Enhanced bidirectional authentication scheme for RFID communications in Internet of Things environment

Enhanced Bidirectional Authentication Scheme for RFID Communications in an Internet of Things Environment

Haixia Li[1,2], Shanyu Tang[1*], *Senior Member, IEEE*

[1] School of Computer Science, China University of Geosciences, Wuhan 430074, China
[2] School of Computer Science and Technology, Hubei Polytechnic University, Huangshi, Hubei, China

***Abstract*—Among the security issues in the environment of the Internet of things (IOT), the security of information source is a privilege to be concerned. To protect data collection and control devices in IOT, first of all, ones shall ensure the authenticity of information source. To address the uncertainty problem of information sources in IOT, identity authentication technology is essential. In this study, we suggested an enhanced bidirectional authentication scheme that is suitable for Radio Frequency Identification (RFID) communications among devices or between devices and control devices in an IOT environment. Specific improvement measures included three aspects: back-up terminals, a condition monitoring device to increase authentication properties, and an alarm mechanism. The enhanced bidirectional authentication protocol presented in this article has the characteristics of excellent performance in security and privacy protection, which could authenticate data contents, even positions and other data properties, and resist the replay or denial of service attacks; at the same time, it could overcome the defect of data asynchrony between the front end and the**

[*] Corresponding author

back end, providing users with excellent forward security. The simulation experiments showed that system reliability was greatly enhanced by adopting the proposed protocol.

Keywords—IOT; RFID; bidirectional authentication; security

1. INTRODUCTION

With the increasing popularity of the Internet of things (IOT) concept and technology, the technical details of wireless sensor networks have been mastered by more and more people, and afterwards, more security issues have been exposed. To safeguard data collection and control devices in IOT, first of all, ones shall ensure the authenticity of information source, which requires the identity authentication mechanism of IOT control system to be more strict in comparison with traditional networks, so as to ensure the legality of access devices. By definition, IOT refers to a kind of network that associates things with the Internet for information interchange and communication to realize intelligent identification, location, tracking, monitoring, and management as appointed agreement by means of information sensing equipment [1]. In an IOT environment, terminal equipments mostly consist of intelligent terminals equipped with Radio Frequency Identification (RFID) labels and identification terminals in charge of reading RFID label information, and a great number of data communications are transported by wireless sensor networks. At the early stage of wireless sensor network technology, the technology was widely used in the military field, so relatively fewer professionals could contact and understand the details of wireless sensor network technology, and relatively fewer security issues were exposed then. In addition, as a mass of RFID technologies having been applied to IOT, some people have already set various means of attacks upon the technical

vulnerability of RIFD, so that the information sources in an IOT environment are faced with severe security challenge [2].

Compared with traditional computer networks, the architecture of IOT environment is more complex. The traditional computer networks exist only as a part of the network structure of IOT system, which leads to a cross-domain authentication problem of control security in an IOT environment. In addition, the variety and quantity of terminal devices of access networks increase greatly, and the terminal devices are no longer only PCs, servers and other similar computing devices in traditional computer networks, but also include intelligent terminals, RFID labels, reader-writers, wireless sensing nodes, short distance wireless communication terminals, mobile communication terminals, cameras, sensor network gateways, and a large number of other new-type devices. These devices not only present a great quantity, and diverse specifications and features which are difficult to be unified. At the same time, they are not provided with the high-performance operational capability like the traditional PCs, servers and other similar devices, so they can only adopt a relatively simple and efficient authentication algorithm, which greatly increases the difficulty of identity authentication in an IOT environment. Furthermore, because of the internal application features of IOT, the access devices of IOT are even more in the state of unattended operation compared with traditional computer networks, which makes the communications among devices out of artificial monitoring and protection. It therefore results in a great increase in difficulty of ensuring the security of information source in an IOT environment.

On the other hand, compared with mobile communication networks, the IOT terminal devices come with some problems, such as great man-made sabotage, illegal embezzlement, etc. As in mobile communication networks, the device terminals of

access networks such as mobile phone, Personal Digital Assistant (PDA) are mostly provided for end users, and can be supervised and protected by users themselves. Network operators need not to monitor the security of terminal devices, and only need to ensure all terminal devices of access networks are legal. But in an IOT environment, as mass amounts of terminal devices are not privately owned by end users, and are kept in the unattended state in the long term, the devices are easily damaged artificially and physically, and their IDs can be embezzled for illegal access. Once an appropriator is able to access the operator network, there is likely to have destruction to networks or data embezzlement. Hence, with respect to traditional mobile communication networks, the authentication scheme for IOT devices shall be more strict to ensure the legality of access devices.

To sum up, the uncertainty of information sources in an IOT environment mainly includes the following:

(1) unauthorized use of terminal devices: the IOT terminal devices being mostly kept in the state of unattended operation, and easily destroyed artificially or robbed of communication modules in terminals for some illegal purposes, such as illegally embezzling for phone calls.

(2) Illegally reading node information: attackers may execute destruction towards terminal devices in physics, so as to expose the non-open connectors of internal devices, and acquire session key, critical data and other information.

(3) Pretending terminal devices or sensor nodes: attackers may pretend terminal devices or sensor nodes to access sensing networks by means of hardware or software, so as to monitor network information, catch data illegally, or send offensive and devastating information to the networks, and attack the whole network security.

(4) Device vulnerability: IOT Terminal devices are mostly RFID labels or wireless sensor nodes with sensory ability, and they just have limited operational capability in comparison with PC. So on one hand, it is difficult for them to burden high calculated quantity of security protocol and identity authentication algorithm; on the other hand, they are more easily cracked and attacked [3].

The purpose of identity authentication is to indeed verify identity each other, build up dependable communication relationship, and ensure the security and reliability of information sources. However, the devices in an IOT environment generally present the features of diverse specifications, jagged processing capacity, unattended operation and keeping motion, and these new features in an IOT environment raise new demands and challenges for identity authentication. Therefore, to solve the authenticity issue of information sources in an IOT environment, a new device identity authentication scheme that fits for the features of IOT shall be introduced to make legal identity authentication for the both sides of information interaction, and ensure the security of communications between information sources. Although some identity authentication schemes have been proposed against the terminal devices of IOT RFID in theory, a whole set of authentication model that fully complies with IOT environments and performs formal verification with a complete system is still unavailable. At the same time, the control system in an IOT environment also present some specificities. The terminal devices used for the control system usually perform a higher operational and storage capacity than those common RFID terminals, which provides guidance on designing an effective identity authentication scheme for the control system in an IOT environment. In this study, our efforts were made to balance resource, efficiency and security upon the features of the control system terminal devices, and select the identity authentication scheme that is best for its actual features.

2. RELATED WORK

A. Relevant research

There are mainly two solutions for ensuring the identity legality and information source reliability of IOT terminal devices. One is the physical protection method for RFID devices, and the other is identity authentication based on cryptology.

The identity authentication scheme using cryptology has a great superiority in security aspect, and there are some existing identity authentication protocols for IOT RFID devices, including the authentication protocols based on hash function: Hash-Lock protocol, random Hash-Lock protocol [4] and Hash-Chain protocol [5]; re-encryption protocols based on ID variation protocol and LCAP protocol.

Hash-Lock protocol and random Hash-Lock protocol [6] were proposed by Weis and other researchers from American MIT. The comparison and authentication work is forwarded through hash function encryption with Hash-Lock protocol towards IOT device ID. Because of the stationarity of ID and hash function, this protocol leads to a fixed Hash value each time, which is tracked easily by attackers. Therefore, Weis et al further suggested a random Hash-Lock protocol on the basis of Hash-Lock protocol, and introduced a random number before Hash encryption towards ID to increase unpredictability of Hash value, which could effectively avoid trailing types of attack. But, this method leads to a significant increase in workload of searching and data communication traffic, and is not suitable for the IOT application system with a large number of labels. Afterwards, Japanese NTT lab proposed a Hash-Chain protocol based on two kinds of Hash-Lock protocols, and they reported that two times of encryption operations towards RFID with the help of the two different hash functions could provide stronger security. However, the protocol causes an increase in

calculating quantity of system, and 2n times of hash calculations and n times of comparisons and searches are necessary for the system with n RFID labels, which brings a great burden for IOT terminal devices with a limited operational capability.

The hash-based ID variation protocol, proposed by Henrici, Muller et al, executes dynamic refreshing towards ID of each conversation, which effectively enhances the privacy of communications among RFID devices. But, this protocol has a hidden danger of out-of-step data at front and rear ends, and it is subject to out-of-step attacks. LCAP protocol [7] is an inquire-response type of protocol with the feature of bidirectional authentication, but still has the same problem as the hash-based ID variation protocol, i.e. it easily leads to out-of-step data at front and rear ends, and so it is unfit in the distributed computing environment.

A famous re-encryption protocol [8] is the general re-encryption protocol scheme [9] capable of achieving RFID label anonymity function, proposed by Golle *et al*. The non-symmetric key encryption system is applied in this encryption scheme, and users can apply for a regular encryption rewriting of RFID label data, which helps to bring definite flexibility for IOT RFID device identity authentication.

These protocols above can be simply classified as one-way authentication protocol and bidirectional authentication protocol in terms of the authentication direction. Therein, one-way authentication protocol includes three kinds of protocols based on hash function: Hash-Lock protocol, random Hash-Lock protocol, and Hash-Chain protocol. These one-way authentication protocols only complete authentication towards RFID device by card reader, and cannot achieve authentication towards card reader by RFID device. Such authentication model is forwarded on the premise that card reader, backstage server and database are fully credible. With one-way authentication model, RFID terminal devices cannot identify the legality of their

communication devices, and are likely to suffer controls by illegal card readers, leading to information disclosure [10]. That is to say that one-way authentication protocols have insufficient security.

Although the ID variation protocol, LCAP protocol and re-encryption protocol on the basis of hash provide with definite features of bidirectional authentication, some deficiencies of other aspects still exist. As an example, the ID variation protocol and LCAP protocol [11] on the basis of hash could lead to the out-of-step information between terminal device of front end and backend database, so they are not appropriate for the authentication process of distributed computing environment. For re-encryption protocol [12], as its adopted ID is fixed and invariable, there exists with the severe problem of label location privacy leak, and the frequently repeated encryption operations bring a heavy burden for its practical application. In general, compared with one-way authentication, although a bidirectional authentication scheme results in an increase in costs, it still has strong security and is appropriate for the IOT control system with strict requirements in security performance [13].

Keunwoo Rhe et al from the Information Communication Security Lab of Korean Sungkyunkwan University proposed an RFID authentication protocol on the basis of inquiry-response mode in the distributed environment of IOT [14]. This protocol solves most deficiencies of the authentication protocols above, and the bidirectional authentication method of inquiry-response mode used in this protocol makes the protocol more secure. At the same time, this protocol solves the out-of-step problem of data at front and rear ends. Thus, it can effectively avoid synchronous attacks, and is appropriate for the identity authentication in the environment of distributed database environment. As this protocol can also effectively resist replay attacks, spoofing attacks, position trailing, and flow analysis attacks which are common in

other hash authentication models, it is currently recognized as a relatively effective IOT RFID identity authentication protocol without any apparent security vulnerabilities.

B. The deficiency of previous authentication protocols

Although the RFID authentication protocol based on inquiry-repose mode is able to solve the typical identity authentication problems of RFID devices in an IOT environment, provided that it is directly applied in an IOT control system, some deficiencies still exist in this protocol:

(1) Control system has a higher requirement for system reliability, and the terminal devices of control system often need backups. But in the identity authentication protocol suggested in literature [15], no information refers to identity authentication for backups of devices.

(2) Under the special environment of IOT control system with a request for strong security, the method of completing identity authentication through the single property confirmation of device ID is still insufficient to satisfy the demands in security [16]. The identity authentication protocol in literature [17] only achieves the authentication towards device ID, and fails to put forward any other extensible authentication properties.

(3) The protocol only describes the protocol process under the circumstance of passing authentication normally, but a complete design in case of an authentication failure is not available. When a device fails to pass authentication, the device is likely to suffer an illegal attack, and the system shall be informed of follow-up and renovation, but the protocol does not provide any relevant alarming measures [18]. Hence, how to design an effective and feasible identity authentication model with

strong security for a combination of the terminal devices in an IOT environment, especially the terminal device features of IOT control system, is the objective of this study.

3. Enhanced Bidirectional Authentication Scheme

A. Improvement measures

Specific improvement measures include the following three aspects:

(1) Introduce back-up terminals: An alternate device is added for each device of access control system, and the alternate device provides with the same functions and communication capacities with the master device, but different ID. When the master device works normally, the alternate device is kept in a hot standby state. When the mater device cannot pass identity authentication resulting from breaking down or suffering attacks, the alternate device takes the place of the mater device at any time to pass identity authentication and complete follow-up work. In the new authentication protocol, some necessary improvements are made, i.e. when the master device fails to pass identity authentication due to some special reasons, the backend database sends incorrect signals to identification reader equipment, and the identification reader equipment will make hot switch to stop communications with the faulted terminals and start the alternate device, as well as sending authentication request to the alternate device.

(2) Introduce a condition monitoring device to increase authentication properties: A condition monitoring device is added for terminal devices, to monitor the operation state of terminal devices when receiving the request of identity authentication such as rated voltage, transmission frequency, communication rate, etc, acquire status information and send to identification reader equipment, and act as the determination

property with encrypted device ID. The introduction of this mechanism not only enhances authentication security, but also can effectively detect whether terminal devices suffer functional damages, which helps to avoid the occurrence that the damaged devices can pass identity authentication, but cannot work properly. In addition, the condition monitoring device is equipped with the hot function for switching and linking with an alternate device when the master device breaks down.

(3) Introduce an alarm mechanism: If a device fails to pass identity authentication and causes mistakes, the system alarm mechanism is introduced to send information to alarm module backstage and inform of alarm type. The designed alarm type here include four categories, and are master device ID information mismatching, alternate device ID information mismatching, master device ID information matching but status information mismatching, and alternate device ID information matching but status information mismatching, respectively.

B. Authentication process

The enhanced bidirectional authentication process towards IOT control system contains the following five steps:

Step 0. Initialization: Each RFID terminal device that accesses to the IOT control system is provided with the sole device ID in the world, and the ID is preserved into the terminal device itself and backend distributed database. In addition, the normal operation state parameters of each terminal device are also preserved in backend database for comparison of state parameters in authentication process. Before identification reader equipment sends an authentication request, both the terminal master device and the alternate device are kept in hot standby state, and the condition monitoring device is linked to the master device.

Step 1. Master device authentication:

a. The identification reader equipment sends the request of identity authentication to the terminal master device and the condition monitoring device, and then sends the generated random numbers to the terminal master device;

b. Condition monitoring device starts to acquire the operation state information of terminal master device, encrypts the information by hash function, and sends the encrypted status information to identification reader equipment;

c. Terminal master device generates a new random number, and cascades its own ID and the two random numbers for encryption by hash function, and then sends the encrypted ID authentication data to the identification reader equipment;

d. The identification reader equipment sends the received information of encryption state, encrypted ID authentication data and the two random numbers to backend database system;

e. For all the preserved device information in backend database, its ID and the two random numbers, as well as normal operation status information of the device are cascaded for hash, to be compared with the received encryption ID authentication data and encryption status information:

e.1 If the two groups of information obtained are matched, the authentication process towards backend terminal device finishes. The server then executes hash for the device ID and the random number generated by terminal device, and send them to the identification reader equipment, switching to Step f;

e.2 If the two groups of information obtained are not matched, the authentication fails, then turning to Step 2;

f. After the identification reader equipment receives the hash data from backend, it sends the data to terminal devices;

g. After terminal devices receive the hash data from the identification reader equipment, they cascade their own ID and the generated random numbers for hash and compare with the received data. If the matching succeeds, the authentication process towards backend devices by terminal devices has passed, and then the whole bidirectional authentication process has completed.

Step 2. The first time of alarming: When the authentication process is forwarded to Step 1 e.2, the authentication fails, and the first time of alarming by system starts on. When backend data fail to find out the devices matched with encrypted ID authentication information, it means the identity of terminal device is illegal, and the system will send alarming information 1 to alarming module, which indicates the illegal identity of master device; when backend data successfully find the devices matched with encrypted ID authentication information, but the status information of encrypted devices cannot be well matched, it means the identity of terminal device is legal but its operating state is incorrect. Maybe it has suffered physical damage, then the system will send alarming information 2 to alarming module, which indicates the incorrect operating status of master device.

Step 3. Device switching, and alternate device authentication: After the system sends the first time of alarming, backend database sends a device switching signal to the identification reader equipment. Next, the identification reader equipment sends a device switching request to the condition monitoring device, and sends a identity authentication request and random numbers to the alternate terminal device. After the identification reader equipment receives the device switching request, it immediately breaks the links with the master device and builds links with the alternate device. Until this step, the switching process of master alternate device has completed, and the follow-up authentication steps are the same as Step 1.

Step 4. The second time of alarming: When the authentication process towards alternate device is forwarded to Step 1 e.2, the authentication fails, and the second time of alarming by the system starts on. When backend data fail to find out the devices matched with encrypted ID authentication information, it means the identity of terminal device is illegal, and the system will send alarming information 3 to alarming module, which indicates the illegal identity of master device; when backend data successfully find the devices matched with encrypted ID authentication information, but the status information of encrypted devices cannot be well matched, it means the identity of terminal device is legal but its operating state is incorrect. It could have suffered physical damage, then the system will send alarming information 4 to alarming module, which indicates the incorrect operating status of master device.

4. FORMALIZED DEFINITION

This section describes the formalized definition on some key words used in the proposed authentication process.

Reader: Identification reader equipment;

TD_{main}: It is the main terminal equipment that is joined up in the control system and provided with RFID label;

TD_{backup}: It is the back-up terminal equipment that is joined up in the control system and provided with RFID label;

$TD_{checker}$: It is the equipment that checks the running status of the terminal equipment.

ID: The ID of the terminal equipment.

Statuslnfo: The operating status information of the terminal equipment;

Reader: The random number generated by the identification reader equipment;

Rtd: The random number generated by the terminal equipment;

$Request_{id}$: The identity authentication requests that the identification reader equipment sends to the terminal equipment and status monitoring equipment;

$Request_{switch}$: Requests to switch equipment;

$Backend_{DB}$: Backend database system;

AlarmingModule: System alarming module;

$Hash_{ID}$(…): The hash function is used to encrypt ID information of equipment. Information in the bracket is the data being encrypted;

$Hash_{st}$(...): The hash function is used to encrypt the operating status information of equipment. Information in the bracket is the data being encrypted;

A→ B:…: It is the data transmitting procedure, indicating that equipment A sends information to equipment B. Following the colon are the information contents;

A← B:...: It is the data acquisition procedure, indicating that equipment A acquires information from equipment B. Following the colon are the information contents;

||: Cascade operator;

$\stackrel{?}{=}$; The comparison of being equal or not;

$Alarming_i$: i=l,2,3,4,: It indicates four pieces of system alarming information.

A. Authentication model

The mode of enhanced bidirectional authentication scheme is as follows:

1) $\mathrm{Re}\,ader \rightarrow TD_{checker} : \mathrm{Re}\,quest_{id}$

2) $\mathrm{Re}\,ader \rightarrow TD_{x} : \mathrm{Re}\,quest_{id}, R_{reader}$

3) $TD_{checker} \leftarrow TD_{x} : StatusInfo$

4) $TD_{x} \rightarrow \mathrm{Re}\,ader : Hash_{id}(ID \| R_{reader} \| R_{td}), R_{td}$

5) $TD_{checker} \rightarrow \mathrm{Re}\,ader : Hash_{st}(StatusInfo)$

6) $\mathrm{Re}\,ader \rightarrow \mathrm{BackendDB} : Hash_{id}(ID \| R_{reader} \| R_{td}), R_{reader}, R_{td}, Hash_{st}(StatusInfo$

7）

$\forall ID_{i,}\ StatusInfo_i\ in\ Backend\ DB\ Hash_{id}(ID_i \| R_{reader} \| R_{id}), R_{reader},$

$R_{id}, Hash_{st}(StatusInfo_i)$

$\forall Hash_{id}(ID_i \| R_{reader} \| R_{id}), Hash_{st}(StatusInfo_i)$

$Hash_{id}(ID_i \| R_{reader} \| R_{id}) ? = Hash_{id}(ID \| R_{reader} \| R_{id})$

$Hash_{st}(StatusInfo_i) ? = Hash_{st}(StatusInfo)$

8）

$if\ \exists ID_{i,}\ StatusInfo_i\ in\ Backend\ DB$

$Hash_{id}(ID_i \| R_{reader} \| R_{id})\ \&\&$

$Hash_{st}(StatusInfo_i) = Hash_{st}(StatusInfo)$

$Backend\ DB \rightarrow \mathrm{Re}\,ader : Hash_{id}(ID_i \| R_{id})$

9)

$\mathrm{Re}\,ader \rightarrow TD_{x} : Hash_{id}(ID_i \| R_{id})$

10)

$Hash_{id}(ID \| R_{id})$

$Hash_{id}(ID_i \| R_{id}) ? = Hash_{id}(ID \| R_{id})$

The above Steps 1 to 10 are the model under the condition that the first authentication is approved. Therein, x=main, namely the terminal equipment is the main equipment. The authentication process for the approved first authentication is shown in Figure 1. Note: the picture only describes the data transmitting process, and no calculation and judge process are described. Thus the serial numbers differ from the above-mentioned formalized description.

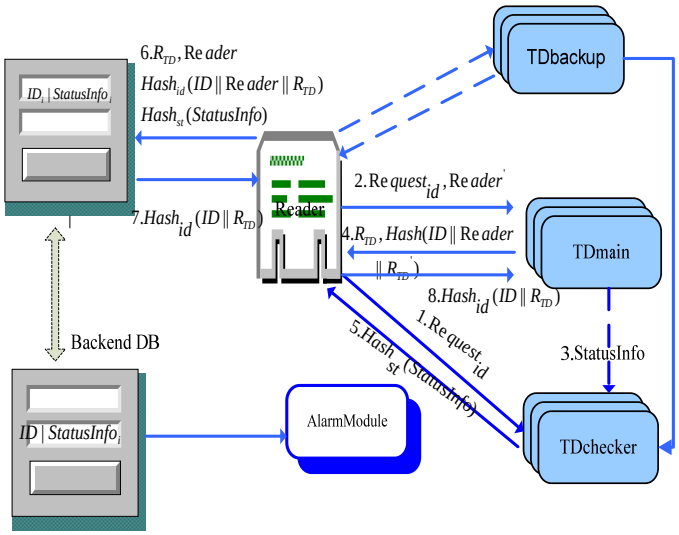

Fig.1. Identity authentication process: the first authentication is approved

When the authentication comes to Step 8, unapproved authentication may occur. Following is the description for the model under the condition that the first authentication is unapproved.

1)-7)(x=main)
8')
$a.\ if\ \forall\ ID_i\ in\ backend\ DB,$
$Hash_{id}(ID_i \| R_{reader} \| R_{TD}),$
$BackendDB \rightarrow AlarmModule : Alarm_1$
$b.\ if\ \exists ID_i\ in\ Backend\ DB, Hash_{id}(ID_i \| R_{reader} \| R_{id}) =$
$Hash_{id}(ID \| R_{reader} \| R_{id}) \&\& Hash_{st}(StatusInfo_i) \neq$
$Hash_{st}(StatusInfo_i)$
$Backend\ \mathrm{DB} \rightarrow AlarmModule : Alarm_2$
$Backend\ \mathrm{DB} \rightarrow \mathrm{Re}ader : \mathrm{Re}quest_{switch}$

9') $\mathrm{Re}ader \rightarrow TD_{checker} : \mathrm{Re}quest_{switch}$
2)-10)(x=backup)

Above is the model under the condition that the first authentication is unapproved but the second authentication is approved after the equipment is switched. In such case, the authentication process is shown in Figure 2. It starts from the alarming signal of system upon the disapproval of first authentication.

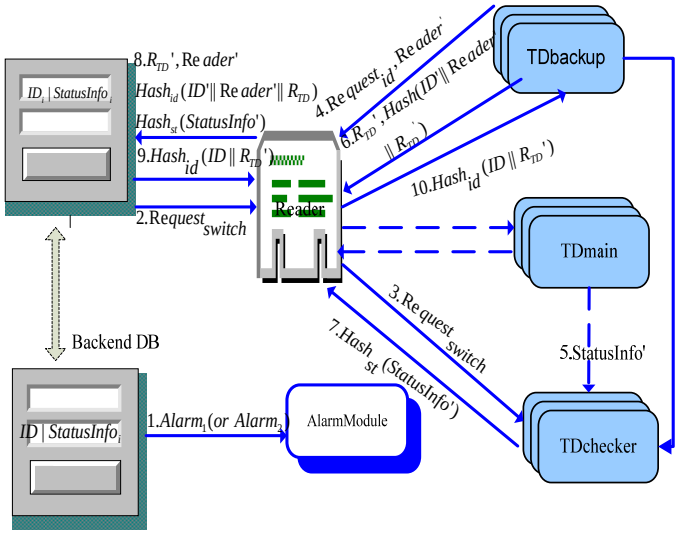

Fig.2. Identity authentication process: the second authentication is approved

When it proceeds to Step 8 and the second authentication fails to be approved again, the model is described as follows:

1)-7)(x=main)

8')

$a.\ if\ \forall\ ID\ \ in\ Backend\ DB,$

$Hash_{id}(ID_i \| R_{reader} \| R_{id}) \neq Hash_{id}(ID \| R_{reader} \| R_{id})$

$Backend\ DB \rightarrow AlarmModule : Alarm_1$

$b.\ if\ \exists ID_i\ in\ Backend\ DB, Hash_{id}(ID_i \| R_{reader} \| R_{id}) =$

$Hash_{id}(ID \| R_{reader} \| R_{id}) \&\& Hash_{st}(StatusInfo_i) \neq$

$Hash_{st}(StatusInfo_i)$

$Backend\ \mathrm{DB} \rightarrow AlarmModule : Alarm_2$

$Backend\ \mathrm{DB} \rightarrow \mathrm{Re}ader : \mathrm{Re}quest_{switch}$

9') $\mathrm{Re}ader \rightarrow TD_{checker} : \mathrm{Re}quest_{switch}$

2)-7)(x=backup)

8")

$a.\ if\ \forall\ ID_i\ \ in\ Backend\ DB,$

$Hash_{id}(ID_i \| R_{reader} \| R_{id}) \neq Hash_{id}(ID \| R_{reader} \| R_{id})$

$Backend\ DB \rightarrow AlarmModule : Alarm_3$

$b.\ if\ \exists ID_i\ in\ Backend\ DB, Hash_{id}(ID_i \| R_{reader} \| R_{id}) =$

$Hash_{id}(ID \| R_{reader} \| R_{id}) \&\& Hash_{st}(StatusInfo_i) \neq$

$Hash_{st}(StatusInfo_i)$

$Backend\ \mathrm{DB} \rightarrow AlarmModule : Alarm_4$

The authentication process is shown in Figure 3, it starts from the alarming signal of system upon the disapproval of first authentication.

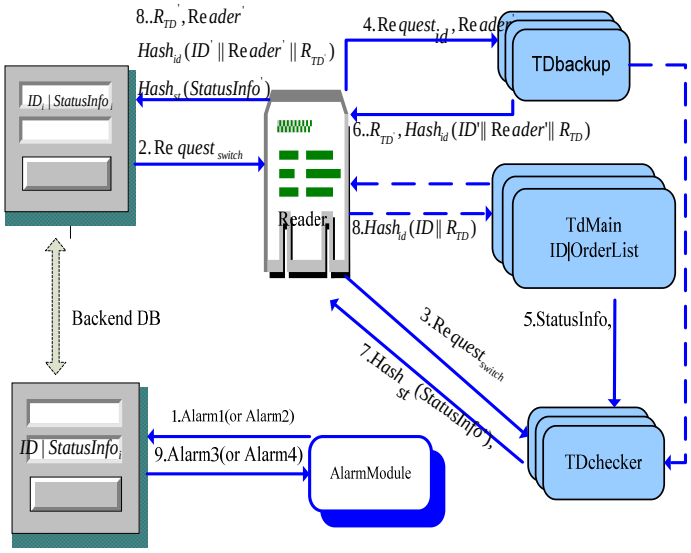

Fig.3. Identity authentication process: the second authentication is not approved

5. AUTHENTICATION MODEL EXTENSION

The existing RFID authentication protocol presented in literature [19] is applicable to an IOT distributed environment, and is on the basis of inquiry-response, which puts forward the bidirectional authentication methods between the IOT control system collecting points and backend combined with some specific security requirements of IOT control system.

In the actual IOT collecting terminal communications environment, to ensure the authenticity of the communication source, some other properties in addition to the legitimacy of the identity of both sides often have to be considered, mainly including the location information of collection points and the judgment on the contents of the control instruction itself. Because of the relevance between data collection work in data collection points and their positions, the position information has a vital

significance to the authenticity of terminal communication source as its identity information does. The attacker could disguise itself as a collection point with legitimate identity and send data to the back-end system from different locations, which results in attack or sabotage. On the other hand, once the position of the collection points with legitimate identity has changed, the collected data themselves would lose practical significance. Therefore, only when both legitimate identity and correct position are guaranteed, the data information transferred from collection points can be real and effective.

For the back-end control terminals, in addition to ensuring the legitimacy of their identity, the correctness of control commands sent by the back-end control terminals should be ensured. Control terminals with legal identity are likely to result in the destruction of the system due to the wrong control command. For example, in the event that malicious control commands in addition to normal control ones are sent, or the normal commands whose contents are within the normal scope are frequently sent, it would result in cumulative error or control failure. Therefore, only the authenticity and validity of three factors, identity, location and contents, are guaranteed, the source security of system can obtain the greatest assurance.

Based on the above analysis, and on the basis of guaranteeing the authenticity of the communication source, namely the legitimate identity of both the sides of communications, the bidirectional authentication schemes previously proposed can be extended, and the authentication of collection points' location information and the judgment mechanism for the control command contents of the back-end control side can be added so as to further ensure the security of communication process and the effectiveness of communication contents. The recognition authentication of collection points' location information can be preceded with the identity authentication at the

same time, and the location information can be part of the authentication contents. One possible scheme is that proceeding the monitoring of collection points' location information and the test of its operational status, or implementing the monitoring of collection points' location information as part of the status information.

The judgment on the control command contents of the back-end control site can be carried out after the authentication has completed, and control instructions are sent to collection points by the back-end through the identification reader equipment, and then the collection points determine the legality of the control commands, thus performing actions based on the results. One possible implementation is to restore legitimate control instruction lists in the terminal collection points so as to verdict the received control commands. In the event that the control command is within the legitimate scope of the commands, the instruction will be executed; otherwise, it will not be implemented. In addition, the threshold value of repeated reception frequency for specific legitimate commands can be set. When the command is repeatedly and continuously sent, and the frequency exceeds the threshold value, the collection points in the terminal will stop receiving the corresponding instructions. The diagram of the safety certification process based on this idea is shown in Figure 4.

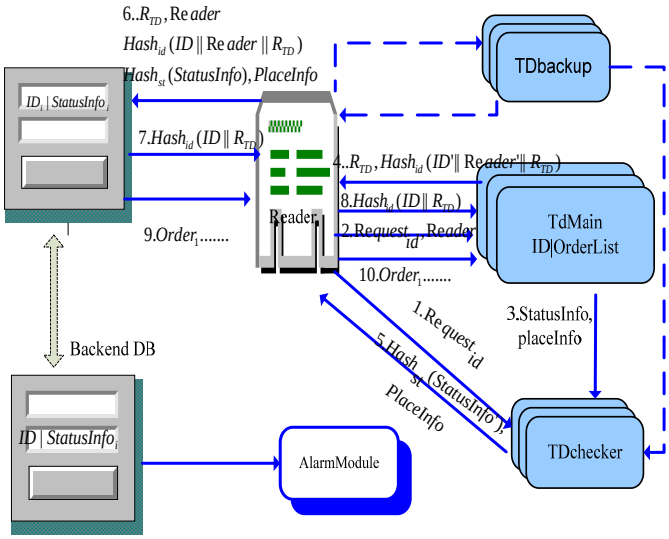

Fig.4. The extended secure authentication process

6. Evaluation and Simulation

The data setting of simulation environment is first described in this section.

The simulation environment consists of two terminal RFID devices. The ID uses the EPC-96 coding scheme [20], and the IDs of the two devices are set as follows:

ID_{main} 02 0003458 00018F 000156DC0

ID_{backup} 02 0003458 00018F 000156DC1

The terminal equipment and the identification reader equipment generate random numbers, respectively, and the format is 8 bit binary code. The status information of terminal equipment is 32 bit binary code. The default status information is as follows:

StatusInfo IA300E0D

MD5 encryption algorithm is used to encrypt ID and the Hash encryption of random numbers, and SHA1 encryption algorithm is utilized to encrypt the status information of terminal equipment and the Hash encryption of random numbers. In practical operation, all the data should be encrypted in the form of hexadecimal character string.

A. Simulation scenario 1

The first authentication is approved. The Reader sends the $Request_{id}$ signal to TD checker and generates a random number 01101111(6F) in the meantime. Reader sends $Request_{w}$ signal to main terminal equipment TD_{main} and the random number lUder. The main terminal equipment TD_{main} generates a random number Rto 01110110(76) upon the reception of the data, and cascades its ID and two random numbers, so that the following is obtained:

4AD5F561449978577C7FD15C3D0806B1DE3509AD

Then MD5 encryption algorithm is used to proceed Hash encryption, obtaining 32 bit encrypted character string:

358216D96314FEE7A0F53B46D853206F

The main terminal equipment sends this character string and Rtd to the Reader. Meanwhile, $TD_{checker}$ acquires the status information of main terminal equipment TD_{main} StatusInfo IA300E0D. And then SHA1 encryption algorithm is used to proceed Hash encryption, yielding 40 bit encrypted character string:

FFBDC2A6B552A3A24CC47FD64BBBD5E4A929A5ER

$TD_{checker}$ sends the encrypted character string to the Reader. The Reader sends the two random numbers and two groups of encrypted character strings to the back-end database Backend DB. The Backend DB cascades all the stored ID information one by one and proceeds Hash operation, as well as compares them with received ID encrypted characters to find the matching value. Also, it proceeds SHA1 Hash operation on the StatusMo information corresponding to this ID, and compares them with the received Statuslnfo encrypted character string. After the comparison and matching, the back-end database cascades the matched ID and Rtd, then the following is obtained:

0233448956FDCE7845890

MD5 encryption algorithm is used to proceed on this character string, resulting in 32 bit encrypted character string:

DA3E5BA0BDC060E3881F864B33616903

The back-end database sends the encrypted character string to the Reader, and the Reader sends the received character string to the main terminal equipment TD_{main}. The TD_{main} cascades its ID and the random number Rtd generated by itself, and proceeds Hash operation, thus obtains the following 32 bit encrypted character string:

DA3E5BA0BDC060E3881F864B33616903

This character string is compared with the received encrypted character string. If the match is successful, the whole authentication process is completed successfully.

B. Simulation scenario 2

The first authentication is unapproved, and the system gives alarming for the first time, but the second authentication is approved. The main terminal equipment suffers a replay attack. In the previous authentication process, it is 01001001(89) and the Rtd is 10110110(B6). The attacker eavesdrops the encrypted ID character string *E08A4B78D706D0E867C4A3790A34F436* and Rtd 10110110(B6) sent to the Reader (old) by the main terminal. In the next authentication, the Reader generates a random number Reader 01001001(89), and sends $Request_{id}$ signal and random numbers to TD_{main}, and sends $Request_{id}$ signal to TDcheckCT as well. This time the attacker sends the encrypted ID character string *6855267DF61E69E8ABB6797D74EF42B3* and Rtd 10110110(B6) intercepted and captured in the previous authentication process to pretend the normal terminal equipment. Meanwhile, $TD_{checker}$ sends the 40 bit encrypted character string

5A61498D5DDD98AAE0D9676891858A3AA1B77C1E

to the reader after encrypting the status information of the real terminal equipment. Afterwards, the Reader sends RreadeP Rtd and two encrypted character strings to the Backend DB. The Backend DB cascades all the stored ID information with Rtd one by one and proceeds Hash operation, as well as compares them with received ID encrypted character string *BCC9CB4FB13456ED8B571E2D4BB273F5*.

If Rreader(old) $\neq$ Rreader, the system fails to find the matching value. At this time, the Backend DB sends the class 1 alarming signal to AlarmingModule, and sends $Request_{switch}$ to the Reader. The Reader then sends the $Request_{switch}$ to the TD_{check}, and starts a new round identity authentication with TD_{backup}.

The Reader generates a random number Rreader' 11000111(C7), and sends the $Request_{id}$ signal and the random number to TD back-up terminal equipment TD_{backup}. The TD_{backup} generates the random number Rtd' 01110111(77) upon the reception of the data, and cascades its ID_{backup} and two random numbers, so that the following is obtained:

013333A8900016F000169DC1E737

Then MD5 encryption algorithm is used to proceed Hash encryption, obtaining 32 bit encrypted character string:

FA573DACE6514BB74A1B6BCDFGHJ0E47

The TD_{backup} sends this character string and Rtd' to the Reader. Meanwhile, $TD_{checker}$ acquires the status information of TD_{backup} IA300E0D. And SHA1 encryption algorithm is used to proceed Hash encryption, resulting in 40 bit encrypted character string:

FFBDC2A6B552A3A24CC47FD64BBBD5E4A929A5TD

The $TD_{checker}$ sends the encrypted character string to the Reader. The Reader sends the two random numbers and two groups of encrypted character strings to the back-end

database Backend DB. The Backend DB cascades all the stored ID information one by one and proceeds MD5 Hash operation, as well as compares them with received ID encrypted character to find the matching value. Also, SHA1 Hash operation is performed on the StatusInfo corresponding to this ID, which is compared with the received Statuslnfo encrypted character string. After the comparison and matching, the back-end database Backend DB cascades the matched ID and Rtd, then the following is obtained:

016666A8900016F000169DC148

MD5 encryption algorithm is used to proceed this character string, obtaining 32 bit encrypted character string:

BF95C1E11F21298D6B701C77777F1996

The back-end database sends the encrypted character string to the Reader, and the Reader sends the received character string to the back-up terminal equipment TD_{backup}. The TD_{backup} cascades its ID_{backup} and the random number Rtd generated by itself, and proceeds Hash operation, thus obtains the following 32 bit encrypted character string:

BF95C1E11F21298D6B701C77777F1996

This character string is compared with the received encrypted character string. If the match is successful, the whole authentication process is completed successfully.

C. Simulation scenario 3

The first authentication is unapproved, and the system then gives class 2 alarming. When the second authentication is unapproved, the system gives class 3 alarming. It simulates that the main terminal equipment suffers physical damage and the back-up terminal equipment suffers a spoofing attack. The Reader sends the $Request_{id}$ signal to $TD_{checker}$ and generates the random number Rreader 01111010(7A) in the meantime. It then sends $Request_{id}$ signal and random number Rreader to main terminal equipment

TD_{main}. The main terminal equipment TD_{main} generates the random number RTD 11110011 (F3) upon the reception of the data, and cascades its ID and two random numbers, so that the following is obtained:

01OOOOA8900016F000729DC05AF1

MD5 encryption algorithm is then used to proceed Hash encryption, obtaining 32 bit encrypted character string:

704E281FEC9E2DD4FC33 51DF364B01F2

The main terminal equipment sends this character string and Rtd to the Reader. Meanwhile, $TD_{checker}$ acquires the status information of main terminal equipment TD_{main}. The TD_{main} suffers physical damage, thus an error occurs in its operation status. The value of operation information acquired by $TD_{checker}$ is 1A5AC2B0, and then SHA1 encryption algorithm is used to proceed Hash encryption, obtaining 40 bit encrypted character string:

C3D6639DCB0482068859B9650E51DD485F8A7AAB

$TD_{checker}$ sends the encrypted character string to the Reader. The Reader sends the two random numbers and two groups of encrypted character strings to the back-end database Backend DB. The Backend DB cascades all the stored ID data one by one and proceeds Hash operation, and compares them with received ID encrypted characters to find the matching value. Also, SHA1 Hash operation is performed on the Statuslnfo corresponding to this ID, which is compared with the received Statuslnfo encrypted character string. However, the operation status information of TD_{main} is inconsistent with the default status information, so the Statuslnfo encrypted character string corresponding to the matched ID is not matched with the received Statuslnfo encrypted character string. At this time, the Backend DB sends the class 2 alarming signal to AlarmingModule, and sends $Request_{switch}$ to the Reader. The Reader then

sends $Request_{switch}$ to TD_{check}, and starts a new round identity authentication with TD_{backup}. In the previous authentication process for TD_{backup}, the attacker pretended the Reader to send $Request_{id}$ and Rreader(fake) 01111111(7E) to TD_{backup}, and received the ID encrypted character string 5BA8BE38AA08C88AEC0A4833348D9CD0 and Rtd' 11000011(C3) sent back by TD_{backup}.

In the event that authentication for the main terminal equipment fails again this time, it switches to the back-up terminal equipment TD_{backup} again. When the reader sends Requestid and Rread' 00101001 (2B) to TD_{backup}, the attacker sends the encrypted ID character string 3AB8BE38CCC8C88AEC0A4833328D9CD0 and Rtd' 11010011(D3) intercepted and captured to pretend a normal terminal device. Meanwhile, TDchecker sends the 40 bit encrypted character string 7645498D5CCC98AAE0D9676891858A3BB1C77C1E to the reader after encrypting the status information of the real terminal equipment. Afterwards, the Reader sends RreadeP Rtd and two encrypted character strings to the Backend DB. The Backend DB cascades all the stored ID data with Rreader' and Rtd' one by one and performs Hash operation, as well as compares them with received ID encrypted character string 4AB8BE38DD08C88AEC0A4811128D9CD.

If Rreader(fake) $\neq$ Rreader', the system fails to find the matching value. At this time, the Backend DB sends the class 3 alarming signal to AlarmingModule. So far the whole authentication process is over, and it fails.

D. Simulation scenario 4

The first authentication is unapproved, and the system gives class 1 alarming. When the second authentication is unapproved, the system gives class 4 alarming. It simulates that the main terminal equipment suffers a replay attack and the back-up

terminal equipment suffers physical damage. In the previous authentication process, the Rreader(old) is 00111100(3C) and the Rtd is ! 0101011 (AB). The attacker eavesdrops the encrypted ID character string FD2273576AF588AADF58B0384586FD48 and Rtd lOlOlOll(AB) sent to the Reader by the main terminal.

In the next authentication, the Reader generates a random number Rreato 10110101(85), and sends $Request_{id}$ signal and random numbers to TD_{main}, and sends $Request_{id}$ signal to $TD_{checker}$ as well. At this time, the attacker sends the encrypted ID character string FD2273576AF588AADF58B0384586FD48 and Rtd lOlOlOll(AB) intercepted and captured in the previous authentication process to pretend a normal terminal device. Meanwhile, $TD_{checker}$ sends the 40 bit encrypted character string A61498D5CCC98AAE0D9676891858A3AA1B77C1E to the reader after encrypting the status information of the real terminal equipment. Afterwards, the Reader sends RreadeP Rtd and two encrypted character strings to the Backend DB. The Backend DB cascades all the stored ID data with Rtd one by one and performs Hash operation, as well as compares them with received ID encrypted character string FD2273576AF588AADF58B0384586FD4.

If Rreader(old) $\neq$ Rreader, the system fails to find the matching value. At this time, the Backend DB sends the class 1 alarming Alarming1 signal to AlarmingModule, and sends $Request_{switch}$ to the Reader. The Reader then sends the $Request_{switch}$ to TD_{check}, and starts a new round identity authentication with TD_{backup}. The Reader generates random number Rreader' 10011111(9F), and sends the $Request_{id}$ signal and the random number to back-up terminal equipment TD_{backup}. TD_{backup} generates the random number Rtd' 111O1OO1(EB) upon the reception of the data, and cascades its ID and two random numbers, so that the following is obtained:

010000A8900016F000169DC19FEB

MD5 encryption algorithm is then used to perform Hash encryption, obtaining 32 bit encrypted character string:

42A7E6F1EE451BA1006706C93E869A39

TD_{backup} sends this character string and Rtd' to the Reader. Meanwhile, $TD_{Checker}$ acquires the status information of TD_{backup}. TD_{backup} suffers physical damage, thus an error occurs in its operation status. The value of operation information acquired by $TD_{checker}$ is 1AEB1026, and SHA1 encryption algorithm is then used to perform Hash encryption, obtaining 40 bit encrypted character string:

F97A9CB86CA5C032B8933EDECD4FEF38C801726F

$TD_{checker}$ sends the encrypted character string to the Reader. The Reader sends the two random numbers and two groups of encrypted character strings to the back-end database Backend DB. The Backend DB cascades all the stored ID data one by one and performs MD5 Hash operation, as well as compares them with received ID encrypted character to find the matching value. Also, SHA1 Hash operation is performed on the StatusInfo corresponding to this ID, which is compared with the received Statuslnfo encrypted character string.

However, the operation status information of TD_{backup} is inconsistent with the default status information, so the Statuslnfo encrypted character string corresponding to the matched ID is not matched with the received Statuslnfo encrypted character string. At this time, the Backend DB sends the class 4 alarming signal to Alarming Module, and sends Request switch to the Reader. So far the whole authentication process is over with failure.

7. CONCLUSION

This paper proposes an enhanced bidirectional identity authentication protocol for RFID communications in IOT with good security and privacy protection. The proposed authentication protocol can verify data content even position, resist replay attacks and denial of service attacks, and achieve the data synchronization between the front and rear ends with good forward security. The improved authentication protocol not only improves the reliability, but also effectively resists most security threats; it is a feasible RFID security authentication protocol. In addition, in the aspect of hardware complexity, the system needs not to add an additional encryption circuit in the terminal hardware, *i.e.* low dependence on hardware. This scheme can meet the design requirements of IOT in three aspects: security, efficiency and cost. It is a kind of identity authentication scheme which is suitable for IOT.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China under Grant 61272469, the Key Programs of Hubei Educational Committee under Grant D20144403, the Science and Technology Study Programs of Hubei Educational Committee under Grant B2015087, the Innovative Talents Project of Hubei Polytechnic University under Grant 12xjz24C, and the Outstanding Youth Science and Technology Innovation Team of Hubei Polytechnic University under Grant 13xtz10.

References

[1] IBM and European Union Launch Joint Research Initiative for Cloud Computing[EB/OL].http://www03.ibm.com/press/us/en/pressrelease/23448.wss.

[2] Li, Jung-Shian; Hsieh, Che-Jen; Lin, Husan-Yeh. A hierarchical mobile-agent-based security operation center. International Journal of Communication Systems, 10.1002/dac.2323, 2013.12.

[3] Andr H, Lagar-Cavilla S, Whitney J A, et al. SnowFlock: Virtual Machine Cloning as a First-Class Cloud Primitive. ACM Trans. Comput. Syst., 2011, 29(1):1-45.

[4] Kim, Sok-Hyong; Kim, Dong-Wook; Suh, Young-Joo. A survey and comparison of multichannel protocols for performance anomaly mitigation in IEEE 802.11 wireless networks. International Journal of Communication Systems, 10.1002/dac.1396, 2013.10.

[5] Google and IBM Announce University Initiative to Address Internet-Scale Computing Challenges [EB/OL]. http://www03.ibm.com/press/us/en/pressrelease/22414.wss.

[6] Van Loan C F. Computing the CS and the generalized singular value decompositions. Numer. Math., 1985, 46: 479-492.

[7] Lee S., Hwang Y,, Lee D., et al, Efficient authentication for low-cost RFID systems, Computational Science and Its Applications, International Conference on Computational Science and Its Applications (ICCSA2005). Berlin:Springer-Verlage, 2005, pp.619-627.

[8] Paige C C, Saunders M A. Towards a generalized singular value decomposition. SIAM J. Numer.Anal., 1981, 18:398-405.

[9] Juels A, Pappu R., Squealii Euros: Privacy protection in RFID-enabled banknotes, In Financial Cryptography, Springer, 2003, pp. 103-121.

[10] Weis S, Sarma S., Rivest R., et al, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing, 2003, pp. 50-59.

[11] Haidine, Abdelfatteh, Design of reliable fiber-based distribution networks modeled by multi-objective combinatorial optimization .International Journal of Communication Systems, 10.1002/dac.1391, 2013 .10.

[12] Chen, Bae-Ling; Kuo, Wen-Chung; Wuu, Lih-Chyau Robust smart-card-based remote user password authentication scheme International Journal of Communication Systems, 10.1002/dac.2368 2014.2.

[13] Dusit N, Ekram H. A Noncooperative Game-Theoretic Framework for Radio Resource Management in 4G Heterogeneous Wireless Access Networks. IEEE Transactions on Mobile Computing, 2008, 7(3): 332-345.

[14] He, Daojing; Chen, Chun; Chan, Sammy; Bu, Jiajun, Strong roaming authentication technique for wireless and mobile networks, International Journal of Communication Systems, 10.1002/dac.1387, 2013.8.

[15] Virapanicharoen J, Benjapolakul W. Fair-efficient threshold parameters selection in call admission control for CDMA mobile multimedia communications using game theoretic framework. Consumer Communications and Networking Conference, 2005, 439-444.

[16] Mavromoustakis, Constandinos X. Mitigating file-sharing misbehavior with movement synchronization to increase end-to-end availability for delay sensitive streams in vehicular P2P devices, International Journal of Communication Systems, 10.1002/dac.2335, 2013.12.

[17] Rhee K,, Kwak J.,Kim S., et al, Challenge-response based RFID authentication protocol for distributed database environment, Proceedings of the 2nd International Conference on Security in Pervasive Computing, 2005, pp.70-84.

[18] Gohar, Moneeb; Jung, Heeyoung; Koh, Seok-Joo. Distributed mapping management of identifiers and locators in mobile-oriented Internet environment Internet environment. International Journal of Communication Systems, 10.1002/dac.2346 , 2014.1.

[19] Varaprasad, G. Stable routing algorithm for mobile ad hoc networks using mobile agent, International Journal of Communication Systems, 10.1002/dac.2354, 2014.1.

[20] Huang, Ding-Jie; Teng, Wei-Chung; Yang, Kai-Ting. Secured flooding time synchronization protocol with moderator. International Journal of Communication Systems, 10.1002/dac.2614 , 2013.9.