# A novel key establishment algorithm for distributed wireless sensor network

**Feng-juan Ma[1*], Da-wei Song[2]**

[1] *Weifang Engineering Vocational College, Shandong Qingzhou 262500, China*

[2] *Weifang Engineering Vocational College, Shandong Qingzhou 262500, China*

**Corresponding author's e-mail: sdw979@163.com*

*Received 15 January 2013, www.cmnt.lv*

**Abstract**

In the security mechanism of distributed wireless sensor network, key management plays a fundamental role. Because the distributed wireless sensor network has a large scale, its node resource is very limited and distributed, key management mechanism of traditional wireless network is not suitable for it. Therefore, a security mechanism based on the combination of elliptic curve cryptosystem and public key is proposed, which realizes safe key establishment and certification. The security of the protocol is analyzed. Energy consumption of the proposed key establishment scheme is simulated and the results show that this protocol is feasible to be applied to wireless sensor networks.

*Keywords:* key establishment; distributed wireless sensor network; energy consumption.

## 1 Introduction

With the continuous development of wireless sensor network (WSN), the scope of its application is more and more wide. Due to wireless sensor network deployed in the lack of physical protection environment usually, so when transmitting sensitive data in particular, it is essential to consider its security. However, Wireless sensor network resource and computing power is limited, and infrastructure can not be established to provide a trusted third party service, making the wireless sensor network (WSN) face a bigger challenge in safety than traditional networks.

In order to realize the communication security of wireless sensor network, currently there are a variety of solutions. Scheme based on symmetric cryptography makes the session key negotiation too complex and requires large storage space. Scheme based on the traditional public key cryptography system needs online trusted third party certification, it is also suitable to wireless sensor network (WSN). Although the secure multi-party computation has no trusted third party, its computation complexity and communication complexity is higher and is not practical. So how to realize the safe and efficient key management becomes an important research topic.

A new key management scheme in heterogeneous wireless sensor networks was proposed by Banihashemian [1]. Location dependent key management in sensor networks without using deployment knowledge was proposed by F. Anjum [2]. An effective key management scheme for heterogeneous sensor networks was proposed by X. Du [3]. Alternative shared key replacement in heterogeneous wireless sensor networks was proposed by S. Banihashemian [4]. A key management scheme for wireless sensor networks using deployment knowledge was proposed by W. Du [5]. A survey on clustering algorithms for heterogeneous wireless sensor networks was proposed by K. Vivek [6]. A distributed group rekeying scheme for wireless sensor networks was proposed by H. N. Seyed [7]. Dynamic key management scheme for wireless sensor network was proposed by F. R. Kong [8]. Energy-efficient distributed deterministic key management for wireless sensor networks was proposed by Xing Zhang [9]. Unconditionally-secure key pre-distribution for triangular grid based wireless sensor network was proposed by S. Mitra [10]. Key pre-distribution schemes for establishing pairwise keys with a mobile sink in sensor networks were proposed by A. Rasheed [11]. Location-aware combinatorial key management scheme for clustered sensor networks was proposed by M. F. Younis [12]. An efficient key distribution scheme for heterogeneous sensor networks was proposed by S. Hussain [13]. A probabilistic analysis for multi-neighbor random key pre-distribution was proposed by W. S. Li [14]. Exact formulae for resilience in random key pre-distribution schemes was proposed by D. H. Yum [15]. A key-management scheme for distributed sensor networks was proposed by L. Eschenauer [16]. In this article, regardless of the attack from the physical layer and data link layer, it is assumed that the network is connected to each other.

In the next section, a key establishment scheme is proposed, including principle of elliptic curve cryptosystem, key factor matrix and the mapping algorithm, key distribution and calculation, the identity authentication, key storage, join and leaving of member nodes. In Section 3, safety analysis of proposed scheme is given. In section 4, simulation and analysis of proposed key establishment is given. Section 5 gives some conclusions finally.

## 2 The proposed key establishment scheme

Firstly, operation of elliptic curve E is defined. $F_p$ represents finite domain and $p \neq 2,3$. $a,b \in F_p$ and it meets the equation $4a^3+27b^2 \neq 0$. $E_{(a,b)}(GF(p))$ represents set made up of point $(x,y)$ meeting equation $y^3 = x^3 + ax + b$

and infinity point $O$. These points constitutes an Abel swarm under add operation. Identity element of swarm element is $O$. $P$ and $Q$ are two points of elliptic curve. If $P=O$, $-P=O$ and $P+Q=Q+P=Q$. $P=(x_1,y_1)$, $-P=(x_1,-y_1)$ and $P+(-P)=O$. If $Q\neq -P$, $P+Q=(x_3,y_3)$. $x_3=u^2-x_1-x_2$, $y_3=u(x_1-x_3)-y_1$, $u=\begin{cases}(y_2-y_1)/(x_2-x_1), & P\neq Q\\ (3x_1^2+a)/(2y_1), & P=Q\end{cases}$. For a random point $G$, the set $(O,G,G+G,G+G+G,\cdots)$ is a cyclic group. $kG$ represents scalar multiplication.

Key distribution and management of large-scale network is solved with appearance of public key technology. PKI adopts public key technology to provide security infrastructure. Usually, PKI ties users and public key together and ensures the integrity of the public key by CA. CA is applicable to large open network environment in wired networks. In the wireless sensor network, sensor nodes can not stand overhead that PKI spending to establish trust chain, so that PKI cannot be applied in the wireless sensor network. This scheme uses idea of the combination of public key and it is different from ordinary public key system. It does not need to open the public key in the key management and it only open public key factor matrix. The user can calculate public key of each node through the given mapping algorithm and a unique identifier.

$T=(a,b,G,n,p)$, where $a$ and $b$ are parameters of ECC, $G$ represents basic point and $n$ represents order of ECC, $p$ represents order of domain $F_p$. For a random integer $k\in F_p$, $k\cdot G$ is set as public key of ECC.

In order to guarantee the security, the key factor matrix is generated by KMC offline and KMC establishes public/private key factor matrix through public/private key pair. The columns of the matrix represent the level of combination and rows represent key variables of each layer. The matrix is $m\cdot n$ matrix. There are $n$ layers and each layer contains $m$ number of key variables. The public/private key factor matrix is as follows.

$$SFM=\begin{bmatrix}k_{11} & k_{12} & \cdots & k_{1n}\\ k_{21} & k_{22} & \cdots & k_{2n}\\ & \cdots & & \\ k_{m1} & k_{m2} & \cdots & k_{mn}\end{bmatrix}$$ represents private key factor matrix.

$$PFM=\begin{bmatrix}k_{11}\cdot G & k_{12}\cdot G & \cdots & k_{1n}\cdot G\\ k_{21}\cdot G & k_{22}\cdot G & \cdots & k_{2n}\cdot G\\ & \cdots & & \\ k_{m1}\cdot G & k_{m2}\cdot G & \cdots & k_{mn}\cdot G\end{bmatrix}$$ is representing public key factor matrix.

The protocols generate public/private key pair through public/private key factor matrix. This method only needs a few resources as seed to generate a large number of public/private key pairs. By mapping algorithm, the user's identity can be mapped to $n$ number of mapping value and KMC calculate public/private key through combination principle. Supposing $n$ number of mapping value of user $A$ is $(i_1,i_2,\ldots,i_n)$. The element of the t-th column and the $i_t-th$ row can be obtained by public key factor matrix. Then private key of user $A$ is calculated.

If user B wants to acquire public key of user A, $n$ number of mapping values are calculated according to the identification of user A and mapping algorithm. User B can calculate the public key of user A, $PK_A=(k_{i_1}\cdot G,k_{i_2}\cdot G,\ldots,k_{i_n}\cdot G)$. User A acquires private key $SK_A$, The verifier can easily calculate the public key. Both sides of communication use public/private key to realize exchange of digital signature and session key. Key exchange and identity authentication are described as follows.

$message1\ \ B\to A: ID_B,[IP_B,[k_b,T_b]K_A]K_B^{-1}$

$message2\ \ A\to B: ID_A,[ID_A,,IP_A,[K_{a+b},k_a,T_a]K_B]K_A^{-1}$

$message3\ \ B\to A: ID_B,[IP_B,[K_{a+b},T_b]K_A]K_B^{-1}$

Key management is offline and can guarantee its absolute security. Each node is easy to get the public key factor matrix and easily carry out identity authentication by unique identifier of other members. It can be assumed that any node trust key management centre $S$. It means that certification between node $A$ and server $S$, certification between node $B$ and server $S$ can be omitted. Communication process is as follows.

Firstly, $B$ generates a random key $k_b$. $k_b$ and time stamp are encrypted using public key of $A$. Then carry out signature using its own private key and send it to $A$.

After $A$ receives information, calculate public key of $B$ by mapping algorithm and $ID$ number of $B$. After decryption, $k_b$ is acquired. Generate random key $k_a$ and time stamp $T_a$, which are transmitted to $B$ after encryption and signature. At last, after $B$ receives information from $A$, it sends confirmation information to $A$, session key $K_{ab}=k_a+k_b$. Transmitted information to node $A$ from node $B$ includes $ID_B$, $IP_B$, $k_a$ and $T_b$. $ID_B$ is $ID$ number of node $B$, $IP_B$ is routing information, $k_a$ is key randomly generated by $B$, $T_b$ and $T_b^{'}$ are time stamps generated by $B$, $K_B$ and $K_B^{-1}$ is public/private pair of node $B$. $k_a$ is random key generated by $A$. $K_{ab}=k_a+k_b$ is session key of $A$ and $B$. $A$ sends $K_{ab}=k_a+k_b$ to $B$, which means that $A$ receives $k_b$, then $B$ sends confirmation information. The both sides use session key $K_{ab}=k_a+k_b$ for communication.

The private key factor matrix is stored in KMC, such that KMC needs absolute security and public key factor matrix is open. Because every member has a unique identifier, simply using a unique identifier, public key factor matrix and the mapping algorithm can calculate the public key of any members. The certification process does not depend on the trusted third party, so that the KMC can generate and save the private key factor matrix offline and in the process of certification it almost does not need the support of infrastructure. In the process of communication, it does not need to build complex certification chain. The traditional authentication system requires a lot of resources to ensure that the public key distribution and storage. Due to the use of seed matrix in this protocol, it only need very little space to store the key. If the key factor matrix is a $m\times n$ matrix, it needs to store the $m\times n$ number of keys. But it there is $m^n$ number of different keys by means of combination.

If a node wants to join to the wireless sensor network for key distribution, KMC distributes a unique identifier for the new node. The new node obtains the public/private key pair,

but the public key factor matrix does not need to change. Any node can calculate public key of the new node according to its unique identifier. If a node is declared to be invalid, KMC needs to broadcast a message: $S \to broadcast : [revoke, cert_r]K_s^{-1}$.

## 3 Safety analysis

Authentication protocol is the foundation of secure communication. Authentication between entities distributes keys or other secrets safely between entities. Sending of confirmation information and authentication of receiving messages is carried out through the security protocol. Because the design of the protocol lacks of mature theory, so the designed authentication protocols often can not achieve expected design requirements, which requires a set of analysis mechanism for security analysis of a designed authentication protocol. We should determine whether it reaches a predetermined target, and whether there is redundant. Also we should detect the existence of security vulnerabilities. In recent years, the formal analysis of security protocols has gradually become a hot research topic in the field of information security. With the aid of formal analysis tools, we can illustrate the correctness of the protocol. At present, there are four major types of formal methods. Modal logic method based on knowledge and belief reasoning, algebraic method based on the knowledge reasoning, research methods based on the communication state machine model and method based on the sequential communication process.

BAN logic is still the most commonly used method of formal analysis of security protocol so far. First of all symbols are defined. BAN logic is a logic method based on knowledge and belief, which mainly includes three processing object: subject, encryption keys and formula (also known as state, statement or proposition). The main body represents nodes of sending and receiving messages.

In this article, the symbol of A, B and S represents special main body, and S represents especial servers. $K_{ab}$ represents shared key of A and B. $K_A$, $K_B$ and $K_S$ represents private keys of A, B and S respectively. $K_A^{-1}$, $K_B^{-1}$ and $K_S^{-1}$ are private keys. $X$ represents formula and $T$ represents time stamp. Its logical symbols are defined as follows.

$P \mid\equiv X$ represents $P$ believes $X$.
$P \mid\sim X$ represents $P$ said $X$ once.
$P \lhd X$ represents $P$ see $X$.
$P \Rightarrow X$ represents $P$ has the authority of $X$.
$\#(X)$ represents $X$ is fresh.
$\overset{k}{\mapsto} P$ represents $k$ is public key of $P$.
$P \overset{X}{\rightleftharpoons} Q$ represents $X$ is secret of $P$ and $Q$.
$P \overset{k}{\leftrightarrow} Q$ represents shared key of $P$ and $Q$ is $k$.
$\langle X \rangle$ represents $X$ uses secret $K$ for secrecy.
$\{X\}_K$ represents $X$ uses key $K$ for encryption.

In the logic rules, formula above horizontal lines represent premise condition and formula below the horizontal represent conclusion.

$$\frac{P \mid\equiv Q \overset{k}{\leftrightarrow} P, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$$ is rule 1. If $P$ trusts that $k$ is shared key of $P$ and $Q$. And $P$ has seen encrypted information $X$ using $P$, then $P$ trusts that $Q$ has said $X$.

$$\frac{P \mid\equiv \mid\overset{k}{\to} Q, P \lhd \{X\}_K^{-1}}{P \mid\equiv Q \mid\sim X}$$, $K$ represents public key of $Q$ and $K^{-1}$ represents private key. If $P$ trusts that $K$ is public key of main body $Q$ and $P$ has seen encrypted information $X$ using $K^{-1}$, $P$ trusts that $Q$ has said $X$.

$$\frac{P \mid\equiv P \overset{X}{\rightleftharpoons} Q, P \lhd \{Y\}_X}{P \mid\equiv Q \mid\sim Y}$$ represents $P$ trusts that $X$ is shared secret of $P$ and $Q$, $P$ has seen encrypted $Y$ using $X$. $P$ trusts that $Q$ has said $Y$.

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$. If $P$ trusts that $X$ is fresh and $P$ trusts $Q$ has said $X$, $P$ trusts that $Q$ trusts $X$.

$$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$. If P believes that Q has the authority of X and believes that Q believe X, P believe X.

$$\frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X}$$. If $P$ trusts that $Q$ has sent information $(X,Y)$, $P$ trusts that $Q$ has sent information $X$.

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$$. If $P$ believes that $X$ is fresh, $P$ believes that $(X,Y)$ is fresh.

$$\frac{P \mid\equiv (X,Y)}{P \mid\equiv X}$$, if $P$ believes $(X,Y)$, $P$ believes $X$.

$$\frac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X}$$, $P$ believes that $Q$ believes $(X,Y)$, $P$ believes that $Q$ believes $X$.

In this mechanism, key distribution is offline and key distribution process is safe. Because the public key can be calculated via a unique identifier, so the public key of each node can be thought to be trusted. Therefore, we can make the following initial assumptions.

$A \mid\equiv \mid\overset{K_S}{\to} S$, $A \lhd [K_B]K_S^{-1}$, $A \mid\equiv S \mid\Rightarrow K_J$, $A \mid\equiv \#(K_J)$, $J = A, B, S$.

$A \mid\equiv \#(T_b)$, $A \mid\equiv B \Rightarrow k_b$, $B \mid\equiv \mid\overset{K_S}{\to} S$, $B \lhd [K_A]K_S^{-1}$, $B \mid\equiv S \mid\Rightarrow K_J$, $B \mid\equiv \#(K_J)$
$B \mid\equiv \#(T_a)$, $B \mid\equiv A \Rightarrow k_a$

Reasoning process of message 1 is as follows

$$\frac{A \mid\equiv \mid\overset{K_S}{\to} S, A \lhd [K_B]K_S^{-1}}{A \mid\equiv S \mid\sim (K_B), A \mid\equiv \# K_B}$$

$$\frac{A \mid\equiv S \mid\equiv (K_B), A \mid\equiv S \Rightarrow (K_B)}{A \mid\equiv (\overset{K_B}{\to} B), A \lhd [[k_b, T_b]K_A]K_B^{-1}}$$

$$\frac{A \mid\equiv B \mid\sim [k_b, T_b]K_A, A \mid\equiv \#(T_b)}{A \mid\equiv B \mid\equiv [k_b, T_b]K_A, A \mid\equiv B \Rightarrow [k_b, T_b]K_A}$$

$$\frac{A|\equiv[k_b,T_b]K_A, A|\equiv|\overset{K_A}{\rightarrow}A}{\dfrac{A|\equiv[k_b,T_b]}{A|\equiv k_b}}$$

## 4 Safety analysis

Network simulation platform of this experiment is NS2.27. Simulation parameters setting are as follows. A total of 100 nodes are randomly distributed in geometry area of 500x500 square meters. The MAC layer uses IEEE802.11 protocol. Coverage range of each node is 50 meters and data transmission rate is 512bps. Once the nodes are deployed, it is no longer moved, until energy runs out. Each data point in the figure is average value of 50 times.

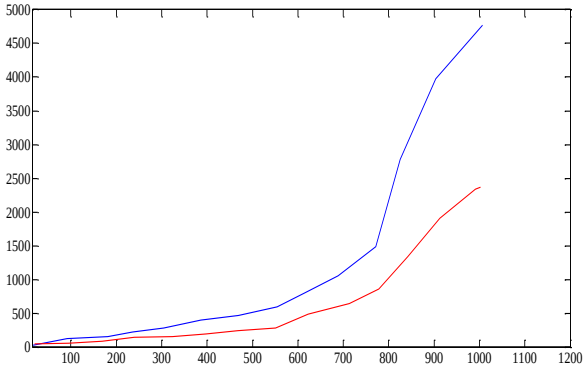



FIGURE 1 Relation between battery capacity and completed handshake times

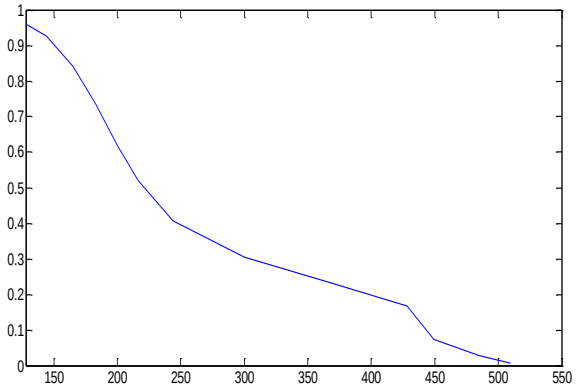



FIGURE 2 Comparison of energy cost of handshake process and its subsequent transmitted data

The elliptic curve cryptosystem is used, therefore in the process of the handshake, the total energy mainly includes: public key encryption, decryption, signature and verification, transmission and receiving of shaking hands information, the hash computing and random number generation. Calculation of public key is the main overhead and the second is the communication overhead. 5% and 10% of battery capacity is used for handshake process and the completed handshake time is shown in figure 1. The blue line represents 10% of battery capacity is consumed and the red line represents 5% of battery capacity is consumed. The horizon axis represents battery capacity, the unit of which is mAh. The vertical axis represents the number of completed handshake. The key management scheme based on identity is used to establish the session key and handshake process is safe and reliable. Once the session key is established, the session key can be used for communication always. In a secure key management protocol, handshaking processes of each node are not too many. Through the analysis, it shows that the new scheme can be used for energy limited wireless sensor network. Session key established by shaking process is safe and effective and the node in the whole life cycle can use the session key for encryption, decryption or communication with fixed nodes. Comparison of energy cost of handshake process and its subsequent transmission of the data is shown in figure 2. The horizon axis represents the number of transmitted bytes including bytes of each handshake and bytes after each handshake. The vertical axis represents proportion of energy consumed by handshake.

Once a session key is established, the both sides of communication can use the key throughout the life cycle, so that the proportion of energy consumed by handshake process declines with increment of amount of transmitted data. When the amount of data transmission is 128 bytes, energy consumption of handshake process accounting for the proportion of the total energy is very big. When the amount of data arrives to 128 KB, the proportion of energy consumed by handshake process is negligible.

## 5 Conclusions

Compared with traditional computer network, wireless sensor network is a special kind of network. Since it has many limitations, it is difficult to use the existing security schemes in wireless sensor network directly. Combined with the thought of public key, a public key scheme based on the identity is proposed for key management used in wireless sensor network. In the absence of online the trusted third party, it achieves the safe and efficient key distribution and the establishment of session key.

## References

[1] Banihashemian S, Bafghi A G 2010 A new key management scheme in heterogeneous wireless sensor networks *Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT '10)* 141-6

[2] Anjum F 2010 Location dependent key management in sensor networks without using deployment knowledge *Wireless Networks* **16**(6) 1587-600

[3] Du X, Xiao Y, Guizani M, Chen H H 2007 An effective key management scheme for heterogeneous sensor networks *Ad Hoc Networks* **5**(1) 24-34

[4] Banihashemian S, Bafghi A G 2010 Alternative shared key replacement in heterogeneous wireless sensor networks in *Proceedings of the 8th Annual Conference on Communication Networks and Services Research (CNSR '10)* 174-8

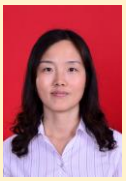
[5] Du W, Deng J, Han Y S, Chen S, Varshney P K 2004 A key management scheme for wireless sensor networks using deployment knowledge *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)* 586-97

[6] Vivek K, Narottam C, Surender S 2011 A survey on clustering algorithms for heterogeneous wireless sensor networks *International Journal of Advanced Networking and Applications* **2**(4) 745–54

[7] Seyed H N, Amir H J, Vanesa D 2011 A distributed group rekeying

scheme for wireless sensor networks *Proceedings of The 6th International Conference on Systems and Networks Communications (ICSNC '11)* 127-35
[8] Kong F R, Li C W 2010 Dynamic key management scheme for wireless sensor network *Journal of Software* **21**(7) 1679-91
[9] Xing Zhang, Jingsha He, Qian Wei 2011 Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks *Wireless Communications and Networking*
[10] S. Mitra, S. Mukhopadhyay, and R. Dutta 2014 Unconditionally-secure key pre-distribution for triangular grid based wireless sensor network," *Journal of Applied Mathematics and Computing* 44(1), pp. 229–249.
[11] A. Rasheed and R. Mahapatra 2011 Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks *IEEE Transactions on Parallel and Distributed Systems*, 23(1), pp. 176-184.
[12] M. F. Younis, K. Ghumman, and M. Eltoweissy 2006 Location-aware combinatorial key management scheme for clustered sensor networks *IEEE Transactions on Parallel and Distributed Systems* 17(8), pp. 865–882.
[13] S. Hussain, F. Kausar, and A. Masood 2007 An efficient key distribution scheme for heterogeneous sensor networks *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC '07)* 388–92
[14] Li W-S, Su T-S, Hsieh W-S 2009 Multi-neighbor random key pre-distribution: a probabilistic analysis *IEEE Communications Letter* **13**(5) 306-8
[15] Yum D H, Lee P J 2012 Exact formulae for resilience in random key pre-distribution schemes *IEEE Transactions on Wireless Communications* **11**(5) 1638-42
[16] Eschenauer L, Gligor V D 2002 A key-management scheme for distributed sensor networks *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)* 41-7

## Author



**Ma Feng-juan, 1975.12, Qinzhou County, Shandong Province, China**

**Current position, grades:** A lecture of Weifang Engineering Vocational College, China.
**University studies:** received his B.Sc. in department of computer science from Liaocheng normal college in China. She received his M. Eng. from Harbin university of science and technology in China.
**Scientific interest:** Her research interest fields include computer software technology, database technology
**Publications:** more than 6 papers published in various journals.
**Experience:** She has teaching experience of 13 years, has completed three scientific research projects.

**Song Da-wei, 1976.12, Qinzhou County, Shandong Province, China**

**Current position, grades:** the Associate Professor of Weifang Engineering Vocational College, China
**University studies:** received his B.Sc. in department of computer science from Shandong university of building materials in China. He received his M. Eng. from Harbin university of science and technology in China.
**Scientific interest:** His research interest fields include computer network technology, database technology
**Publications:** more than 12 papers published in various journals.
**Experience:** He has teaching experience of 15 years, has completed three scientific research projects.