情報保護學會論文誌
第19卷 第2號, 2009. 4

무선센서네트워크를 위한 랜덤키사전분배기법의 경로키 설정에 대한 재고*

권 태 경,[1†] 이 종 협,[2] 송 주 석[2‡]
[1]세종대학교, [2]연세대학교

Revisiting Path-Key Establishment of Random Key Predistribution for Wireless Sensor Networks*

Taekyoung Kwon,[1†] JongHyup Lee,[2] and JooSeok Song[2‡]
[1]Sejong University, [2]Yonsei University

요 약

본 논문에서는 무선센서네트워크를 위한 랜덤키사전분배기법의 경로키 설정에 대해서 재고한다. 먼저 랜덤키사전분배기법의 기본적인 단계인 경로키 설정이 성능면에서 비실용적임을 보이고, 이를 크게 개선하기 위한 새로운 기법을 제시하고 그 성능을 분석한다.

ABSTRACT

In this short paper, we revisit the random key predistribution methods for wireless sensor networks with regard to their intrinsic phase called the path-key establishment. First we show that the path-key establishment is less practical than expected and may degrade the performance of key establishment significantly. We then propose a novel path-key establishment method for those schemes and analyze its advantageous performance improvement.

Keywords: Wireless sensor networks, network security, key predistribution

I. Introduction

Wireless sensor networks are dense wireless networks of sensor nodes collecting and disseminating data in a distributed manner. Sensor nodes are usually small resource-constrained devices so may sense around themselves, communicate over wireless channels within short ranges, and fall into the sleep mode for saving their power. Since they are deployed in unattended fashions even in hostile environments, security functions including secure key establishment are very significant, many studies have been devoted to this challenging area since the first elegant proposal of key predistribution by Eschenauer and Gligor[1-10]. Among them, we are interested in the key predistribution schemes [1,3,5], which are composed of three phases such as key (installation), shared key discovery (for neighboring nodes having shared keys), and path- establishment (for neighboring nodes not having shared keys). With those schemes, we observe that path-key

접수일(2009년 2월 24일), 게재확정일(2009년 3월 3일)

* 이 논문은 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임. (KRF-2007-314-D00254)

† 주저자, tkwon@sejong.ac.kr
‡ 교신저자, jssong@emerald.yonsei.ac.kr

establishment phase has been somewhat neglected in practical senses.

In this paper, after reviewing the random key predistribution briefly, we remark that the computation and overhead for path-key establishment grows exponentially as the number of hops increases establishing the path, in order to attain a certain connectivity. For higher connectivities, the path-key could become impractical. Thus, we propose a novel *path-key offering* method for improving path-key establishment with regard to connectivity and efficience, and provide rigorous analyses.

II. Random Key Predistribution and Its Problem

2.1 Three Phases of Random Key Predistribution Schemes

Eschenauer and Gligor first introduced the random (probabilistic) key predistributiion scheme, RKP, 2002[5], and then Chan et al. proposed its improvement with q-composite and multi-path methods connectivities as well as the random pairwise-key predistribution scheme, RP, in 2003[1]. Since seminal studies, a number of related schemes have been proposed[2-4],6,8-10]. RKP scheme show the basic structure of those schemes, consisting of three main phases under large pool of random keys (with node identities in such schemes as RP). In Phase 1, a set of sub- are selected at random from the large key pool and pre-installed to each node. In Phase 2, after deployment, each node discovers common keys with all its neighboring nodes, saying, in wireless range, by exchanging key identities (meaning node identities in RP). The common keys a single shared key, as in RP) are then used for a new pairwise key. In Phase 3, if there is no intersected between sub-key sets of two neighboring nodes, a path-key establishment step is proceeded, so that could establish a path-key through two or more hops between them. This procedure has been a technique in the related probabilistic key establishment schemes for wireless sensor networks. RP scheme and more derivatives of RKP follow those three phases[2-4,6,8-10].

2.2 Overhead of Path-Key Establishment

With regard to the path-key establishment step, we remark that the computation and communication could grow exponentially as the number of hops increases in establishing the actual path with broadcast, in order to attain a certain connectivity p. Since the 1-hop connectivity p_1 , meaning connectivity in Phase 2, between any two neighboring nodes should be given in a probabilistic manner storage efficiency of sensor nodes, as referred to in Eq. 1 in the following section, the path-key should be done to the amount of filling the gap between p and p_1 for any two neighboring which must be high. Even in the standard example of [5] such that p_1 = 0.5 for storing 250 keys from the 100,000-key pool, the path-key establishment is likely to run so frequently for p. The path extended beyond neighbors should result in further message broadcast and exchange of neighbor and so on. For higher connectivities, the path-key establishment could become impractical. in the following section, we propose a path-key offering method to cope with this problem.

III. Path-Key Establishment with Path-Key Offering

Suppose that a sensor node u has neighbors v and w, respectively, denoting unidentified and identified Here we mean by "identified" that the node share a key and so connected with u, while the unidentified does not. We define a list of identified neighbors of u by $\ell_{\mathrm{id}}(u)$, and that of unidentified by $\ell_{\mathrm{un}}(u)$, so that $w \in \ell_{\mathrm{id}}(u)$ and $v \in \ell_{\mathrm{un}}(\mathrm{u})$. Let $L_{\mathrm{id}}(u)$ be a list of pairs, $\langle v, k \rangle$, for all v and values given to u, such that v is an unidentified neighbor and k is one of key identities broadcast by v in Phase 2. Similarly let $L_{\mathrm{un}}(u)$ be those of unidentified neighbors. For simplicity, we also let $S(v)$ a set of key identities broadcast by v in Phase 2. We say, $K(w)$ denotes a set of key identities intersect between the keys of w and v-nodes satisfying that w is not sharing with its own neighbors. also say, $V(w)$ denotes the identified neighbors of w, broadcast by w itself through $b(w)$. path-key offering means that w offers to u the keys satisfying $S(v) \cap K(w)$, so that u and v can a shared key. We denote this by PKO(w, u, v) as follows. Let CPK(u, w, v) denote the classical establishment assuming that a trusted path through w is already found between u and v.

First, u broadcasts $b(u)$, that is a pair of its own identity and the list $L_{\mathrm{un}}(u)$ implying its unidentified and their key lists. Similarly, other nodes may also broadcast the pairs, for example, $b(v)$. each identified node w, set a 2-tuple of lists, $c(w) = \langle K(w), V(w) \rangle$. Subsequently u runs PKO(w, u, v) some w for identifying v, if there are keys satisfying $S(v) \cap K(w)$. Otherwise, in case of satisfying $v \in V(w)$, u runs CPK(u, w, v) as in the legacy Phase 3. PKO(w, u, v) may rule out many of CPK(u, w, v).

Algorithm 1. Path-key establishment with path-key offering

```
broadcast $b(u) = \langle u, L_{un}(u) \rangle$ to all $w \in \ell_{id}(u)$,
where $L_{un}(u) = \{<v,k> | v \in \ell_{un}(u), k \in S(v)\}$
for each $w \in \ell_{id}(u)$ do
    $c(w) = \langle K(w), V(w) \rangle$,
    where $K(w) = \{k | \langle *,k \rangle \in L_{un}(u) \wedge \langle *,k \rangle \notin L_{id}(w)\} \cap S(w)$, $V(w) = \{v | \langle v,* \rangle \in L_{id}(w)\}$
end for
for each $v \in \ell_{un}(u)$ do
    for each $w \in \ell_{id}(u)$ do
        if $S(v) \cap K(w) = \varnothing$ then
            PKO($w$, $u$, $v$)
            break
        end if
    end for
end for
for each $v \in \ell_{un}(u)$ do
    for each $w \in \ell_{id}(u)$ do
        if $v \in V(w)$ then
            CPK($u$, $w$, $v$)
            break
        end if
    end for
end for
```

IV. Analysis

Let us denote by p_1 the 1-hop connectivity, which is the probability that two nodes share at least a key be connected directly. Then, when we assume that the size of key pool is ξ and each node has m keys, p_1 for RKP is given by

$$p_{1,RKP} = 1 - \frac{\binom{\xi}{m}\binom{\xi - m}{m}}{\binom{\xi}{m}}, \tag{1}$$

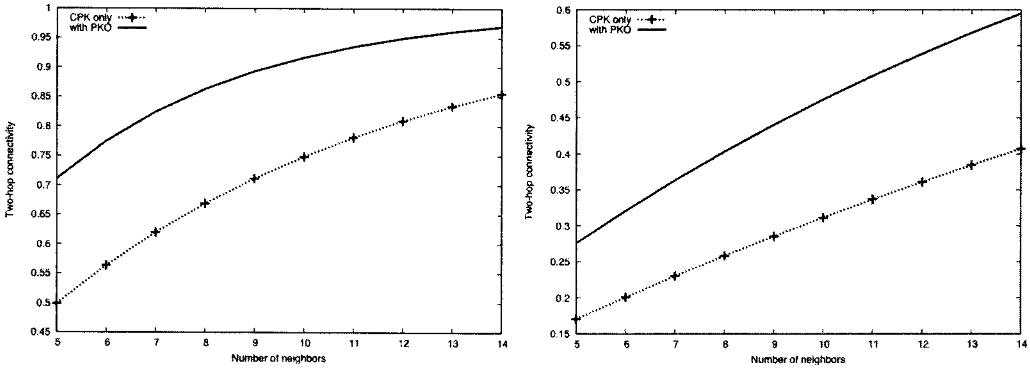
and p_1 for RP is given by

$$p_{1,RP} = \frac{m}{N}, \tag{2}$$

where N is the total number of sensor nodes.

We start from the analysis of [7] for considering multi-hop connectivities. Suppose that two neighboring u and v have failed to discover their common keys within a single hop, while u has n' neighbors. two-hop connectivity p_2 then means the probability of being connected within a two-hop path:

$$p_2 = \sum_{k=1}^{n'} \binom{n'}{k} p_1^k (1 - p_1)^{n'-k} [1 - (1 - p_c p_1)^k], \tag{3}$$



(a) (b)

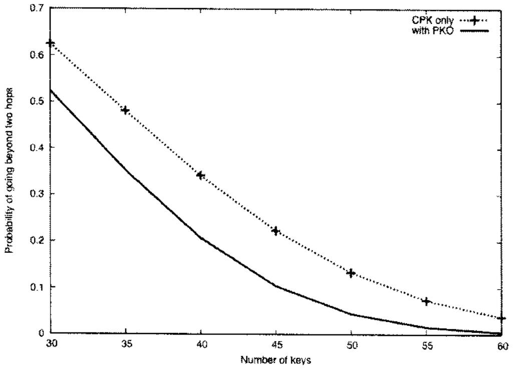
[Fig. 1] Two-hop connectivities according to the number of neighbors. (a) RKP (ξ = 4000, m = 50 p1 = 0.469) (b) RP (N = 200, m = 50, p1 = 0.25)

where $\binom{n'}{k}p_1^k(1-p_1)^{n'-k}$ denotes that, among n' neighbors, k nodes are identified and connected with p_1. Then, those k neighbors are also identified and connected by each other with p_cp_1, where p_c is the probability that any two of those neighbors reside within each other's communication range. that p_c = 0.5865 if the communication range is circular regardless of its radius. Readers are referred [7] for p_c. Thus, $[1-(1-p_cp_1)^k]$ is the probability that at least one of those k nodes is paired with v.

As shown in Eq. 3, the node u could use, in part, only limited neighbors which reside within the range of v. If there is no neighbor who shares a key with v, then the search path should expanded with more hops resulting in more overhead. On the contrary, with PKO, u can be helped all of its connected neighbors within its own communication range, which means that u can borrow connected neighbors' key pools in part. For fairness, if a connected neighbor of u resides out of communication range of v, then u borrows the keys shared with v from that neighbor, of which probability is p_1. Otherwise, u borrows the shared keys, in part, such that the neighbor has not used for its connection with v. However, even in case that all shared keys are already used by the neighbor, it rather assures that CPK can be done no more than within two hops. Thus, with PKO, we gain that u can utilize the keys (shared with v) of all connected neighbors regardless of their actual connection to v, while also making CPK enjoy it. It means that p_c of Eq. 3 can be ruled out, with PKO. Finally, p_2 with PKO, denoted as $p_{2,PKO}$, is given by

$$p_{2,PKO}=\sum_{k=1}^{n'}\binom{n'}{k}p_1^k(1-p_1)^{n'-k}[1-(1-p_1)^k]. \qquad (4)$$

[Fig. 1] illustrates according to the number of neighbors, that PKO improves two-hop connectivities significantly compared to the case of using CPK only, with both schemes such as RKP and RP. When the number of neighbors is 10, the two-hop connectivity is improved by 22.4% for RKP and 52.6% for RP. If there still remains a neighbor which is not connected within two hops either by PKO or CPK, then the CPK process is extended beyond two hops, which may require broadcast beyond those neighbors. Thus, after the connection within two hops has failed, the number of messages may increase exponentially by $O((n')^{h-2})$, where h is the number of hops in the extended path.



〔Fig. 2〕 Probability of going beyond two hops according to the number of keys, (RKP, ξ = 4000)

Let p_3 denote the probability of going beyond two hops such that $p_3 = (1-p_1)(1-p_2)$. It represents then the probability of the communication overhead that increases exponentially. Fig. 2 illustrates p_3 according to the number of keys, with regard to the CPK only case and the case with PKO. We could observe that PKO allows less communication overhead than the CPK only case, due to that the probability of going beyond two hops for further CPK process is getting lower with PKO.

References

〔1〕 H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Proceedings of IEEE Symposium on Security and Privacy, pp. 197-215, May 2003.

〔2〕 W. Du, J. Deng, Y.S. Han, S. Chen, and P. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," Proceedings of IEEE INFOCOM, pp. 586-597, Mar. 2004.

〔3〕 W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transaction on Information and System Security, vol. 8, no. 2, pp. 228-258, Feb. 2005.

〔4〕 W. Du, J. Deng, Y.S. Han, S. Chen, and P. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," IEEE Transaction on Dependable Secure Computing, vol. 3, no. 1, pp. 62-77, Jan.-Mar. 2006.

〔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 (CCS′′02), pp. 41-47, Nov. 2002.

〔6〕 D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," Proceedings of the 2nd ACM workshop on Security of ad-hoc and sensor networks (SASN'04), pp. 29-42, Oct. 2004.

〔7〕 D. Huang, M. Mehta, A. Liefvoort, and D. Medhi, "Modeling pairwise key establishment for random key predistribution in large-scale sensor networks," IEEE/ACM Transaction on Networking, vol. 15, no. 5, pp. 1204-1215, Oct. 2007.

〔8〕 J. Lee, T. Kwon, and J. Song, "Location-aware key management using multi-layer grids for wireless sensor networks," Applied Cryptography and Network Security ACNS'06, LNCS 3989, pp. 390-404, 2006.

〔9〕 D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03), pp. 52-61, Oct. 2003.

〔10〕 D. Liu and P. Ning, "Location-based pairwise key establishments for relatively static sensor networks," in Proc. 1st ACM workshop onSecurity of ad-hoc and sensor networks (SASN'03), pp. 72-82, Nov. 2003.