Enhance Safety of Telecare Medicine Information System With A RFID-based Authentication Scheme

[1]He Jialiang, [2]Xu Zhiqiang and [3]Xu Xiaoke

*[*1,3]1 College of Information and Communication Engineering, Dalian Nationalities University, China*
[2]2 Department of digital media technology, Sichuan College of Media and Communications, China
E-mail: urchin2012@sina.com; starsep928@yahoo.com.cn; xuxiaoke@sohu.com

Abstract

Medication Safety is an important issue for patients. Telecare medicine information system using RFID technology is used to reduce the medication errors and improve the patient safety. In this paper, we show the weaknesses of Keerti Srivastava et al.'s authentication scheme. In order to enhance medication safety for patients, we propose a new lightweight RFID authentication scheme based on dynamic ID. This scheme only requires O(1) work to identify and authenticate a tag in the backend server, so it is practical, secure and efficient for health care domain.

Keywords: *Radio frequency identification; Authentication scheme; Medication safety; Telcecare*

1. Introduction

Radio Frequency Identification (RFID) is a technology with objectives to enable the non-contact, automatic and unique identification of objects using radio waves. It plays an important role in the medical management domain for improving the patient safety, it ensure that patients receive the correct medications and medical devices, prevents the distribution of counterfeit drugs and medical devices, manage assets such as hospital equipment, medical records, etc., track patients and staff and provide data for medical information systems[17]. So, designing a RFID authentication scheme which has well security and high efficiency becomes a hot research field.

With the increasing need of patient safety, RFID systems that ensure communication through a wireless channel are popular in pharmaceutical industry or in hospitals [17]. Usually, a typical RFID system consists of RFID tags, RFID readers and the server. In a medical RFID system, tags are labeled on the drugs, equipments and containers and also patients wear RFID tagged wristbands (Pallet tag) so that the drug information and patient information can be checked for integrity [17]. The consequence of attack from an adversary may endanger the safety of the patient seriously, so a secure and efficient medication management scheme is needed in health care domain.

In order to enhance medication safety for patients, we will propose a new dynamic ID RFID authentication protocol based on one way hash function. This protocol can resist common security and privacy requirements for the tag and the server. Especially, it only requires O (1) work to identify and authenticate a tag in the server, so has well performance.

The rest of the paper is organized as follows: section2 briefly review the related work of RFID security protocol and its application in the domain of medication management. Our proposed RFID authentication protocol is presented in section3, followed by security analysis in section4. Finally, we conclude the paper in section5.

ISSN: 1738-9976 IJSIA

2. Related Work

RFID security protocols have been investigated for about ten years. In 2003, Juels et al. proposed a scheme towards the privacy and security is to "kill" a RFID tag at a point of sale[9], however, it is impracticable as all the previous details of communication is lost. In 2004, Henrici and Muller proposed a dynamic ID scheme based on one way hash function [10], for protecting the tag from location privacy. However, after an unsuccessful session, it replies with the same hash ID, which makes it traceable and vulnerable to impersonation attack. In 2006, Lim and Kwon proposed a mutual authentication scheme to provide backward and forward un-traceability [11], however, this scheme isn't meet tag untraceability as they have announced. In 2007, Chien presented an ultra-lightweight mutual authentication protocol to provide strong authentication and strong integrity [12], however, this protocol is also vulnerable to resist de-synchronization attack, DOS attack, and more seriously, it isn't meet tag untraceability. In 2009, Lee et al. proposed an ultra-lightweight RFID protocol with mutual authentication as an improvement to Gossamer protocol [13]. However, it is vulnerable to resist disclosure attack, cloning attack, de-synchronization attack, and it isn't meet tag untraceability. In 2013, Sonam Devgan Kaul and Amit K. Awasthi presented a RFID authentication protocol to check the accuracy of the association of drug and patient information to enhance medication safety [17], however, their scheme has some shortcomings in security and performance [19]. There many works [2-8, 14-16] have been proposed that give secure implementation of certain healthcare functions.

The notations used in this paper are summarized in Table 1.

Table 1. The Notations Used in This Paper

Symbol	Meaning
ID	Identifier of a tag (The length is l)
k	Secret value mutually shared by back-end server and tag (The length is l)
Data	Information of the tagged object
H()	An one-way hash function, H: $\{0,1\}^{l*} \rightarrow \{0,1\}^{l}$ (The length of output is l)
PRNG()	The pseudo random number generator (The length of output is l_R, usually $l_R < l$)
$\oplus$	XOR operator
$\|\|$	Concatenation operator
R	Random number
Rr	The random number generated by the reader (The length is l_R)
Rt	The random number generated by the tag(The length is l_R)
T	Current date and time of input device
θ	Expected time interval for a transmission delay
F	Failure information of authentication
Pre-x	The previous value of x
A→B:M	A sends message M to B

In 2014, Keerti Srivastava et al. proposed a hash based mutual RFID tag authentication protocol in telecare medicine information system to ensure the accuracy of medication safety[20], Let’s review this scheme.

This protocol consists of three phases: Initialization Phase, Authentication Phase and Updating Phase.

Initialization phase:

(1) In this phase, the server assigns a tag identity $ID_i \in \{0, 1\}^1$ and the secret key $k_i \in \{0, 1\}^1$, for all tags, stores (ID_i, k_i) in both the tag memory and in the database of the server. A RFID reader has no knowledge of the pair (ID_i, k_i).

(2) The tag and reader have its own random number generator.

(3) The server, reader, and each tag has a current date and time of input device.

(4) The server collects the information ID, k_j and k_{j-1} for each tag.

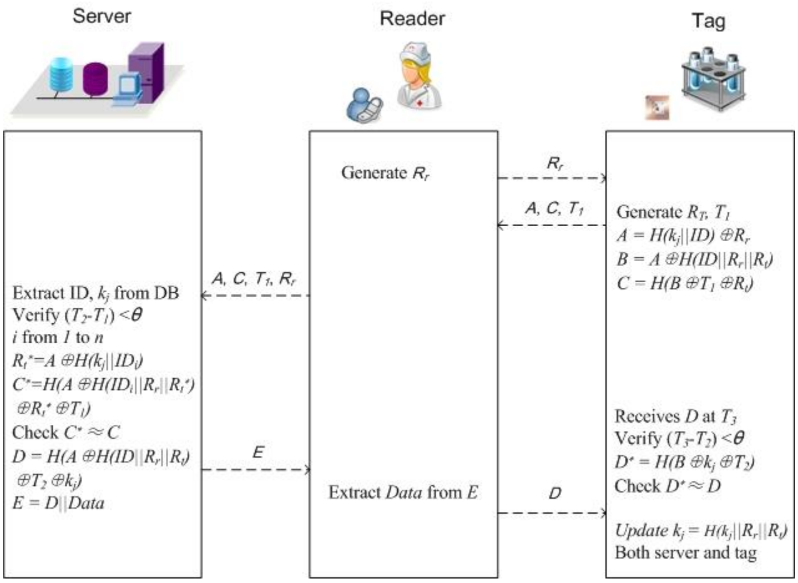

Server
Reader
Tag
Generate R_r
R_r
A, C, T_1
Generate R_T, T_1
$A = H(k_j||ID) \oplus R_r$
$B = A \oplus H(ID||R_r||R_t)$
$C = H(B \oplus T_1 \oplus R_t)$
A, C, T_1, R_r
Extract ID, k_j from DB
Verify $(T_2\text{-}T_1) < \theta$
i from 1 to n
$R_t^* = A \oplus H(k_j||ID_i)$
$C^* = H(A \oplus H(ID_i||R_r||R_t^*)$
$\oplus R_t^* \oplus T_1)$
Check $C^* \approx C$
$D = H(A \oplus H(ID||R_r||R_t)$
$\oplus T_2 \oplus k_j)$
$E = D||Data$
E
Extract *Data* from E
D
Receives D at T_3
Verify $(T_3\text{-}T_2) < \theta$
$D^* = H(B \oplus k_j \oplus T_2)$
Check $D^* \approx D$
Update $k_j = H(k_j||R_r||R_t)$
Both server and tag

Figure 1. Authentication Phase of this Protocol

Authentication phase: In this phase, Server, reader and tag follow the following steps to mutually authenticate each other.

(1)When the Reader wants to communicate with the tag, the reader generate a pseudo random number $R_r \epsilon \{0, 1\}^1$ and send R_r to the tag via an insecure communication channel.

(2)After receiving the random number R_r, the tag generates a pseudo random number $R_t \epsilon \{0, 1\}^1$ and the current time stamp T_1, then computes authentication factor A, B and C, $A = H(k_j|| ID) \oplus R_r$, $B = A \oplus H(ID||R_r||R_t)$, $C = H(B \oplus T_1 \oplus R_t)$ subsequently sends the request message (A, C, T_1) to the reader.

(3)After receiving the message (A, C, T_1), the reader sends the response message (A, C, T_1, R_r) to the server after reforming the message by adding R_r.

(4)After receiving the required information about tag from database, the server performs the following calculation using the saved information of each tag.

The server firstly verify the validity of time stamp T_1 by verifying $(T_2 – T_1) < \theta$ to judge the authentication request. If it finds correct, then the server computes $R_t^* = A \oplus H(k_j||ID)$, checks $C^* = H(A \oplus H(ID||R_r||R_t^*) \oplus R_t^* \oplus T_1) \approx C$, repeats above steps until C^* is the same as a C extracted from response message sent by reader. If so, then right tag is found. The server computes $D = H(A \oplus H(ID||R_r||R_t) \oplus T_2 \oplus k_j)$, $E = D||Data$, then delivers the message E to the reader.

If the server fails to find the right tag, it is judged an abnormal authentication message and the session is terminated.

(5)After receiving E from server, the reader extracts Data from $E = Data||D$ and sends the remaining message D to the tag.

Finally, the tag authenticates the server by following calculation based on the message D at time T_3 received from the reader. If $(T_3 − T_2) < \theta$, then the tag computes $D^* = H(B \oplus k_j \oplus T_2) \approx D$,then tag authenticates the server by confirming that the above calculated hashed value is identical to received D from the reader.

Updating phase: After achieving the mutual authentication, the server and the tag computes a new dynamic identity and secret key for the next session so that the tag become anonyms and it cannot be traced.

(1)The tag computes $k^{new} = H(k_j||R_r||R_t)$, and updates (k_i) with (k^{new}).

(2)The server computes $k^{new} = H(k_i||R_r||R_t)$, and updates (k_i) with (k^{new})..

This scheme is a dynamic ID based lightweight RFID authentication protocol. However, there some weaknesses in performance and security about this scheme as follows:

(1)Scalability is a desirable property in almost any system, enabling it to handle growing amounts of work in a graceful manner[1]. A scalable RFID system should be able to handle large numbers of tags without undue strain, and a scalable RFID protocol should therefore avoid any requirement for work proportional to the number of tags[18]. In the step 4 of authentication phase, the server the server computes $R_t^* = A \oplus H(k_j||ID)$, checks $C^* = H(A \oplus H(ID||R_r||R_t^*) \oplus R_t^* \oplus T_1) \approx C$, repeats above steps until C^* is the same as a C extracted from response message sent by reader. That is to say, the server must perform a linear search of its database to identify and authenticate a tag. For each legal tag entry that in the database in turn, it computes the lightweight cryptographic function three times that would be produced by that tag and compares it with the received authentication application. Each tag which is found in database successfully it would perform 3*((n+1)/2) (Only column (k_j) would be calculated for comparision) times record-by-record hash function calculation for comparision, such a linear search runs in O(n) time, where n is the number of elements in the database. More seriously, Each tag which is found in database failed it would perform 2*3*((n+1)/2) times (Both column pair (k_j) and pair (k_{j-1}) would be calculated for comparision) record-by-record hash function calculation for comparision. Such a costly search function will potentially cause scalability issues as the tag population increases. When n is a big number, the burden of the server is very heavy.

(2)In the step 5 of authentication phase, the authors verify $(T_3 - T_2) > \theta$, however, T_2 is generated in the server and isn't transmitted from the server to the tag in step4 and step5, so the tag cannot gets T_2.

(3)To save the protocol from de-synchronization attack, the authors assume that after achieving the mutual authentication, the server and the tag update (k_i) simultaneous. However, the authors isn't presents how to judging achieving the mutual authentication between the server and the tag, because the channel between the reader and the tag is insecure, an attacker can block or intercept the message being transmitted between the reader and the tag easily, so updating phase is a wishful assumption of the authors.

Based on the above analysis, we propose a new dynamic ID based lightweight RFID authentication protocol as follows.

3. The New Proposed Schemes to Enhance Medication Safety

This protocol consists of two phases: Initialization phase and Authentication phase.

Initialization phase:

(1)In this phase, the server assigns a tag identity $ID_i \in \{0, 1\}^l$ and the secret key $k_i \in \{0, 1\}^l$, for all tags, stores (ID_i, k_i) in both the tag memory and in the database of the server. A RFID reader has no knowledge of the pair (ID_i, k_i).

(2)The tag and reader have its own random number generator.

(3)The server, reader, and each tag has a current date and time of input device.

(4)The server collects the information ID, k_j and k_{j-1} for each tag.

Authentication phase: In this phase, Server, reader and tag follow the following steps to mutually authenticate each other.

(1)When the Reader wants to communicate with the tag, the reader generate a pseudo random number $R_r \in \{0, 1\}^l$ and send R_r to the tag via an insecure communication channel.

(2)After receiving the random number R_r, the tag generates a pseudo random number $R_t \in \{0, 1\}^l$ and the current time stamp T_1, then computes authentication factor A, B, $A = H(R_r||R_r) \oplus ID$, $B = H(k_j \oplus T_1 \oplus R_t \oplus R_r)$ subsequently sends the request message (A, B, T_1, R_t) to the reader.

(3)After receiving the message (A, B, T_1, R_t), the reader sends the response message (A, B, T_1, R_t, R_r) to the server after reforming the message by adding R_r.

(4)After receiving the message (A, B, T_1, R_t, R_r), then the server firstly verify the validity of time stamp T_2 by verifying $(T_2 – T_1) < \theta$ to judge the authentication request. If it finds correct, then the server computes $ID^* = A \oplus H(R_r||R_r)$.

The server should match whether there exists certain ID_i in column (ID) of the database, which could make $ID_i = ID^*$. If there exists such record, the tag be considered as a legitimate tag, the server will find k_j^* and k_{j-1}^* corresponding to ID^*, then the server should calculate $B^*= H(k_j^* \oplus T_1 \oplus R_t \oplus R_r)$, and check $B^* \approx B$, if identically, then the server computes $C = H(B \oplus T_2 \oplus k_j)$, $D = C||Data$, then delivers the message D, T_2 to the reader. Subsequently the server updates $k_i = H(k_j||R_r||R_r)$ and $k_{j-1}= k_j$.

If $B^*<>B$, the server should calculate $B^{**}= H(k_{j-1}^* \oplus T_1 \oplus R_t \oplus R_r)$, and check $B^{**} \approx B$, if identically, the tag would be considered as a legitimate tag, but in the last authentication access, the tag has not updated k_i successfully for some reason, then the server computes $C = H(B \oplus T_2 \oplus k_j)$, $D = C||Data$, then delivers the message D, T_2 to the reader. Subsequently the server updates $k_i = H(k_j||R_r||R_r)$, but keeps k_{j-1} unaltered.

If there not exists certain ID_i in column ID of the database, the authentication is failed, F(failure information) would be sent to the reader.

Praiseworthily, in this phase, only two times (Or three times) hash operations would be needed in verifying and authenticating a tag, so time complexity of hash function calculation achieves O(1).

(5)After receiving D from server, the reader extracts Data from $D = Data||C$ and sends the remaining message C to the tag. Finally, the tag authenticates the server by following calculation based on the message C at time T_3 received from the reader. If $(T_3 - T_2) < \theta$, then the tag computes $D^* = H(B \oplus k_j \oplus T_2) \approx D$,then tag authenticates the server by confirming that the above calculated hashed value is identical to received D from the reader. The tag computes $k^{new} =H(k_j||R_r||R_t)$, and updates ($k_i$) with ($k^{new}$).

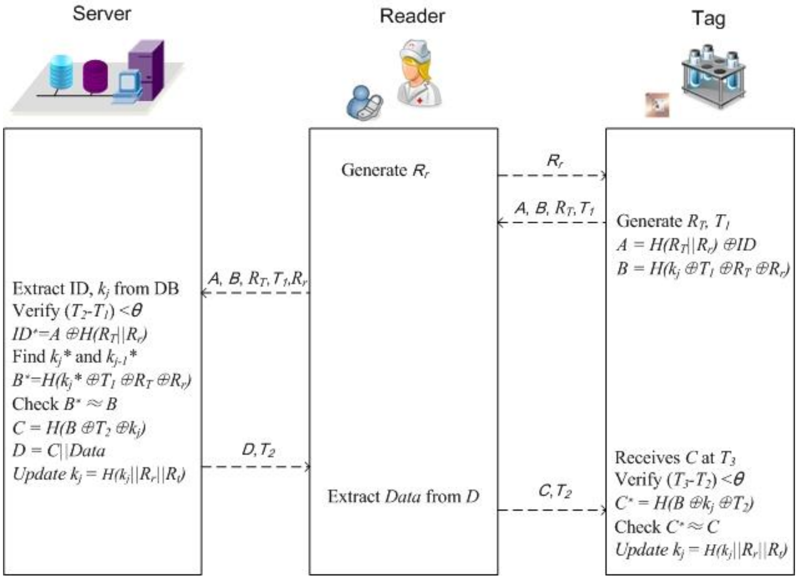

Server
Reader
Tag
Generate R_r
R_r
A, B, R_T, T_1
Generate R_T, T_1
$A = H(R_T||R_r) \oplus ID$
$B = H(k_j \oplus T_1 \oplus R_T \oplus R_r)$
A, B, R_T, T_1, R_r
Extract ID, k_j from DB
Verify $(T_2\text{-}T_1) < \theta$
$ID^*=A \oplus H(R_T||R_r)$
Find k_j^* and k_{j-1}^*
$B^*=H(k_j^* \oplus T_1 \oplus R_T \oplus R_r)$
Check $B^* \approx B$
$C = H(B \oplus T_2 \oplus k_j)$
$D = C||Data$
Update $k_j = H(k_j||R_r||R_t)$
D, T_2
Extract $Data$ from D
C, T_2
Receives C at T_3
Verify $(T_3\text{-}T_2) < \theta$
$C^* = H(B \oplus k_j \oplus T_2)$
Check $C^* \approx C$
Update $k_j = H(k_j||R_r||R_t)$

Figure 2. Authentication Phase of New Proposed Protocol

4. Security Analysis

In this section, we present the security analysis of our scheme. Our protocol can withstand against de-synchronization attack, impersonation attack, replay attack, parallel session attack, man in middle attack and cloning attack and also achieve mutual authentication, tag untraceability.

(1)Achieve mutual authentication

In our protocol, mutual authentication between tag, reader and the server is achieved on the assumption that the communication channel between the server and the reader is secure as it is wired, while the communication channel between the reader and the tag is insecure as it is wireless. The server to tag authentication is done by the message B and tag to server authentication is done by the message C. An adversary cannot modify the message B and C as both them are protected by one way hash function.

(2)Resist impersonation attack

To make the protocol secure from tag impersonation attack, both A and B are protected by secure one way hash function and any modification in request message (A, B) will be detected by the server by verifying B. The legitimate server reply the message C to the tag in order to enable the tag to authenticate the reader or server. So, because the attacker has no way to find ID and k_j of the legitimate tag, he cannot form the same request message C, which makes our proposed protocol secure against server impersonation attack.

(3)Resist de-synchronization attack

As k_j of a tag is mutative, even if loss of message, power failure or loss of connection with the server happens during an authentication access, it will lead to de-synchronization between the server and the tag, this protocol can solve this problem in the next authentication access by searching pre-column (k_{j-1}) and continuing the verification process. So this protocol can resist dy-synchronization attack well.

(4)Resist replay attack and parallel session attack

Our proposed protocol can withstand against replay attack and parallel session attack as replaying a request message (A, B) of one session into another session is useless as freshly generated random numbers are used and the authenticity of the request is verified by checking the freshness of the time stamp T_1, T_2 and secret information is updated after each successful session and also by replaying a request message within the valid time frame window, cannot give an attacker, the common key between the reader and the tag.

(5)Tag untraceability

An adversary can intercept the response message (A, B) from a tag, and analyze the information carefully and try to detect the user location privacy by tracking the tag. Because the tag generates a new random number R_t during each authentication access, and shields ID with $H(R_t \| R_r)$, so the adversary cannot determine which tag does the response from the message (A, B). So this protocol can meet tag untraceability.

(6)Resist man in middle attack

In our protocol, an adversary cannot act as the middle man in between the tag and the reader as the transaction messages are secured by one way hash functions and adversary can intercept in the transaction only if he knows the secret parameters, but it is not possible to find out all the secret parameters correctly at the same time.

(7)Resist cloning

An adversary cannot find the secret parameters and the random numbers as the secret parameters, key and identity are dynamic by nature which use freshly generated pseudo random numbers which makes him unable to make the fake tag and prevent our protocol from cloning attack.

Table 2 indicates a comparison of results between Keerti Srivastava et al.'s authentication scheme and our proposed scheme in terms of performance.

Table 2. Comparison of Performance

Performance	**Item**	**Keerti Srivastava et al.'s**	**Ours**
Storage cost	Tag	2*l*	2*l*
Computation cost	Tag	5*h*	4*h*
	Reader	*r*	*r*
	Server(illegal tag)	2(n+1)**h*	2*h*
	Server(legal tag)	3(n+1)**h*	3*h*
Traffic cost	T to R	3*l*	4*l*
	R to T	2*l*	2*l*
	Total	5*l*	6*l*
	Rounds	5	5
Hardware cost	Tag	H, T, r	H, T, x
Time complexity	Server	O(n)	O(1)

'*l*' denotes the length of ID, '*r*' denotes pseudo random number generator, '*h*' denotes one way hash function, 'T' denotes clock generator.

5. Conclusion

As the consequence of any small error in hospitals, seriously endanger the safety of the patient. In this paper, we show the weaknesses of Keerti Srivastava et al.'s authentication scheme. Thus, we present a new dynamic ID based lightweight RFID authentication protocol, which is designed to enhance medication safety. In spite of low storage capacity and limited computational and communicational capacity of tags, our scheme withstand against de-synchronization attack, impersonation attack, replay attack, parallel session attack, man in middle attack and cloning attack and achieve mutual authentication, tag untraceability which make our protocol secure and efficient for domain of telecare medicine information system. The performance properties of our proposed schemes are analyzed as well by comparing with Keerti Srivastava et al.'s authentication scheme.

Acknowledgements

This research was supported by Fundamental Research Funds for the Central Universities (No. DC201502060402), and Program for Liaoning Excellent Talents in University (No. LJQ2013125)

References

[1] A. B. Bondi, "Characteristics of Scalability and Their Impact on Performance", In Proceedings of the Second International Workshop on Software and Performance - WOSP 2000, **(2000),** pp. 195-203.

[2] H.-Y. Chien, C.-C. Yang, T.-C. Wu and C.-F. Lee, "Two RFID-based Solutions to Enhance Inpatient Medication Safety", Journal of Medical Systems, vol. 35, no. 3, **(2011),** pp. 369-375.

[3] P. R. Sun, B. H. Wang and F. Wu, "A New Method to Guard Inpatient Medication Safety by the Implementation of RFID", Journal of Medical Systems, vol. 32, no. 4, **(2008),** pp. 327-332.

[4] H.-H. Huang and C.-Y. Ku, "A RFID Grouping Proof Protocol for Medication Safety of Inpatient", Journal of Medical Systems, vol. 33, no. 6, **(2009),** pp. 467-474.

[5] A. Juels, "Yoking Proofs" for RFID Tags. First International Workshop on Pervasive Computing and Communication Security, IEEE Computer Society, **(2004),** pp. 138-143.

[6] Y.-z. Li, Y.-b. Cho, N.-K. Um and S.-H. Lee, "Security and Privacy on Authentication Protocol for Low-cost RFID", IEEE International Conference on Computational Intelligence and Security, vol. 2, **(2006),** pp. 1101-1104.

[7] F. Wu, F. Kuo and L.-W. Liu, "The Application of RFID on Drug Safety of Inpatient Nursing Healthcare", ICEC '05 Proceedings of the 7th International Conference on Electronic Commerce, **(2005),** pp. 85-92.

[8] P. Peris-Lopez, A. Orfila, A. Mitrokotsa and J. C. A. Van der Lubbe, "A Comprehensive RFID Solution to Enhance Inpatient Medication Safety", International Journal of Medical Informatics. vol. 80, no. 1, **(2011),** pp.13-24.

[9] A. Juels, R. L. Rivest and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", The 8th ACM Conference on Computer and Communications Security, **(2003),** pp. 103-111.

[10] D. Henrici and P. Muller, "Hash-Based Enhancement of Location Privacy for Radio Frequency Identification Devices Using Varying Identifiers", International Workshop on Pervasive Computing and Communication Security - PerSec 2004, IEEE Computer Society, **(2004),** pp. 149-153.

[11] C. H. Lim and T. Kwon, "Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer", Information and Communications Security, Lecture Notes in Computer Science, Springer, vol. 4307, **(2006),** pp. 1-20.

[12] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, **(2007),** pp. 337-340.

[13] Y. C. Lee, Y. C. Hsieh, P. You and T. C. Chen, "A New Ultralightweight RFID Protocol with Mutual Authentication", Information Engineering, 2009, ICIE '09, WASE International Conference, **(2009),** vol. 2, pp. 58-61.

[14] Y.-C. Yu, T.-W. Hou and T.-C. Chiang, "Low Cost RFID Real Lightweight Binding Proof Protocol for Medication Errors and Patient Safety", Journal of Medical Systems, vol. 36, no. 2, **(2012),** pp. 823-828.

[15] M. M. Pérez, M. N. Cabrero-Canosa, J. V. Hermida, L. C. García, D. L. Gómez, G. V. González and I. M. Herranz, "Application of RFID Technology in Patient Tracking and Medication Traceability in Emergency Care. Journal of Medical Systems, vol. 36, **(2012),** pp. 3983-3993**.**

[16] P. J. Hawrylak, N. Schimke, J. Hale and M. Papa, "Security Risks Associated with Radio Frequency Identification in Medical Environments", Journal of Medical Systems, vol. 36, **(2012),** pp. 3491-3505**.**

[17] S. D. Kaul and A. K. Awasthi, "RFID Authentication Protocol to Enhance Patient Medication Safety", Journal of Medical Systems, vol. 37, **(2013),** p. 9979.

[18] B. Song and C. J. Mitchell, "Scalable RFID Security Protocols Supporting Tag Ownership Transfer", Computer Communications, vol. 34, **(2010),** pp. 556-566.

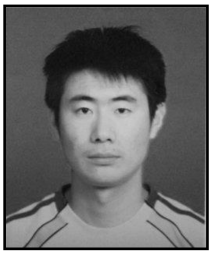
[19] Y. Xu, J. He, J. Wang and D. Wang, "Enhance Patient Medication Safety With A RFID-based Authentication Scheme", International Journal of u- and e- Service, Science and Technology, **(2014),** vol. 8, no. 4, pp. 85-94.

[20] K. Srivastava, A. K. Awasthi, S. D. Kaul and R. C. Mittal, "A Hash Based Mutual RFID Tag Authentication Protocol in Telecare Medicine Information System", Journal of Medical Systems, vol. 39, **(2014),** pp. 153-157.

Authors

He Jialiang, he was born in 1977, received the PhD degree in computer software and theory from Jilin University of China in 2012 and the Master degree in computer application from Jilin University of China in 2004. Now he is an associate professor at College of Information and Communication Engineering, Dalian Nationalities University, China. His papers have been published in some well-known international Journals and IEEE conferences. His main interests include Mobile Internet, Internet of Things, and Intelligent Business Information Processing.

Xu Zhiqiang, he was born in 1981, received the Bachelor degree in communication Engineering from Communication University of China in 2004 and the Master degree in Electronics & Communication Engineering from Communication University of China in 2012. At present, he is an assistant professor of Communication & Media Institute of Sichuan, China. He is experienced the fields of Mobile Internet, Internet of Things, Intelligent Information Processing, etc., he also is a candidate of MSc of Technopreneurship & Innovation Program in Nanyang Technological University in Singapore.



Xu Xiaoke, he obtained his Bachelor (2002) in Electronic and Information Engineering and PhD (2008) in Communication and Information System from Dalian Maritime University in China. Now he is working at College of Information and Communication Engineering, Dalian Nationalities University. His research interests include complex networks and complex systems, nonlinear time series analysis, human mobility and dynamics applied to information spreading, and online social network analysis.