International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.225-236
http://dx.doi.org/10.14257/ijsia.2013.7.5.21

Construction of Trusted Wireless Sensor Networks with Lightweight Bilateral Authentication

Ping Guo[1], Jin Wang[1], JieZhong Zhu[2], YaPing Cheng[1] and Jeong-Uk Kim[3]

[1] *School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2] *Bing Jiang College, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[3]*Department of Energy Grid, Sangmyung University, Seoul 110-743, Korea*

Abstract

Sensor networks are ad hoc mobile networks that include sensor nodes with limited computational and communication capabilities. They have become an economically viable monitoring solution for a wide variety of applications. Obviously, security threats need to be addressed and, taking into account its limited resources, the use of lightweight authentication is strongly recommended. In this paper, a lightweight authentication model for wireless sensor networks composed of a key management and an authentication protocol is presented. It is based on the use of trusted primitives with very low computational requirements, which obtains better results than other proposals in the literatures.

Keywords: *wireless sensor networks, trusted network platform, lightweight bilateral authentication*

1. Introduction

With the rapid development of Internet, a secure and reliable network has been becoming a very important issue. Nowadays, most of the network applications adopt many different kinds of secure ways for their network systems, such as data encryption, intrusion detection, virtual private network and distant authentication *etc*. However, most of these traditional security technologies just amend on the unsecure infrastructures which they are born with insecurity, inefficiency and can't solve the security problems radically. Such as wireless sensor networks (WSN) are wireless networks with special characteristics due to the total absence of infrastructure or administrative support[1]. They have low resources, like limited bandwidth, low or medium computational capability and energy constraints. In spite of these limitations, WSN are useful for situations where communication is needed but there is no infrastructures or it has been heavily damaged. During the process of building secure WSN network, we had deep experience over the matters. In accordance with the WSN security requirements, combining with its network concrete situations, a trusted WSN has been constructed. Trusted WSN is not a combination of lots of security technologies and lots of security products. We think it is trustworthy as long as it reaches security requirements we need and satisfies security requests we want. Combining with the WSN features and the ideas of trusted network, research on constructing trusted WSN based on a bilateral authentication protocol has been carried out. We aim to protect data authenticity, integrity, confidentiality and non-repudiation in WSN.

The rest of the article is outlined as follows. We summarize related work on authentication of sensor networks. We discuss the trusted mechanism to construct the security WSN. Then

ISSN: 1738-9976 IJSIA

we put forward a bilateral authentication for WSN, and evaluate its performance. Finally, we conclude this article.

2. Related Work

To achieve security in wireless sensor networks, it is important to be able to perform various cryptographic operations, including encryption, authentication, and so on. However, authentication has been regarded as the first protective measure for WSN. Early WSN's authentication mechanism using symmetric cryptography, comparing with the asymmetric cryptography technology, greatly simplifies the key calculation and reduces the communication load. It does not need the trusted third party, which node directly through the key negotiation message to determine the session key, but it also requires prior stored system master key. When a new node is added, the pre-distribution key mechanism is not flexible, because the all the old keys of the existing nodes and broadcast messages are updated, which is not easy to achieve, and the master key is easy to cause physical intrusion. With the development of sensor network technology, more and more WSN security based on asymmetric cryptography. The literature [2] proposed the security architecture of WSN based on RSA algorithm, for each node must be strong enough to perform the traditional RSA algorithm, and negotiating session key by a group of nodes, which requires high static topology. The literature [3] proposes authentication scheme of TinyPK RSA conveniently to realize the WSN entity authentication based on the scheme, but there is a single point of failure. The literature [4] presents strong user authentication protocol adopting a global certification scheme converting single point authentication into N nodes authentication, which the intrusion tolerance of WSN has been enhanced, however, there is no better defense against DoS (Denial of Services) attack. The literature [5] puts forward an ECC algorithm authentication and access control protocol, providing the new node dynamically join WSN, a key established with its neighbor nodes in the process of negotiating session key. Although the protocol has higher efficiency, saving storage and bandwidth than the literature [3], the two sensor nodes need to have the same configuration at the same time, assuming that each node should have the same tolerance interval if it is captured.

In recent years, authentication mechanism based on identity for WSN has been widely studied, because it has the following advantages:(1)overcoming the heavy certificate public key certificate management mechanism based on the certificate, no overhead, the implicit key authentication; (2)identity information as the geographic information, IP address or ID number, is very important and sometimes in practical application. The literature [6] designs a key agreement based on a BF-IBE (Boneh and Franklin Identity-Based Encryption) [7] between nodes authenticated. The literature [8] proposes a suitable negotiating session key agreement for WSN node. The above scheme partly overcomes the defects of certificate-based authentication system, but inevitably cryptosystem based on bilinear pairings is used, and the pairing operation is more complex than RSA, ECC operation [9], which causes a great pressure on resource constrained sensor nodes.

3. Key Technologies of Constructing Trusted Wireless Sensor Networks

Trusted Network Platform (TNP) has been put forwarded based on concepts of Trusted Calculating Platform (TCP). TCP[1] gives emphasis to the security of low-level of a computer and the security of operating system. However, TNP gives emphasis to the security of network model or infrastructure. The framework of TNP has been put forwarded by a branch of information security trade organization in 2002. Its definition is[10] if activities in network and the consequences of those activities can be predicted and controlled, then the

network is trusted. Compared with the concepts of traditional network, trusted network emphasizes strongly on providing the abilities of activity control, activity supervising, activity authentication and activity management, and constructs correspondent system to maintain the trusty of network. In terms of aims of wireless sensor networks, a trusted platform should be built in order to provide a single access point for all of the users and provide all kinds of security services. It's important to construct a universal and electronic identity authentication based on trusted WSN.

3.1. Characters of Wireless Sensor Networks

(i) wireless nature of communication
(ii) resource limitation on sensor nodes
(iii) lack of fixed infrastructure
(iv) unknown network topology prior to deployment
(v) high risk of physical attacks on unattended sensors

3.2. Key Technologies of Constructing Trusted Wireless Sensor Networks

3.2.1. Trusted Entity Security based on TPM

The security of computer hardware platform is protected by trusted platform module(TPM).TPM[11] is a micro system that has encryption calculating component and storage component, which can support the security of upper operating system. TPM as a trusted root evaluates the security of BIOS and operating system, protects the environment trusted, and passes the trusted chain on to the next. The basic idea of trusted calculating network is from an original trusted root which can be passed between all the applications on the platform. Even the platform changes, the chain would be kept and not be changed. Because of this kind of platform, the calculating environment is trusted on the platform, and all kinds of operations on the calculating environment are trusted, so the security of entities is promised. That is the trusted chain mechanize.

3.2.2. Identity Authority Based on Digital Certificate

Digital certificate provides identity certificates for users, including individual, enterprises, gateways, and banks, who undertake information exchange and business affairs. The digital certificate is unique, which provides the link between the public key of a user and its identity. To realize the function, digital certificates must according to the international standard of X.509, and its original root must be reliable. So there should be an organization that is trusted by all the users, taking charge of granting and managing the digital certificates, and promising the network security. So public key infrastructure (PKI) builds certificate authority (CA) as the third trusted part, and CA is the core of PKI.

3.2.3. Accessing Technology Based on Role Binding with Identity

There are distinct groups of users in campus network, such as teacher-group, student-group, and administrative group, which is very convenient to set different rights for different users according to their identity, and deploy accessing and controlling policies efficiently. Even binding the users' identities with their roles, allocating sets of users and sets of roles efficiently, a user can access system resources by named a appropriate role under a given environment, which every role has its corresponding right and it is a core of security control

policy. Reliable identity authority and effective accessing control enhance the trusty of campus network.

3.2.4. Data Encryption Technology Based on Requirements

Data encryption is an important technology to construct the security campus network, and is a core of the whole information security. Public key encryption has been used universally, and played an important role in digital signature, identity authority and data encryption in the process of constructing the trusted campus network. Both public key encryption and secret key encryption are applied in trusted campus network, and each exerts its advantage, which provides strong supports to the security of operating system and different applications combining with the technologies of identity authority and accessing control according to different requirements.

3.2.5. System Redundancy Technology Based on Tolerance

Research on tolerance about trusted calculation or trusted network is not enough, [12, 13] said that redundant technology should be a necessary and important protection to build the trusted platform. Tolerant technology includes error tolerance and intrusion tolerance. Error tolerance focuses on tolerating the errors of hardware and software, while intrusion tolerance focuses on tolerating vicious attacks. Anyway, tolerant technology provides an ability of recovering from intrusion and attack, including reallocating resources and system redundancy. We consider redundant technology much to provide special protections for important systems, important data bases, and important information during the process of constructing trusted campus network.

3.2.6. Security Management Technology Based on Uniform Platform

With the development of network applications and advanced technologies, the more illegal access and vicious attacks, the less security of network. Firewalls, virtual personal network, intrusion detection system, identity authority, and data encryption played important roles in network security, but all these technologies, each does things in its own way, resulting in irrelative, isolated “information nodes” which cannot support each other, and work together efficiently. However, trusted network needs a uniform security management platform (USMP) to configure as a whole, control every layer of network, realize centralized supervision for all of the network security resources, predigest management of network security, and improve level of network security.

According to these technologies, the framework of trusted campus network is shown as Figure 1.

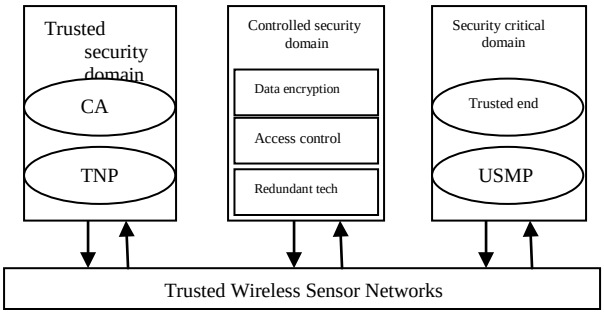


Figure 1. Framework Architecture of Trusted Campus Network

4. Constructing Trusted Wireless Sensor Network Based on Lightweight Bilateral Authentication

Bilateral authentication protocol between MU (Mobile Users) and LCA (Lightweight Certificate Authority) [14, 15] is shown below.

Step1: MU requires LCA to access WMN.

Step2: LCA responds MU: $LCA \rightarrow MU : R_{LCA}$, R_{LCA} is a random number generated by LCA.

Step3: MU receives LCA's message, signs R_{LCA} with its private key, attaches its slavery public key and generates a random number R_{MU}. At that the same time, MU computes $\alpha = Sign_{PK_{LCA}}(h(PK_{MU}^{(Slavery)} \mid R_{MU} \mid Sign_{SK_{MU}}(R_{LCA}))$, and returns $MU \rightarrow LCA : \{PK_{MU}^{(Slavery)}, Sign_{PK_{LCA}}(R_{MU}), Sign_{SK_{MU}}(R_{LCA}), \alpha\}$ to LCA, with $Sign_{PK_{LCA}}(R_{MU})$ which is a signature produced using LCA's public key sign R_{MU}.

Step4: LCA uses its private key to verify $Verf_{SK_{LCA}}(Sign_{PK_{LCA}}(R_{MU}))$ and $Verf_{SK_{LCA}}(\alpha) = Verf_{SK_{LCA}}\{Sign_{PK_{LCA}}(h(PK_{MU}^{(Slavery)} \mid R_{MU} \mid Sign_{SK_{MU}}(R_{LCA}))\}$ to promise data integration during transportation. According to $PK_{MU}^{(Slavery)} = Sign_{SK_{LCA}}(ID_{MU} \mid PK_{MU}^{(Master)})$, LCA is easy to judge that MU was registered already, and it use $PK_{MU}^{(Master)}$ to decrypt $Sign_{SK_{MU}}(R_{LCA})$ and get R_{LCA} to verifies MU own a private key corresponding to $PK_{MU}^{(Master)}$ that proves MU is a legal user. That is the whole process that LCA authenticated MU.

Step5: MU firstly uses LCA's certificate $Cert_{LCA}$ to verify $Verf_{PK_{LCA}}\{Sign_{SK_{LCA}}(Sign_{PK_{MU}^{(Master)}}(R_{MU}))\}$, and uses its private key to verify $Verf_{SK_{MU}}(Sign_{PK_{MU}^{(Master)}}(R_{MU}))$ and gets R_{MU}, comparing it with the original R_{MU} that generated in step 3 and judging whether they are same. MU then uses its private key to verify $Verf_{SK_{MU}}(\beta) = Verf_{SK_{MU}}(Sign_{PK_{MU}^{(Master)}}(h(Cert_{LCA} \mid R_{MU}))$ for integration decision and at the same time to judge whether LCA is legal. That the whole process that MU authenticated LCA.

The bilateral authentication process is shown as Figure 2.

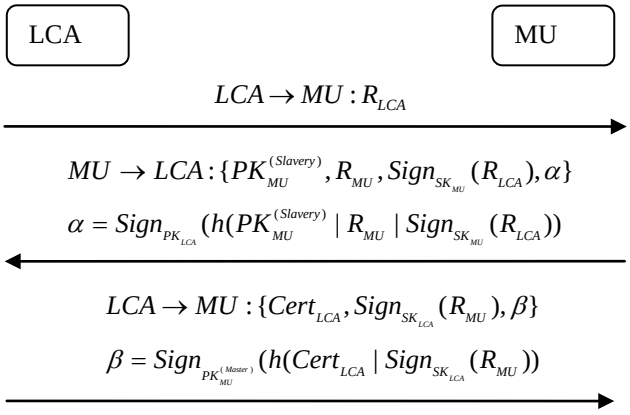


Figure 2. Bilateral Authentication between MU and LCA

5. Discussion

In this section, we discuss the performance of our bilateral authentication. The computation cost is measured with other authentication protocols for WSN in other literatures. And then the communication cost is compared with other schemes put forward by some reference listed in the end.

5.1. Computation Cost

Authentication efficiency is mainly measured by the various calculation performed between LCA and the user. Our bilateral authentication protocol compared calculation cost with other authentication protocols is shown in Table 1. For the sake of fairness, just comparing the public key system. (Note: our scheme adopts discrete logarithms elliptic curve cryptographic algorithms, mainly on a group G point multiplication computation)

TG_e : Time needing for the operation taking the form of $e(P,Q)$ for $P,Q \in G$;

TG_{mul} : Time needing for the operation taking the form of aP for $a \in Z_N^*$ and $P \in G_1^*$;

TG_{add} : Time needing for the operation taking the form of $P+Q$ for $P,Q \in G$;

$TG_{\exp}$: Time needing for the operation taking the form of $a^b \mod N$ for $a,b \in Z_N^*$;

T_H : Time needing for the operation taking the form of unilateral HASH function;

T_{Mac} : Time needing for the operation of computing MAC.

Table 1. Comparison of the Computation Cost Between this Paper and the References

	Reference [17]	Reference [18]	Our work	Reference[16]	Reference [19]
Public key system	Certificate-based	Certificate-based	Lightweight CA	Identity-based	Certificate less
Algorithm	RSA	ECC	ECC	Paring	Bilateral lineal parings
Computation cost for user			$4TG_{mul}+2T_H$	$3TG_{mul}+3T_H$	$5TG_{\exp}+2T_H$
Computation cost for server			$2TG_{mul}+T_H$	$2TG_e+2TG_{mul}+TG_{add}+3T_H$	
Exchange times	2	2	2	1	2
Certificate	Y	Y	N	N	N
Application	WSN	WSN	WSN	Mobile ends	Mobile users
Bilateral authentication	Y	N	Y	N	N

The references [17] and [18] implements authentication and session key agreement between two sensor nodes. The reference [16] achieves authentication and session key agreement between the client and the server. The reference [19] realizes authentication and session key agreement between two mobile users. Our protocol realizes the bidirectional authentication between user and LCA, and LCA only needs few calculation. In general, our scheme comparing with other literatures, the computation cost is small, primarily point multiplication on a group G, no complicated pairings and exponential operation. We

implement our protocol signature and verification with ECDSA algorithm[20], shown as Figure 3 and Figure 4.

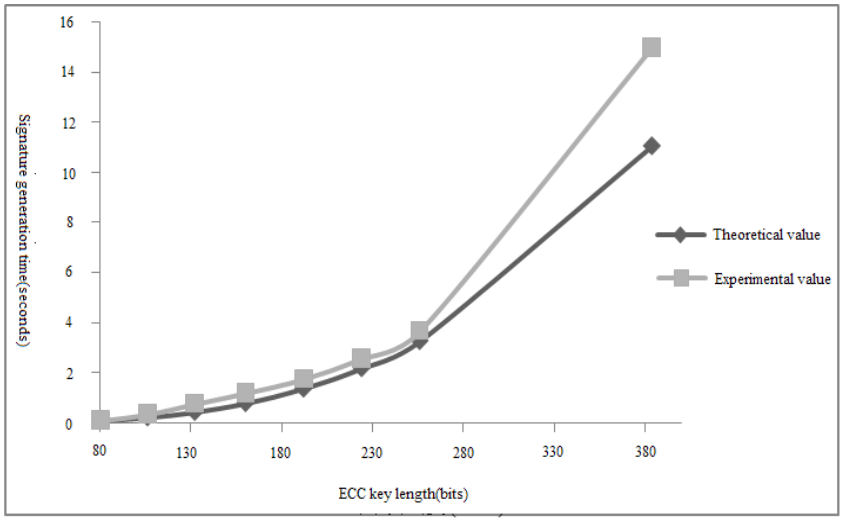


Figure 3. Theoretical Time and Experimental Time of ECC Signature with Different Key Length

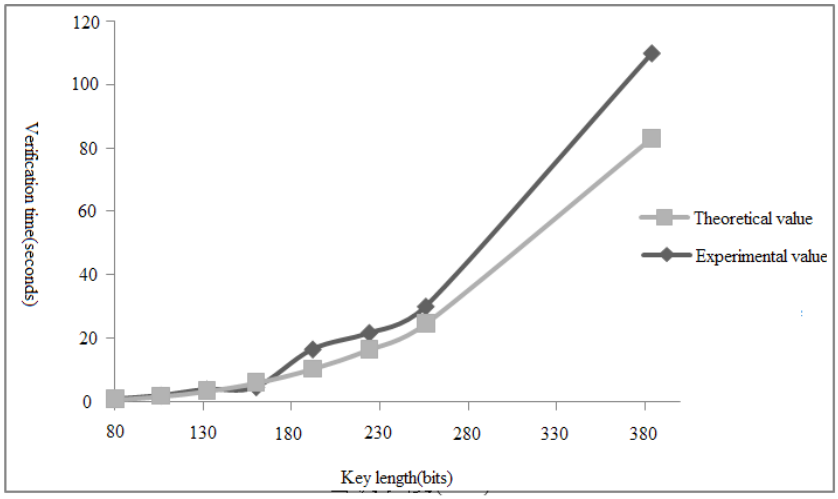


Figure 4. Theoretical Time and Experimental Time of ECC Signature Verification with Different Key Length

5.2. Communication Cost

The energy consumption analysis, generally uses an indirect measure method, whereby the transmission message number and size to estimate the node energy consumption. For example, the protocol SPINS for radio transmission energy consumption of up to about 97%, and the energy consumption is less than 3% encryption. The literatures [21, 22] research shows that radio transmission energy consumption ratio is a symmetric encryption operation three times power of 10. Therefore, minimizing the data packet transmission rate of sensor nodes to life is very important. Assessment of transmission energy consumption, need to calculate the total length of protocol to exchange information. This chapter to transmit a

message to the average size of protocol for evaluating

Given 16bits ID, 64bits random number, 320bits signature, 160bits HMAC, 160bits public key, 160bits private key and 70bytes certificate, LCA and MU finish two-way authentication protocol, among the process, MU needs to send 136bytes, LCA needs to send 174bytes.

We use OPNET (Optimized Network Engineering Tools) simulator [23] to test the various factors affecting communication. The simulation results are as shown in Figure 5. Our scheme compares the other different key authentication schemes under the same experimental conditions with the transmission bits during MU completing once authentication.

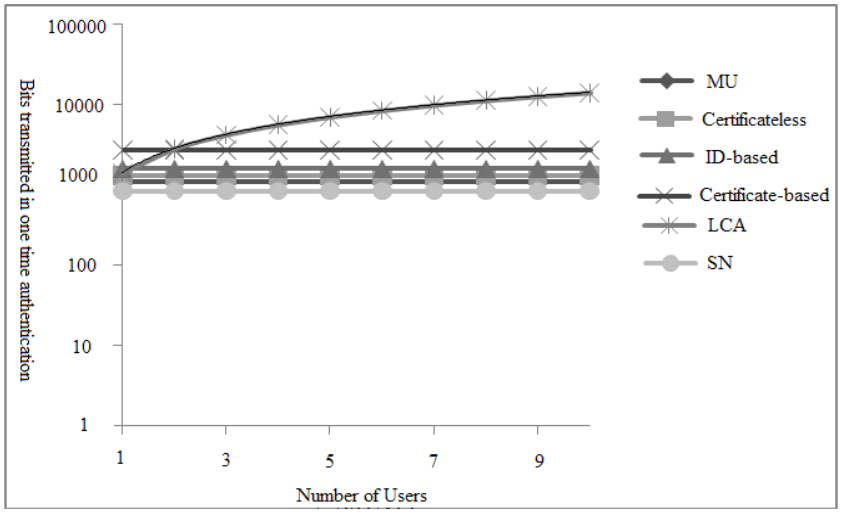


Figure 5. Sensor Nodes Transmitting Bits during once Authentication in Different Schemes

As shown in Figure 5, all refer the mutual authentication between MU and nodes. The reference [19] is based on a certificate less authentication in wireless sensor network, which transmits 1288bits in once authentication. The reference [16] is based on the identification of the WSN authentication, in which probably needs 1568bits to be transmitted. The reference [17] is based on the WSN certificate authentication scheme, and 2688bits have been transmitted in once authentication. However, our schema probably needs 1088bbits and 832bits respectively for MU and node. LCA is a server and provides authentication services to MUs or nodes, so needs more bits to send about 1392bits. Seen by the graph, MU in the authentication process only needs less number of bits for transmission, superior to other solutions.

6. Conclusion

Due to the openness of wireless networks, the key security is more important. How to design a CA system with the advantages of the traditional certificate-based CA system which protects the security and credibility of authentication and key distribution, and avoids the complication of certificate management, thus is more applicable to the wireless networks. Our work is designed to solve the problem. Combination of lightweight CA ideas, designing a bilateral authentication protocol between the user and LCA. We build a prototype, implement critical algorithms of encryptions and decryptions, run the system, and evaluate system security. Analysis showed that: LCA simplifies the complexity of the traditional certificate-based CA system with the advantages of generating public key lightweight, verification lightweight, no certificate management, and communication less, which can resist a variety

of attacks that are easy to invade the resource-constrained wireless environment.

Acknowledgments

We would like to express our gratitude to our University and college for supporting our work. This work was funded in part by China Meteorological Administration under CMA grants [2013]NO 069. It was also supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Knowledge Economy (MKE) Korea, and by the Natural Science Foundation of Jiangsu Province (No. BK2012461). Professor Jeong-Uk Kim is the corresponding author.

References

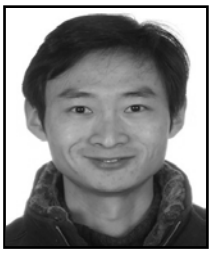
[1] T. C. Group, "TCG Specification Architecture Overview", Journal of Communication, vol. 18, no. 22, **(2003)**.
[2] J. Kong, P. Zerfos and H. Luo, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks", Proceedings of the 9th International Conference on Network Protocols, Riverside, CA, USA, **(2001)** November 11-14.
[3] R. Watro, D. Kong and F. C. Sue, "TinyPK: Securing Sensor Networks with Public Key Technology", Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, **(2004)** Oct. 25, Washington, DC, USA
[4] Z. Benenson, N. Gedicke, and O. Raivio, Realizing Robust User Authentication in Sensor Networks. Proceedings of Workshop on Real-World Wireless Sensor Networks, Stockholm, Sweden, **(2005)** June 20-21.
[5] Y. Zhou, Y. Zhang and Y. Fang, "Access Control in Wireless Sensor Networks", Ad Hoc Networks, vol. 8, no. 5, **(2007)**.
[6] H. B. Cheng and G. Yang, "An Authenticated Identity-based Key Establishment and Encryption Scheme for Wireless Sensor Networks", The Journal of China Universities of Posts and Telecommunications, vol. 13, no. 2, **(2006)**.
[7] Z. F. Zhang, D. S. Wong, J. Xu and D. G. Feng, "Certificateless Public-key Signature: Security Model and Efficient Construction", Proceedings of the 4th International Conference on Applied Cryptography and Network Security, Singapore, **(2006)** June 6-9.
[8] G. Yang, J. T. Wang, and H. B. Cheng, "A Key Establish Scheme for WSN Based on IBE and Diffie-hellman Algorithms", Acta electronic sinica, vol. 35, no. 1, **(2007)**.
[9] D. R. Brown, "SEC 2: Recommended Elliptic Curve Domain Parameters", Journal of Information Security and Networking, vol. 12, no. 5, **(2011)**.
[10] C. X. Shen, H. G. Zhang and D. G. Feng, "Summarize of information security", China Science, China Science and Technology Press, vol. 13, no. 37, **(2007)**.
[11] N. Liu, "Research on trusted calculation based on TPM", Journal of Bei Jing Institute of Technology, Press of China Mechanical Industry, vol. 23, no. 4, **(2008)**.
[12] Y. P. Chi, Y. Fang and Y. Y. Wu, "Research on constructing trusted calculating network", Journal of College of Bei jing Electronic Science and Technology,Press of of College of Bei jing Electronic Science and Technology, vol. 13, no. 14, **(2005)**.
[13] L. S. Zhou, J. Yang and P. Z. Tan, "Technology of identity authentication and its developing trend", Communication Technology, China Communication Technology Press, vol. 42, no. 10, **(2009)**.
[14] X. L. Dong, L. H. Wang and Z. F. Cao, "New public key cryptosystems with lite certification authority", IEEE Transaction on Mobile Computing, vol. 5, no. 6, **(2006)**.
[15] Y. Pang, L. C. Wang and Z. F. Cao, "Lite-CA based key pre-distribution scheme in wireless sensor network", Journal of Communications, vol. 30, no. 3, **(2009)**.
[16] L. J. Dang, W. D. Kou, J. Zhang and F. Guo, "Improvement of Mobile IP Registration Using Self-certified Public Keys", IEEE Transactions on Mobile Computing, vol. 1, no. 4, **(2007)**.
[17] Z. J. Zhang, L. H. Zhu, and H. Tang, "An Hierarchical Authentication Scheme for Wireless Sensor Networks", Journal of Southeast University,Southeast University Press, vol. 38, no. 9, **(2008)**.
[18] T. Y. Wu and Y. M. Tseng, "An ID-Based Mutual Authentication and Key Exchange Protocol for Low-Power Mobile Devices", Chinese Journal of Computer, Science Press, vol. 53, no. 7, **(2010)**.
[19] F. Q. Cheng, Z. Y. Peng, and W. Song, "Certificateless Authentication for Trusted Key Sharing in Trusted Database", Journal of Frontiers of Computer Science and Technology, vol. 4, no. 9, **(2010)**.
[20] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, AMS, vol. 48, no. 1, **(1987)**.

[21] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen Victor and D. E. Culler, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, Springer, vol. 10, no. 8, **(2004)**.
[22] G. Anastasi, M. Conti, M. Francesco and A. Passarella, "Energy Conservation in Wireless Sensor Networks: A Survey", Ad Hoc Networks, Elsevier, vol. 7, no. 3, **(2009)**.
[23] Y. Sun Yi and C. Meng Cheng, "Handout of OPNET Communication Simulation", National defense science and technology press,China, **(2005)**.

Authors

Ping Guo obtained her B.S and M.S degree in the Computer Software and Theory from LanZhou University, China in 1997 and 2005, respectively. She received Ph.D degree in Nanjing University of Science and Technology(NUST) in 2012. She is a lecturer in the College of Computer & Software, Nanjing University of Information Science & Technology(NUIST) from 2005 till now. Her research interests focus on wireless network security, multiple-hop wireless networks authentication and key management.

Jin Wang Dr. Jin Wang received the B.S. and M.S. degree in the Electronical Engineering from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received Ph.D. degree in the Ubiquitous Computing laboratory from the Computer Engineering Department of Kyung Hee University Korea in 2010. Now, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and technology. His research interests mainly include routing algorithm and protocol design, performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.



Jiezhong Zhu obtained his Masters in Computer Engineering from HoHai University, China in 2004. Now, he is an associated professor in Bing Jiang College, Nanjing University of Information Science & Technology(NUIST). His research interests include wireless communication network, information security and cloud computing.

YaPing Cheng obtained her Masters in System Analysis and Data Integration from University of Information Science & Technology(NUIST), China in 2006. Now, she is an associated professor in the College of Computer & Software, Nanjing University of Information Science & Technology(NUIST). Her research interests include image processing, information security and digital watermarking.

Jeong-Uk Kim obtained his B.S. degree in Control and Instrumentation Engineering from Seoul National University in 1987, M.S. and Ph.D. degrees in Electrical Engineering from Korea Advanced Institute of Science and Technology in 1989, and 1993, respectively. He is a professor in SangMyung University in Seoul. His research interests include smart grid demand response, building automation system, and renewable energy.