Cluster Computing
https://doi.org/10.1007/s10586-017-1681-y

Research on the access control protocol Priccess design of network privacy protection

Xu Ma[1] · Kai Kang[1] · Wanshun Lu[1] · Li Xu[1] · Chen Chen[1]

Received: 18 October 2017 / Revised: 27 December 2017 / Accepted: 29 December 2017

Abstract
To provide a more reliable security for the network privacy, the access control protocol Priccess design of network privacy protection was studied. First of all, this paper presented the problems in wireless network security, and points out the key technologies, including privacy protection, user authentication, trust management, network security communication architecture and other technologies. Then, it made a brief analysis of the composition of the Priccess protocol, a wireless communication network in the roaming authentication scheme and wireless sensor network privacy data protection scheme. Furthermore, the roaming authentication scheme and wireless sensor networks data privacy protection in a wireless communication network was established. Finally, the results of the evaluation of the message load of Priccess protocol proved it was efficient for most of the user access devices, which could provide more efficient protection for the privacy of the network communication.

Keywords Priccess design · Privacy protection · Wireless network security · DAS · Sensor network

1 Introduction

Under the network environment, the right infringement becomes prominent. Safety critical wireless sensor network system often requires that wireless sensor networks owns strict credibility, mainly in the reliability, timeliness and security, and so on. It need to ensure that the data can be efficient, timely, reliable and secure from the source node to the Sink node. So it is better to design a high efficiency and reliable wireless sensor network protocol architecture to provide credibility guarantee. Over the past 10 years, researchers of domestic and foreign have carried out a lot of research on wireless sensor networks, and have made some important progress, but the problem is far from being solved. Existing research work mainly focuses on efficient data collection, real-time fault tolerance, vulnerability assessment, and privacy protection of nodes and data. Design methods include [1]: graph theory, probability analysis, game theory and other theoretical methods.

✉ Xu Ma
q9769987meitanji@163.com

[1] School of Mathematics and Computer Science, Ningxia Normal University, Guyuan 756000, Ningxia, China

2 Description of the problem

There are three problems in the research of current wireless network security [2]: firstly, for the traditional wireless network applications, although there are a lot of security solutions, but these methods have their own limitations, especially the wireless network itself and its own business for security and privacy has a diverse need. This paper takes roaming services as the example, summarizes the development and evolution of the roaming authentication technology, and points out their limitations and the future work direction. Secondly, the development of wireless networks is fast, new standards, technology and applications continue to emerge, because of different types and uses of wireless network security, privacy and the related technologies have different requirements, leading to the existing security solutions are not suitable for these emerging industries, so people need to identify their new security and privacy requirements, research and development of the corresponding protection scheme. This paper takes the intelligent power grid service offering as an example. Firstly, it describes the information security challenges, then it proposes the design principle and implementation method of the "security service"; then, the two major security issues associated with the "security service provision" are discussed and the possible solutions are proposed. Lastly, the suggestions for the future research

Published online: 12 February 2018

directions are put forward. Thirdly, with the progress of social civilization, people's awareness of security and privacy and the idea of continuous expansion, in particular, there is a higher privacy needs of a variety of emerging network value-added services. For military, medical and financial and other security sensitive industries, the ability to meet the stringent requirements of privacy protection has become the first choice to measure the availability of wireless networks.

3 State of the art

3.1 Key technologies of wireless network security

As the research hotspot and difficulty in information field, network security involves cross multiple disciplines, including key management, secure routing, intrusion detection and so on. Among them, privacy protection, security, user authentication, user authentication, trust management and network security communication architecture are the most critical security technology that affect the successful implementation of wireless networks, are the basis of many security services.

3.1.1 Privacy protection

Wireless network in the actual application process is faced with a serious risk of leakage of privacy information leakage or tampering. For example: in mobile communications, mobile communication information may be leaked; in the military field, wireless sensors are deployed in an important area for monitoring, the data collected often carry important information, if the data is leaked or tampered, it would cause serious threat or decision-making errors; wireless network privacy data breaches will seriously affect the development of wireless networks. Therefore, it is important to study and solve the problem of privacy protection.

3.1.2 User authentication

In order to allow a user that have a legal status to join the network and obtain its reservation service, and to prevent illegal users access to network data at the same time, to ensure the security of the wireless network, the network must use the user authentication mechanism to verify the legitimacy of the user identity. User authentication is one of the most important security operations, all other security services are dependent on it in a way.

3.1.3 Trust management

As an important complement to the security means based on cryptography, trust management has significant advantages in resisting internal attacks in wireless networks, identifying malicious nodes and selfish nodes, improving system security, fairness and reliability. Trust management provides a new and effective security solution for the self organization network which is the core of trust computing model or has no network infrastructure.

3.1.4 Network communication architecture security

Network communication architecture, including network access protocol and a variety of network communication protocols. The complexity of wireless network application determines the complexity of its structure. Building secure network communication architecture cannot without the safe network communication architecture [3–5].

3.2 Priccess protocol

Priccess protocol [6] includes six phases: system initialization, user queries, sensor nodes validate, establish secure channel between the user and the network sensor nodes, new users join and user revocation stage. During the system initialization phase, the network owner and all the users create their own private key. Then, the network owner divides all the users into different groups, and maintains a list of access list pool as well as preinstalls on the group access list pool in the corresponding sensor node. In generating user query phase, if the user generates a new query, the corresponding query commands and the ring signature are required, and then sent to the sensing node. In the sensor nodes verification phase, if the query information through the verification, the node will answer queries command. The new users are added to the stage in which the users wish to join the network. Similarly, the user revocation phase occurs when the user is revoked. This paper only focus on the access control in the sensing network without the security of nodes. In addition, in Priccess, Elliptic Curve Cryptography (ECC) has been used because that the technology has great advantages in terms of computational efficiency, key size and signature size compared with RSA technology.

4 Methodology

4.1 Roaming authentication scheme in wireless communication networks

Roaming authentication background: with the wireless communication systems (such as GSM, 3G, roadside vehicle communication systems, wireless metropolitan area network), and the deployment of wireless and mobile networks covering the world wide range of wireless and mobile networks have become a reality. People can use mobile devices

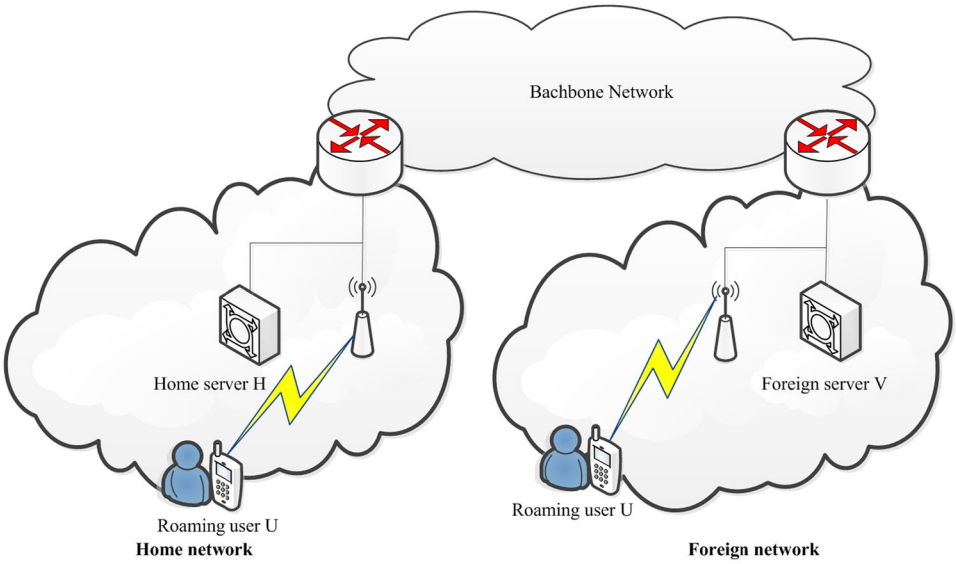


Fig. 1 Overview of roaming services

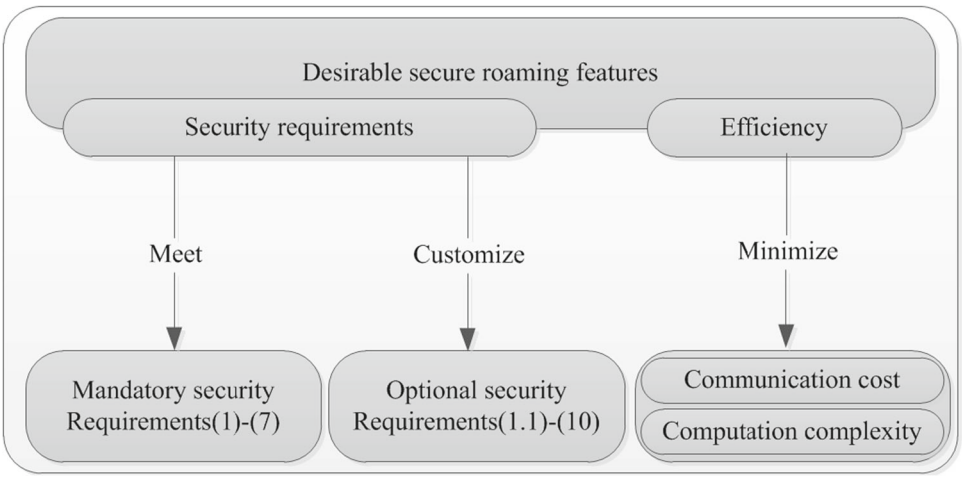


Fig. 2 Desirable features secure roaming

to access the network access services at "any time, anywhere", while not restricted by the coverage of their ordered network. This need to provide roaming services to protect the continuity of network connection when users travel from one network to another network. As shown in Fig. 1, without considering the type of the network, the usual roaming scenario [3] consists of three entities: the roaming user U, its access to the foreign server V, and the local server for the user U. Usually V and H signed a roaming agreement, so that the user U in the external network that the user V manage, it can access the service through V. Prior to this, it needs to be make the appropriate validation between U and V.

Roaming authentication requirements and challenges: the security and efficiency of roaming services [7] are mainly derived from the resource constraints of mobile users, the security requirements of authentication delay and roaming applications. It is important to know the requirements of the roaming authentication protocol in a clear way: (1) *server authentication* a roaming user should be allowed to authenticate to the server to avoid potential fraud and other malicious attacks. (2) *An order confirmation* access to the external network must be authenticated by the mobile user to ensure its legitimacy. (3) *A user revocation service* the service is needed to terminate roaming users once the user's subscription expires. (4) *Establish a key* a session key is established between the user and the foreign server to protect the data that is exchanged between them. (5) *Low computational complexity and communication overhead* typically, a mobile user is limited by power supply, processing power, and storage space. Therefore, the roaming authentication process should be efficient. In addition, the process should be fast enough, so as to maintain continuous connectivity for mobile users. (6) *The basic user anonymity and non traceability* the user should be anonymous, and its activity can not be linked to any listener. (7) *the ability to resist attacks* roaming agreements should have the ability to resist multiple attacks (such as DoS attack, replay attack, deposit-case attack). As shown in Fig. 2, the main challenge in developing a roaming authen-

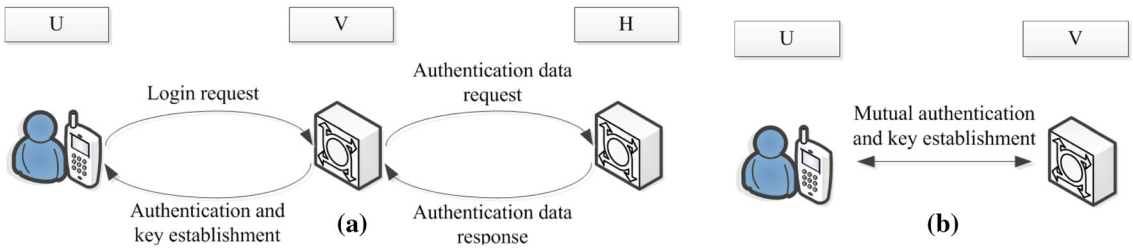


Fig. 3 The roaming authentication structure: **a** three square roaming structure, and **b** two party roaming

tication protocol is to provide robust security efficiently [that is, efficiently meeting (1)–(7) mandatory requirements and customized (1.1)–(10)].

Existing roaming authentication method: existing roaming authentication protocols can be divided into two categories: three party and the two party. As shown in Fig. 3a, the method of the three party requires a total of three parties, the simple process is as follows: when the login request of user U is received, foreign server V sends a validation request to the local server H of the user U. The local server H checks whether the user U is a legitimate user of its own, and whether the server V is a valid foreign server. After receiving the response to the local server H, the server uses the secret information that the H provided to perform validation [8], as well as a key with the user U. Another case is shown in Fig. 3b, and the two party method does not require the participation of the local network. That is to say, without the help of the local server H, there has the mutual authentication and session key establishment between the foreign server V and user U.

4.2 Privacy data protection scheme for wireless sensor networks

A variety of different attributes of the data is collected continuously by sensor network data source node. Data which with different attributes have different uses, and there are also differences in data acquisition with the same attribute. Therefore, the wireless sensor network data has the properties of one, and the time of the two-dimensional characteristic. Definition 1, attribute (Attribute): a data source node that collects the data simultaneously can be represented as a data set:

$$D = (d_1, d_2, \ldots, d_x) \tag{1}$$

Each element of D represents a metadata. Subdivision can be obtained by dividing the data set.

$$P = \{D_1, D_2, \ldots, D_m\} \tag{2}$$

Then a sequence of elements can be get in the P by the specified rules.

$$A = \{a_1, a_2, \ldots, a_m\} \tag{3}$$

Each element of sequence A is called an attribute (Attribute). The division and arrangement rules can be developed and changed according to the actual application scenario of wireless sensor networks.

Definition 2 time (Time): the data source node can be distinguished by their acquisition time. Given a fixed time slice length T_Δ, from a sensor network system to start running, the time period of a given moment can be divided into a time series (sequence time).

$$T = \{t_1, t_2, \ldots, t_n\} \tag{4}$$

The elements are arranged in chronological order. Each element in the sequence is called a time slice (Slot Time). If all data collected by a data source node in a wireless sensor network is considered as a two-dimensional plane [9], which is determined by the time and attribute class, the two-dimensional plane will be divided into many subspaces by time and property. Time of the data and the properties of the two dimensional properties are shown in Fig. 4.

If it uses S_{ij} to represent the data of the i attribute of the j time slice, then all data collected by a data source node can be represented as a matrix S.

$$S = \begin{pmatrix} S_{11} & \cdots & S_{1n} \\ \vdots & \ddots & \vdots \\ S_{m1} & \cdots & S_{mn} \end{pmatrix} \tag{5}$$

TPP scheme is a kind of multi attribute privacy data protection scheme based on wireless sensor network, which can be applied to various wireless sensor network model. In order to simplify the description, the storage network model can be used, which is shown in Fig. 5. Namely, in the wireless sensor network that with the crowd as the service object, the data source node collects all the data which is transmitted and stored in the node.

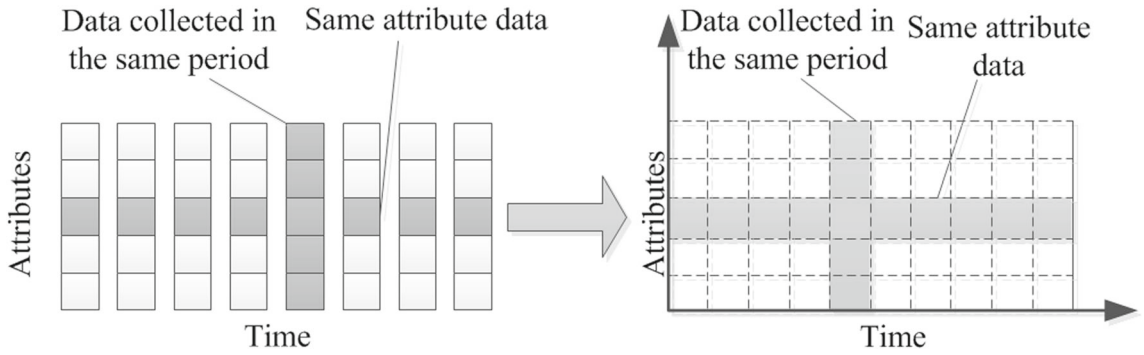
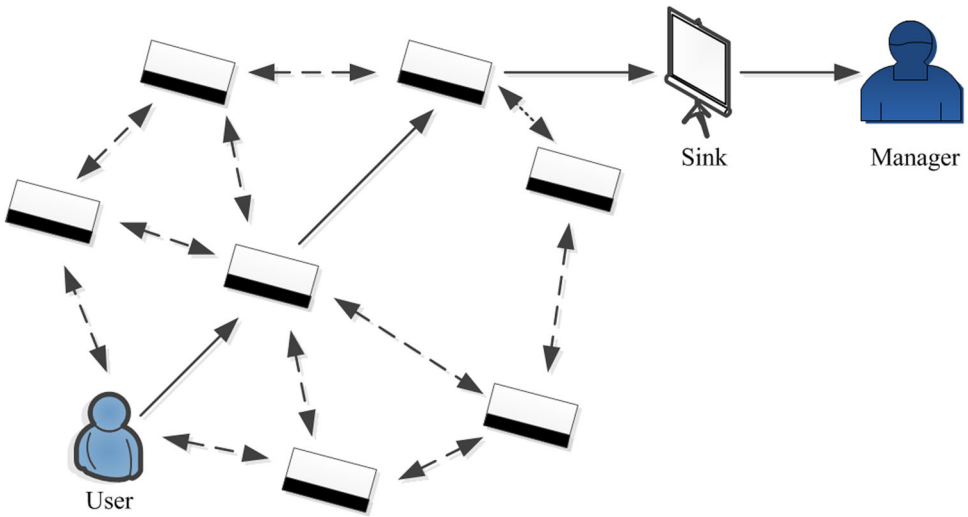


Fig. 4 Time a property of two-dimensional characteristics

Fig. 5 Network model



In order to provide sufficient security and privacy controls, the data that the data source node collects are divided into many sub spaces according to their properties and the time two dimensional attribute [10]. A lightweight key generation scheme could be designed (Key, Generation Scheme KGS) to generate the corresponding sub key for the data in each subspace. KGS programs run simultaneously with the collection of data on the data source node. In each time slice, the privacy data is collected, and the corresponding sub key of each attribute is generated. After the node uses the corresponding sub key to encrypt the data, the node transmits the data to the Sink node through the sensor network. Because the data is encrypted, so no one can read the data that are stored in the sensor network Sink node. If someone wants to read and use some of the data, he must send the required data corresponding to the properties of the Attribute-time (Attribute-time) (a, t) to the corresponding data source node request the corresponding sub key firstly. In the data source node [11], a decision mechanism is designed to decide whether to respond to the requests that from the Sink side, depending on the different needs (such as the intention of the user, etc.). Only by getting the corresponding sub key to read the required data.

4.3 Key generation scheme KGS

The key generation scheme is designed to generate a different encryption key for each sub space in the data source node. That is, the data generated in each sub space S of the data matrix S_{ij} generates a corresponding sub key k_{ij}, so the sub key matrix K. So the sub key matrix K can be obtained.

$$K = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mn} \end{pmatrix} \tag{6}$$

It is generally believed that the energy and computing power of wireless sensor nodes are very limited. The encryption algorithm that used in the traditional network is too large, too complex and too much energy consumption. So a lightweight hash function is chose to design a key generation scheme. Hash function has been applied and has been widely used in wireless sensor networks. A KGS key generation scheme is proposed by using the improved Hashi (Hash Chain One-way) technology [12]. In order to facilitate the description, firstly to introduce the symbol that used in the

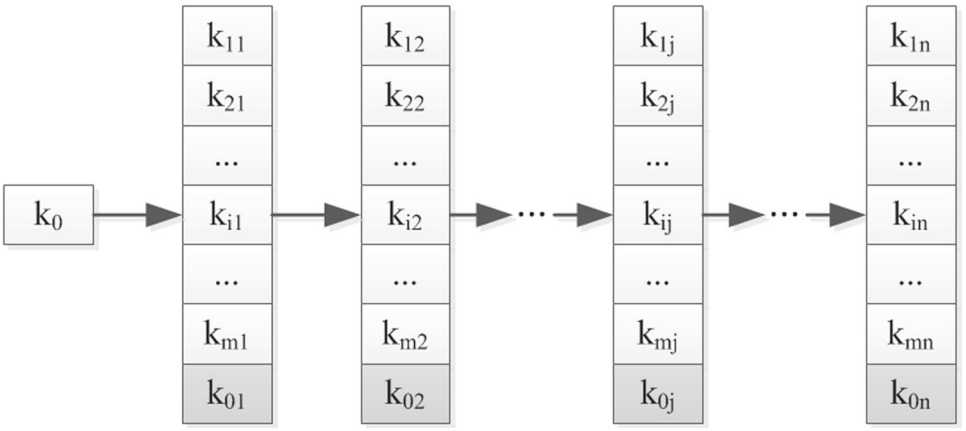


Fig. 6 Schematic diagram of key generation scheme

algorithm. That is, the assumption is that the hash function is represented as $H = Hash()$, each data source node stores the only seed key k_0 as the initial input of the hash chain. The length of the generated k_{ij} is

$$\left|k_{ij}\right| = l \tag{7}$$

To retain the length of the key is L, so the length of each hash value in the hash chain is:

$$|H_i| = l \times m + L \tag{8}$$

The working flow of the KGS scheme is as follows. At the beginning of each time slice ti, the hash value is used as the input to calculate the corresponding hash value:

$$H_i = Hash(H_{i-1}) \tag{9}$$

The input is the seed key H_1 when the k_0 is calculated repeatedly to generate a hash chain:

$$H = \{H_1, H_2, \ldots, H_n\} \tag{10}$$

Each hash value H_i is divided into m + 1 segments, named as $k_{oi}, k_{1i}, \ldots, k_{mi}$, respectively,

$$\begin{cases} |k_{oi}| = L \\ |k_{1i}| = |k_{2i}| = \cdots = |k_{mi}| = l \end{cases} \tag{11}$$

$k_{1i}, k_{2i}, \ldots, k_{mi}$ is used as a sub key corresponding to the sub space $S_{1i}, S_{2i}, \ldots, S_{mi}$, and k_{oi} is called a key reserved, which is never used and will not be transmitted in the network. Such a repetition, the matrix of the sub key can be obtained which is needed for the data in all sub space:

$$K = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mn} \end{pmatrix} \tag{12}$$

The work diagram of the KGS key generation scheme is shown in Fig. 6, and the detailed process of the KGS scheme is given in Algorithm 1.

Algorithm 1 key generation scheme KGS:

Input: the seed key k_0, the number of attributes is m, the sub key length is l, the retention key length is L.

Output: sub key matrix K.

Step:

Step 1: Calculation:

$$H_1 = Hash(k_0) \tag{13}$$

Its length is $|H_i| = l \times m + L$.

Step 2: H_1 will be divided into m+1, called $\{k_{0l}, k_{1l}, \ldots, k_{ml}\}$ respectively, and $|k_{oi}| = L, |k_{1i}| = |k_{2i}| = \cdots = |k_{mi}| = l$; Select $k_{11}, k_{21}, \ldots, k_{m1}$ as the first column of the sub key matrix;

Step 3: $\forall i \in \{i | 1 < i \leq n, i \in N\}$, to calculate $H_i = Hash(H_{i-1})$, and $|H_i| = l \times m + L$;

Step 4: H_1 will be divided into m+1, called $\{k_{0i}, k_{1i}, \ldots, k_{mi}\}$ respectively, and $|k_{oi}| = L, |k_{1i}| = |k_{2i}| = \cdots = |k_{mi}|$;

Step 5: Return key matrix $K = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{m1} & \cdots & k_{mn} \end{pmatrix}$.

As is well known, the traditional one-way hash chain has the following basic features: Given a hash value H_i, the hash value can not be obtained by calculating the H_{i-1}; to calculate the hash value H_{i+1}, the hash value H_i should be know firstly; We will discuss the security of the KGS key generation scheme based on the above two basic features: for the same time, because there is no generation relationship between the sub keys generated, so it can not generate any other sub key in the same time. That is, the KGS scheme is the same level of security; by the characteristics of one-way hash chain (1), you can know the given H_i, it can not obtain the H_{i-1} by the

calculation of the hash value at any time. That is, the KGS scheme [13] is one-way secure; Because the retention k_{oi} is not used and will never be transmitted in the network, the k_{oi} is missing, even though the same time slice of all other sub key $k_{1i}, k_{2i}, \ldots, k_{mi}$ is obtained, the hash value can not be got by H_i. Thus, it can be derived through the feature (2) of the one-way hash chain: Because the H_i cannot be got, a hash value also cannot be got by H_{i+1} at any time. That is, the KGS program is also down safe; in summary, it can be concluded that any number of a group of sub keys can not be obtained by computing the other sub key. That is, the KGS key generation scheme can guarantee the security of all the sub keys generated by them.

4.4 Data extraction scheme DAS

The core of the DAS data extraction scheme is that when a data source node receives a (a, t) request from a sensor network Sink node, it generates the corresponding sub key k_{ij}, and then transmits it to the Sink node. In order to facilitate the description, the same symbol that introduced in the last section are used. That is, the assumption is that the hash function is represented as $H = Hash()$, each data source node only stores the seed key k_0 as the initial input of the hash chain. The length of the k_{ij} is $|k_{ij}| = l$, and the length of the key is L, so the length of each hash value is $|H_i| = l \times m + L$. In addition, we assume that the time of the beginning of the TPP scheme is T_1, and the length of each time slice is T_Δ. The working flow of the DAS scheme is as follows. A request from the Sink node contains a property (a, t). By the request time t, it is easy to calculate the value of the time slice by the following formula j.

$$j = \left\lceil \frac{(t - T_1)}{T_\Delta} \right\rceil \tag{14}$$

Using the initial key k_0 on the node, the hash value H_j of the j corresponding to the hash chain can be calculated by the following formula.

$$H_j = Hash^j(k_0) \tag{15}$$

The function of the above formula is to obtain the required hash value by inputting the seed key k_0 in J times hash calculation. Among them, the length of H_j is:

$$|H_j| = l \times m + L \tag{16}$$

Similarly, according to the attribute of Sink (a, t), from the request attribute a, it can be defined as the corresponding attribute class of a, which is corresponding to the J of time slice:

$$i = Addr(a) \tag{17}$$

And then, the (a, t) is calculated by the following formula. The sub space corresponding to the subspace corresponding to the data is k_{ij}:

$$k_{ij} = Subkey(H_j, l \times i - l, l) \tag{18}$$

The formula represents that intercepting a sub string from hash value H_j, the beginning of the sub string position is in the position of the $(l \times i - l)$ position, and the length of the interception of the sub string L. The detailed process of the DAS data extraction scheme is given in Algorithm 2.

Algorithm 2 data extraction algorithm DAS:
Input: attribute time to (a, t).
Output: the corresponding sub key k_{ij}.
The data extraction algorithm DAS step are as follows:

Step 1: According to the attribute of (a, t), the position of the corresponding sub space is calculated respectively:

$$i = Addr(a),\ j = \left\lceil \frac{(t - T_1)}{T_\Delta} \right\rceil \tag{19}$$

Step 2: According to j, the corresponding hash value $H_j = Hash^j(k_0)$ is calculated by using the initial key k_0, its length is $|H_j| = l \times m + L$;
Step 3: According to i, the corresponding sub key $k_{ij} = Subkey(H_j, l \times i - l, l)$ is calculated;
Step 4: Return to k_{ij}.

In order to avoid the problem of calculating the required sub key with the initial key k_0 for each request, an improved scheme of TPP scheme is designed, which makes it more suitable for sensor networks by a useful trade off between computational overhead and storage overhead. The main idea is that in the key generation phase, a hash value H_{yN} is stored in each N time slice, where the value of N can be dynamically adjusted according to the computing power of the data source node processor and the memory size. After the H_{yN}, N hash value can be calculated by H_{yN}. Based on this improvement, the data source node can be re described to respond to the request from Sink, how to calculate the corresponding sub key. When the data source node receives a property of the Sink node from the sensor network a attribute to time (a, t), by the request time t, it can be easily calculated by the formula (14) that the requested data sub key is located in the time slice $j = \left\lceil \frac{(t-T_1)}{T_\Delta} \right\rceil$. Due to the value of N in fixed applications is known, the value of y can be calculated by the following formula. By the value of Y, that is the hash value H_{yN} which is the last one that stored in the data source node before the time slice J.

$$y = \left\lceil \frac{j}{N} \right\rceil \tag{20}$$

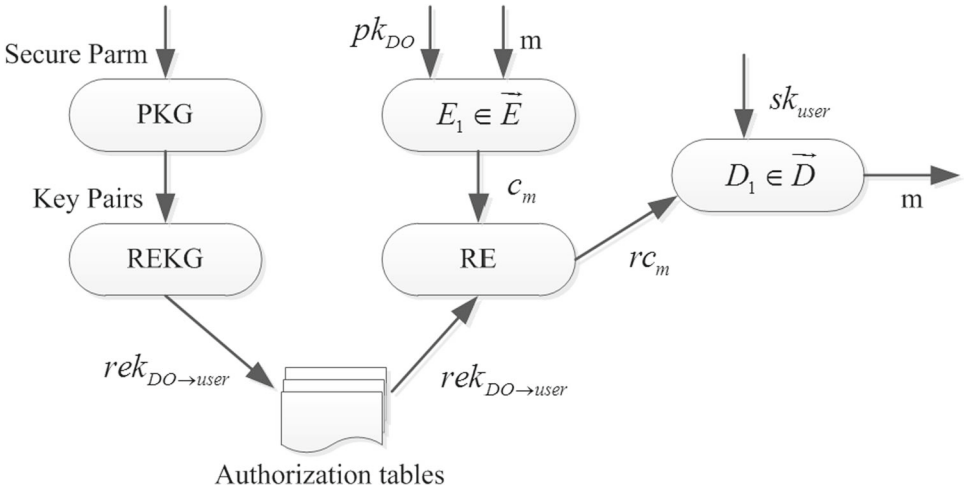


Fig. 7 DSP re-encryption mechanism

Therefore, the corresponding hash value H_j of the time slice j can be directly calculated by the following formula by the use of hash value H_{yN}.

$$H_j = Hash^{j-yN}(H_{yN}) \tag{21}$$

The improved data extraction scheme is described like the Algorithm 3:

Algorithm 3 data extraction algorithm improvement program:

Input: the property of a time on the (a, t), the hash value of the storage cycle N output: corresponding to the sub key k_{ij}.

Step:

Step 1: According to the property of a time to (a, t), the location of the corresponding subspace can be calculated:

$$i = Addr(a),\ j = \left[\frac{(t - T_1)}{T_\Delta}\right] \tag{22}$$

Step 2: By the storage period N, it can be calculated that the last hash value is stored in the data source node is H_{yN} before the time slice j. $y = \left[\frac{j}{N}\right]$;

Step 3: The hash value that corresponding to the j is $H_j = Hash^{j-yN}(H_{yN})$;

Step 4: According to i, the corresponding sub key is $k_{ij} = Subkey(H_j, l \times i - l, l)$;

Step 5: Return to k_{ij}.

In the improved scheme at the expense of a small amount of storage space for the data source node, which greatly improves the response speed of the data source node. It can reduce the computation cost and energy consumption of the sensor nodes effectively, which makes the scheme more suitable for wireless sensor networks with limited resources [14–16].

4.5 Re-encrypted access control enhancement mechanism

4.5.1 Re-encryption mechanism of service providers

Definition 3: DSP re encryption mechanism, Fig. 7 consists of five components: encryption algorithm ($\vec{E}$), re-encryption key generator (REKG), private key generator (PKG) and decryption algorithm($\vec{D}$). It allows DSP to encrypt a c_m (ciphertext) into different encryption (re-ciphertext) rc_m. c_m is a cipher text of the public key encrypted by the m in the data owner, and rc_m is a cipher text c_m encrypted by $rek_{DO\to user}$. In this approach, assuming that M can be any clear data. Such as a tuple or a key, E1 is the first encryption algorithm, $E_1 \in \vec{E}$, and D1 is the corresponding decryption algorithm to E1, $D_1 \in \vec{D}$. When inputting pk_{DO} and m, the algorithm E1 outputs c_m. When inputting the c_m and the re- encryption key $rek_{DO\to user}$, the algorithm RE can generate access control to enhance the encrypted rc_m. rc_m can be decoded into information m only under the action of legal user's sk_{user} and the algorithm D1. Next, the function of the five components will be introduced in Fig. 7.

Through inputting the full parameter (secure parm) 1^k, the PKG outputs the key (pk_{user}, sk_{user}) for legitimate user. Such as generating keys for the user Alice, encryption algorithm E1 and decryption algorithm D1 usage can be expressed as the following form:

$$\begin{cases} PKG(1^k) \to (pk_A, sk_A) \\ E_1(pk_{DO}, m) \to c_m \\ D_1(sk_{user}, rc_m) = \text{m} \end{cases} \tag{23}$$

By entering the keys $(pk_{DO}, sk_{DO}, pk_{user}, sk_{user})$, the encryption key generator REKG can generate a re-encryption

Table 1 Securities information table

userid	name	stockid	Number	Buyprice	Curprice
1021	Tina	601234	500	5.0	8.3
1022	Krsa	026543	100	17.2	15.3
1023	Mary	632108	600	45.0	46.0
1024	Smile	001234	1000	25.38	20.8
1025	Haha	002436	200	80.38	100.8
1026	Zhaya	600654	800	38.0	42.8
1027	Moon	060753	1000	26.2	20.8

Table 2 The information table of the securities of the cipher text

id	ekey	etuple	ind1	ind2
1	c_{randk1}	c_{t1}	abcd020	thjks20
2	c_{randk2}	c_{t2}	abcd100	thjks60
3	c_{randk3}	c_{t3}	abcd600	thjks300
4	c_{randk4}	c_{t4}	abcd060	thjks800
5	c_{randk5}	c_{t5}	abcd080	thjks1000
6	c_{randk6}	c_{t6}	abcd110	thjks1100
7	c_{randk7}	c_{t7}	abcd150	thjks1200

key for legitimate users $rek_{DO\to user}$. The generated re-encryption key for any legal user can be expressed as the following form:

$$REKG(pk_{DO}, sk_{DO}, pk_{user}, sk_{user}) \to rek_{DO\to user} \quad (24)$$

When inputting the encrypted key $rek_{DO\to user}$ and c_m in the encryption module, the access control that enhanced by the encrypted rc_m will output. The enhanced access control of encrypted module [17–19] can be expressed as the following form:

$$RE(rek_{DO\to user}, c_m) \to rc_m \quad (25)$$

4.5.2 First encryption

In database service scenarios, it is generally believed that the DSP data content is not trusted or DSP itself is an internal attacker. So before the data owners entrust the data to the DSP [20], the important and sensitive data information is required to be converted into a form of protection to protect the privacy of data privacy breaches. This conversion is implemented in this method by using the first encryption.

Definition 4: the first encryption E1 is executed by DO, which indicates that any one of the source database ti or any selected random key randki can be encrypted into the corresponding cipher text by public key pk_{DO} of DO.

$$\begin{cases} DO : E_1(pk_{DO}, ti) \to c_{ti} : DSP \\ DO : E_1(pk_{DO}, \text{randki}) \to c_{randki} : DSP \end{cases} \quad (26)$$

Table 1 shows the securities information table (Stocks), and Table 2 is the corresponding encryption relations table (Encrypted-Stocks) to Table 1. From these two tables, it can be seen that they have the same number of rows. The id attribute represents the unique identifier of the encrypted tuple. The ekey attribute is the obtained corresponding cipher text that is the first encryption algorithm to function on the source database of the tuple. The DO encryption [3] is generated by pk_{DO}, and the encryption key is generated by random encryption key randki in multi encryption key method. The indj attribute is an additional index information to improve the query efficiency of the encrypted database. In general, the r has any relationship with the following patterns $R(A_1, \ldots, A_n)$ in express database, it is generated to r^k with the patterns $R^k(id, ekey, etuple, ind1, \ldots, indn)$ in the first time the encryption.

4.5.3 Authorization list

There are two licenses to be created respectively, "user-re-key" and "user-counter".

- user-re-key (userid, name, rekey). Each tuple in the table "user-re-key" corresponds to a legitimate user's information, such as user identity (userid), name (name), and encryption key (rekey). The value of the "rekey" attribute can only be used by the DSP, and then encrypted by the authorized table of the authority. Each user of the system has a unique user identity, that is, the value of the user identity (userid) property cannot be duplicated. The value of the name (name) attribute can be repeated. Each user has a unique re encryption key, that is, the value of the re encryption key (rekey) property is not repeatable [21].
- user-counter(userid,tid). Table "user-counter" includes that the tuple identifier that each user is authorized to access and the corresponding relationship between user identity, such as the tuple identifier (tid) and user identity (userid).

The data owner delegates the two licenses to the DSP in a secure manner. Secure transmission mode, such as the transmission or transmission of a secure channel through the DSP public key. In order to describe the enhanced access control in DSP, we give the authorization table "user-re-key", which is corresponding to Table 1 (Table 3). 100,801 is the identity of the user Mike, and the 100,802 is the identity of the user's Jack. In Table 4, an authorization table is given to "user-counter", the access authorization matrix [22] lists all of the tuple that a user is authorized to access as shown in

Table 3 The authorization table corresponds to Table 1

userid	name	rekey
10081	Mike	dxvsd
10082	Jack	csvr
10083	Kate	cvt56
10084	Jone	cg7hs
10085	Mary	drth7

Table 4 Authorization table "User-Counter"

userid	tid
100,801	1, 3, 5, 6
100,802	2, 3, 4, 6, 7
100,803	1, 5
100,804	4
100,805	3, 6, 7

	t1	t2	t3	t4	t5	t6	t7
Mike	1	0	1	0	1	1	0
Jack	0	1	1	1	0	1	1
Kate	1	0	0	0	1	0	0
Jone	0	0	0	1	0	0	0
Mary	0	0	1	0	0	1	1

Fig. 8 Access authorization matrix

Fig. 8. For example, a user who is aware of the identity of the first row in the table "user-counter" is able to access the tuple t_1, t_3, t_5, t_6, in the actual "user-counter" table, each of the authorized users to access a row.

5 Results analysis and discussion

In order to evaluate the message load of Priccess protocol, the following four evaluation criteria can be used: message load, execution time, message complexity and energy consumption. Execution time is measured by the execution time of each operation in the protocol. The complexity of message [23] shows the amount of messages when make the user's query. Without consideration of Baotou, the message load of the Priccess protocol has the following two cases. One is not required to establish a secure channel between the network users and the nodes, while the message load is $20 \times m + 36$ bytes. Another has to establish a secure channel between the network users and the nodes, when the message load is $20 \times m + 56$ bytes.

Figure 9 shows the execution time of a particular group member number (m) and the changing ECC key length (L),

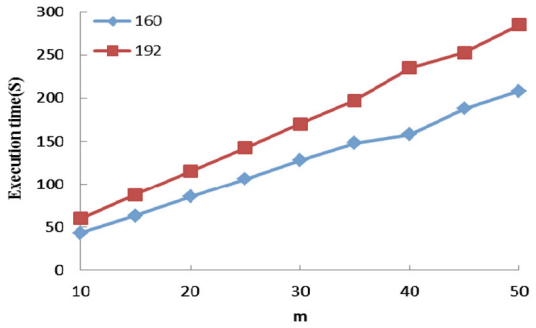


Fig. 9 The execution time of a user query

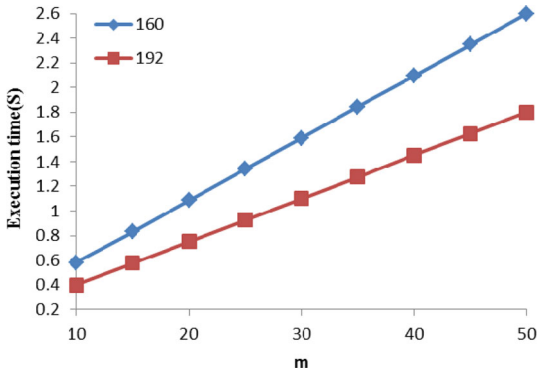


Fig. 10 The execution time of the node verification

resulting in the user query phase. For example, in the m = 10 and l = 160, the execution time is 45.3 ms, while the m = 50 and l = 160 (l = 192), the execution time is 212.4 ms (282.9 ms). Keep in mind that the user query phase is running on a 1.8 GHz laptop, considering the frequency of most smart phones is higher than 1 GHz, so the protocol for most of the user access devices (such as laptops and PDA) are efficient.

Figure 10 shows the execution time of a particular group member number (m) and the change of the ECC key length (L) in the node verification phase. For example, experiments show when m = 10 and l = 160, the verification time that reflected by Imote2 is 0.385 seconds, while m = 40 and l = 160 (l = 192), the execution time is 1.473 s (2.084 s). As mentioned above, the verification time [24] of the node is independent of the size of the network. That is to say, even if the size of the sensor network is extended in thousands, the delay of the node verification phase will not increase. The delay is determined by the number of components selected (m) directly. Considering the execution time of the secure channel between the user and the node, for the ECDH key exchange technology, Imote2 has been used to generate the session key for 0.034 s. Among them, the ECC key size is 160 bits. Experiments show that the Imote2 spends 0.984 μs and the user spend 0.39 ms respectively to conduct the 64 bits data AES encryption. As mentioned above, the message complexity of Priccess is independent of the size of the network (total

Table 5 Energy consumption of Priccess protocol

m	10	20	30	40	50
Node verification cost (160) (J)	0.35	0.66	0.98	1.29	1.45
Node verification cost (192) (J)	0.50	0.96	1.42	1.88	2.33

number of nodes). The equation [25] $E = U \times I \times \mathrm{t}$ is used to estimate the energy consumption of signature verification, in which the U is expressed as a voltage, i is represented by the current, and t is expressed by time delay. Therefore, the energy consumption and execution time is a linear relationship. The Imote2 node uses three AA battery, so the U is about 4.5 V, and in the current of the active state Imote2 I is 200 mA. Table 5 lists the energy consumption of the Priccess protocol when the L and M changes. For example, when m = 20 and l = 160, the energy consumption of the Imote2 node is about 0.662 J.

6 Conclusions

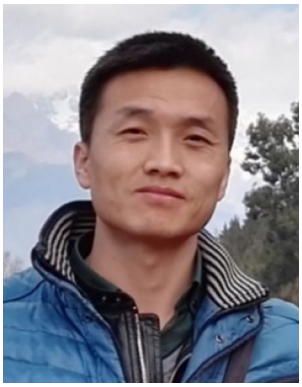
This paper analyzes the problem of control protocol in privacy preserving access, and describes the Priccess protocol and some important issues on this protocol. Therefore, Priccess protocol can be applied to the resource constrained sensor nodes as well as it also can be extended. However, there are limitations in the field of wireless network communication. The traditional roaming authentication scheme is one of them. The roaming authentication process is to let the foreign server communicate with the local server. In order to strengthen the protection of access control, the paper introduces the mechanism of re encryption access control, which constitutes a novel Priccess control protocol in privacy protection access of network and can provide more efficient protection for the privacy of network communication.

Acknowledgements This study is supported by "Ningxia Autonomous Region Advantageous Discipline (Grant No. ND20151031)".

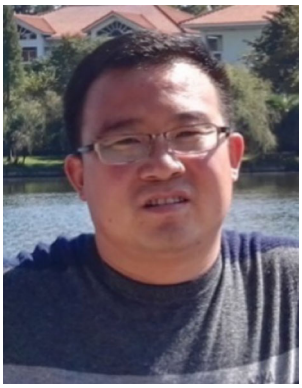
References

1. Shin, M., Ma, J., Mishra, A., et al.: Wireless network security and interworking. Proc. IEEE **94**(2), 455–466 (2006)
2. Li, N., Zhang, N., Das, S.K., et al.: Privacy preservation in wireless sensor networks: a state-of-the-art survey. Ad Hoc Netw. **7**(8), 1501–1514 (2009)
3. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**(6), 53–57 (2004)
4. Walters, J.P., Liang, Z., Shi, W., et al.: Wireless sensor network security: a survey. Secur. Distrib. Grid Mob. Pervasive Comput. **1**(8), 367 (2007)
5. Wood, A.D., Stankovic, J.: Denial of service in sensor networks. Computer **35**(10), 54–62 (2002)
6. Shi, E., Perrig, A.: Designing secure sensor networks. IEEE Wirel. Commun. **11**(6), 38–43 (2004)
7. Buttyán, L., Gessner, D., Hessler, A., et al.: Application of wireless sensor networks in critical infrastructure protection: challenges and design options [security and privacy in emerging wireless networks]. IEEE Wirel. Commun. **17**(5), 44–49 (2010)
8. Sweeney, L.: Achieving k-anonymity privacy protection using generalization and suppression. Int. J. Uncertain. Fuzziness Knowl. Based Syst. **10**(05), 571–588 (2002)
9. Want, R., Hopper, A., Falcao, V., et al.: The active badge location system. ACM Trans. Inf. Syst. (TOIS) **10**(1), 91–102 (1992)
10. Kargl, F., Papadimitratos, P., Buttyan, L., et al.: Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Commun. Mag. **46**(11), 110–118 (2008)
11. Wood, A., Virone, G., Doan, T., et al.: ALARM-NET: wireless sensor networks for assisted-living and residential monitoring. Univ. Virginia Comput. Sci. Dep. Tech. Rep. **2**(9), 90–93 (2006)
12. Ostfeld, A., Uber, J.G., Salomons, E., et al.: The battle of the water sensor networks (BWSN): a design challenge for engineers and algorithms. J. Water Resour. Plan. Manage. **134**(6), 556–568 (2008)
13. Al Ameen, M., Liu, J., Kwak, K.: Security and privacy issues in wireless sensor networks for healthcare applications. J. Med. Syst. **36**(1), 93–101 (2012)
14. Kundur, D., Luh, W., Okorafor, U.N., et al.: Security and privacy for distributed multimedia sensor networks. Proc. IEEE **96**(1), 112–130 (2008)
15. Li, H., Lin, K., Li, K.: Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. Comput. Commun. **34**(4), 591–597 (2011)
16. Akyildiz, I.F., Pompili, D., Melodia, T.: Underwater acoustic sensor networks: research challenges. Ad hoc Netw. **3**(3), 257–279 (2005)
17. Zhao, J., Zhang, P., Cao, G., et al.: Cooperative caching in wireless p2p networks: design, implementation, and evaluation. IEEE Trans. Parallel Distrib. Syst. **21**(2), 229–241 (2010)
18. Baker, S.D., Hoglund, D.H.: Medical-grade, mission-critical wireless networks [designing an enterprise mobility solution in the healthcare environment]. IEEE Eng. Med. Biol. Mag. **27**(2), 86–95 (2008)
19. Khan, M.K., Alghathbar, K.: Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors **10**(3), 2450–2459 (2010)
20. Felt, A., Evans, D.: Privacy protection for social networking apis. Web 2.0 Secur. Priv. (W2SP'08) **5**(7), 56–60 (2008)
21. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. **47**(4), 445–487 (2005)
22. He, D., Bu, J., Zhu, S., et al.: Distributed access control with privacy support in wireless sensor networks. IEEE Trans. Wirel. Commun. **10**(10), 3472–3481 (2011)
23. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
24. Xiao, Y., Chen, H., Yang, S., et al.: Wireless network security. EURASIP J. Wirel. Commun. Netw. **20**(1), 1–3 (2009)
25. Li, M., Lou, W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wirel. Commun. **17**(1), 51–58 (2010)

Xu Ma Master of Computer Science and Technology, Professor, graduated from Shaanxi Normal University in 1994. Worked in Ningxia Normal University. His research interests include cloud computing, big data, network technology, embedded system, etc.



Kai Kang Master of Computer Science and Technology, Associate Professor, graduated from Shaanxi Normal University in 2005. Worked in Ningxia Normal University. His research interests include network technology, networking, software engineering, embedded systems.



Wanshun Lu Master of Applied Mathematics, Associate Professor, graduated from Ningxia University in 2008. Worked in Ningtxia normal university. His research interests focus on complex analysis and its application in mechanics.

Li Xu Master of Applied Mathematics, Lecturer, graduated from Ningxia University in 2008. Worked in Ningxia normal university. Her research interests focus on Scientific and Engineering Computing.

Chen Chen Master of Computer Science and Technology, graduated from Northeast Petroleum University in 2012. Worked in Ningxia Normal University. His research interests focus on networking, embedded systems, parallel computing.