A Resource-Optimal Key Pre-distribution Scheme for Secure Wireless Sensor Networks

Tran Thanh Dai*, Cao Trong Hieu**, Choong Seon Hong***
Dept. of Computer Engineering, Kyung Hee University
E-mail : daitt@networking.khu.ac.kr, hieuct@networking.khu.ac.kr,
cshong@khu.ac.kr

Abstract

Security in wireless sensor networks is very pressing especially when sensor nodes are deployed in hostile environments. To obtain security purposes, it is essential to be able to encrypt and authenticate messages sent amongst sensor nodes. Keys for encryption and authentication must be agreed upon by communicating nodes. Due to resource limitations and other unique features, obtaining such key agreement in wireless sensor network is extremely complex. Many key agreement schemes used in general networks, such as trusted server, Diffie-Hellman and public-key based schemes, are not suitable for wireless sensor networks [1], [2], [5], [7], [8]. In that situation, key pre-distribution scheme has been emerged and considered as the most appropriate scheme [2], [5], [7]. Based on that sense, we propose a new resource-optimal key pre-distribution scheme utilizing merits of the two existing key pre-distribution schemes [3], [4]. Our scheme exhibits the fascinating properties: substantial improvement in sensors' resource usage, rigorous guarantee of successfully deriving pairwise keys between any pair of nodes, greatly improved network resiliency against node capture attack. We also present a detailed analysis in terms of security and resource usage of the scheme.

1. Introduction

Wireless sensor networks are comprised of many extremely small devices, called sensors, which are capable of sensing physical stimuli such as light, temperature, and sound. These sorts of networks have several unique characteristics. First of all, sensor networks don't require any fixed infrastructure (except perhaps for a base station). They are purely ad hoc in nature meaning that nodes may join (i.e.-activate) or leave (i.e.-fail) constantly. Secondly, individual sensor nodes are designed to be inexpensive as they must be purchased in large quantities for most purposes. This low cost requirement means that sensor nodes are severely resource constrained. Finally, since sensors run on battery power, energy consumption is a huge concern. In many cases, there is no way to replace a sensor's battery, resulting in a node failure once the battery is exhausted. These bring about a need for energy and memory efficient algorithms for sensor networks.

When sensor networks are deployed in hostile environment, security becomes extremely critical, as they are prone to be easily compromised by different types of malicious attacks. For instance, an adversary can effortlessly listen to the traffic, impersonate one of the network nodes, or deliberately provide misleading information to other nodes. To provide security, communication should be encrypted and authenticated. The open problem is how to guarantee secure communications between sensor nodes by, for example, setting up a key agreement between communicating nodes? [2]. To deal with the key agreement problem, there are three categories of scheme: key distribution center scheme, public key scheme, and key pre-distribution scheme. However, constrained computation and energy resources of sensor nodes often make the two first schemes worthless [1], [2], [5], [7], [8]. The third category of key management scheme is key pre-distribution scheme, where keying material is delivered to all sensor nodes prior to deployment. There have been a number of documents proving that this kind of scheme is only feasible solution to key agreement problem in sensor networks [2], [5], [7]. Based on these analyses, we come up with a new key pre-distribution scheme in which utilizing advantages of two existing schemes [3], [4].

In this paper, we propose a new key pre-distribution scheme. The fascinating and principal contributions of the scheme are roughly listed as follows:

1. Essential improvement in sensors' resource usage including memory and energy usage.
2. Rigorous guarantee of successfully deriving pairwise keys that enable node-to-node authentication.
3. Greatly improved network resiliency against node capture attack.
4. Theoretical analysis of security, communication and computation overhead.

Our scheme is based on S. Choi's key pre-distribution scheme [3] and combine Blom's key generation scheme [4] with it. Our later analysis shows that our combined scheme is much better than each of the two schemes.

The rest of the paper is organized as follows: section 2 briefly describes key pre-distribution schemes in the recent

This work was supported by MIC and ITRC project.

literature; section 3 gives an overview of our building blocks; section 4 is used to present our combined key pre-distribution scheme; section 5 present analyses of the security and resource usage of our scheme; lastly, Section 6 is a brief conclusion to highlight the major points of our scheme.

2. Related Works

L. Eschenauer and V. Gligor proposed a random key pre-distribution scheme (referred as basic probabilistic key sharing scheme in the rest of this paper): prior to sensor network deployment, each sensor node is distributed a ring of keys, each key ring consisting of randomly chosen k keys from a large pool of P keys, which is generated off-line. To agree on a key for communication, two nodes find one common key within their key rings and use that key as their shared secret key [5].

S.J. Choi and H.Y. Youn proposed a key pre-distribution scheme guaranteeing that any pair of nodes can find a common secret key between themselves by using the keys assigned by LU decomposition of a symmetric matrix of a pool of keys. The detailed description will be mentioned later in the paper [3].

Du et al. proposed a method to improve the basic scheme by exploiting a priori deployment knowledge. Specifically, by using node deployment knowledge and a wise key ring setup, the sensor networks get much higher probability of establishing a secure link between any pairwise of nodes [6]. They also proposed a pairwise key pre-distribution scheme for wireless sensor networks. This scheme first uses Blom's key generation scheme [4] as a building block to generate multiple key spaces, a pool of tuple (D, G) , where matrices D and G are as defined in Blom's scheme. Then considering the pool of tuple (D, G) as a pool of key as in the basic scheme, it utilizes the idea of the basic scheme to establish a common secret key between any pair of nodes [2].

3. Overview of Our Building Blocks

3.1 LU key decomposition scheme

This scheme consists of four off-line steps. The following are detailed discussions of these steps.

Step 1 (Large key pool generation): In this step, a large pool of keys P with size s is generated along with their identifiers. This pool will be used for the symmetric matrix formation step.

Step 2 (Symmetric key matrix formation): In this step, a *NxN* symmetric key matrix M is generated where *N* is the maximum number of sensor nodes that can be deployed. Each element M_{ij} of *M* is assigned a distinct key from key pool P such that $M_{ij} = M_{ji}, i, j = \overline{1, N}$.

Step 3 (LU decomposition): In this step, LU decomposition is applied to matrix M. The results of this decomposition are two matrices L and U. L is a $N \times N$ lower triangular matrix and U is an $N \times N$ upper triangular matrix such that M = LU.

Step 4 (LU key pre-distribution): In this step, every sensor node is randomly assigned one row from the L matrix and one column from the U matrix, respectively. Specifically, the ith row of L (Lr(i)) and the ith column of U (Uc(i)) always go together when assigned to a sensor node.

Finding a common key: Assume that sensor Si and sensor Sj contains (Lr(i), Uc(i)) and (Lr(j), Uc(j)) respectively. When Si and Sj need to find a common secret key between them for future use, they first exchange their columns, and then compute vector products as follows:

S_i: $Lr(i) \times Uc(j) = M_{ij}$

S_j: $Lr(j) \times Uc(i) = M_{ji}$

Because M is the symmetric matrix, and thus $M_{ij} = M_{ji}$. M_{ij} (or M_{ji}) is then used as a common key between S_i and S_j.

3.2 Blom's symmetric key generation scheme

During the pre-deployment phase, firstly, a (λ + 1) x N matrix G over a finite field GF(q), where N is the maximum number of sensor nodes in the network and λ is the security parameter discussed above, is constructed. G is considered as public information. Since each pairwise key is represented by an element in GF(q), if the length of pairwise keys is 64 bits, then we should choose q as the smallest prime number that is larger than 2^{64}. In order to achieve the λ-secure property any $\lambda + 1$ columns of G must be linearly independent. Secondly, a random (λ + 1) x (λ + 1) symmetric matrix D over GF(q) is computed and used to compute an N x (λ + 1) matrix A, which is equal to $A = (D.G)^T$, where $(D.G)^T$ is the transpose of $D.G$. Matrix D needs to be kept secret and should not be disclosed to adversaries or any sensor node. Because D is symmetric, it is easy to see: $K = A.G = (A.G)^T$. Thus, $K_{ij} = K_{ji}$, where K_{ij} is the element in K located in the ith row and jth column. Finally, the kth row of matrix A and the kth column from matrix G is stored at sensor node k, where $k = \overline{1, N}$.

After deployment, two sensor nodes i and j can find the pairwise key between them by exchanging their columns of G and using their private rows of matrix A to compute

$$K_{ij} = K_{ji} = A(i).G(j) = A(j).G(i)$$

4. Our key pre-distribution scheme

Our proposal of a new key pre-distribution scheme is a combination of the two above-mentioned schemes with some modifications so that it is more appropriate for the memory-constrained characteristic of wireless sensor networks. Accordingly, we only store in each sensor node keying materials used to derive two key halves which constitute a pairwise key. The first key half is generated by LU key decomposition scheme. The second half is generated after deployment by using Bloom's key computation scheme. The figure 2 below illustrates the components of a pairwise key.

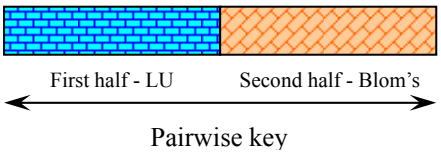

Fig. 1. Components of a pairwise key

Following is the detail of our key pre-distribution proposal. It consists of two phase: *key pre-distribution phase* and *shared key establishment phase*.

4.1 Key pre-distribution phase

During the key pre-distribution phase, we need to assign keying information to each node, such that after deployment, neighboring sensor nodes can find a secret key between them. Suppose that each sensor node has a unique identification whose range is from 1 to *N*. On one hand, the key pre-distribution phase resorts to LU key decomposition scheme. That is, we have to go through four steps as described above(section 3.1). On the other hand, each sensor node must be assigned the other keying information used by Blom's key generation scheme. That is, we have to provide column G(j) and row A(j) to node j.

4.2 Pairwise key establishment phase

The followings are detailed steps happening in sequence so that two nodes S_i and S_i can derive a common pairwise key:

1. S_i and S_j use some mechanism to discover the location of the other (i.e, using query broadcast messages).
2. S_i and S_j exchange with each other a message consisting of a column Uc(i) (Uc(j)) from matrix U and a seed to generate G(i) (G(j)) from matrix G.
3. S_i and S_j then compute the first half of the pairwise key as follows: $S_i : L_r(i) \times U_c(j) = M_{ij}$ $S_j : L_r(j) \times U_c(i) = M_{ji}$
4. S_i and S_j compute the second half of the pairwise key using the following equation: $K_{ij} = K_{ji} = A(i).G(j) = A(j).G(i)$.

The simplest way is to concatenate the first half with the second half. The pairwise key can also be created by using an one-way function. This pairwise key is stored in the two sensors' memory for further use.

5. Analysis of Our Scheme

5.1 Memory Usage and Security Analysis

In this section, we analyze our scheme in comparison with the three existing key pre-distribution schemes from which highlighting the merits of our scheme: Laurent Eschenauer and D. Gligor's scheme (basic probabilistic key sharing scheme), Bloom's scheme, and Sung Jin Choi and Hee Yong Youn's scheme (LU key decomposition scheme).

The reason that we analyze the basic probabilistic key sharing scheme in comparison with our scheme is that this scheme has been used as a building block in many key distribution schemes in wireless sensor networks such as in [1], [2], [6], [7]. Hence, showing drawbacks of this scheme is to show drawbacks of other schemes relying on it. Actually, this scheme has some drawbacks. The first one is that the shared key between any two neighboring nodes is found based on a probability of a key's occurrence in their key rings. It follows that there still exists a probability that any two neighboring nodes cannot find a common shared key. Therefore, in a bad case, a node may need to use a multi-link path to establish a pairwise key with one of its neighbors. Obviously, this imposes communication cost on those communicating nodes. In the worst case, a disconnected key graph may be created. It means that there exist unsecured communication links in the whole network. The second one is that each sensor node in this scheme has to memorize the full length of each key in its key ring. It is even worse when noticing that many keys in the ring are not utilized after deployment. The third one is that compromise of one key does lead to the compromise of another link between pairs of uncompromised nodes. On the contrary, our proposed scheme overcomes these drawbacks by guaranteeing any two neighboring nodes to directly derive a pairwise key. Moreover, instead of storing the full length of each shared key in memory initially, each sensor node only needs to store the keying information used for generating two halves of pairwise keys when needed. Hence sensors' memory usage is reduced. We can also improve sensors' memory usage by noticing that L and U are a lower triangle matrix and an upper triangle matrix, respectively. Each row of L and each column of U have two portions. The first portion consists of nonzero elements. The second portion consists of zero elements. Therefore, to store one row of L and one column of U in each sensor, we only need to store the nonzero portions of them and two values specifying the number of zero elements in each row and column, respectively. This storing method will be extremely effective if the size of network is very large.

Now we dig into the demerits of Blom's scheme to highlight the merits of our proposal. Blom's scheme has λ-secure property. That is, the network is perfectly secure if no more than λ nodes are compromised. Increasing λ results in greater network resiliency but also results in higher memory usage within each sensor node. Thus, it is obvious that λ plays an important role in securing the whole network. But in our proposal, the role of λ is very minor. The reason is that our pairwise key consists of two different parts: one part from LU scheme, the other part from Blom's scheme. Thus, if an adversary compromises even more than λ nodes, it only knows the keys of those nodes; all the remaining pairwise keys are still uncompromised. For this reason, we can choose a small value for λ to reduce memory usage within each sensor node.

We also find out some drawbacks in LU key decomposition scheme. The first drawback is that in this scheme, the authors did not mention how to effectively store

one row of L and one column of U in each sensor as mentioned above. The worse drawback is that the sensors in network initially have to memorize the full length of all keys in rows and columns of L and U respectively. In contrast, in our scheme, each sensor only needs to memorize keying information in a row and a column with their length reduced by half. From the figure 3, it is apparent that our scheme is much more efficient than LU decomposition scheme, especially when sensor nodes are deployed in the great number.

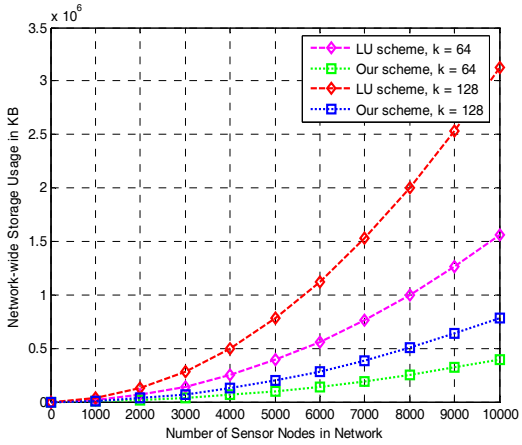

Fig. 2. Network-wide storage usage of our scheme and LU scheme ($\lambda = 40$)

5.2 Communication Overhead Analysis

In our scheme, communication overhead for pairwise key establishment is considerably reduced. The traffic in the initial broadcast of each node is reduced. In the Eschenauer et al., the information needed to transmit is the list of identifiers of the keys on a sensor node's key ring. The traffic is very higher than that in the broadcast of our scheme because in case of our scheme the information needed to broadcast is receiver (Sj)'s identifier to query the location of receiver. Furthermore, there is no need to include the path-key establishment phase as in Eschenauer's proposal because any two sensor nodes within their communication range can directly derive a shared key between them.

6. Conclusions

We have presented a new pairwise key pre-distribution scheme for wireless sensor network. Our scheme utilizes merits of the two existing key pre-distribution schemes with some modifications to make it more suitable for wireless sensor networks. Our scheme has a number of fascinating properties. First, our scheme guarantees that any pair of neighboring nodes can directly derive a common secret key between themselves by combining LU key decomposition scheme and Blom's key generation scheme. Second, compared to the existing key pre-distribution schemes, our scheme is substantially more memory and energy usage-optimal. Thus, it is more suitable for memory-limited devices like sensor nodes. Third, our scheme is rather flexible because some security features can be added into the scheme to make it more robust. It is also scalable because sensor nodes do not need to be deployed simultaneously; they can be added later, and still be able to derive secret keys with existing nodes.

References

[1]. H. Chan, A. Perrig, and D. Song. "Random key predistribution schemes for sensor networks", IEEE Symposium on Security and Privacy, 2003.

[2]. W. Du, J. Ding, Y. Han, and P. Varshney. "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks", Proceedings of the ACM Conference on Computer and Communication Security (CCS'03), Washington, D.C., October 27-30, 2003.

[3]. S. Choi and H. Youn. "An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Networks", EUC Workshops 2005, LNCS 3823, pp. 1088-1097, IFIP International Federation for Information Processing, 2005.

[4] R. Blom. "An optimal class of symmetric key generation systems", Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), Lecture Notes in Computer Science, Springer-Verlag, 209:335-338, 1985.

[5] L. Eschenauer and V.D. Gligor. "A key-management scheme for distributed sensor networks", Proceedings of the 9th ACM conference on Computer and communication security, Nov. 2002.

[6] Wenliang Du; Jing Deng; Han, Y.S.; Shigang Chen; Varshney, P.K. "A key management scheme for wireless sensor networks using deployment knowledge", INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. Volume 1, 7-11 March 2004 Page(s): Digital Object Identifier 10.1109/INFCOM.2004.1354530.

[7] D. Liu and P. Ning. "Establishing Pairwise Keys in Distributed Sensor Networks", Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003.

[8] W. Lei, C. Zhi-ping, J. Xin-hua. "Researches on Scheme of Pairwise Key Establishment for Distributed Sensor Networks", WMuNeP'05, October 13, 2005, Montreal, Quebec, Canada.