TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 10/13 pp627-633
Volume 20, Number 6, December 2015

Byzantine Fault-Tolerant Routing for Large-Scale Wireless Sensor Networks Based on Fast ECDSA

Jiawei Xu*, Keda Wang, Chao Wang, Feng Hu, Zhenhua Zhang, Shiyi Xu, and Jie Wu

Abstract: Wireless sensor networks are a favorite target of Byzantine malicious attackers because of their limited energy, low calculation capability, and dynamic topology, and other important characteristics. The Byzantine Generals Problem is one of the classical problems in the area of fault tolerance, and has wide application, especially in distributed databases and systems. There is a lot of research in agreement and replication techniques that tolerate Byzantine faults. However, most of this work is not suited to large-scale wireless sensor networks, due to its high computational complexity. By introducing Fast ECDSA (Elliptic Curve Digital Signature Algorithm), which can resist timing and energy attacks, and reduce the proportion of verifying signature algorithm to generating signature algorithm to 1.2 times, we propose a new Byzantine fault-tolerant routing algorithm for large-scale wireless sensor networks with double-level hierarchical architecture. In different levels, the algorithm runs different BFT protocols. Theory and simulation results have proved that this algorithm has high security and the number of communication rounds between clusters is reduced by 1/3, which balances the network load. At the same time, the application of Fast ECDSA improves the security level of the network without burdening it.

Key words: wireless sensor networks; Byzantine Generals Problem; fault-tolerant routing; Elliptic Curve Digital Signature Algorithm (ECDSA); LEACH-protocol

1 Introduction

In a wireless sensor network, malicious nodes are referred to as Byzantine nodes, which are caused by software bugs, operation mistakes, missing keys, energy exhaustion, or attacks. Large-scale wireless sensor networks are collections of a substantial number of nodes deployed in rugged surroundings. The topology of the network is dynamic, and each node is a potential routing node, making the network more vulnerable to be attacked. The influence of Byzantine nodes is important to the reliability and the usability of the entire network. Because of the serious resource constraints of sensors, traditional public-key cryptographies such as RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) cannot be used in this case. Therefore, the design of lightweight Byzantine fault-tolerant protocols may enhance the fault-tolerant ability of large-scale wireless sensor networks.

The Byzantine Generals Problem has been mainly employed in solving fault-tolerance and credibility problems in modern cryptography and distributed

• Jiawei Xu, Chao Wang, and Feng Hu are with the Department of Communication and Information Engineering, Shanghai University, Shanghai 200072, China. E-mail: xujiawei91@163.com; wangchao@staff.shu.edu.cn; sdhf911103@163.com.
• Jie Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA. E-mail: jiewu@temple.edu.
• Zhenhua Zhang is with Ltd. Huawei, Shenzhen 518219, China. E-mial: zzh@163.com.
• Shiyi Xu is with the Institute of Computer Engineering and Science, Shanghai University, Shanghai 200072, China. xusy@shu.edu.cn.
• Keda Wang is with China Information Security Research Institute, Beijing 102200, China. E-mail: wkd@yeah.com.
∗ To whom correspondence should be addressed.
Manuscript received: 2015-06-30; accepted: 2015-07-27

systems, and is widely used in military, financial, and Internet research. Recently, research on Byzantine fault-tolerant problems in LANs and WANs has made great progress. In 2008, Liskov and Rodrigues[1] made a great breakthrough in Web systems by using the Byzantine fault-tolerant problem. In the same year, Vandiver[2] described the design, implementation, and evaluation of a replication scheme to handle Byzantine faults in transaction processing database systems. In 2010, Amir et al.[3] presented the first hierarchical Byzantine fault-tolerant replication architecture suitable for systems that cover multiple disjoint sites. The security of this algorithm is based on the RSA public-key cryptosystem, which is inferior to the new research public-key cryptosystem ECC in both computational complexity and in the key size, and the RSA algorithm cannot be used in a wireless sensor network. Wu et al.[4] wrote a short note about Byzantine fault-tolerant protocols in a survey of attacks and countermeasures in MANET. Hsieh[5] and Liu et al.[6] have also reported research about Byzantine fault-tolerant in MANET. In 2013, Vempaty et al.[7] analyzed the effect of false information from the Byzantines on target state estimation and obtained the minimum fraction of Byzantines that "blinds" the fusion center. In the same year, Lin et al.[8] proposed an energy-efficient cooperative geographic routing to reach energy-efficient routing in wireless sensor networks. In 2014, Koh et al.[9] proposed a dynamic witness concept together with distributed forwarder node monitoring to validate the transmitted fusion data. This scheme offered better resilience against Byzantine nodes and improved energy efficiency compared to existing witness-based approaches. In the same year, Vempaty et al.[10] investigated system design issues in FDR-based distributed detection and demonstrated that improved system design may be achieved by employing the Kolmogorov–Smirnov distance metric instead of the deflection coefficient. They also analyzed the performance of FDR-based distributed detection in the presence of Byzantines. In 2015, Bhuiyan et al.[11] and Li et al.[12] presented an approach to make the WSN resilient to the faults, called FTSHM. This approach guarantees a specified degree of fault tolerance and searches the repair points in clusters in a distributed manner, and places a set of back-up sensors at those points in such a way that still satisfies the engineering requirements. In the same year, Zhou et al.[13] from Tsinghua University applied WiFi to sensor networks to balance between low cost and high accuracy.

This paper proposes a new Byzantine fault-tolerant routing algorithm for large-scale wireless sensor networks. This algorithm has high security and the number of communication rounds between clusters is reduced by 1/3. By using the Fast ECDSA algorithm, which can resist timing and energy attacks, we can decrease the proportion of verifying signature algorithm and accelerate the speed of signature algorithm by 1.2 times. In so doing, the security level of the algorithm is increased without aggravating communication.

2 BFT Protocol

The Byzantine Generals Problem was derived from military problems during the Byzantine Empire period (5th to 15th century)[14]. The original Byzantine army problem supposed that several divisions of the Byzantine army surrounded a town occupied by the enemy. Each division was led by a general (commander) and the generals were allowed to communicate with each other only by means of messengers. Assume that some generals might become traitors who would deliberately deliver an incorrect message to others. Therefore, care should be taken by each general in case one receives incorrect messages, and all the final decisions should be made on the basis of a majority agreement, so that no betrayed general can disturb the military plan. Three conditions should be considered:

(1) No solutions can be made if more than 1/3 of the generals betrayed their positions.

(2) A solution can be obtained by using an Oral Message (OM) algorithm as the number of betrayed generals accounting for less than 1/3.

(3) A solution can be obtained by using a Signed Message (SM) algorithm as the number of loyal generals accounting for more than 2/3.

The BFT protocol is a Byzantine Fault Tolerance asynchronous protocol, developed by Castro and Liskov using the Quorum system and state machine replication technology[15]. It was used to resolve a number of unknown Byzantine error node problems. BFT uses an elected leader to coordinate the protocol and proceed through a series of views. Considering network energy consumption and password authentication problems, the role of leading node is taken by the cluster head node in our algorithm. When a leading node changes into a non-trusted one, it requires the other nodes to elect a new leading node within the cluster, and refresh the view information of the cluster, but there is no need of redistributing the cluster. The network structure and role differentiation will be introduced in the next section.

The BFT protocol goes through three rounds of communication to ensure the information's consistency with the cluster view, and requires that a majority of nodes reaches agreement in every round. Supposing the cluster has f Byzantine error nodes, and the total number of nodes in the cluster is less than $3f+1$, so it needs no less than $2f+1$ nodes to agree with every communication. In the first round of the BFT communication protocol, the leading node updates the local number of nodes with updated information by broadcasting a pre-prepared message to give other nodes this updated information and the number in their cluster. In the second round of the BFT communication protocol, the nodes that have received the pre-prepared message will broadcast a prepared message to the other nodes. When some nodes receive a pre-prepared message and $2f$ prepared messages (Prepare Certificate Status), they emit Commit messages in the cluster, and the third round communication of the BFT protocol begins. During the third round of communication, if some nodes receive $2f+1$ Commit messages, it means that the updated information has passed through the coherence protocol and has been executed.

3 Algorithm Framework

Aiming at large-scale wireless sensor networks with double-level hierarchical architecture, this paper proposes a new Byzantine fault-tolerant routing algorithm. The algorithm requires at least $3f+1$ nodes to tolerate f Byzantine nodes to ensure the fault-tolerant ability.

The algorithm framework is described as follows:

- Complete an OM(f) algorithm between the nodes at the local level by running three rounds of the BFT protocol.
- Using lighted threshold digital signatures based on Fast ECDSA to ensure communication security in the cluster.
- The messages sent from the cluster head take a signature based on Fast ECDSA.
- At the global level, the cluster-head nodes complete the OM(f) algorithm by running two rounds of an optimal BFT protocol.
- At the routing level, the algorithm uses a security enhancement algorithm, including Authentication factor and Certainty factor.

4 Feasibility Simulation Analysis

To evaluate the feasibility of our algorithm, we propose theory and simulation analysis between two preset algorithms. The simulation platform is OPNET Model Release 14.5.

Considering the common case, we suppose N to be the total number of nodes in a wireless sensor network, with f Byzantine malicious nodes. The communication message and the round number are important parameters with which we can analyze the network usage and data processing rate of the algorithm. We define the number of data packets sent in a communication round as the communication message. One round is the time starting from when some node begins broadcasting information until all the other nodes receive the information. So a communication round is defined as the total number of rounds needed to finish the communication.

Preset algorithm I, running an OM algorithm at the global level, needs at least $f+1$ rounds of communication. The total communication messages are $F(N,f)=(N-1)(N-2)\cdots(N-f-1)$.

For Preset algorithm II, running an SM algorithm in clusters, the communication message is $F(M,f)=(M-1)(M-2)\cdots(M-f-1)$, and running an SM algorithm between different clusters, the communication message is $F(k,f)=(k-1)(k-2)\cdots(k-f-1)$. Preset algorithm II needs at least $2(f+1)$ rounds communication, and the total amount of communication messages is $F(M,f)+MF(k,f)$.

As a preset algorithm running an OM algorithm at the global level, Preset algorithm II is the prototype of our algorithm. Preset algorithm II divides N nodes into M clusters; each cluster contains k nodes. Figures 1 and 2 are the result we obtained from the matching communication messages with the communication rounds in different N and different $r=f/N$.

From the comparison results above, we find that in the same N and $r=f/N$, a hierarchical architecture needs more communication rounds, but its total communication messages and network consumptions both decrease rapidly.

In this paper, the new algorithm runs on different Byzantine fault-tolerant protocols for different levels, yielding a greater reduction in communication rounds than with the traditional hierarchical architecture. The total communication messages have been reduced to $\frac{2}{3}F(M,f)+MF(k,f)$. Meanwhile, the new

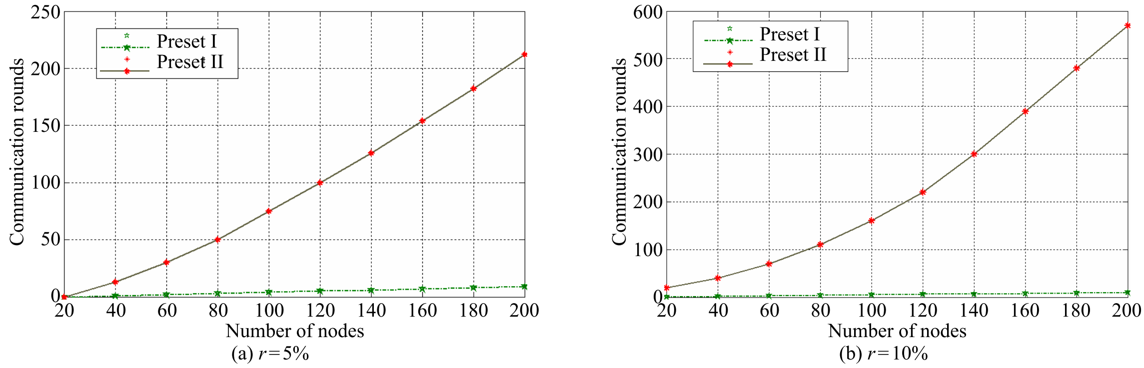

Fig. 1 Contrast between communication rounds.

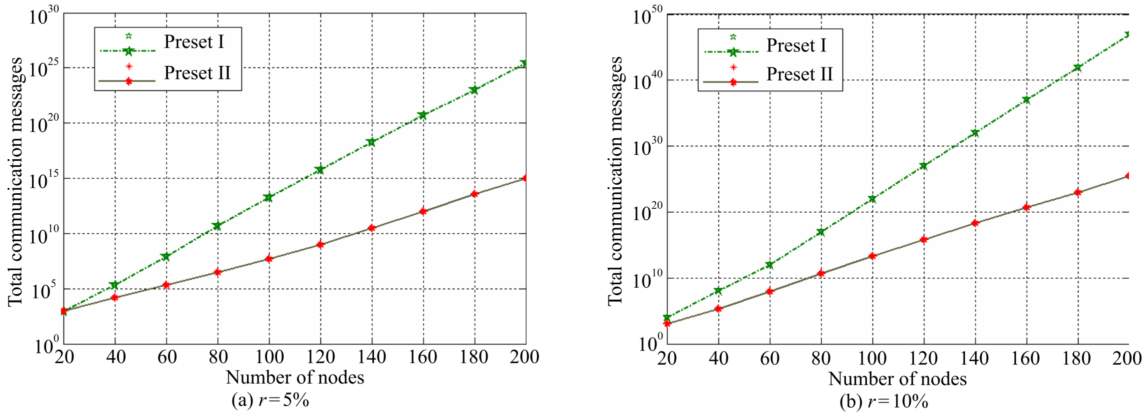

Fig. 2 Contrast between total communication messages.

algorithm brings in the Fast ECDSA algorithm. The security level has thus been greatly enhanced without aggravating the communication.

5 Algorithm Description

5.1 Lightweight threshold scheme based on Fast ECDSA

The Fast ECDSA implementation process in our algorithm is as follows: First, it defines an elliptic curve domain parameter $D = (O, a, b, p)$, where O is the finite field $GF(p^n)$, $a, b \in GF(p^n)$, p is a base point. If node A sends a message m to node B, the Fast ECDSA signature generation is as follows:

(1) A selects a secret random integer $k, k_A \in [1, n-1]$;

(2) A computes $kG = (x_1, y_1)$ (where y_1 is not needed to perform the computation) and $r = x_1 \bmod p_1^n$;

(3) A computes $k^{-1} \bmod p_1^n$;

(4) A computes $e = \text{MD5}(m)$;

(5) A computes $s = k^{-1}(e + rk_A) \bmod p_1^n$; if $s = 0$, then return to Step (1);

(6) The Fast ECDSA signature of message m is the integers (r, s); A sends $(m \| r \| s \| k_A)$ to B.

The signature verification process is as follows:

(1) When B receives the signature, it must verify that r and s are integers in the interval $[1, n-1]$. If any verification fails then the signature is rejected.

(2) B computes $e = \text{MD5}(m)$ and $w = s^{-1} \bmod p_1^n$;

(3) B computes $u_1 = ew \bmod p_1^n$ and $u_2 = rw \bmod p_1^n$;

(4) B compute $a = (u_1 + u_2 \times k_A) \bmod p_1^n$;

(5) B compute a multiplying point of $a \times G$ and $v = x_1 \bmod p_1^n$ on a Montgomery curve;

(6) If $v = r$, then the signature of A is accepted.

Simulation result shows that using a Fast ECDSA algorithm can reduce the time ratio to verify and generate the signature from 2 to 1.2, a reduction of about 40%. The point multiplication uses a binary shift NAF coding algorithm, while adopting point addition and point multiplication of the not calculated value of y under Projective coordinate, thus avoiding many modular inverse algorithms. The detailed algorithm can be viewed in the author's research paper on the ECDSA algorithm based on Montgomery-form ECC[16] .

Each cluster has a security certificate whose security is based on a Montgomery-type elliptic curve cryptosystem, which is sent to the cluster head node of each cluster by the base station; at the same time, it uses a Fast ECDSA algorithm to optimize the lightweight design of a $(2f+1,\ 3f+1)$ threshold scheme[17]. Suppose that the cluster contains f Byzantine error nodes, and the total number of nodes in the cluster is less than $3f+1$, so each communication round needs no less than $2f+1$ nodes to agree with it.

Each cluster has a public key and a private key. The public key is divided into a partial key, allocated to each node in the cluster, which can be used by each node to partially sign for information. Each node has information that can verify the effectiveness of each partial signature in the cluster; the cluster head node can integrate information for the collected partial signatures in some clusters. The other nodes can only communicate with the remaining nodes in the same cluster; the cluster head node can achieve not only communication between a cluster and base station, but also communication among the clusters. Each piece of information sent by the cluster head carries a digital signature based on Fast ECDSA.

5.2 Different Byzantine fault-tolerant protocols for different levels

The local level runs three rounds of BFT protocol to eliminate the effects of Byzantine nodes. Suppose each message sent from a cluster head is correct and safe; communication at the global level is effected by each cluster head. The cluster head disseminates messages to the other cluster heads, receives global messages, and distributes them to the local nodes.

The cluster-head nodes complete an OM(f) algorithm by running two rounds of an optimal BFT protocol at the global level. Running two rounds of an optimal BFT protocol at the global level is much simpler than at the local level. In the first round, the base station assigns a sequence number to a message and sends a proposal message containing this assignment to the other cluster heads. In the second round, any cluster head receiving the proposal sends an accept message, acknowledging the proposal, to the rest of cluster heads. When a cluster head receives a proposal message and $\lfloor s/2 \rfloor$ matching accept messages—it orders the corresponding behavior. A detailed description of the algorithm follows:

(1) A node sends an update that contains a logical time stamp i to its cluster head. The cluster head proposes an update with time stamp $i+1$ after it receives a reply for an update with time stamp i.

(2) When the base station receives an update, it assigns a global sequence number to the update; this assignment is encapsulated in a proposal message and sent to the other cluster heads. Each cluster head generates a threshold signature on the constructed proposal and sends the signed proposal to the other cluster heads.

(3) When a cluster head receives a signed proposal, it forwards it to the nodes in its cluster. Upon receiving a proposal, a node constructs an accept message that contains a matching partial signature and sends it to its cluster head. After receiving $2f+1$ accept messages, the cluster head combines the partial signatures and sends them to the other cluster heads.

(4) The cluster head forwards the incoming accept messages to the nodes in its cluster. A node orders the corresponding behavior after it receives a proposal message and $\lfloor s/2 \rfloor$ matching accept messages from the other clusters.

(5) The routing level improves the swarm intelligence algorithm by using a security enhancement algorithm that includes an authentication factor and a Certainty factor. The Ant packet contains public key information from its upper node, and updates this public key information to its own. $W_{\text{Credibility}}(A, B)$ represents the credibility of node B to node A and is influenced by latency, loss ratio, and dump energy. Its value limits the routing choice of node A. The improved forward Ant packet and backward Ant packet are structured as Fig. 3.

For detailed information about the preparation stage, setup stage, acquisition latency, and the Wormhole anti-attack of the Ant colony algorithm, please refer to Ref. [18].

6 Conclusions

Wireless sensor networks are a favorite target of Byzantine malicious attackers for their limited energy,

Ant-ID (4 bits)	S-addr (4 bits)	Cred (4 bits)	Date (64 Bytes)	Pre-PK (20 Bytes)
T-stamp (4 bits)	Dest (4 bits)	Nodes (4 bits)	Hops (4 bits)	

(a) Forward

Ant-ID (4 bits)	S-addr (4 bits)	Dest (4 bits)
Cred (4 bits)	Nodes (4 bits)	Hops (4 bits)

(b) Backward

Fig. 3 Forward Ant packet and backward Ant packet.

low calculation capability, dynamic topology, and other special characterics.

We found large-scale wireless sensor networks to be highly scalable due to their double-level hierarchical architecture; they excel in network topology management, energy minimization, and application to distributed applications.

For an N-node wireless sensor network, suppose there are S clusters with S cluster-head nodes. The message exchange complexity has been reduced from $O(N^2)$ to $O(S^2)$ in comparison with a flat architecture, and the scalability of network has also been enhanced. The algorithm proposed operates different rounds of Byzantine fault-tolerant protocol at different levels, which can reduce the total communication messages from $F(N,f)=(N-1)(N-2)\cdots(N-f-1)$ to $\frac{2}{3}F(M,f)+MF(k,f)$; the number of communication rounds between clusters is reduced by 1/3 which balances the network load effectively.

Compared with the traditional RSA Public Key cryptosystem, the new research focus, ECC, gains the ascendancy in both computational complexity and key size. By using the Fast ECDSA algorithm, the security level of the algorithm proposed has been greatly enhanced without aggravating the communication. Theory analysis and simulation results prove that this algorithm has effectively eliminated the effects of Byzantine nodes, offers balanced energy consumption, and improves fault-tolerance for a large-scale wireless sensor network.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Nos. 61332019, 61572304, 61272056, and 60970006); the Innovation Grant of Shanghai Municipal Education Commission (No. 14ZZ089), Shanghai Key Laboratory of Specialty Fiber Optics and Optical Access Networks (No. SKLSFO2014-06).

References

[1] B. Liskov and R. Rodrigues, Tolerating Byzantine faulty clients in a quorum system, in *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems, (ICDCS06)*, Lisbon, Portugal, 2006.

[2] B. Vandiver, Detecting and tolerating Byzantine faults in database systems, PhD dissertation, MIT, USA, 2008.

[3] Y. Amir, C. Danilov, D. Dolev, J. Kirsch, J. Lane, C. Nita-Rotaru, J. Olsen, and D. Zage, Steward: Scaling Byzantine fault-tolerant replication to wide area networks, *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 1, pp. 80–93, 2010.

[4] B. Wu, J. M. Chen, J. Wu, and M. Cardei, A survey of attacks and countermeasures in mobile ad hoc networks, in *Wireless Network Security on Signals and Communication Technology*, Y. Xiao, X. Shen, and D.-Z. Du, Eds. Springer, 2007, pp. 103–135.

[5] H. C. Hsieh, The agreement problem in the mobile network, Master degree dissertation, Chaoyang University of Technology, Taichung, China, 2004.

[6] Y. Liu, N. H. Yu, and X. L. Feng, A cluster-based solution to BGP on mobile ad hoc network, (in Chinese), *Journal of Electronics & Information Technology*, vol. 28, no. 12, pp. 2386–2389, 2006.

[7] A. Vempaty, O. Ozdemir, and P. K. Varshney, Target tracking in wireless sensor networks in the presence of Byzantines, in *16th International Conference on Information Fusion*, Istanbul, Turkey, 2013.

[8] B. Lin, W. J. Wang, Q. Y. Yin, H. X. Li, and R. Yang, An energy-efficient geographic routing based on cooperative transmission in wireless sensor networks, *Science China Information Sciences*, vol. 56, no. 7, p. 072302, 2013

[9] J. Y. Koh, J. C. M. Teo, and W.-C. Wong, Mitigating Byzantine attacks in data fusion process for wireless sensor networks using witnesses, in *Proceedings of the 2014 IEEE ICCS*, Macau, China. 2014.

[10] A. Vempaty, P. Ray, and P. K. Varshey, False discovery rate based distributed detection in the presence of Byzantines, *IEEE Transactions on Aerospace and Electronic System*, vol. 50, no. 3, pp. 1826–1840, 2014.

[11] M. Z. A. Bhuiyan, G. J. Wang, J. N. Cao, and J. Wu, Deploying wireless sensor networks with fault-tolerance for structural health monitoring, *IEEE Transaction on Computers*, vol. 64, no. 2, pp. 382–395, 2015.

[12] J. J. Li, J. Wu, and Z. N. Ma, Frequency and similarity-aware partitioning for cloud storage based on space-time utility maximization model, *Tsinghua Science and Technology*, vol. 20, no. 3, pp. 233–245, 2015.

[13] Z. M. Zhou, C. S. Wu, Z. Yang, and Y. H. Liu, Sensorless sensing with WiFi, *Tsinghua Science and Technology*, vol. 20, no. 3, pp. 1–6, 2015.

[14] Y. H. Min, Byzantine generals problem, *Science Technology for China's Mass Media in Chinese*, vol. 3, no. 3, pp. 35–38, 2006.

[15] M. Castro and B. Liskov, Authenticated Byzantine fault tolerance without public-key cryptography, Technical Memo MIT/LCS/TM-589, MIT Laboratory for Computer Science, 1999.

[16] C. Wang, X. Y. Shi, and Z. H. Niu, The research of the promotion for ECDSA algorithm based on Montgomery-form ECC, (in Chinese), *Journal on Communications,* vol. 31, no. 1, pp. 9–13, 2010.

[17] Y. Desmedt, Some recent research aspects of threshold cryptography, *Lecture Notes in Computer Science*, vol. 1396, pp. 158–173, 1998.

[18] C. Wang, X. Y. Jia, and Q. Lin, Trust-based secure routing algorithm for wireless sensor networks, (in Chinese), *Journal on Communications*, vol. 29, no. 1, pp. 105–112, 2008.

Chao Wang received the PhD degree from Tongji University in 1999. Currently, he is the Information Security Committee Vice Chair of China Electronics Institute, committeeman of CCF, IEEE Shanghai Section Secretary, IEEE Shanghai CAS Chapter Vice Chair, and IEEE Shanghai Computer Chapter Vice Chair. His research interests include wireless sensor network, network information security and ECC, and quantum computing cryptography.

Shiyi Xu received his PhD degree from Fudan University in 1964. Currently, he is the professor of Shanghai University. He is the Fault-Tolerant Committee Past-Vice Chair of CCF. His research interests include the fault-tolerant computing theory and technology and trusted computing system design.

Jie Wu is the chair and a Laura H. Carnell Professor in the Department of Computer and Information Sciences at Temple University. Prior to joining Temple University, USA, he was a program director at the National Science Foundation and a distinguished professor at Florida Atlantic University. He received his PhD degree from Florida Atlantic University in 1989. His current research interests include mobile computing and wireless networks, routing protocols, cloud and green computing, network trust and security, and social network applications. Dr. Wu regularly published in scholarly journals, conference proceedings, and books. He serves on several editorial boards, including *IEEE Transactions on Computers*, *IEEE Transactions on Service Computing*, and *Journal of Parallel and Distributed Computing*. Dr. Wu was general co-chair/chair for IEEE MASS 2006 and IEEE IPDPS 2008 and program co-chair for IEEE INFOCOM 2011. Currently, he is serving as general chair for IEEE ICDCS 2013 and ACM Mobi Hoc 2014, and program chair for CCF CNCC 2013. He was an IEEE Computer Society Distinguished Visitor, ACM Distinguished Speaker, and chair for the IEEE Technical Committee on Distributed Processing (TCDP). Dr. Wu is a CCF Distinguished Speaker and a Fellow of the IEEE. He is the recipient of the 2011 China Computer Federation (CCF) Overseas Outstanding Achievement Award.

Keda Wang is currently a senior engineer in China Information Security Research Institute. His research interest is information security. He received his bachelor degree in 2000 from Beijing Technology and Business University.

Feng Hu is currently a PhD candidate in Shanghai University. His research interest is information security. He received his bachelor degree in 2012 from Xi'an University of Science and Technology.

Jiawei Xu is currently a master student in Shanghai University. Her research interest is information security. She received her bachelor degree in 2014 from Shanghai University of Electric Power.

Zhenhua Zhang is currently a member in Huawei Technologies Co. Ltd. Her research interest is information security. She received her master degree in 2011 from Shanghai University.