

A Secret Handshake Scheme for Mobile-hierarchy Architecture based Underground Emergency Response System

Guofang Dong ^{*,**,***,****}, Bin Yang ^{*,**,***}, Yang Ping ^{****}, Wenbo Shi ^{*****}

^{*}.National Engineering Laboratory for Vacuum Metallurgy, Kunming University of Science and Technology, Kunming 650093,China;

^{**}.Key Laboratory for Nonferrous Vacuum Metallurgy of Yunnan Province, Kunming University of Science and Technology, Kunming 650093,China;

^{***}.School of Metallurgy and Energy Engineering, Kunming University of Science and Technology, Kunming 650093,China;

^{****}. School of Electrical and Information Technology, Yunnan nationalities university, Kunming 650031, china

^{*****}. PLA Academy of national defense information, The PLA Information Engineering University, Zhengzhou 450001, China

^{*****} School of Computer and Communication Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China

dongguofang1@163.com

Abstract—Wireless Sensor Networks (WSNs) is one of the most important solutions for emergency applications, such as fire, flood and volcano monitoring, especially underground disasters. In this paper, we propose a mobile-hierarchy WSN architecture for underground emergency response system and a secure handshake scheme for the mobile-hierarchy architecture. In the discussions, the proposed secret attribute handshake scheme verifies the legitimacy of a node over an insecure wireless communication channel and accomplish the secret attributes negotiation. Mobile-hierarchy WSN architecture is evaluated in underground emergency response system by experiments. It shows good efficiency by extensive simulations in special emergency scenario. Moreover, it enables a new efficient solution to underground emergency response system.

Keywords— Underground emergency response system, secret handshake, mobile-hierarchy WSN.

I. INTRODUCTION

Emergency response system is one of the key applications in wireless sensor network which have displaced the well-established and widely-deployed wired communication networks. WSN has the potential to organize the capture, processing, and communication of critical data for emergency response.

In recent years, several emergency response system using WSNs are proposed. In 2007, SENDROM (Sensor Network for Disaster Relief Operations Management) was proposed for earthquakes in Turkey. The architecture of SENDROM consists of sensor nodes named Cnodes, Snodes, Standalone nodes, Embedded nodes. Embedded nodes is capable of detecting vibration during an earthquake. Cnodes invoke the Snodes and Inodes and then send the received data to the Central SENDROM Database [1]. The INSYEME (Integrated System for Emergency) system defines an integrated system

to support emergency operations. In order to support forecasting methods to monitor and predict the disaster evolution, the system is composed of a variety of fixed and mobile processing nodes which collect data from the environment [2]. The WINSOC (WSN with Self-Organization Capabilities for critical and emergency applications) detects rainfalls for estimating the chance occurrence of landslides. The architecture WINSOC is categorized into two layers. The lower layer consists of WSNs that sample and collect data from the Deep Earth Probe and transmit data to the upper layer which aggregates the data and forwards them to the sink [3]. The USN4D (Ubiquitous WSN For Development) system provides early warning for air pollution and disseminates surveillance information for the citizens and tourists. It is composed of four components: Data collectors, Python code, Database, End User Interface [4]. The MITag (Medical Information TAG) system tries to automatically track patients throughout each step of the disaster response process from disaster scenes. It supports a variety of wireless sensors such as GPS, pulse oximetry, blood pressure, temperature, heartbeats [5]. In those systems, the role of a sensor node is to sense the environment, communicate, exchange and process data with other nodes in certain area, make decisions.

Secret handshake is a useful cryptographic mechanism which allows two entities of the same group to validate each other secretly [6]. Thus, secret handshake concept can certainly be adopted into mobile-hierarchy architecture based underground emergency response system to achieving a secure secret attribute matching.

In this paper, we present a mobile-hierarchy WSN architecture for underground emergency response system and a secure attribute matching handshake scheme based on Attribute-based encryption and Predicate Encryption which

can be used to extend fuzzy authentication and data fusion by intersecting set elements and matching attributes privately.

II. MOBILE-HIERARCHY BASED UNDERGROUND EMERGENCY RESPONSE SYSTEM

Mine galleries run twenty kilometers deep underground of Huize Pb-Zn mine. The experimental mobile-hierarchy architecture based underground emergency response system is installed in the part of representative galleries. The diagram of the whole structure of the system can be drawn as figure 1. The system consists of a surveillance PC, a sink node, fifteen reference nodes and one or more mobile nodes. The reference nodes are arranged as Figure 1.

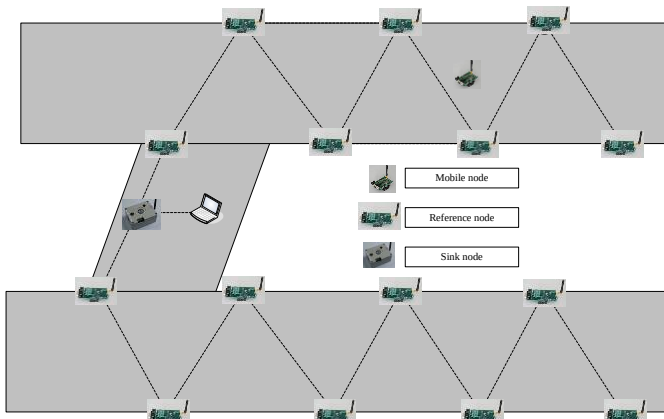


Figure 1. Mobile-hierarchy based underground emergency response system

The operative scenario we refer to is constituted by an information retrieval area, where nodes sensing a phenomenon of emergency are deployed, with one or more mobile guard users with mobile node moving around it and querying for data. In order to respond in the first time, a mobile node gets permanently connected to the network, it sends a query asking for information on certain geographical region, and then waits for the corresponding data.

A mobile node querying a WSN while moving. The node close to the surveillance PC called sink node, is in charge for communicating with mobile nodes and reference nodes. The nodes in the inner WSN, called reference nodes, communicate in a multihop fashion to reach sink node and a direct fashion to mobile node. Reference nodes are in charge of a certain zone. We assume a large number of sensor nodes to be deployed around a gallery in Huize Pb-Zn mine for detecting an emergency around the gallery. Furthermore, we assume each sensor node to be aware of its geographical position, for instance by storing in each node its coordinates during deployment. Alternatively, a distributed localization scheme can be used, where network nodes cooperate in order to reconstruct their spatial distribution. Reference nodes are the second control nodes for management, they in charge of managing the communications from and to mobile nodes. We assume each sink node to be aware of its position and of the position of the closest sink node and to have a unique

progressive identifier. Mobile nodes are moving nodes around the deployment area where the reference nodes are deployed.

Reference nodes are disseminated along the WSN network perimeter, but no particular constraint is applied to their density. In particular, it is assumed that the mobile node is always reachable, thus resulting in several disconnections experienced from the mobile node, and it is assumed that the reference nodes form a subnetwork, as they are necessarily connected to each other. Mobile nodes are assumed to move according to a constrained random waypoint mobility model, where their position is constrained to stay along the peripheral area inside which the WSN is deployed. The communication architecture needs to be designed in such a way that a mobile node is allowed to send a query and to receive related responses, managing in a transparent way possible disconnections. It implies defining proper interfaces among mobile node, reference node and sink node.

The routing protocols in the proposed WSNs architecture is influenced by many challenging factors. Al-Karari et al. summarize some of the routing challenges and design issues that affect routing process in WSNs as follow: Node deployment, Energy consumption without losing accuracy, Data Reporting Model, Node/Link Heterogeneity, Fault Tolerance, Scalability, Network Dynamics, Transmission Media, Connectivity etc [7].

Heinzelman et. al. [8] introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH is a cluster-based protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as clusterheads and change this role to other clusterhead evenly for distributing the energy load among the sensors in WSN. In LEACH, the clusterhead nodes compress data collecting from nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. Therefore, this protocol is most appropriate when there is a need for constant monitoring by WSN.

Because the system needs all the data immediately. Then, periodic data transmissions are necessary which may drain the limited energy of the sensor nodes. After a given interval of time, a randomized rotation of the role of the clusterhead is conducted so that uniform energy dissipation in the sensor network is obtained.

III. SECRET HANDSHAKE SCHEME

In this section, the proposed secret handshake scheme is described. Firstly, it is assumed that there is a trust third party. 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 $h_p \in G_p$ and $h_q \in G_q$ then

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

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

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

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

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 $x_i = (p_1, \dots, p_n)$ with $p_i \in \mathbb{Z}_n$, and chooses random $s, a, b \in \mathbb{Z}_n$ and $R_{3,i}, R_{4,i} \in G_r$ for $i=1$ to n . it outputs the ciphertext C_{xi} and give C_{xi} to node x_i .

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

The trust third party generate attributes vector for node $v_i = (A_1, \dots, A_n)$, and recall SK $(p, q, r, g_q, \{h_{1,i}, h_{2,i}\}_{i=1}^n)$, and chooses random $r_{1,i}, r_{2,i} \in \mathbb{Z}_p$ for $i=1$ to n , random $R_5 \in G_r$, random $f_1, f_2 \in \mathbb{Z}_q$, and random $Q_6 \in \mathbb{Z}_q$. It then outputs the SK_{v_i} and give SK_{v_i} to node v_i .

$$SK_{v_i} = (K = R_5 \cdot Q_6 \cdot \prod_{i=1}^n h_{1,i}^{-r_{1,i}} \cdot h_{2,i}^{-r_{2,i}}, \{K_{1,i} = g_p^{r_{1,i}} \cdot g_q^{f_1 \cdot A_i}, K_{2,i} = g_p^{r_{2,i}} \cdot g_q^{f_2 \cdot A_i}\}_{i=1}^n) \quad (4)$$

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

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

$$F = e(C_0, K) \cdot \prod_{i=1}^n e(C_{1,i}, K_{1,i}) \cdot e(C_{2,i}, K_{2,i}) \quad (5)$$

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

$$\begin{aligned} & e(C_0, K) \cdot \prod_{i=1}^n e(C_{1,i}, K_{1,i}) \cdot e(C_{2,i}, K_{2,i}) \\ &= e(g_p^s, R_5 Q_6 \prod_{i=1}^n h_{1,i}^{-r_{1,i}} h_{2,i}^{-r_{2,i}}) \cdot \prod_{i=1}^n e(H_{1,i}^s Q^{a \cdot p_i} R_{3,i}, g_p^{r_{1,i}} g_q^{f_1 \cdot A_i}) e(H_{2,i}^s Q^{b \cdot p_i} R_{4,i}, g_p^{r_{2,i}} g_q^{f_2 \cdot A_i}) \\ &= e(g_p^s, R_5 Q_6) \cdot e(g_p^s, \prod_{i=1}^n h_{1,i}^{-r_{1,i}} h_{2,i}^{-r_{2,i}}) \cdot \prod_{i=1}^n e(h_{1,i}^s R_{1,i}^s g_q^{a \cdot p_i} R_0^{a \cdot p_i} R_{3,i}, g_p^{r_{1,i}} g_q^{f_1 \cdot A_i}) \\ & \quad \cdot \prod_{i=1}^n e(h_{2,i}^s R_{2,i}^s g_q^{b \cdot p_i} R_0^{b \cdot p_i} R_{4,i}, g_p^{r_{2,i}} g_q^{f_2 \cdot A_i}) \\ &= e(g_p^s, \prod_{i=1}^n h_{1,i}^{-r_{1,i}} h_{2,i}^{-r_{2,i}}) \cdot \prod_{i=1}^n e(h_{1,i}^s g_q^{a \cdot p_i}, g_p^{r_{1,i}} g_q^{f_1 \cdot A_i}) \cdot \prod_{i=1}^n e(R_{1,i}^s R_0^{a \cdot p_i} R_{3,i}, g_p^{r_{1,i}} g_q^{f_1 \cdot A_i}) \\ & \quad \cdot \prod_{i=1}^n e(h_{2,i}^s g_q^{b \cdot p_i}, g_p^{r_{2,i}} g_q^{f_2 \cdot A_i}) \cdot \prod_{i=1}^n e(R_{2,i}^s R_0^{b \cdot p_i} R_{4,i}, g_p^{r_{2,i}} g_q^{f_2 \cdot A_i}) \end{aligned}$$

$$\begin{aligned} &= e(g_p^s, \prod_{i=1}^n h_{1,i}^{-r_{1,i}} h_{2,i}^{-r_{2,i}}) \cdot \prod_{i=1}^n e(h_{1,i}^s g_q^{a \cdot p_i}, g_p^{r_{1,i}} g_q^{f_1 \cdot A_i}) \cdot \prod_{i=1}^n e(h_{2,i}^s g_q^{b \cdot p_i}, g_p^{r_{2,i}} g_q^{f_2 \cdot A_i}) \\ &= e(g_p^s, \prod_{i=1}^n h_{1,i}^{-r_{1,i}}) \cdot e(g_p^s, \prod_{i=1}^n h_{2,i}^{-r_{2,i}}) \cdot \prod_{i=1}^n e(h_{1,i}^s, g_p^{r_{1,i}}) e(h_{2,i}^s, g_p^{r_{2,i}}) \\ & \quad e(g_q^{a \cdot p_i}, g_p^{r_{1,i}}) \cdot e(g_q^{a \cdot p_i}, g_q^{f_1 \cdot A_i}) \\ & \quad \cdot \prod_{i=1}^n e(h_{2,i}^s, g_p^{r_{2,i}}) \cdot e(h_{2,i}^s, g_q^{f_2 \cdot A_i}) \cdot e(g_q^{b \cdot p_i}, g_p^{r_{2,i}}) \cdot e(g_q^{b \cdot p_i}, g_q^{f_2 \cdot A_i}) \\ &= \prod_{i=1}^n e(g_q^{a \cdot p_i}, g_q^{f_1 \cdot A_i}) \cdot \prod_{i=1}^n e(g_q^{b \cdot p_i}, g_q^{f_2 \cdot A_i}) \\ &= \prod_{i=1}^n e(g_q, g_q)^{(af_1 + bf_2)p_i \cdot A_i} = 1 \end{aligned}$$

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

IV. DISCUSSIONS AND EXPERIMENTS

In this section, related discussions and experiments are given. Traditional user authentication methods mainly utilize the possession of a token or the knowledge of a secret in order to establish the identity of an individual. As a form of cryptography, secret handshakes are shared only with select and elect nodes. It enables two nodes who belong to the same group to authenticate each other in a way that hides their affiliation to that group from all others. Also it can be used to extend fuzzy mutual authentication and data fusion by intersecting set elements and matching attributes privately.

Wen et al. proposed a new revocable secret handshake scheme with backward unlinkability in 2011. Their scheme achieves the impersonator resistance against group authority (GA), such that group members are protected from being impersonated and framed by a malicious group authority. Furthermore, the revocation, unlinkability and traceability are obtained in the scheme. Assume the intractability of $q+1$ Square Roots Problem and Decisional Bilinear Diffie-Hellman Problem, the scheme is provably secure in the random oracle model [9]. Lu et al. propose a secure same-symptom-based handshake (SSH) scheme for the mHealthcare social network (MHSN). In their SSH scheme, each patient is granted with a pseudo-ID and its private key corresponding to his symptom. When two patients meet, only if they have the same symptom, they can use their private keys to achieve mutual authentication. They proved the proposed SSH is secure in the MHSN scenarios with the provable security technique [10]. Ethala et al. proposed a secret handshake system named Secret Handshake Issue and Validate Authority (SHIVA) with two authorities, Issue Authority and Validate Authority. Ethala et al. shows that their methodology occupy lesser memory space and reduce number of communication of sensor nodes for the authentication model by experiments [11]. Kawai et al. introduce a Secret handshake scheme with request-based-revealing (SHRBR). In SHRBR, the group authority can check whether handshake players belong to the own group without revealing a member ID. After a handshake player A executes a handshake protocol with B, if A wants to reveal a handshake partner, A requests group authority to reveal a handshake partner's ID B by bringing forth his own ID and secret information. [12]. The comparisons among Wu et al.'

scheme [9], Lu et al.'s scheme [10], Ethala et al.'s scheme [11], Kawai et al.'s scheme [12] and the proposed scheme is summarized in Table 1.

TABLE 1. Comparison discussions

	[9]	[10]	[11]	[12]	proposed
Fuzzy authentication	×	×	×	×	✓
Mutual authentication	✓	✓	✓	✓	✓
The number of third party	1	1	2	2	1

The evaluation scenario is designed for evaluating the implementation of the system and then discuss the results of the evaluation that we have carried out for assessing the effectiveness and efficiency of the system.

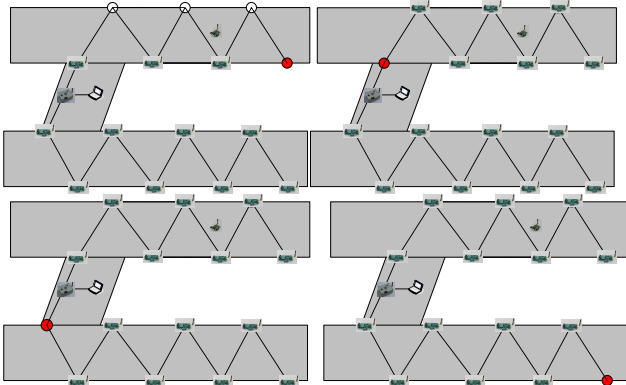


Figure 2. Four test emergency points for experiments

The experiment chooses four test emergency points for emergency response evaluation as shown in figure 2. The red points denote emergency spot, these points are marked as point 1, point 2, point 3, point 4.

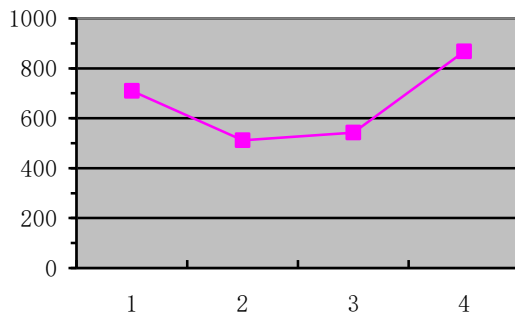


Figure 3. Average response time at four test points

Firstly, the experiment record the time of emergency response 20 times at each point. As shown in figure 3, the average response time of point 1, point 2, point 3, point 4 are 709ms, 511ms, 543ms, 867ms separately. Apparently, the system provide an efficient response time in this experiment.

V. CONCLUSIONS

In this paper, a new architecture is proposed where mobile nodes try to query a largely deployed underground emergency

sensors. The proposed mobile-hierarchy architecture shows good efficiency by extensive simulations in a special emergency scenario. Furthermore, a secure attribute matching handshake scheme is proposed. It employs attributes to describe policy and achieve the fuzzy authentication and data fusion and adopts attribute encryption to implement an attribute matching procedure, provides a balance between confidentiality and availability. The proposed mobile hierarchy based system enables a new efficient solution to underground emergency response system.

ACKNOWLEDGMENT

This study was supported by the Application Foundation Research Project of Yunnan Science and Technology Department (No. 2011FZ168), the National Science foundation of China (no. 61461056), the National Natural Science Foundation of China (Nos.61202447, 61472074), the Natural Science Foundation of Hebei Province of China (No. F2013501066), the Northeastern University at Qinhuangdao Science and Technology Support Program (No. xnk201307), the Fundamental Research Funds for the Central Universities (No.N130423008)

REFERENCES

- [1] E. Cayirci and T. Coplu. "SENDROM: Sensor Networks for Disaster Relief Operations Management". Wireless Networks, Vol. 13 Issue 3, June 2007. pp. 409-423.
- [2] R. Fantacci, D. Marabissi and D. Tarchi; "A novel communication infrastructure for emergency management: the In.Sy.Eme. vision". Wirel. Commun. Mob. Comput. 2010. pp.1673-1681.
- [3] M. V. Ramesh. "Real-time Wireless Sensor Network for Landslide Detection". In Proc. of the Third International Conference on Sensor Technologies and Applications (SENSORCOMM). 2009. pp. 405-409.
- [4] A. Bagula, M. Zennaro, G. Inggs, S. Scott and D. Gascon. "Ubiquitous Sensor Networking for Development (USN4D): An Application to Pollution Monitoring". Sensors 2012. Vol. 12. pp.391- 414.
- [5] T. Gao, C. Pesto, L. Selavo, Y. Chen, J. Ko, J. Lim, A. Terzis, A. Watt, J. Jeng, B. Chen, K. Lorincz, and M. Welsh. "Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results". In Proc. of the IEEE Conference on Technologies for Homeland Security, 2008. pp.187 – 192
- [6] Yamin Wen, Zheng Gong. "A Dynamic Matching Secret Handshake Scheme without Random Oracles". Network and System Security, Lecture Notes in Computer Science, Vol 8792, 2014, pp 409-420
- [7] J.N. Al-Karari, A.E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communications, December 2004.
- [8] W.B Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," In the Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), 2000.
- [9] Yamin Wen, Fangguo Zhang, "A New Revocable Secret Handshake Scheme with Backward Unlinkability", 7th European Workshop, EuroPKI 2010, LNCS, Vol 6711, 2011, pp 17-30.
- [10] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, Xuemin Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network", Mobile Networks and Applications, 2011, Volume 16, Issue 6, pp 683-694
- [11] Kamalanaban Ethala, R. Seshadri, N. G. Renganathan and M. S. Saravanan, "SECRET HANDSHAKE ISSUE AND VALIDATE AUTHORITY BASED AUTHENTICATION SYSTEM FOR WIRELESS SENSOR NETWORK", Journal of Computer Science, Volume 9, Issue 9, 2013, Pages 1174-1180

- [12] Yutaka Kawai, Noboru Kunihiro, "Secret handshake scheme with request-based-revealing", Computers & Mathematics with Applications, Volume 65, Issue 5, March 2013, Pages 786-798



Guofang Dong, She was born in China in 1979. He received his B.E. and M.E. from Chongqing University of Posts and Telecommunications, China, in 2001 and 2007, respectively. She has been working towards her Ph.D. in Kunming University of Science and Technology. Her current research interests include wireless sensor networks, information security.



Bin Yang, He was born in China in 1965. He received his B.E. from Northeastern University, China, in 1987. He received his M.E. from Kunming University of Science and Technology, China, in 1990. He received his Ph.D. from Kunming University of Science and Technology, China, in 1998. Now he is the professor of Kunming University of Science and Technology.



Ping Yang (December, 1982~), was born in Hubei, Wuhan, and received her Master degree from BIT in Beijing. Now she is a lecturer in the Operations at Academy of National Defence Information.



Wenbo Shi received the M.S. degree from the Inha University, Incheon, South Korea, in 2007 and the Ph.D. degree from the Inha University, Incheon, South Korea, in 2010. Later, he joined School of computer and communication engineering, Northeastern University at Qinhuangdao, China. His main research interests include cryptography, network security and so on.