Communication Cost Optimized Key Establishment Scheme Based On Secret Sharing

Lan Zongxiao
National University of Defense Technology,Changsha,Hunan
517003047qq@gmail.com

Xiageming
National University of Defense Technology,Changsha,Hunan
xiageming@126.com

Abstract

With the rapid development of Wireless Sensor Networks(WSNs), however, its security issues have become outstanding because of the inclement deploying environment, and the open communication channel. Due to the constraints of limited hardware resources and computational capabilities, most of the defense mechanism are based on symmetric key. In this paper, we present a algorithm *DPC*, *Data Partitioning with Coding*.Based on *DPC*, we proposed a secret sharing-based scheme to protect the establishment of session key in WSNs. As a result, be means of optimizing the communication cost, the scheme is suitable for WSNs.

Keywords Secret Sharing, Wireless sensor network, Optimization

1. Introduction

With the increasing demand for environmental monitoring or intelligent transmission etc. wireless sensor networks (WSNs) have been deployed extensively. The application requirements leads to the increase of the scale of wireless sensor network. If depend on the radio data transmission mechanism entirely, however, the resource and energy consumption of the sensor nodes will be too large. The effective use of end-to-end transmission in sensor network can guarantee the efficiency and reduce the consumption. Due to the inclement deploying environment, and the open communication channel, sensor network is vulnerable to attack. It's not feasible to use asymmetric cryptography in sensor network because of the constraints of limited hardware resources and computational capabilities[1].

Therefore adequate defense mechanism based on symmetric cryptography should be proposed to secure the key establishment in end-to-end transmission. Pairwise key establishment is a fundamental security service in sensor networks[2]. In [3],the authors proposed schemes provided by LEAP to establish and update keys using pairwise shared keys for each node. And the local collaboration-based group key updating scheme has been proposed[4]. However, in these schemes, the sensor network ensure the security in the process of establishing and updating keys. In [5], the author present *multipath key reinforcement*, which is based on secret sharing to enhance the security. To reconstruct the link key, the adversary must eavesdrop on all the links between the key establish node and its reinforce neighbors, for all the expanded communication cost. The analogous scheme *multiple logically disjoint path* presented in [6], which is based on threshold secret sharing.

Secret sharing especially threshold secret sharing requires a calculation of more complex, such as the Lagrange interpolating polynomial[7]. When the key is transmitted in multiple paths, the communication cost will expand exponentially, bring the huge energy consumption. Being aware of such problems, in this paper, we present a communication cost optimized key establishment scheme based on secret sharing. Optimization of communication cost will result in security performance degradation inevitably. Our scheme makes a trade-off between them by using a non-perfect secret sharing.

2. Related Work

The first secret share schemes were introduced by Shamir[7] and Blakley[8] in 1979. In these (k,n) threshold schemes, the shares of any k participants are sufficient to recover the complete secret, yet any k-1 or less shares leak nothing about the secret. In [9], the presented schemes apply secret sharing in wireless sensor network to against aggregator compromises. The authors design a secret multipath aggregation (SMA) scheme, to deal with security under the contingency of compromise. Due to the constraints of limited hardware resources and computational capabilities, however, these schemes are not suitable for sensor network.

In [10], Kurihara presented a secure and high-speed secret sharing scheme using XOR operation. It's an ideal secret for the recovery and the share have the same data length. In [11], the authors proposed a new scheme using XOR operation, achieved high-speed processing and reduced the data size using pseudo-random numbers. Although in these schemes, have high-speed distribution and recover processing, their communication cost expand seriously.

A secret sharing scheme is non-perfect if some subsets of participants cannot recover the secret value but have some information about it[12]. While in perfect secret sharing scheme, the data size of each share have a lower bound, that is the size of the secret. Therefore, to optimize the communication cost, we presented a *non-perfect secret sharing* scheme using XOR operation.

3. Solution Approach

3.1 system model

Network model

In this scheme, we combine single-step key transmission protocol and secret sharing to achieve the key establishment. And our work is based on wireless sensor network using pre-distribution keys.

Single-step key transmission protocol establish key supported by pre-distribution keys based on symmetric encryption. The processing of key establishment between node A and B described as follows:$E_k(key, t_A, c)$. E_k represent the symmetric encryption

algorithm using key k, *key* is the session key to be establish, t_A represent the time stamp or Serial number, yet the c represent the authentication field.

Assumptions

In this paper, we assume the following.

1)All the sensor nodes have completed the discovery of pre-shared keys.

2)All sensor nodes are static in the processing of key establishment.

3)Each transmission path in our work is stable in the processing of key establishment.

4)Between Node A and Node B, there are n disjoint paths, and discovered pre-shared keys no less than n.

Notations

In Table 1, the notations used in this paper is described.

Table 1. Notations

Notation	Description
$\|\|$	Concatenation of bit sequences
$\oplus$	A bit-wise XOR operation
S	The secret to be share($S \in \{0,1\}^{t \cdot p}, t > 0$)
θ_i	The i-th block divided from the origin secret
$\|x\|_n$	x mod n
β_i	Share given to i-th participant $P_i(i = 0, \cdots, n-1)$

3.2 secret sharing-based key establishment

To optimize the communication cost, we present a algorithm *DPC*s, *Data Partitioning with Coding*. Based on *DPC algorithm*, we proposed the multipath key establishment protocol. As shown in Figure 1, that is the session key establishment between node A and node B using *DPC algorithm*. Between node A and B have established n disjoint paths $route_1, \cdots, route_n$, throuth the finding of pre-shared keys. In *DPC algorithm*, we define the coding key x, which is used to recover secret. And the share serial number $i_k (k = 1, \cdots, n)$ refer to each path $route_k$ determine the decoding order together with the coding key. To ensure the coding key x and the sequence of i_k only relevant to node A and B, we calculate x and sequence of i_k using the pre-shared keys between node A and B.

The pre-shared keys are independent between each node-pairs, feasible to calculate the coding key and the sequence of i_k. Using the pre-shared keys $k_1, k_2, \cdots, k_n$, we calculated the pseudo-random x and sequence of i_k:

$$\begin{aligned} f(k_1, k_2, \cdots, k_n) &= x \\ F(k_1, k_2, \cdots, k_n) &= (i_1, i_2, \cdots, i_n) \end{aligned} \tag{1}$$

In our scheme, $f(k_1, k_2, \cdots, k_n)$ is a multivariate hash function which has a codomain of $[0, \cdots, n-1]$. And $F(k_1, k_2, \cdots, k_n)$ is a lightweight sequence generate function:

$$F(k_1, k_2, \cdots, k_n) = (i_1, i_2, \cdots, i_n) \quad k_{i_1} \leq k_{i_2} \leq \Lambda \leq k_{i_n}$$

Functions $f(k_1, k_2, \cdots, k_n)$ and $F(k_1, k_2, \cdots, k_n)$ were defined in all nodes, and before the establishment of session key, node-pair use them to calculate the coding key x and sequence of i_k. The implementation of the protocol between node A and node B contains three steps:

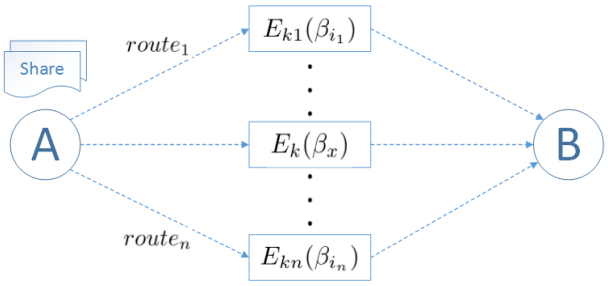

Figure 1. Multipath key establishment based on *DPC*

Step 1 secret distribution:
Node A generate a new session key S ($S \in \{0,1\}^{n \cdot p}, n > 0$), and create shares $\beta_0, \cdots, \beta_{n-1}$ from it using *DPC algorithm*, in which there is one share β_x correspond to the coding key x.

Step 2 secret transmission:
Encrypt each share using the pre-shared key between A and B, and each path without using a same key. Then transfer these encrypted shares to node B through disjoint paths $route_1, \cdots, route_n$. Each share's transmission path is determined be the sequence of i_k. The i-th share transmit through path $route_i$, for instance, the share θ_{i_2} transmit through path $route_2$.

Step 3 secret recovery:
Before recovery the session key, select the single key k_x from the pre-distribution key pool. When node B received shares up to n, recovery the secret using *algorithm DPC*, ie. the session key between node A and Node B. From now, the multipath key establishment protocol has achieved.

The multipath key establishment protocol is based on the *DPC algorithm*. This algorithm can reduced the data size of multiple secret shares significantly. *DPC* includes two parts, secret distribution and secret recovery. The implementation detail of *DPC algorithm* will be described in the following sections.

3.3 secret distribution algorithm

When node A and B begin to establish session key, node A generate a random value with the same length of pre-distributed key, which is called secret S ($S \in \{0,1\}^{n \cdot p}, n > 0$) in our work. The secret distribution algorithm create secret shares from the secret S, and then distribute them to disjoint paths. The detail description of the distribution processing is shown as below:

Step 1 Divide S into n pieces of p-bit block:

$$S = \theta_0 \parallel \theta_1 \parallel \cdots \parallel \theta_{n-1} \tag{2}$$

Step 2 Make the n blocks in sequence, then execute XOR operations within adjacent blocks, create the segment β_i:

$$\beta_i = \theta_i \bigoplus \theta_{|i+1|_n} (i = 0, \cdots, n-1) \tag{3}$$

Step 3 Before the distribution processing, the coding key x($x \in [0, \cdots, n-1]$) have been calculated in node A. Execute extra XOR operation for segment β_x, renew this segment:

$$\beta_x = \theta_x \bigoplus \theta_{|x+1|_n} \bigoplus \theta_{\left|x+\lceil \frac{n}{2} \rceil\right|_n} \tag{4}$$

From now, we have generated all share β_i for participant $P_i(i = 0, \cdots, n-1)$

3.4 secret recovery algorithm

After node B received all the shares, *DPC algorithm* begin to recover the secret, that is the session key. Node B calculated the coding key x and the sequence of i_k before the recovery processing, which determined the right order of decoding. The detail description of the recovery processing is shown as below:

Step 1 Execute XOR operation for the segments, recover the block $\theta_{\left|x+\lceil\frac{n}{2}\rceil\right|_n}$:

$$\begin{aligned}\bigoplus_{i=0}^{n}\beta_i &= (\bigoplus_{i=0}^{x-1}\beta_i)\bigoplus\beta_x\bigoplus(\bigoplus_{j=x+1}^{n-1}\beta_j)\\ &= \theta_0\bigoplus(\bigoplus_{k=1}^{n-1}\theta_k)\bigoplus\theta_0\bigoplus\theta_{\left|x+\lceil\frac{n}{2}\rceil\right|_n}\\ &= \theta_{\left|x+\lceil\frac{n}{2}\rceil\right|_n}\end{aligned} \tag{5}$$

Step 2 Then from $y = \left|x + \lceil\frac{n}{2}\rceil\right|_n$, recover all the blocks in turn until all the blocks have been recovered:

$$\begin{aligned}\theta_{|y+1|_n} &= \theta_y\bigoplus\beta_y\\ \theta_{|y+2|_n} &= \theta_{|y+1|_n}\bigoplus\beta_{|y+1|_n}\\ &\cdots\\ \theta_{|x+1|_n} &= \theta_x\bigoplus\beta_x\bigoplus\theta_{\left|x+\lceil\frac{n}{2}\rceil\right|_n}\\ &\cdots\end{aligned} \tag{6}$$

Step 3 Recover secret S from all the blocks:

$$S = \theta_0 \parallel \theta_1 \parallel \cdots \parallel \theta_{n-1} \tag{7}$$

Then select the key k_x from pre-distribution key pool, the session key K between node A and B can be computed as:

$$K = k_x\bigoplus S \tag{8}$$

4. Evaluation

In this section, we first analytically evaluate the performance of the proposed multipath key establishment protocol based on *DPC*, and compare it to some previously proposed key establishment schemes. Then, we analyse the security of the *DPC algorithm*, estimate the *DPC algorithm* in terms of its defense capability against node compromise. We evaluate that the proposed algorithm *DPC* can optimize the communication costs and make a trade-off of the security performance. By means of conducting simulations, we show that the proposed algorithm *DPC* can optimize the communication cost and make a trade-off of the security performance.

4.1 performance evaluation

We analyse the performance of the proposed multipath key establishment scheme(MKE) in terms of computational costs and communication costs, then compare it with the previous multipath key reinforcement scheme(MKR) and multiple logically disjoint path scheme(MLDP). The main results are shown in Table 2.

computational costs

In our scheme, the main computational cost is the cost in the secret distribution and secret recovery. Considering a secret S ($S \in \{0,1\}^{n\cdot p}, n > 0$), which is the session key, n is the number of disjoint paths as well as p is the length of share transmit on each path. We define L to be the length of the secret, as $L = np$. During the distribution phase, it needs $(n+1)p$ bit-wise XOR operations. As well as during the recovery phase, it needs $(2n-1)p + np = (3n-1)p$ bit-wise XOR operations. Node A and B both need to calculate the coding key x($x \in [0, \cdots, n-1]$), which require λ computational cost. The overall computational costs of our scheme is $4np+2\lambda$, can also be expressed as $4L+2\lambda$. In multipath key reinforcement scheme, it needs $nL + n\mu$ bit-wise XOR operations, in which μ is the computational cost of generating a L-bit random number. Similar to multipath key reinforcement scheme, it needs $nL + n\mu$ bit-wise XOR operations in multiple logically disjoint path scheme.

As shown in Equation 1, function $f(k_1, k_2, \cdots, k_n)$ is a multivariate hash function with lightweight operation. Therefore, the λ and μ both have light effect in our comparison. With the $n > 3$, our scheme has a lower computational costs compared with the two previous schemes.

communication costs

Each path has an average length of h hops in this paper. In our scheme, node A needs to send out n shares with length of p-bit. Because of all the shares are forwarded hop-by-hop via the path between node A and B, then the communication costs $C = n \times h \times p = hL$, which is roughly equivalent to single path key transmission' costs. In multipath key reinforcement scheme and multiple logically disjoint path scheme, each node need send out n L-bit shares to achieve the key establishment. Therefore, the communication costs in these two schemes are both $C = n \times L \times h = nhL$.

The analysis results show that our scheme has n times of the efficiency improvement. The trade-off for this benefit in the proposed scheme is the degradation of the security performance. We will analyse the security performance in the next section, to show that the security degradation is within the acceptable range.

Table 2. Performance comparison to previous schemes

	MKE	MKR	MLDP
computational costs	$4L + 2\lambda$	$nL + n\mu$	$nL + n\mu$
communication costs	hL	nhL	nhL

4.2 security evaluation

To evaluate the security of the proposed multipath key establishment scheme, we analyse the *DPC algorithm* and estimate its security. Then we use simulations to show that this scheme makes a good trade-off between performance and security.

estimation of *DPC*

The proposed *DPC algorithm* is non-perfect secret share, which inevitably leads to security degradation. In this paper, we use coding-based secret share to control the security degradation within acceptable range, moreover, optimize the communication costs significantly. In our scheme, we have two objectives in security: increase the lower bound of share subset lead to leak partial secret and increase the lower bound of share subset lead to leak complete secret.

Before analyse the lower bound of share subset, we define *NLB* to be number leaked blocks. In *DPC algorithm*, a share subset Φ can derive partial secret only when $\beta_x \in \Phi$ and $|\Phi| \geq \lceil\frac{n}{2}\rceil$ (because of the space limited, not all the proofs listed). When $|\Phi| = \lceil\frac{n}{2}\rceil$, the subset Φ can derive one block with probability:

$$P_{(NLB=1)} = \frac{2}{C_n^{\lceil\frac{n}{2}\rceil}} \tag{9}$$

When $\lceil \frac{n}{2} \rceil < |\Phi| < n$, let the subset size $|\Phi| = k$, then the probability of r ($1 \le r \le k - \lceil \frac{n}{2} \rceil + 1$) blocks leaked is:

$$P_{(NLB=r)} = 2 \times \frac{C_{n-(\lceil \frac{n}{2} \rceil + r - 1) - 1}^{k-(\lceil \frac{n}{2} \rceil + r - 1)}}{C_n^k} \tag{10}$$

The share subset Φ can derive the complete secret depend on $|\Phi| = n$. When $|\Phi| = n$, all of the shares can derive the secret apparently.

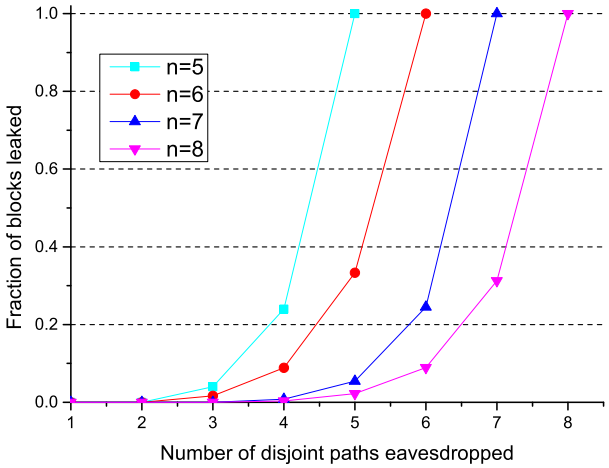

Figure 2. The fraction of blocks leaked according to subset size of eavesdropped shares (ignore the probability of eavesdropping a disjoint path)

In Figure 2, we show that *DPC algorithm* has relative security performance degradation whereas it's based on non-perfect secret share. When the share subset $|\Phi| \le n - 1$, the adversary has no chance to eavesdrop the link between node A and B, as well as the adversary has no chance to eavesdrop a block if $\Phi \le \lceil \frac{n}{2} \rceil$. Even if $|\Phi| = n - 1$, the fraction of blocks leaked will not more than 0.4. By the way, as shown in Figure 2, the scheme with an odd number of disjoint paths has better security performance relative to which has even number of disjoint paths.

evaluation of *MKE*

We evaluate the effectiveness of the presented multipath key establishment scheme by simulating the 10000 sensor nodes deployed on a planar field. In our simulation, each node has 50 neighbours with the proper deployment density. The adversary eavesdrop on each disjoint path by compromise the nodes on it. A pairwise nodes communication is compromised only if the session key is compromised, that is all the disjoint paths to be used to transmit the session key were compromised in our scheme.

We plot the simulation results in Figure 3, which indicates the fraction of communication compromised versus the number of compromised nodes. Figure 3 shows that our multipath key establishment scheme acts similarly to the previously proposed schemes in security. When the number of compromised nodes less than 225, its security performance even outperform the multipath reinforcement scheme.

The adversary require to eavesdrop multiple relevant keys in order to eavesdrop the session key between node pairs. The trade-off for the multipath key establishment scheme is the increased communication costs. The benefit of *DPC algorithm* is remaining the security unchanged, while the communication costs optimized

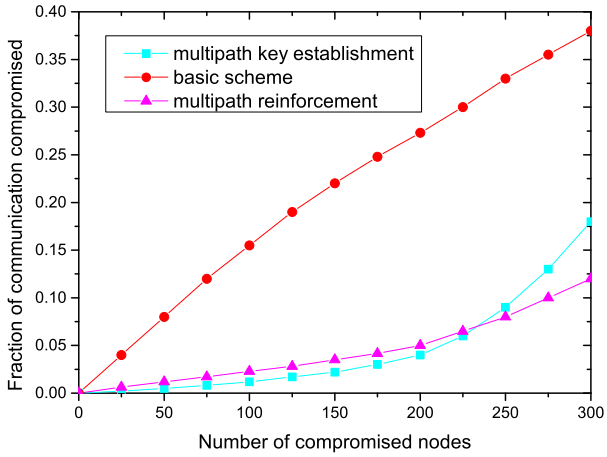

Figure 3. The fraction of blocks leaked according to subset size of eavesdropped shares (ignore the probability of eavesdropping a disjoint path)

significantly. In our scheme, the blocks of the secret as well as the complete of the secret have small probability to be eavesdropped.

5. Conclusions

We have presented a new multipath key establishment scheme using non-perfect secret share for wireless sensor network. We analyse the overhead roundly to show that our scheme optimize the communication costs and make a trade-off of the security performance.

Acknowledgments

This work is supported in part by Natural Science Foundation of China grants 61070201.

References

[1] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," *NAI Labs Technical Report*, vol. 00, no. 010, 2002.

[2] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 1, pp. 41–77, 2005.

[3] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500–528, 2006.

[4] W. Zhang and G. Cao, "Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 1. IEEE, 2005, pp. 503–514.

[5] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. IEEE, 2003, pp. 197–213.

[6] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," in *Network Protocols, 2003. Proceedings. 11th IEEE International Conference on*. IEEE, 2003, pp. 326–335.

[7] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[8] G. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 AFIPS National Computer Conference*. Monval, NJ, USA: AFIPS Press, 1979, pp. 313–317.

[9] T. Claveirole, M. Dias de Amorim, M. Abdalla, and Y. Viniotis, "Securing wireless sensor networks against aggregator compromises," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 134–141, 2008.

[10] J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka, "On a fast (k,n,k)-threshold secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 91, no. 9, pp. 2365–2378, 2008.

[11] Y. Nagai, H. Kang, and K. Iwamura, "A key management system with a storage-saving secret sharing scheme in a sensor network," in *The International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2013)*. The Society of Digital Information and Wireless Communication, 2013, pp. 35–39.

[12] O. Farràs, T. Hansen, T. Kaced, and C. Padró, "Optimal non-perfect uniform secret sharing schemes," 2014.