A Secure Handshake Scheme with Pre-negotiation for Mobile-hierarchy City Intelligent Transportation System under Semi-honest model

Shuai Li*, Peng Gong*, Qian Yang*, Xiao Peng Yan*, Jiejun Kong**, and Ping Li*

* National Key Laboratory of Mechatronic Engineering and Control, School of Mechatronical Engineering, Beijing Institute of Technology, Beijing, China

** Department of Computer Sciences, University of Florida, Gainesville, FL, USA

lshuai@ndrc.gov.cn, {penggong,yangqian,yanxiaopeng}@bit.edu.cn, jkong@cs.ucla.edu, liping85@bit.edu.cn

Abstract— **Mobile-hierarchy architecture was widely adopted for query a deployed wireless sensor network in an intelligent transportation system recently. Secure handshake among mobile node and ordinary nodes becomes an important part of an intelligent transportation system. For dividing virtual communication area, pre-negotiation should be conducted between mobile node and ordinary node before formal handshake. Pre- negotiation among nodes can increase the odds for a successful handshake. The mobile node negotiates with an ordinary sensor node over an insecure communication channel by private set intersection. As an important handshake factor, Attribute set is negotiated privately among them in local side. In this paper, a secure handshake scheme with pre-negotiation for mobile-hierarchy city intelligent transportation system under semi-honest model is proposed.**

Keywords—**Attribute-based handshake; Private set intersection; Intelligent transportation system; Wireless sensor network; Attribute Encryption**

I. INTRODUCTION

The significant advances in hardware manufacturing technology and the advent of the Micro-Electro-Mechanical-Switches (MEMS) paved the way for building smart sensor nodes that are capable of performing three important functions: sensing, processing, and wireless communication. In order to fundamentally solve traffic jam, parking and emergency traffic problem, intelligent transportation systems (ITS) is proposed. ITS is an advanced information technology, data communication transmission technology, electronic sensor technology, control technology and the effective integration of computer technology applied to the entire surface traffic management system. The typical ITS handles the multimedia information, current state attributes and communication functions.

A multi-agent system that carries out the mixed integer programming model and the space–time network flow model was proposed by Shah et al., wherein each agent can decide on its own behavior for the situation of its environment [1]. A solution for solving the problem of congestion and traffic management was proposed by Ameur et al., which based on cooperative multi-agent based principled negotiation between agents [2]. Ahmed et al. and Bachmann et al. discussed a practical traffic and transportation problem as a data fusion problem [3, 4]. Various significant contributions were made to the field of data fusion in transportation systems [5]. If two sensor nodes have the same current state attributes, it is possible for them to perform data fusion, provide mutual support. Secret handshake was introduced recently by Balfanz et al. and Su et al. [6, 7], it is a useful cryptographic mechanism which allows two members of the same group to authenticate each other secretly. Therefore, secret handshake concept can certainly be applied to mobile-hierarchy city intelligent transportation system to achieve secure attribute matching. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets [8]. In this paper, we present a secure attribute matching handshake scheme with pre-negotiation based on bilinear pairings and private set intersection which can be used to extend fuzzy authentication and data fusion by intersecting set elements and matching attributes privately [9].

The structure of this paper is organized as follows. Section II gives the preliminaries. The proposed scheme is described in Section III. The security analysis is given in Section IV. Finally, the conclusions are drawn in Section V.

II. PRELIMINARIES

A. Bilinear maps

Let G_1 and G_2 be two multiplicative cyclic groups of prime order p. Let g be a generator of G_1 and e be a bilinear map, e: $G_1 \times G_1 \rightarrow G_2$. The bilinear map e has the following properties:

- Bilinearity: for all $g_1, g_2 \in G_1$ and a, $b \in Z_p$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
- Non-degeneracy: $e(g, g) \neq 1$.

We say that G_1 is a bilinear group if the group operation in G_1 and the bilinear map e: $G_1 \times G_1 \rightarrow G_2$ are both efficiently

computable. Notice that the map e is symmetric since $e(g^a, g^b) = e(g,g)^{ab} = e(g^b, g^a)$.

B. Decisional Bilinear Diffie-Hellman Assumption

Let G_1 and G_2 be two multiplicative cyclic groups of prime order p. a bilinear map e: $G_1 \times G_1 \rightarrow G_2$ and a generator g of G_1, The Decisional Bilinear Diffie-Hellman problem (DBDH) in (G_1, G_2, e) is that no probabilistic polynomial-time algorithm B can distinguish $e(g,g)^{abc}$ given (g^a, g^b, g^c) from an element $e(g,g)^z$ with more than a negligible advantage Adv. We define the advantage of a distinguisher against the DBDH as follows:

$$Adv = \left|\Pr[B(g^a, g^b, g^c, e(g,g)^{abc}) = 0] - \Pr[B(g^a, g^b, g^c, e(g,g)^z) = 0]\right| \quad (1)$$

C. Semi-honest model

A semi-honest party is one who follows the prescribed actions in the protocol with the exception that it keeps all its intermediate computations. All parties may record all message from the protocol execution and try to compute as much as possible in the protocol, and perform any additional polynomial-time computation apart from the prescribed protocol. We adopt the standard definition from Brickell and shmatikov's scheme [10].

Definition 1 (computational indistinguishability): $S \subseteq \{0,1\}^*$. Two ensembles (indexed by S), $X \overset{def}{=} \{X_w\} winS$ and $Y \overset{def}{=} \{Y_w\} winS$ are computationally indistinguishable if for every family of polynomial-size circuits, $\{D_n\} n \in N$, there exists a negligible function $\mu : N \rightarrow [0,1]$ so that

$$pr[D_n(w, X_w) = 1] - pr[D_n(w, Y_w) = 1] | < \mu(|w|) \quad (2)$$

Definition 2: protocol π securely computes deterministic functionality f in the presence of static semi-honest adversaries if there exist probabilistic polynomial-time simulators S_1 and S_2 such that

$$\{S_1(x, f(x,y))\}_{x,y \in (0,1)^*} \overset{c}{\equiv} \{view_1^{\pi}(x,y)\}_{x,y \in (0,1)^*} \quad (3)$$

$$\{S_2(x, f(x,y))\}_{x,y \in (0,1)^*} \overset{c}{\equiv} \{view_2^{\pi}(x,y)\}_{x,y \in (0,1)^*} \quad (4)$$

D. Homomorphic properties of Paillier's encryption

The product of two ciphertexts $E(m_1,r_1) \cdot E(m_2,r_2)$ will decrypt to the sum of their corresponding plaintexts (m_1,m_2),where r_1 and r_2 are random number.

- $D(E(m_1,r_1) \cdot E(m_2,r_2) \bmod n_2) = m_1 + m_2 \bmod n$

The product of a ciphertext $E(m_1,r_1)$ with a plaintext g^{m2} raising g will decrypt to the sum of the corresponding plaintexts (m_1,m_2).

- $D(E(m_1,r_1) \cdot g^{m2} \bmod n_2) = m_1 + m_2 \bmod n$

An encrypted plaintext $E(m_1,r_1)$/ $E(m_2,r_2)$ raised to the power of another plaintext m_2 /m_1 will decrypt to the product of the two plaintexts (m_1,m_2),

- $D(E(m_1,r_1)^{m2} \bmod n^2) = m_1 m_2 \bmod n$
- $D(E(m_2,r_2)^{m1} \bmod n^2) = m_1 m_2 \bmod n$

An encrypted plaintext $E(m_1,r_1)$ raised to a constant k will decrypt to the product of the plaintext m_1 and the constant k,

- $D(E(m_1,r_1)^{k} \bmod n^2) = k m_1 \bmod n$

III. PROPOSED SCHEME

It is assumed that there is a trust third party.The mobile node group require a public/private key pair (PK_{si}},SK_{si}) for Paillier encryption and digital signatures. We notate digital signatures of message x as Sign (x). The trust third party run the setup algorithm to obtain (p, q, r, G, G_T, e) with $G = G_p \times G_q \times G_r$. Here, G_p, G_q, G_r denotes the subgroups of G having order p, q, and r, respectively. Observe that $G = G_p \times G_q \times G_r$. If g is a generator of G, then the element g^{pq} is a generator of G_r; the element g^{pr} is a generator of G_q; and the element g^{qr} is a generator of G_p. If $h_p \bullet G_p$ and $h_q \bullet G_q$ then

$$e(h_p, h_q) = e((g^{qr})^{a_1}, (g^{pr})^{a_2}) = e(g^{a_1}, g^{ra_2})^{pqr} = 1 \quad (5)$$

where $a_1 = \log_{g^{qr}} h_p$ and $a_2 = \log_{g^{pr}} h_q$.

A. Pre-negotiation

- The mobile node A with attribute set $X=(x_1,x_2,\ldots,x_k)$ and ordinary node B with attribute set $Y=(y_1,y_2,\ldots,y_k)$. Both X and Y are drawn from some common domain.
- A computes a polynomial $f(y)=(y-x_1)(y-x_2)\ldots(y-x_k)= \sum_{i=1}^{k} \alpha_i y^i$ of degree k with roots $x_1,x_2,\ldots,x_k$ and sends B encrypted coefficients, $Enc(\alpha_1)$, $Enc(\alpha_2)$,…, $Enc(\alpha_k)$. B evaluates A's polynomial at each point y in his dataset through computing $Enc(r \cdot f(y)+y)$ with a random number r for each y. When A decrypts the ciphertexts, A gets the value of the corresponding elements for each of the elements in X∩Y, whereas the result is random for all other values.
- B computes a polynomial $f(x)=(x-y_1)(x-y_2)\ldots(x-y_k)= \sum_{i=1}^{k} \beta_i x^i$ of degree k with roots $y_1,y_2,\ldots,y_k$ and sends A encrypted coefficients, $Enc(\beta_1)$, $Enc(\beta_2)$,…, $Enc(\beta_k)$. A evaluates B's polynomial at each point x in his dataset through computing $Enc(r \cdot f(x)+x)$ with a random number r for each x. When B decrypts the ciphertexts, B gets the value of the corresponding elements for each of the elements in X∩Y, whereas the result is random for all other values.

B. Handshake

Next, it computes g^p, g^q,and g^r as generateors of G_p, G_q, G_r, respectively. It then chooses $R_{1,i}$, $R_{2,i} \bullet G_r$ and $h_{1,i}, h_{2,i} \bullet G_p$ uniformly at random for i=1 to n, and $R_0 \bullet G_r$ uniformly at random. The public parameters include (N=pgr, G, G_T, e) along with:

$$PK = (g_p, g_r, Q = g_p \cdot R_0, \{H_{1,i} = h_{1,i} \cdot R_{1,i}, H_{2,i} = h_{2,i} \cdot R_{2,i}\}_{i=1}^{n}) \quad (6)$$

The master secret key SK is ($p,q,r,g_q,\{h_{1,i},h_{2,i}\}_{i=1}^{n}$).

After setup algorithm is finished, chooses policy vector for agent $x_i=(p_1,\ldots\ldots,p_n)$ with $p_i \bullet Z_n$, and chooses random s, a, b $\bullet Z_n$ and $R_{3,i}$, $R_{4,i}$ $\bullet G_r$ for i=1 to n. it outputs the ciphertext C_{xi} and give C_{xi} to user x_i.

$$C_{xi}=(C_0=g_p{}^{s},\{C_{1,i}=H_{1,i}{}^{s}\cdot Q^{a\bullet p_i}\cdot R_{3,i},C_{2,i}=H_{2,i}{}^{s}\cdot Q^{b\bullet p_i}\cdot R_{4,i}\}_{i=1}^{n} \quad (7)$$

The trust third party generate attributes vector for user $v_i=(A_1,\ldots\ldots,A_n)$, and recall SK ($p,q,r,g_q,\{h_{1,i},h_{2,i}\}_{i=1}^{n}$), and chooses random $r_{1,i}$, $r_{2,i}$ $\bullet Z_p$ for i=1 to n, random $R_5 \bullet G_r$, random $f_1,f_2,\bullet Z_q$, and random $Q_6 \bullet Z_q$. It then outputs the SK_{vi} and give SK_{vi} to user v_i.

$$SK_{v_i}=(K=R5\cdot Q6\cdot\prod_{i=1}^{n}h_{1,i}{}^{-r_{1,i}}\cdot h_{2,i}{}^{-r_{2,i}},\ \{K_{1,i}=g_p{}^{r_{1,i}}\cdot g_q{}^{f_1\cdot A_i},K_{2,i}=g_p{}^{r_{2,i}}\cdot g_q{}^{f_2\cdot A_i}\}_{i=1}^{n}) \quad (8)$$

The trust third party define host v_i's attributes match user x_i's policy as $v_i.x_i=(A_1,\ldots\ldots,A_n).(p_1,\ldots\ldots,p_n)=0$.

When user A x_i communicates with user B v_i, user v_i show their SK_{vi} to x_i, x_i will compute equation:

$$F=e(C_0,K)\cdot\prod_{i=1}^{n}e(C_{1,i},K_{1,i})\cdot e(C_{2,i},K_{2,i}) \quad (9)$$

If F=1, v_i's attributes match x_i's policy, if not, mismatch. The detailed proofs of computation are given as follows:

$$e(C_0,K)\cdot\prod_{i=1}^{n}e(C_{1,i},K_{1,i})\cdot e(C_{2,i},K_{2,i})$$

$$=e(g_p{}^{s},R_5Q_6\prod_{i=1}^{n}h_{1,i}{}^{-r_{1,i}}h_{2,i}{}^{-r_{2,i}})\cdot\prod_{i=1}^{n}e(H_{1,i}{}^{s}Q^{a\cdot p_i}R_{3,i},g_p{}^{r_{1,i}}g_q{}^{f_1\cdot A_i})\cdot e(H_{2,i}{}^{s}Q^{b\cdot p_i}R_{4,i},g_p{}^{r_{2,i}}g_q{}^{f_2\cdot A_i})$$

$$=e(g_p{}^{s},R_5Q_6)\cdot e(g_p{}^{s},\prod_{i=1}^{n}h_{1,i}{}^{-r_{1,i}}h_{2,i}{}^{-r_{2,i}})\cdot\prod_{i=1}^{n}e(h_{1,i}{}^{s}R_{1,i}{}^{s}g_q{}^{a\cdot p_i}R_0{}^{a\cdot p_i}R_{3,i},g_p{}^{r_{1,i}}g_q{}^{f_1\cdot A_i})$$

$$\cdot\prod_{i=1}^{n}e(h_{2,i}{}^{s}R_{2,i}{}^{s}g_q{}^{b\cdot p_i}R_0{}^{b\cdot p_i}R_{4,i},g_p{}^{r_{2,i}}g_q{}^{f_2\cdot A_i})$$

$$=e(g_p{}^{s},\prod_{i=1}^{n}h_{1,i}{}^{-r_{1,i}}h_{2,i}{}^{-r_{2,i}})\cdot\prod_{i=1}^{n}e(h_{1,i}{}^{s}g_q{}^{a\cdot p_i},g_p{}^{r_{1,i}}g_q{}^{f_1\cdot A_i})\cdot\prod_{i=1}^{n}e(R_{1,i}{}^{s}R_0{}^{a\cdot p_i}R_{3,i},g_p{}^{r_{1,i}}g_q{}^{f_1\cdot A_i})$$

$$\cdot\prod_{i=1}^{n}e(h_{2,i}{}^{s}g_q{}^{b\cdot p_i},g_p{}^{r_{2,i}}g_q{}^{f_2\cdot A_i})\cdot\prod_{i=1}^{n}e(R_{2,i}{}^{s}R_0{}^{b\cdot p_i}R_{4,i},g_p{}^{r_{2,i}}g_q{}^{f_2\cdot A_i})$$

$$=e(g_p{}^{s},\prod_{i=1}^{n}h_{1,i}{}^{-r_{1,i}}h_{2,i}{}^{-r_{2,i}})\cdot\prod_{i=1}^{n}e(h_{1,i}{}^{s}g_q{}^{a\cdot p_i},g_p{}^{r_{1,i}}g_q{}^{f_1\cdot A_i})\cdot\prod_{i=1}^{n}e(h_{2,i}{}^{s}g_q{}^{b\cdot p_i},g_p{}^{r_{2,i}}g_q{}^{f_2\cdot A_i})$$

$$=e(g_p{}^{s},\prod_{i=1}^{n}h_{1,i}{}^{-r_{1,i}})\cdot e(g_p{}^{s},\prod_{i=1}^{n}h_{2,i}{}^{-r_{2,i}})\cdot\prod_{i=1}^{n}e(h_{1,i}{}^{s},g_p{}^{r_{1,i}})\cdot e(h_{1,i}{}^{s},g_q{}^{f_1\cdot A_i})\cdot$$

$$e(g_q{}^{a\cdot p_i},g_p{}^{r_{1,i}})\cdot e(g_q{}^{a\cdot p_i},g_q{}^{f_1\cdot A_i})$$

$$\cdot\prod_{i=1}^{n}e(h_{2,i}{}^{s},g_p{}^{r_{2,i}})\cdot e(h_{2,i}{}^{s},g_q{}^{f_2\cdot A_i})\cdot e(g_q{}^{b\cdot p_i},g_p{}^{r_{2,i}})\cdot e(g_q{}^{b\cdot p_i},g_q{}^{f_2\cdot A_i})$$

$$=\prod_{i=1}^{n}e(g_q{}^{a\cdot p_i},g_q{}^{f_1\cdot A_i})\cdot\prod_{i=1}^{n}e(g_q{}^{b\cdot p_i},g_q{}^{f_2\cdot A_i})\cdot$$

$$=\prod_{i=1}^{n}e(g_q,g_q)^{(af_1+bf_2)p_i\cdot A_i}=1$$

where $\prod_{i=1}^{n}p_i\cdot A_i=x_i\cdot v_i\equiv 0 \bmod N$

IV. SECURITY ANALYSIS

Theorem 1: Assume that the mobile agent with attribute set $X=(x_1,x_2,\ldots,x_k)$ and ordinary node B with attribute set $Y=(y_1,y_2,\ldots,y_k)$. After pre-negotiation, A and B learns nothing more than the elements of $X\cap Y$.

Proof. of Correctness: Given the encrypted coefficients $Enc(\alpha_1)$, $Enc(\alpha_2)$,…, $Enc(\alpha_k)$ of the polynomial f(y), B computes $Enc(r\cdot f(y)+y)$, uses the homomorphic properties of the encryption system to evaluate the polynomial at each elements of A's elements. B decrypts the ciphertexts. For each of the elements in $X\cap Y$, the result of this decryption is the value of the corresponding elements, whereas the result is random for all other values. The procedure is same for B.

A and B's privacy: Assume that the proof defines a polynomial $f(x)=(x-y_1)(x-y_2)\ldots(x-y_k)=\sum_{i=1}^{k}\beta_i x^i$. For B that operates in the real model, there is a B* operating in the real model. B sends to A encrypted coefficients $Enc(\beta_1)$, $Enc(\beta_2)$,…, $Enc(\beta_k)$. B* sends to A coefficients $\beta^*_1,\beta^*_2,\ldots,\beta^*_k$, the k roots of this polynomial are the inputs that B* sends to the trusted third party in the ideal implementation, such that for every input $Enc(r\cdot f(x)+x)$ of A, the views of the party B*, A in the real model is indistinguishable from the views of B, A in the real model. The standard definition of security in the static semi-honest model refers to Section II.

Assume that the length of the prime number p is 512,1024, 1536 bits in modular exponentiation, The protocol is implemented in C using MIRACL library and server configuration: Microsoft Windows xp Professional 2002 Service Pack 3, Intel(R) Core(TM), CPU 2.53 GHz, 3.98 GB of RAM [11]. The average time for computing a single modular exponentiation is 0.9 ms for 512-bit, 6ms for 1024-bit, and 28ms for 1536-bit module. According to average time for computing a single modular exponentiation, it is observed that the proposals computation time is effective.

V. CONCLUSIONS

In this paper, a secure attribute matching handshake scheme with pre-negotiation which employs attributes to describe policy and achieves the fuzzy authentication and data fusion is proposed. The proposed scheme adopts private set intersection for pre-negotiation, and adopts attribute encryption to implement an attribute matching procedure. It provides a balance between confidentiality and availability. According to security analysis, it satisfies the correctness and privacy requirements. Furthermore, it laid a solid foundation for private negotiation among sensor agents and give a self protect for each agent. In the future, a s attribute matching handshake scheme with pre-negotiation under the malicious model will be considered.

ACKNOWLEDGMENT

This research was supported in part by National Natural Science foundation of China (No.61201180), Beijing Natural Science Foundation (N0.4132055), and Excellent Young Scholars Research Fund of Beijing Institute of Technology. Corresponding author: Peng Gong.

REFERENCES

[1] N. Shah, S. Kumar, F. Bastani, and I. L. Yen, "Optimization models for assessing the peak capacity utilization of intelligent transportation systems," *European Journal of Operational Research*, vol.216, no. 1, 2012, pp. 239-251,

[2] M. E. A. Ameur and H. Drias, "A Cooperative multi-agent system for traffic congestion management in VANET. *Advances in Computer Science, Engineering & Applications*, vol.166, 2012, pp 499-508

[3] M. Ahmed and M. Abdel-Aty, "A data fusion framework for real-time risk assessment on freeways," *Transportation Research Part C: Emerging Technologies*, vol. 26, 2013, pp. 203-213

[4] C. Bachmann, B. Abdulhai, M. J. Roorda, and B. Moshiri, "A comparative assessment of multi-sensor data fusion techniques for freeway traffic speed estimation using microsimulation modeling," *Transportation Research Part C: Emerging Technologies*, vol. 26, 2013, pp. 33-48

[5] K. Lawrence, M. Lyudmila, and E. F. Nour-Eddin, "Sensor and Data Fusion:Taxonomy, Challenges and Applications," *Handbook on Soft Computing for Video Surveillance*. Chapman & Hall, USA, 2012, pp. 139-183.

[6] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, H. Wong, "Secret handshake from pairing-based key agreements." *In Proc. IEEE S&P '03*, 2003, pp 180–196.

[7] R. Su, "On the security of a novel and efficient unlinkable secret handshakes scheme," *IEEE Commun Letter,* vol.13, no.9, 2009, pp.712–713.

[8] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," In Proc. *the 17th international conference on Theory and application of cryptographic technique*, 1999;223-238.

[9] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient Private Matching and Set Intersection," *In Proc. EUROCRYPT04, LNCS,* Springer Berlin/Heidelberg, vol. 3027, 2004, pp.1-19.

[10] J. Brickell and V. Shmatikov, "Privacy-Preserving Graph Algorithms in the Semi-Honest Model," *Advances in Cryptology - ASIACRYPT 2005, LNCS,* Springer Berlin/Heidelberg,vol. 3788, 2005, pp. 236-252.

[11] M. Scott, MIRACL: Multiprecision integer and rational arithmetic c/c++ library,1988C2007. Homepage at http://www.shamus.ie/

Shuai Li received the BS degree in Mechatronical Engineering from Beijing Institute of Technology, Beijing, China, in 2004, and the MS degree in information perception and resistance from the Beijing Institute of Technology, Beijing, China, in 2006. He is currently a Ph.D candidate in the major of weapon system and application engineering at the Beijing Institute of Technology. His research interests are in the areas of intelligent detection and control, terminal information resistance and information security in wireless communication

Peng Gong received the BS degree in Mechatronical Engineering from Beijing Institute of Technology, Beijing, China, in 2004, and the MS and Ph.D. degrees from the Inha University, Korea, in 2006 and 2010, respectively. In July 2010, he joined the School of Mechatronical Engineering, Beijing Institute of Technology, China. His research interests include link/system level performance evaluation and radio resource management in wireless systems, information security, and the next generation wireless systems such as 3GPP LTE, UWB, MIMO, Cognitive radio and so on.

Qian Yang received the B.E. degree in detection, guidance and control techniques and the M.E. degree in measurement technique and automation equipment from the Beijing Institute of Technology, Beijing, China, in 2005 and 2007, respectively. She is currently a doctoral student in mechanical and electronic engineering at the Beijing Institute of Technology.Her research interests are in the areas of intelligent detection and control, signal processing and information security in wireless communication.

Xiao Peng. Yan received the B.E. degree in mechanical and electronic engineering and the M.E. degree in pattern recognition and intelligent system, and the Ph.D. degree in weapon system and application Engineering from the Beijing Institute of Technology, Beijing, China, in 1999, 2003 and 2009, respectively. He is an Associate Professor with the School of Mechatronical Engineering, Beijing Institute of Technology, where he has been a faculty member since 2003. His research interests are in the areas of radio proximity detection, signal processing in proximity sensor and information security in wireless communication.

Jiejun Kong received the Ph.D. degree in computer science from the University of California, Los Angeles, in 2004. He was a senior researcher in Scalable Network Technologies, Inc. and a post-doctoral researcher in the Network Research Lab of Computer Science Department at UCLA. He is interested in developing efficient, scalable, and secure network protocols for wireless networks. His research topics include secure and anonymous routing, authentication, access control, distributed data harvesting, and network security modeling in mobile wireless networks, in particular, those with challenging network constraints and high security demands, such as mobile ad hoc networks and underwater sensor networks. He has contributed to the design, implementation, and testing of network protocols within the NSF iMASH, ONR MINUTEMAN/STTR, NSF WHYNET and all QualNet/EXata commercial software development projects. He is now collaborating with Beijing Institute of Technology and Southeast University on wireless networking research.

Ping Li received the B.S. and M.S. degree in Mechantro nical Engineering from Dalian Jiaotong University, Dali an, China, in 1985 and 1987, respectively, and the Ph.D. degrees from the Beijing Institute of Technology, China , in 1995. In Sept. 1996, she joined School of Mechatron ical Engineering, Beijing Institute of Technology, China .Her research interests include information countermeas ure in wireless systems, information security, terminal information resistance and information security in wireless communication.