SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

April 2018, Vol. 61 048103:1–048103:3
https://doi.org/10.1007/s11432-017-9212-2

Cross-cluster asymmetric group key agreement for wireless sensor networks

Jiamin ZHENG[1], Yu-an TAN[1,2], Qikun ZHANG[3], Xiaosong ZHANG[1,4], Liehuang ZHU[1] & Quanxin ZHANG[1*]

[1]*School of Computer Science and Technology, Beijing Institute of Technology, Beijing* 100081*, China;*
[2]*Research Center of Massive Language Information Processing and Cloud Computing Application, Beijing* 100081*, China;*
[3]*Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002*, China;*
[4]*Department of Computer Science and Technology, Tangshan University, Tangshan* 063000*, China*

Received 13 June 2017/Accepted 19 July 2017/Published online 10 February 2018

Citation Zheng J M, Tan Y A, Zhang Q K, et al. Cross-cluster asymmetric group key agreement for wireless sensor networks. Sci China Inf Sci, 2018, 61(4): 048103, https://doi.org/10.1007/s11432-017-9212-2

Wireless sensor networks have some obvious negative characteristics, such as limited communication range, energy constraints, and vulnerability. A group key agreement in this environment requires lightweight cross-cluster, computation, and communication overhead, and a highly safe group key agreement protocol. With these demands in mind and with the goal of unscrambling current theories [1–5], we propose a cross-domain lightweight asymmetric group key agreement to establish a safe and efficient group communication channel between sensor nodes.

The certifiable asymmetric group key agreement proposed in this article has the following advantages.

(1) Crossing-cluster capacity. The sensor nodes participating in the group key agreement can be distributed in different clusters, and a crossing-cluster asymmetric group key agreement is achieved through bridge technology when the communication capacity of the sensor nodes is limited, to transmit the information exchanged between the remote sensor nodes safely.

(2) Lightweight calculation. As the asymmetric group key is involved in larger communications and their calculations, compared with a symmetry group key agreement, the calculation and communication loads of the sensor node are accomplished by a cluster head node through unequal computing technology. This can alleviate resource restrictions of sensor nodes and achieve the performance of an asymmetric group key agreement, which provides the scheme with the security and flexibility of an asymmetric group key agreement, as well as lightweight calculation in the symmetric group key agreement.

(3) The group key is self-certified. After the group member calculates the group key, it can verify the correctness of the calculated group key on its own by mapping the function simply, rather than by an additional round of broadcast communication.

Preliminary. (1) Bilinear mapping. The definition of bilinear mapping is as follows: Suppose G_1 is the addition group, G_2 is multiplicative cycle group, and they have the same large prime number order q, $q \geqslant 2^k + 1$, where k is a safety parameter under a discrete logarithm assumption. G_1 and G_2 are a pair of bilinear groups. Suppose $G_1 = \langle g_1 \rangle$. e is calculable bilinear mapping, $e : G_1 \times G_1 \rightarrow G_2$.
Nature 1 (Bilinear)**.** For all $g_1, g_2 \in G_1$, and $a, b \in Z_q^*$, there is $e(ag_1, bg_2) = e(g_1, g_2)^{ab}$.

* Corresponding author (email: zhangqx@bit.edu.cn)

Nature 2 (Nondegeneracy)**.** That is, $e(g_1, g_2) \neq 1$.
Nature 3 (Calculability)**.** There is an efficient algorithm, such that for $g_1, g_2 \in G_1$, $e(g_1, g_2)$ is calculable.

(2) Computing complexity.

Assumption 1 (Discrete logarithm problem)**.** Suppose $g_1, g_1' \in G_1$. Find an integer a that makes $g_1' = ag_1$ difficult to calculate.

Assumption 2 (Divisible computational Diffie-Hellman (DCDH) problem)**.** Suppose a triad $(g_1, ag_1, bg_1) \in G_1$, for the unknown numbers $a, b \in Z_q^*$. It is difficult to calculate $(a/b)g_1$.

Lightweight intercluster asymmetric group key agreement protocol. It is proposed that a lightweight intercluster asymmetric group key agreement protocol is certified between wireless sensor nodes. Take one group key agreement of sensor nodes in one cluster as an example. There are two hypotheses that need to be considered.

The set of low-energy nodes in cluster head U_i is $U = \{u_{i,1}, u_{i,2}, \ldots, u_{i,n}\}$, and the set of its corresponding identities is $I = \{\mathrm{id}_{u_{i,1}}, \mathrm{id}_{u_{i,2}}, \ldots, \mathrm{id}_{u_{i,n}}\}$. The public key pair of any nodes $U_{i,j}$ $(1 \leqslant j < N)$ is $(\mathrm{sk}_{i,j}, \mathrm{pk}_{i,j})$, $\mathrm{sk}_{i,j} \in Z_q^*$, $\mathrm{pk}_{i,j} = \mathrm{sk}_{i,j} g_1$. U_i is a cluster head with higher energy in this cluster, and the set of its corresponding identity is id_{U_i}.The public/private key pair of U_i is $(\mathrm{SK}_i, \mathrm{PK}_i)$, where $\mathrm{SK}_i \in Z_q^*$, $\mathrm{PK}_i = \mathrm{SK}_i g_1$.

Each node can know identity information of other members before executing the protocol.

(1) Generation of alliance key between cluster heads. Suppose the set of cluster heads of N clusters is $\phi = U_1, U_2, \ldots, U_n$. Any cluster head U_i $(1 \leqslant i \leqslant N)$ chooses $\mathrm{SK}_i \in Z_q^*$ randomly, and calculates $\mathrm{PK}_i = \mathrm{SK}_i g_1$. The public/private key pair of U_i $(1 \leqslant i \leqslant N)$ is $(\mathrm{SK}_i, \mathrm{PK}_i)$, where SK_i is reserved secretly by the cluster head. PK_i is broadcast and opened to the public.

To build a complete trinity tree, make cluster head U_i $(1 \leqslant i \leqslant N)$ of N clusters as the nodes of the leaves of the trinity tree. $T_{h,l}$ are the non-leaf nodes, h is the number of layers (height) of the node in the tree, and l $(1 \leqslant h \leqslant \lfloor \log_3^N \rfloor, 1 \leqslant l \leqslant \lfloor N/3 \rfloor)$ is the l-th node in the layer.

Each leaf node U_i $(1 \leqslant i \leqslant N)$ can calculate the public key of its parent node $T_{h,\lfloor i/3 \rfloor}$ $(0 \leqslant i \leqslant N)$ by using its own private key and the public key of its sibling node. That is, the private key of its parent node is $\mathrm{TX}_{h,\lfloor i/3 \rfloor} = H_1(e(\mathrm{PK}_{i+1}, \mathrm{PK}_{i+2})^{\mathrm{SK}_i}) = H_1(e(\mathrm{PK}_i, \mathrm{PK}_{i+2})^{\mathrm{SK}_{i+1}}) = H_1(e(Y_i, Y_{i+1})^{\mathrm{SK}_{i+2}}) = H_1(e(g_1, g_1)^{\mathrm{SK}_i \mathrm{SK}_{i+1} \mathrm{SK}_{i+2}})$. $\mathrm{TX}_{h,\lfloor i/3 \rfloor}$ is reserved secretly, and the corresponding public key of its parent $\mathrm{TY}_{h,\lfloor i/3 \rfloor} = \mathrm{TX}_{h,\lfloor i/3 \rfloor} g_1$ is broadcast. Each leaf node is calculated upwardly to the root node $T_{0,0}$. When a leaf node U_j $(1 \leqslant j \leqslant N)$ does not have a sibling node, the private key of its parent node can be calculated by $\mathrm{TX}_{h,\lfloor j/3 \rfloor} = H_1(e(g_1, g_1)^{\mathrm{SK}_j})$, and the corresponding public key of its parent node is $\mathrm{TY}_{h,\lfloor j/3 \rfloor} = \mathrm{TX}_{h,\lfloor j/3 \rfloor} g_1$. When a leaf node U_j $(1 \leqslant j \leqslant N)$ lacks one sibling node, the private key of its parent node can be calculated by $\mathrm{TX}_{h,\lfloor j/3 \rfloor} = H_1(e(\mathrm{PK}_{i+1}, g_1)^{\mathrm{SK}_i}) = H_1(e(\mathrm{PK}_i, g_1)^{\mathrm{SK}_{i+1}}) = H_1(e(g_1, g_1)^{\mathrm{SK}_i \mathrm{SK}_{i+1}})$, and the corresponding public key of its parent node is $\mathrm{TY}_{h,\lfloor j/3 \rfloor} = \mathrm{TX}_{h,\lfloor j/3 \rfloor} g_1$. According to the nature of bilinear mapping, all cluster head nodes (leaf nodes) can calculate the same private key of the tree root node $T_{0,0}$. This private key is considered a shared alliance key between cluster heads.

(2) Cross-cluster sensor node key agreement. If the sensor nodes participating in the group key agreement are distributed in a different cluster, then the process of the cross-cluster group key agreement is as follows.

(i) Each sensor node $u_{i,t}$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$ chooses two numbers $m_{i,t}, q_{i,t} \in Z_q^*$. Then it calculates $Q_{i,t} = q_{i,t} g_1$, $T_{i,t} = ((m_{i,t} + \mathrm{sk}_{i,t})/q_{i,t}) g_1$, $M_{i,t} = m_{i,t} \mathrm{PK}_i$, and sends $(\mathrm{id}_{u_{i,t}}, Q_{i,t}, T_{i,t}, M_{i,t})$ to cluster head U_i. (Note: $(\mathrm{id}_{u_{i,t}}, Q_{i,t}, T_{i,t}, M_{i,t})$ is conserved on a memory card in advance to reduce the number of online calculations and to extend the sensor life.)

(ii) After receiving $(\mathrm{id}_{u_{i,t}}, Q_{i,t}, T_{i,t}, M_{i,t})$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$, cluster head $U_i (1 \leqslant i \leqslant N)$ verifies the equation $e(Q_{i,t}, T_{i,t}) =?e(g_1, \mathrm{SK}_i^{-1} M_{i,t}) e(g_1, \mathrm{pk}_{i,t})$. If it is true, U_i can ensure that $(\mathrm{id}_{u_{i,t}}, Q_{i,t}, T_{i,t}, M_{i,t})$ is sent by $u_{i,t}$, make $M_{U_i} = \mathrm{TX}_{0,0}$, and calculate $f_{i,t} = \mathrm{SK}_i^{-1} M_{U_i} M_{i,t}$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$.

(iii) Between each cluster head U_i $(1 \leqslant i \leqslant N)$, the information of the sensor nodes participating in the group key agreement in each cluster $f_{i,t}$ is transmitted and shared commonly. For the sake of convenience, suppose there are two clusters whose sensor nodes participate in a group key agreement, which is a cross-cluster group key agreement between cluster head U_i and cluster head U_j. Then, U_i will send the information about the internal nodes participating in the key agreement $(f_{i,t}, Q_{i,t}, T_{i,t}, \mathrm{pk}_{i,t})$ $(1 \leqslant t \leqslant n)$ to U_j, and U_j will send the information about the internal nodes participating in the key agreement $(f_{i,t}, Q_{i,t}, T_{i,t}, \mathrm{pk}_{i,t})$ $(1 \leqslant t \leqslant n)$ to U_i as well.

- U_i chooses a random number $q_{U_i} \in Z_q^*$, and calculates $Q_{U_i} = q_{U_i} g_1$, $T_{U_i} = ((m_{U_i} + \mathrm{SK}_i)/q_{U_i}) g_1$, $\mathrm{PK} = \sum_{t=1}^{n} \mathrm{pk}_{i,t} + \sum_{t=1}^{n} \mathrm{pk}_{j,t}$, $\mathrm{QT} = \prod_{t=1}^{n} e(Q_{i,t}, T_{i,t}) \times \prod_{t=1}^{n} e(Q_{j,t}, T_{j,t})$, $P = m_{U_i} \mathrm{PK}$, $R = \mathrm{QT}_{m_{U_i}^2}$, and $\phi_{U_i} = m_{U_i} g_1 U_i$. U_i can calculate group encryption key $\mathrm{ek}_{U_i} = (R, P)$ and group de-

Table 1 Complexity analysis of authenticated protocols

Protocol	Modular exponentiation	Tate pairing	Scalar multiplication	Length of message sent	Length of message received
Lee et al. [6]	3	0	n	$2\|G_1\|$	$n\|G_1\|$
Tsai [7]	2	3	3	$3\|G_1\|$	$(n+1)\|G_1\|$
Chen et al. [8]	n	4	$4n+1$	$(2n+3)\|G_1\|$	$(2n+3)\|G_1\|$
Zhang et al. [9]	$n+5$	4	$5n+2$	$(n+4)\|G_1\|$	$(n+4)\|G_1\|$
Ours	–	5	2	$4\|G_1\|$	$(n+4)\|G_1\|$

cryption key $\mathrm{dk}_{U_i} = e(\phi_{U_i}, \sum_{t=1}^{n} f_{i,t} + \sum_{t=1}^{n} f_{j,t})$. Then, U_i broadcasts $(\mathrm{id}_{U_i}, f_{i,1}, f_{i,2}, \ldots, f_{i,n}, f_{j,1}, f_{j,2}, \ldots, f_{j,n}, Q_{U_i}, T_{U_i}, R, P)$ to the sensor nodes in the same cluster.

• Similarly, U_j chooses a random number $q_{U_j} \in Z_q^*$, and calculates $Q_{U_j} = q_{U_j} g_1$, $T_{U_j} = ((m_{U_j} + \mathrm{SK}_j)/q_{U_j}) g_1$, $\mathrm{PK} = \sum_{t=1}^{n} \mathrm{pk}_{j,t} + \sum_{t=1}^{n} \mathrm{pk}_{i,t}$, $\mathrm{QT} = \prod_{t=1}^{n} e(Q_{j,t}, T_{j,t}) \times \prod_{t=1}^{n} e(Q_{i,t}, T_{i,t})$, $P = m_{U_j}\mathrm{PK}$, $R = \mathrm{QT}_{m_{U_j}^2}$, $\phi_{U_j} = m_{U_j} g_1 U_j$. U_j can calculate group encryption key $\mathrm{ek}_{U_j} = (R, P)$ and group decryption key $\mathrm{dk}_{U_j} = e(\phi_{U_j}, \sum_{t=1}^{n} f_{j,t} + \sum_{t=1}^{n} f_{i,t})$. Then, U_j broadcasts $(\mathrm{id}_{U_j}, f_{j,1}, f_{j,2}, \ldots, f_{j,n}, f_{i,1}, f_{i,2}, \ldots, f_{i,n}, Q_{U_j}, T_{U_j}, R, P)$ to the sensor nodes in the same cluster.

(iv) Group key calculation. After each node in each cluster $u_{i,t}$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$ receives the broadcast from cluster head U_i $(1 \leqslant i \leqslant N)$, it verifies $e(Q_{U_i}, T_{U_i}) =? e(g_1, m_{i,t}^{-1} f_{i,t}) e(g_1, \mathrm{PK}_i)$. If the equation is true, each $u_{i,t}$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$ can ensure that $(\mathrm{id}_{U_i}, f_{i,1}, f_{i,2}, \ldots, f_{i,n}, f_{j,1}, f_{j,2}, \ldots, f_{j,n}, Q_{U_i}, T_{U_i}, R, P)$ is sent by cluster head U_i. Then, each $u_{i,t}$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$ can obtain group encryption key $\mathrm{ek}_{u_{i,t}} = (R, P)$, and calculate $\phi_{i,t} = f_{i,t} m_{i,t}^{-1}$ and group decryption key $\mathrm{dk}_{u_{i,t}} = e(\phi_{i,t}, \sum_{i=1,t=1}^{i=n,t=n} f_{i,t}) = e(m_{U_i} g_1, \sum_{i=1,t=1}^{i=n,t=n} f_{i,t})$ by using its own key parameter $m_{i,t}$.

(v) The group key is self-certified. $u_{i,t}$ $(1 \leqslant i \leqslant R,\ 1 \leqslant t \leqslant n)$ verifies equation $e(P, \phi_{i,t}) \mathrm{dk}_{u_{i,t}} =? R$ to verify the correctness of $\mathrm{ek}_{u_{i,t}}$ and it calculates $\mathrm{dk}_{u_{i,t}}$.

Complexity analysis. We compared and analyzed the literature from recent years that can be quantified. All of these protocols are suitable for wireless sensor networks. Thus, they are comparable and representative. According to data from these protocols, comparative analysis involves the complexity of calculation and communication, and the protocol consumption of the total energy. Table 1 lists a comparison and analysis between the agreements of this study and four comparable and representative group key agreement protocols in the calculation of complexity and traffic.

Conclusion. We proposed a cross-cluster asymmetric group key agreement protocol for wireless sensor networks. As a sensor network is vulnerable to attack, an asymmetric group key agreement protocol is proposed, that is, the sensor nodes exchange information using an asymmetric cryptosystem. As the sensor node resources are limited, the scheme adopts asymmetric calculation, making the sensor node bear lightweight calculation and communication.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. U1636213), Natural Science Foundation of Henan Province (Grant No. 162300410322), and Beijing Municipal Natural Science Foundation (Grant No. 4172053).

References

1 Zhu R J, Tan Y A, Zhang Q X, et al. Determining image base of firmware for ARM devices by matching literal pools. Digit Invest Int J Digit Foren Incident Response, 2016, 16: 19–28
2 Zhu H F, Tan Y A, Zhang X S, et al. A round-optimal lattice-based blind signature scheme for cloud services. Future Gener Comput Syst, 2017, 73: 106–114
3 Xue Y, Tan Y A, Liang C, et al. An optimized data hiding scheme for deflate codes. In: Soft Computing. Berlin: Springer, 2017. 1–11
4 Zhang X S, Tan Y A, Xue Y, et al. Cryptographic key protection against FROST for mobile devices. Cluster Comput, 2017, 20: 2393–2402
5 Du X J, Guizani M, Xiao Y, et al. Transactions papers a routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. Int J Comput Technol Appl, 2009, 8: 1223–1229
6 Lee C C, Lin T H, Tsai C S. A new authenticated group key agreement in a mobile environment. Ann Telecommun, 2009, 64: 735–744
7 Tsai J L. A novel authenticated group key agreement protocol for mobile environment. Ann Telecommun Ann Des télécommun, 2011, 66: 663–669
8 Chen Y, He M X, Zeng S K, et al. Universally composable asymmetric group key agreement protocol. In: Proceedings of the 10th International Conference on Information, Communications and Signal Processing, Singapore, 2016
9 Zhang L, Wu Q H, Domingo-Ferrer J, et al. Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications. IEEE Trans Inf Foren Secur, 2015, 10: 2352–2364