An ID-Based Random Key Pre-distribution Scheme for Wireless Sensor Networks*

Tran Thanh Dai and Choong Seon Hong**

Networking Lab, Department of Computer Engineering, Kyung Hee University, Korea
daitt@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract. When wireless senor networks (WSNs) are deployed in hostile areas, they indeed need to be secured by security mechanisms. To do this, cryptographic keys must be agreed on by communicating nodes. Unluckily, due to resource constraints, the key agreement problem in wireless sensor networks becomes quite intricate. In this paper, we propose a new ID-based random key pre-distribution scheme that is comparable to Du et al.'s scheme [2] in terms of network resiliency and memory usage. On the other hand, our later analysis shows that our scheme outperforms Du et al.'s scheme in terms of computational and communication overhead.

Keywords: ID-based, random key pre-distribution, key agreement, security, wireless sensor networks.

1 Introduction

There has been a trend that WSNs have been getting mature together with wider and wider applications and deployments. In such trend, providing security services based on solving the key agreement problem becomes one of the major concerns. Unfortunately, due to resource constraints of WSNs, such problem becomes quite intricate. Motivated by such challenge, in this paper, we propose a highly resilient, robust, resource-efficient, and ID-based random key pre-distribution scheme. Our scheme as analyzed later is much like Du et al.'s scheme [2] (*Du's scheme*) regarding network resiliency with the same memory cost. Moreover, our scheme significantly improves resource usage relating to computational and communication overhead compared to Du's scheme. The rest of this paper is organized as follows: section 2 mentions the related work; section 3 describes our ID-based random key pre-distribution scheme; section 4 analyzes the resiliency of our scheme against node capture attack and presents the performance analysis in terms of memory usage, communication overhead, and computational overhead; section 5 concludes the paper and states our future work.

2 Related Work

Matsumoto and Imai proposed an efficient scheme (IM scheme) for the key agreement problem between two entities [1]. Fig. 1 illustrates how a pairwise

* This work was supported by MIC and ITRC Project.
** Corresponding author.

Y. Shi et al. (Eds.): ICCS 2007, Part IV, LNCS 4490, pp. 590–593, 2007.

key $K_{ij} = K_{ji}$ is generated where N - maximum number of deployable nodes; $m = \log_2(N)$ - number of bits used to represent an effective ID of each entity; l - number of $(m \times m)$ symmetric matrices M_ωs over finite field $GF(2)$; y_i $(i = \overline{1, N})$ - m-dimensional vector, effective ID of node S_i; y_i $(i = \overline{1, N})$ - m-dimensional vector, effective ID of node S_i.

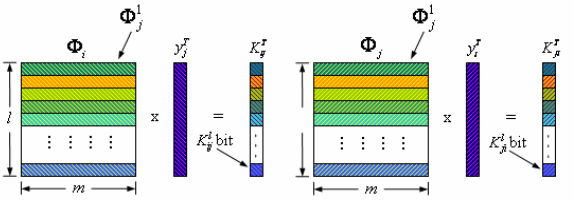

Fig. 1. Pairwise key generating in MI scheme

3 ID-Based Multiple Space Key Pre-distribution Scheme

3.1 Keying Material Pre-distribution Phase

During this phase, we have to pre-distribute keying material to each node such that after deployment neighboring nodes can derive a pairwise key between them using this material. This phase is performed as follows. First, a central server generates λ key spaces. Each key space Ω_i consists of l $(m \times m)$ symmetric matrices $M_{i\omega}$s as defined in IM scheme. Then, we randomly choose μ distinct key spaces from key spaces for each node. For each space chosen by node S_j, we first compute keying material Φ_{ji} and then store it at this node. Therefore, each node S_j has distinct values of Φ_{ji}s. Using MI scheme; two nodes can derive a pairwise key if they have both chosen a common key space.

3.2 Pairwise Key Establishment Phase

After deployment, each node needs to discover whether it shares any key space with its neighbors. Suppose that nodes S_i and S_j are neighbors, then they instantly broadcast a message containing the following information: each node's effective ID and the indices of the key spaces it carries. If they figure out that they have an identical index of a key space (or identical key space Ω_s), they can easily compute their pairwise key using MI scheme. Conversely, there is the case that two nodes who even are neighbors could not establish a pairwise key. To tackle this problem, the method presented in [2] could be utilized. Due to the limited size of paper, we do not discuss in detail here.

4 Security and Performance Analysis

Our security evaluation is conducted by finding the answer to two questions: (i) Given that b nodes are captured, what is the probability that at least one key space is broken? (ii) Given that b nodes are captured, what fraction of the additional communications (communications among un-captured nodes) also becomes compromised? These two questions are already answered in [2]. The answer to the first question is as follows:

$$P(\text{at least one space is broken}|C_b) = \lambda \sum_{k=m}^{b} \binom{b}{k} \left(\frac{\mu}{\lambda}\right)^k \left(1-\frac{\mu}{\lambda}\right)^{b-k}. \quad (1)$$

The answer to the second question is the following equality:

$$P(s \text{ is broken}|C_b) = \sum_{k=m}^{b} \binom{b}{k} \left(\frac{\mu}{\lambda}\right)^k \left(1-\frac{\mu}{\lambda}\right)^{b-k}. \quad (2)$$

where s denotes an additional secure communication link.

To analyze our scheme performance, we evaluate its memory usage, communication overhead, and computational overhead using Du's scheme as a benchmark. For each key space, according to MI scheme, each node S_i has to spend $m \times l$ bits on storing the value of Φ_i. Thus the total memory usage (KB) for each node with μ chosen key spaces is: $\frac{m \times l \times \mu}{8 \times 1024}$. This value is exactly identical to the memory consumption of Du's scheme. Concerning the communication overheads of our scheme and Du's scheme, we draw a self-explanatory comparison as shown in fig. 2.

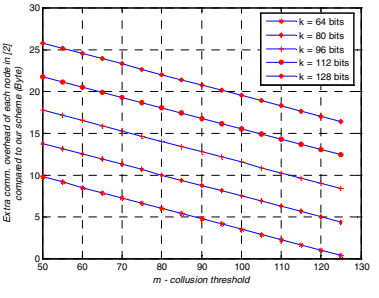

Fig. 2. Extra communication overhead of each node in [2] compared to our scheme

Regarding computational overhead, to compute a pairwise key, each node of our scheme needs to perform a multiplication of a $(l \times m)$ matrix and an $(m \times 1)$ effective ID. Therefore, each node needs $l \times m$ single-precision multiplications while each node in [2] needs to do $2 \times (m-1) \times l^2$ single-precision multiplications. It follows that the computational overhead of our scheme is far less than that in [2]. The numbers in fig. 3 reinforce our argument.

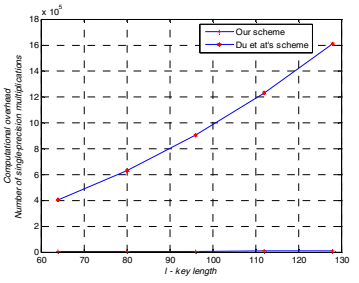

Fig. 3. Computational overhead in each node with various key lengths

5 Conclusions and Future Work

This paper proposes a new key pre-distribution scheme for WSNs that can be considered as a refinement of two types of schemes: ID-based key pre-distribution scheme and random key pre-distribution scheme. As a result, our scheme possesses a number of attractive properties. First, our scheme is scalable and flexible in terms of network size. Second, our scheme substantially improves network resiliency against node capture attack compared to schemes [3], [4] and are comparable to Du's scheme. The performance of our scheme is also investigated to show its efficiency. Accordingly, our scheme is the same as Du's scheme in terms of memory usage. Moreover, our scheme is more efficient than Du's scheme concerning communication overhead. Finally, computational overhead of our scheme is argued to be far less than that of Du's scheme. However, our scheme is still vulnerable to node replication attack and key-swapping collusion attack. Therefore, in our future work, we would like to explore additional mechanisms to efficiently and radically thwart these attacks.

References

1. Matsumoto, T., Imai, H.: On the Key Predistribution System: A Practical Solution to the Key Distribution Problem. CRYPTO'87, LNCS Vol. 293, 8(1987)185-193
2. Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A.: A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Info. Sys. Sec., Vol. 8, No. 2, 5(2005)228-258
3. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. Proc. of the 9th ACM Conference on Computer and Communications Security, 11(2002) 41-47
4. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. Proc. IEEE Symposium on Security and Privacy, 5(2003)197-213