Poster Abstract: A Constrained Random Perturbation Vector-Based Pairwise Key Establishment Scheme for Wireless Sensor Networks

Chia-Mu Yu[1,2], Ting-Yun Chi[2], Chun-Shien Lu[1]*, Sy-Yen Kuo[2]
[1] Institute of Information Science, Academia Sinica, Taiwan, ROC
[2] Graduate Institute of Electrical Eng., National Taiwan University, Taiwan, ROC

ABSTRACT

This paper presents a *Constrained Random Perturbation Vector-based* (CRPV) pairwise key establishment scheme and its variant, CRPV+ scheme, for wireless sensor networks (WSNs). Compared to all existing schemes which satisfy only some requirements in a so-called versatileness criteria, the CRPV+ scheme meets all requirements. In particular, the performance improvement of our schemes does not rely on tradeoffs among different requirements, but comes from the use of our constrained random vector strategy.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General Security and protection; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design Wireless communication

General Terms

Security, Algorithm, Design

Keywords

Pairwise Key Establishment, Random Perturbation, Sensor Network Security

1. MOTIVATION

Five requirements needed to be satisfied for a key establishment scheme in WSNs were presented in Zhang *et al.* [2] and are briefly summarized as follows: 1) *Resilience to Large Number of Node Compromise* (RLNNC), 2) *Guaranteed Key Establishment* (GKE), 3) *Direct Key Establishment* (DKE), 4) *Resilience to Network Topology* (RNT), and 5) *Efficiency* (EFF). We observe that, in addition to these five requirements, two more requirements should be considered so as to thoroughly evaluate the key establishment schemes in WSNs. They are 6) *Scalability* (SCA) and 7) *Independence to Hardware* (IH). Scalability should be fulfilled since a key establishment scheme should be applied to a WSN without regard to its number of sensor nodes. On the other hand, independence to hardware is necessary because, when the network is heterogeneous, a key establishment scheme should have the ability to be performed on different kinds of hardware without modifying the hardware setting. For convenience, these seven requirements are generally called *versatileness criteria*. Compared to the existing key establishment schemes which only make tradeoffs among requirements of the versatileness criteria, the RPB scheme [2] has satisfied the first four requirements of versatileness criteria. Nevertheless, the requirements, EFF, SCA, and IH, are not always satisfied. In this paper, a CRPV+ scheme is proposed to satisfy all the requirements of versatileness criteria.

2. THE PROPOSED METHOD

The proposed methods, CRPV and CRPV+, which are based on Blom's concept [1] and our proposed constrained random vector strategy, can satisfy all the requirements of versatileness criteria. In the following, the notations used in this paper are the same with [1]. Please refer to [3] for more detailed description and simulation results of the proposed method.

2.1 Off-line Step of CRPV scheme

We assume that the network consists of N sensor nodes with fixed IDs, $\mathcal{I} = \{s_1, s_2, \ldots, s_N\}$ and $s_1 < s_2 < \cdots < s_N$. We also assume that q $(> N)$ is a prime number, and λ is an appropriate security parameter, which leverages the security level and storage. Before off-line step is executed, some parameters such as the number of least perturbed bits r and the desired key length L should be determined. Let the largest possible element of A and K be μ and ν, respectively. Let ℓ be the least number of bits necessary to represent ν. Since each round of execution of the CRPV can generate $(\ell - r)$ bits of a pairwise key, the CRPV should be executed m $(= \lceil \frac{L}{\ell - r} \rceil)$ times to obtain a pairwise key with desired key length L. Now, we explain the off-line step of the CRPV from executing the c-th round of the CRPV. At first, as in Blom's scheme, we randomly generate a symmetric matrix $D^{(c)} \in \mathbb{F}_q^{(\lambda+1)\times(\lambda+1)}$ and a matrix $G^{(c)} \in F_q^{(\lambda+1)\times s_N}$. After that, we calculate the matrix $A^{(c)} = (D^{(c)} \cdot G^{(c)})^T$. Let Φ_{s_i} denote the set of legitimate perturbations for $s_i \in \mathcal{I}$. Φ_{s_i} can be constructed as follows. Let $c_{\min}(\alpha, r)$ be the value of α which has least r bits of its binary representation set to 0. Similarly, let $c_{\max}(\alpha, r)$ be the value of α which has

*Contact Author: lcs@iis.sinica.edu.tw

MobiHoc'08, May 26–30, 2008, Hong Kong SAR, China.
ACM 978-1-60558-073-9/08/05.

least r bits of its binary representation set to 1. Let $G_{i,-}$ and $G_{-,j}$ be the i-th row and j-th column of a matrix G, respectively. For any vector $\phi^{(c)}_{s_i} \in \Phi^{(c)}_{s_i}$ which is obtained when the c-th round of the CRPV is performed, it must satisfy the following constraints:

$$(A^{(c)}_{s_i,-} + \phi^{(c)}_{s_i}) \cdot G^{(c)}_{-,s_j} \geq c_{\min}(A^{(c)}_{s_i,-} \cdot G^{(c)}_{-,s_j}, r) \qquad (1)$$

$$(A^{(c)}_{s_i,-} + \phi^{(c)}_{s_i}) \cdot G^{(c)}_{-,s_j} \leq c_{\max}(A^{(c)}_{s_i,-} \cdot G^{(c)}_{-,s_j}, r) \qquad (2)$$

$$0 \leq A^{(c)}_{s_i,k} + \phi^{(c)}_{s_i,(k)} \leq \mu, \qquad (3)$$

where $i \neq j$, $1 \leq i,j \leq N$, $1 \leq k \leq (\lambda+1)$, and $\phi^{(c)}_{s_i,(k)}$ is the k-th element of $\phi^{(c)}_{s_i}$. Eqs. (1) and (2) mean that after perturbation is added to $A_{s_i,-}$ of the sensor node s_i, the most significant $\ell - r$ bits of the corresponding Blom's key are retained for every other sensor node s_j. The constraint indicated in Eq. (3) should be satisfied because the CRPV only permits non-negative numbers in A. In addition, if there are some values larger than μ after perturbation is applied, then the number of bits used to represent the elements of A will vary. Thus, every $\phi^{(c)}_{s_i}$ that satisfies Eqs. (1)$\sim$(3) is one of the elements in $\Phi^{(c)}_{s_i}$.

Following the construction of $\Phi^{(c)}_{s_i}$, we want to add perturbation on each row vector of $A^{(c)}$ and then store the s_i-th vector of $A^{(c)}$ into the sensor node s_i. For every $s_i \in \mathcal{I}$, a row vector $\phi^{(c)}_{s_i}$ is randomly selected from $\Phi^{(c)}_{s_i}$. Then, a matrix $W^{(c)}$ is calculated, where $W^{(c)}_{s_i,-}$ $(= A^{(c)}_{s_i,-} + \phi^{(c)}_{s_i})$ is stored into the sensor node s_i.

2.2 On-line Step of CRPV scheme

Assume that the sensor nodes u and v want to have a common key. When c-th time CRPV is executed, they first exchange their columns of $G^{(c)}$, $G^{(c)}_{-,u}$ and $G^{(c)}_{-,v}$. Then, u and v calculate $\kappa^{(c)}_{u,v} = W^{(c)}_{u,-} \cdot G^{(c)}_{-,v}$ and $\kappa^{(c)}_{v,u} = W^{(c)}_{v,-} \cdot G^{(c)}_{-,u}$, respectively. Because the perturbation on Blom's common key due to the added perturbation is limited within the least r bits, the c-th part of pairwise key $X_{u,v}$ between u and v is $X^{(c)}_{u,v} = f_{\ell,r}(\kappa^{(c)}_{u,v}) = f_{\ell,r}(\kappa^{(c)}_{v,u})$, where $f_{\ell,r}(x)$ is the first $(\ell - r)$ bits of binary representation of a number x.

2.3 Communication-free CRPV (CRPV+)

In the CRPV, the communication between two sensor nodes only requires to exchange the respective column of G, which can be known by an adversary. If the s_i-th column of G can be generated by sensor node s_i, then no communication is needed. Recall that the only requirement for G is that any $(\lambda + 1)$ columns of G should be linearly independent [1]. Thus, Vandermonde matrix is fascinating for our use since it can be generated by only one pre-defined element. In addition, if β is the primitive element of $\mathbb{F}_q$, then any $(\lambda+1)$ columns of G are linearly independent [1]. Note that Vandermonde matrix is of the form that the i-th column is generated by $\left[\begin{array}{ccccc} 1 & \beta^i & (\beta^i)^2 & \cdots & (\beta^i)^\lambda \end{array}\right]^T$. Therefore, if an appropriate Vandermonde matrix is used as G, then the CRPV+ is constructed.

2.4 Performance Evaluation

If CRPV is used, then, for sensor node s_i, the row vectors $A^{(c)}_{i,-}$ and column vectors $G^{(c)}_{-,i}$ are needed to stored, resulting in $O(\lambda)$ storage overhead. If CRPV+ is used, for sensor node s_i, only row vectors $A^{(c)}_{i,-}$ and an element s are needed to stored. Thus, the storage overhead for CRPV+ is $O(\lambda)$. For different i and j, $\lambda+1$ multiplications and λ additions are needed to carry out the multiplication of $A_{i,-}$ and $G_{-,j}$ in CRPV. However, by using Horner's rule, $\lambda + 1$ multiplications and λ additions are also sufficient to simultaneously carry out the generation of $G_{-,j}$ and the multiplication of $A_{i,-}$ and $G_{-,j}$ in CRPV+. In CRPV, the communication happens only when two sensor nodes exchange their column vectors. Because the length of a column vector is $O(\lambda)$, the communication overhead is $O(\lambda)$ as well. On the other hand, it can be easily observed that there is no communication needed for CRPV+. Because the CRPV and CRPV+ schemes can be regarded as a generalization of Blom's scheme, the security can be perfectly guaranteed before $\lambda+1$ sensor nodes are captured by an adversary. Due to this observation, we only consider the case that the number of captured nodes is larger than $\lambda + 1$. To compromise a secure link between two uncaptured sensor nodes, an adversary must capture more than $\lambda+1$ sensor nodes, and try to recover the matrix D. However, the relation between A and D in Blom's scheme does not exist when perturbations have been applied on A. To recover D, the adversary must recover A from W. We have derived [3] to know that the computational complexity for breaking $D^{(c)}$, $1 \leq c \leq m$, is $\Omega(m * \prod_{i=1}^{\lambda+1} |\Phi_i|)$ for both CRPV and CRPV+ schemes. The performance of the RPB scheme superior to many renowned key establishment schemes had been shown in [2]. We have a comprehensive comparison among CRPV, CRPV+, RPB, and some other famous schemes, from the viewpoint of considering versatileness criteria [3]. When focusing on the comparison between RPB and CRPV+, we have the following improvements. 1) The computation and communication overhead incurred by the calculation and transmission of hash values in the RPB scheme [2] will be avoided in the CRPV+ scheme, while the storage overhead is the same in both schemes. Since the energy consumption of the sensor nodes with different operating modes has a 10^3 order difference, this improvement could be significant because the transmission of hash values will consume energy of the sensor nodes on the routing path. 2) The scalability of RPB will be limited because the IDs of sensor nodes should be particularly chosen. Furthermore, due to fixed packet size, if more bits are used to represent ID, then less bits are left for carrying data, leading to lower throughput. Since CRPV+ does not have the special ID constraint, it possesses properties of scalability and hardware independence.

3. CONCLUSION

Based on the proposed constrained random vector strategy, CRPV and CRPV+ schemes are proposed for key sharing in WSNs and evaluated under the versatileness criteria. Both of them are also implemented on the real sensor nodes to correctly evaluate the performance and overhead [3].

4. REFERENCES

[1] R. Blom, "An optimal class of symmetric key generation systems," *EUROCRYPT*, 1984.

[2] W. Zhang, M. Tran, S. Zhu, and G. Cao, "A random perturbation-based scheme for pairwise key establishment in sensor networks," *ACM MobiHoc*, 2007.

[3] `homepage.ntu.edu.tw/~d95921015/MobiHoc08.pdf`