCII 2007, LNCS 4551, pp. 808-817, 2007.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *A survey on sensor networks*, IEEE Communications Magazine, 40(8):102-114, August 2002.

[8] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. *Security in Distributed, Grid, and Pervasive Computing*, Chapter 17, Auerbach Publications, CRC Press, 2006.