A Robust Pair-wise Rekeying Protocol in Hierarchical Wireless Sensor Networks

An-Ni Shen and Song Guo
School of Computer Science and Engineering, University of Aizu, Japan
{d8102105,sguo}@u-aizu.ac.jp

ABSTRACT

To support secure communications for many applications in wireless sensor networks (WSNs), some strategies have been proposed to develop the pair-wise rekeying protocol. However, most existing schemes suffer the node capture attack. In this paper, we present a perturbation-based pair-wise rekeying scheme for a hierarchical WSN. Our security analysis shows that the proposed scheme is robust to the node capture attack.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; E.3 [**Data Encryption**]: *Code breaking*

General Terms

Design, Security

Keywords

Key management, rekeying

1. INTRODUCTION

It is desirable to design key distribution protocols to support secure and robust pair-wise communication among any pair of sensors in WSNs. Conventional asymmetric key cryptosystem, such as Diffie-Hellman and RSA, can not be implemented in WSNs because sensor nodes have very limited capacities. Therefore, only lightweight energy efficient key distribution mechanisms are affordable.

When a WSN runs for a long time using a fixed key on a link, it enhances the probability for the adversaries to decrypt the key by analyzing adequate messages eavesdropped or by capturing some nodes. Under this circumstance, the entire network security might be threatened. Thus, it is necessary to update pair-wise keys periodically. In order to solve this problem, some rekeying protocols, *e.g.*, [2], have been proposed recently.

Most existing schemes suffer the node capture attack [1], by which an adversary might easily capture a group of sensor devices to acquire their sensitive data and then derive some secret information to further compromise the subsequent keys between other non-captured nodes. This motivates us to design new rekeying protocols by exploiting the characteristic of the perturbation polynomial [3] that can achieve high robustness to this attack.

CoNEXT Student Workshop'09, December 1, 2009, Rome, Italy.
ACM 978-1-60558-751-6/09/12.

2. PRELIMINARIES

A sensor network is divided into clusters, which are the minimum unit for detecting events. A cluster head (CH) coordinates all the sensor nodes (SNs) inside a cluster. As the basis of our pair-wise rekeying protocol for any wireless link between a CH and a SN, the polynomial-based key predistribution scheme originally proposed by Blundo *et al.* [1] works as follows.

Let F_q be a finite field, in which q is the maximum prime number satisfying $q < 2^\ell$ that can accommodate a cryptographic key with ℓ bits. To achieve t-resilience using the scheme of Blundo *et al.* [1], a random symmetric bivariate polynomial $f \in F_q[x, y]$ of degree t in each variable is chosen as the master secret polynomial:

$$f(x, y) = \sum_{i=0}^{t} \sum_{j=0}^{t} a_{ij} x^i y^j. \quad (1)$$

The coefficients a_{ij} ($a_{ij} = a_{ji}$) are randomly chosen from F_q. A node with Id $u \in F_q$ is preloaded the univariate polynomial:

$$g_u(y) = f(u, y). \quad (2)$$

The shared key $K_{v,u}$ between nodes v and u is

$$g_v(u) = f(v, u) = g_u(v), \quad (3)$$

which both parties can compute using the fact that $f(x, y)$ is symmetric. The security proof in [1] ensures that this scheme is unconditionally secure and t-collusion resistant; *i.e.*, a coalition of no more than t compromised nodes cannot know anything about the key shared by any two non-compromised nodes. However, an attacker who compromises $t+1$ nodes can use interpolation to recover the master polynomial $f(x, y)$.

Our proposed pair-wise rekeying protocol exploits the characteristic of the perturbation polynomial, which was originally introduced in [3]. Given a finite field F_q, a positive integer r ($r < \ell$), and a set of node Ids S ($S \subset \{0, \cdots, q-1\}$), a polynomial set Ω is a set of perturbation polynomials regarding r and S if any polynomial $\phi(\cdot) \in \Omega$ has the following *limited infection* property:

$$\forall S_j \in S, \phi(S_j) \in \{0, \cdots, 2^r - 1\}. \quad (4)$$

3. A PAIR-WISE REKEYING PROTOCOL

Before sensor devices are deployed into usage, some secret information should be pre-assigned as follows. Each cluster head a needs to be preloaded with a unique Id CH_a and a perturbed polynomial $\overline{g}_{CH_a}(y)$:

$$\overline{g}_{CH_a}(y) = g_{CH_a}(y) + \phi_{CH_a}(y). \quad (5)$$

Similarly, for each sensor node i, the security server preloads it with a unique Id SN_i and a perturbed polynomial $\overline{g}_{SN_i}(y)$:

$$\overline{g}_{SN_i}(y) = g_{SN_i}(y) + \phi_{SN_i}(y). \quad (6)$$

After the key pre-assignment phase, wireless sensors are randomly distributed in a given area, and later on, some clustering algorithm shall organize the network into a hierarchical structure. Now we consider the intra-cluster protocol for pair-wise key establishment and the subsequent rekeying as described in the followings.

- Step 1: At the beginning of each rekeying phase, CH_a randomly generates a new univariate polynomial function $p_{CH_a}(y)$. For each of its sensor node SN_i, CH_a updates the corresponding pair-wise key K_{CH_a,SN_i} as

  $$K_{CH_a,SN_i} = H^{\ell-r}(p_{CH_a}(SN_i)), \quad (7)$$

  in which $H^k(x)$ returns a hashed value based on the most significant k bits of x.

- Step 2: CH_a uses the preloaded polynomial to construct

  $$w_{CH_a}(y) = p_{CH_a}(y) + \overline{g}_{CH_a}(y) \quad (8)$$

  and broadcasts $w_{CH_a}(y)$ and CH_a to all its sensor nodes.

- Step 3: Upon receiving the broadcast message, each SN_i evaluates three candidate keys K^*, K^+ and K^- as follows, respectively.

  $$K^* = H^{\ell-r}\left(w_{CH_a}(SN_i) - \overline{g}_{SN_i}(CH_a)\right) \quad (9)$$

  $$K^+ = H^{\ell-r}\left(w_{CH_a}(SN_i) - \overline{g}_{SN_i}(CH_a) + 2^r\right) \quad (10)$$

  $$K^- = H^{\ell-r}\left(w_{CH_a}(SN_i) - \overline{g}_{SN_i}(CH_a) - 2^r\right) \quad (11)$$

- Step 4: The exact new pair-wise key is determined once a message over this link can be decoded successfully using one of the candidate keys.

Note that due to the characteristic of the perturbation polynomial [3], only one of the candidate keys (9) - (11) will be validated as the new pair-wise key between SN_i and CH_a, *i.e.*,

$$K_{CH_a,SN_i} \in \left\{K^*, K^+, K^-\right\}. \quad (12)$$

The inter-cluster rekeying protocol for CH-CH links works in a similar manner and thus is omitted here.

4. SECURITY ANALYSIS

In this section, we give a security analysis for our proposed rekeying protocol in terms of robustness to the node capture attack. We assume that an adversary has compromised n_c sensor nodes in cluster a, denoted as CS_k $(k = 1, \cdots, n_c > t)$, and has obtained all their preloaded information.

To derive the polynomial $p_{CH_a}(y)$ that is used to generate the new pair-wise key as shown in (7), the adversary needs to break $\overline{g}_{CH_a}(y)$ because $p_{CH_a}(y) = w_{CH_a}(y) - \overline{g}_{CH_a}(y)$ and $w_{CH_a}(y)$ is the public information broadcasted by CH_a. Furthermore, for any sensor node y of CH_a, the corresponding pair-wise key $K_{CH_a,y}$ satisfies:

$$\begin{aligned} K_{CH_a,y} &= H^{\ell-r}\left(w_{CH_a}(y) - \overline{g}_{CH_a}(y)\right) \\ &= H^{\ell-r}\left(w_{CH_a}(y) - g_{CH_a}(y) - \phi_{CH_a}(y)\right) \\ &= \begin{cases} H^{\ell-r}\left(w_{CH_a}(y) - g_{CH_a}(y)\right), & \text{or} \\ H^{\ell-r}\left(w_{CH_a}(y) - g_{CH_a}(y) - 2^r\right). \end{cases} \end{aligned}$$

The above equation shows that to break $\overline{g}_{CH_a}(y)$ is equivalent to break $g_{CH_a}(y)$ or $f(CH_a, y)$. This can be done by collecting a number of polynomials $\overline{g}_{CS_k}(y)$ stored in the compromised sensor nodes, which satisfy

$$\overline{g}_{CS_k}(y) = f(CS_k, y) + \phi_{CS_k}(y). \quad (13)$$

It can be formulated as a linear equation system as follows.

$$\sum_{i=0}^{t} a_{ij} \cdot (CS_k)^i + b_{kj} = d_{kj}, 0 \le j \le t, 1 \le k \le n_c \quad (14)$$

Note that a_{ij} and b_{kj} are the variables of this linear equation system, which are defined by (1) and the following equation

$$\phi_{CS_k}(y) = \sum_{j=0}^{t} b_{kj} \cdot y^j, 1 \le k \le n_c, \quad (15)$$

respectively. On the other hand, the values of d_{kj} are known to the adversary:

$$\overline{g}_{CS_k}(y) = \sum_{j=0}^{t} d_{kj} \cdot y^j, 1 \le k \le n_c. \quad (16)$$

By applying a similar reasoning technique in [3], we can derive that the probabilities to break $f(x, y)$ and $g_{CH_a}(y)$ (*i.e.*, $f(CH_a, y)$) in one attempt are both $\omega^{-(t+1)}$, in which $\omega = |\Omega| \ge 2$. Finally, we can conclude that the computational complexity for breaking $p_{CH_a}(y)$ under the condition of $t+1$ compromised nodes is $\Omega\left(\omega^{t+1}\right)$.

5. CONCLUSIONS

The traditional pair-wise rekeying protocol [2] suffers the node capture attack. Once $t+1$ nodes are compromised, all previous and future keys for any pair of nodes will be disclosed. Our proposal can significantly improve the security level by reducing this probability from 1 down to $\omega^{-(t+1)}$.

6. REFERENCES

[1] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. *Lecture Notes in Computer Science*, 740:471–486, 1993.

[2] A. Chadha, Y. Liu, and S. Das. Group key distribution via local collaboration in wireless sensor networks. In *IEEE SECON*, pages 46–54, July 2005.

[3] W. Zhang, M. Tran, S. Zhu, and G. Cao. A random perturbation-based scheme for pairwise key establishment in sensor networks. In *ACM MobiHoc*, pages 90–99, September 2007.