International Journal of u-and e-Service, Science and Technology
Vol.7, No.4 (2014), pp.85-94
http://dx.doi.org/10.14257/ijunnesst.2014.7.4.9

# Enhance Patient Medication Safety With A RFID-based Authentication Scheme

[1]Xu Youjun, [*2]He Jialiang, [3]Wang Jian, [4]Wang Dongxing

[1,3,4]1 College of Computer Science and Information Technology, Daqing Normal University, China
[*2]2 College of Information and Communication Engineering, Dalian Nationalities University, China
E-mail: xu_youjun@sohu.com; urchin2012@sina.com; virtualcat@21cn.com; peak_email@sina.com

## Abstract

*Medication Safety is an important issue for patients. Automated patient medication system using RFID technology is used to reduce the medication errors and improve the patient safety. In this paper, we show the weaknesses of Sonam Devgan Kaul 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 and is particularly suitable for the low-cost RFID systems because only one-way hash function, XOR operation and concatenation operation are needed in tag part, so it is practical, secure and efficient for health care domain.*

***Keywords:*** *Radio frequency identification; Authentication scheme; Search scheme; Secure medication system*

## 1. Introduction

Radio Frequency Identification (RFID) technology can play a key 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]. RFID is an identification technology that uses radio waves to identify objects remotely and automatically. 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 mayendanger the safety of the patient seriously. So a secure and efficient medication management scheme is needed in health care domain.

In this paper, we present a secure lightweight RFID authentication protocol based on dynamic ID to prevent patient from medication errors. Due to low storage capacity and limited computational and communicational capacity of tags, we only use pseudo random

ISSN: 2005-4246 IJUNNEST

number generator function, one way hash function and Xor operation in our authentication protocol.

The rest of the paper is organized as follows: Section 2 briefly review the related work of RFID security protocol and its application in medication management. Our proposed RFID authentication protocol is presented in Section 3, followed by security analysis in Section 4. Finally, we conclude the paper in Section 5.

## 2. Related Work

RFID security protocols have been investigated for about ten years. In 2003, Juels et al. presented a scheme towards the privacy and security is to kill the 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 hash based dynamic ID scheme in which one way hash function is used and ID is changed after each session [6], to protect the tag from location privacy, but after an unsuccessful session, it replies with the same hash ID, which makes it traceable and vulnerable to impersonation attack and backward traceability. In 2006, Lim and Kwon proposed mutual authentication scheme to provide backward and forward un-traceability [13], however, this scheme isnot meet tag untraceability yet. In 2007, Hung-Yu Chien presented an ultra-lightweight mutual authentication protocol to provide strong authentication and strong integrity[4], however, this protocol is also vulnerable to resist de-synchronization attack, DOS attack, and isnot meet tag untraceability. In 2008, Lopez et al. introduced a Gossamer protocol for the low-cost RFID systems [2], However, it is still vulnerable to resist de-synchronization attack and DOS attack. In 2009, Lee et al. proposed an ultra-lightweight RFID protocol with mutual authentication as an improvement to Gossamer protocol [11]. However, it is vulnerable to resist disclosure attack, cloning attack, de-synchronization attack, and it isnot meet tag untraceability.

For improving the accuracy of healthcare management, Ari Juels presented “Yoking Proof” in 2004[8], which can make two tags to be tracked simultaneously. However, this scheme is not secure enough against replay attack from an adversary. In 2005, Wu et al. presented the application of RFID technology on drug safety of inpatient nursing healthcare [10]. Sun et al. also presented a new mechanism to prevent the risk of medication error in 2008[5]. In 2010, Lo and Yeh presented denial of proof attack on grouping proof RFID authentication algorithms [14]. In 2011, Peris-Lopez et al. presented inpatient safety RFID system which cover almost every phase of the drug administration process [18], however, this scheme is vulnerable to denial of proof attack and the generated medication evidence cannot defend against counterfeit evidence generated from the hospitals. Subsequently, many security schemes and their improvements [3, 7, 12, 15, 16, 19] have been proposed to improve patient safety.

In order to enhance medication safety for patients, we will propose a new dynamic ID based lightweight RFID authentication protocol which uses only one way hash function, pseudo random number generator function and Xor operation in tag part. This protocol can resist common security and privacy requirements for the tag and the server. Especially, it has well performance which only requires O(1) work to identify and authenticate a tag in the backend server.

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

**Table 1. The Notations Used in this Paper**

| Symbol | Meaning |
|---|---|
| ID | The unique index code of a tag (The length is $l$) |
| k | Secret key for a tag (The length is $l$) |
| Info | Information of the corresponding tag stored in the backend server |
| 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 |
| $r_1$ | The random number generated by the reader (The length is $l_R$) |
| $r_2$ | The random number generated by the tag(The length is $l_R$) |
| T | Current date and time of input device |
| $\theta$ | 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 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], Let's reviews this scheme.

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

Initialisation phase: 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 ($ID_i$, $k_i$ ).

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 $r_1 \in \{0, 1\}^l$ and send $r_1$ to the tag via an insecure communication channel.

(2)After receiving the random number $r_1$, the tag generates a pseudo random number $r_2 \in \{0, 1\}^l$ and computes an authentication factor $A_1$ and $A_2$, $A_1 = H(k_i \oplus r_1) \oplus r_2$, $A_2 = H(ID_i \| r_1 \| r_2 \| k_i \| T)$ where T is the current time stamp, subsequently sends the request message ($A_1$, $A_2$, T ) to the reader and saves $r_1$, $r_2$ in its memory.

(3)After receiving the message ($A_1$, $A_2$, T), the reader first verify the validity of time stamp T by checking $(T' - T) < \theta$ to judge the authentication request where T' is the current time of the reader. If it finds incorrect, the authentication request is rejected, else the reader sends ($r_1$, $A_1$, $A_2$, T') to the server.

(4)After receiving the message ($r_1$, $A_1$, $A_2$, T'), then the server firsly verify the validity of time stamp T' by verifying $(T'' - T') < \theta'$ to judge the authentication request. If it finds correct, then the server finds $r_2^*$ for i^th tag pair ($ID_i$, $k_i$) and verify the authenticity of $r_2^*$ by verifying computed $A_2^*$ with the received $A_2$, For $1 \leq i \leq n$, $r_2^* = A_1 \oplus H(k_i \oplus r_1)$, $A_2^* = H(ID_i \| r_1 \| r_2^* \| k_i \| T'')$. If it is not verified for any pair ($ID_i$, $k_i$), then the session is dismissed, otherwise, the server authenticates the tag and computes the mutual authentication factor $A_3 = H(ID_i \oplus r_1 \oplus r_2 \oplus k_i)$ and sends $A_3$ to the reader.

(5)The reader directly sends $A_3$ to the tag. Finally, Tag verify the authenticity of received $A_3$ by the computed $A_3^* = H(ID_i \oplus r_1 \oplus r_2 \oplus k_i)$. If $A_3$ equals to $A_3^*$, then mutual authentication can be done.

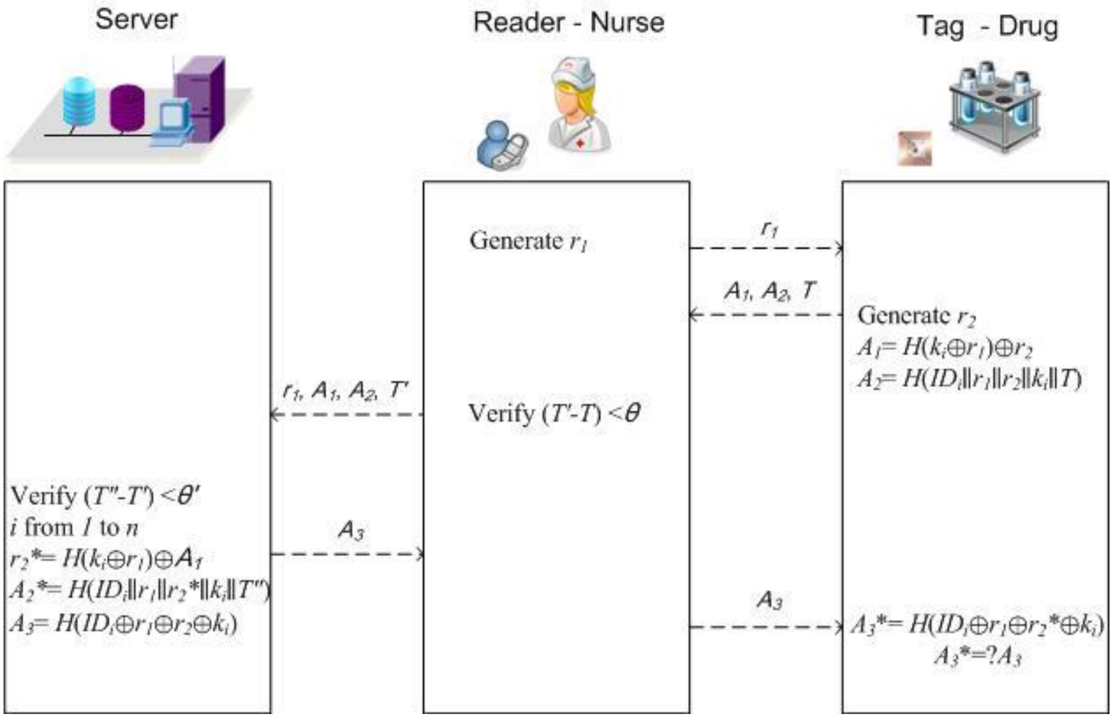
Server
Reader - Nurse
Tag - Drug
Generate $r_1$
$r_1$
$A_1, A_2, T$
Generate $r_2$
$A_1= H(k_i \oplus r_1) \oplus r_2$
$A_2= H(ID_i \| r_1 \| r_2 \| k_i \| T)$
$r_1, A_1, A_2, T'$
Verify $(T'-T) < \theta$
Verify $(T''-T') < \theta'$
$i$ from $1$ to $n$
$r_2^* = H(k_i \oplus r_1) \oplus A_1$
$A_2^* = H(ID_i \| r_1 \| r_2^* \| k_i \| T'')$
$A_3= H(ID_i \oplus r_1 \oplus r_2 \oplus k_i)$
$A_3$
$A_3$
$A_3^* = H(ID_i \oplus r_1 \oplus r_2^* \oplus k_i)$
$A_3^* =? A_3$

**Figure 1. Authentication Phase of This Protocol**

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 $ID_i^{new} = H(ID_i \oplus r_1 \oplus r_2)$, $k_i^{new} = H(k_i \| r_1 \| r_2)$, and updates pair $(ID_i, k_i)$ with pair $(ID_i^{new}, k_i^{new})$.

(2)The server computes $ID_i^{new} = H(ID_i \oplus r_1 \oplus r_2)$, $k_i^{new} = H(k_i \| r_1 \| r_2)$, and updates pair $(ID_i, k_i)$ with pair $(ID_i^{new}, k_i^{new})$. To save the protocol from desynchronization attack, the pair $(ID_i, k_i)$ is still stored in the database of the server.

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

(1)We can see that in this scheme clock generater is used in tag part. As we know, low-cost passive tags has limited rescources, so it is impractical arrangement like that, so this scheme is not suitable for the low-cost RFID systems.

(2)In the step 4 of authentication phase, the server firsly verify the validity of time stamp T' by verifying $(T'' - T') < \theta'$ to judge the authentication request. If it finds correct, then the server finds $r_2^*$ for ith tag pair $(ID_i, k_i)$ and verify the authenticity of $r_2^*$ by verifying computed $A_2^*$ with the received $A_2$, For $1 \leq i \leq n$, $r_2^* = A_1 \oplus H(k_i \oplus r_1)$, $A_2^* = H(ID_i \| r_1 \| r_2^* \| k_i \| T'')$. Because $T'' <> T$ obviously, so it cannot find pair $(ID_i, k_i)$ in the database of the server, it may be a mistake in writing, but T is not transmitted in the step 3 of authentication phase, so it is an obscure problem.

(3)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[20]. In the step 4 of authentication phase, the server finds $r_2^*$ for ith tag pair $(ID_i, k_i)$ and verify the authenticity of

$r_2$* by verifying computed $A_2$* with the received $A_2$, For $1 \le i \le n$, $r_2^* = A_1 \oplus H(k_i \oplus r_1)$, $A_2^* = H(ID_i \parallel r_1 \parallel r_2^* \parallel k_i \parallel T'')$. 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 two 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 2*((n+1)/2) (Only column pair ($ID_i$, $k_i$) 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 failedly it would perform 2*2*((n+1)/2) times (Both column pair ($ID_i$, $k_i$) and pair ($ID_i^{new}$, $k_i^{new}$) 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.

(4)To save the protocol from desynchronization attack, the authors assume that after achieving the mutual authentication, the server and the tag update pair ($ID_i$, $k_i$) simultaneous. However, the authors isnot 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: Initialisation phase and Authentication phase.

Initialisation phase: 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 ($ID_i$, $k_i$).

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 generates a pseudo random number $r_1 \in \{0, 1\}^l$ and a timestamp T, then sends $r_1$ to the tag via an insecure communication channel.

(2)After receiving a random number $r_1$, the tag generates a pseudo random number $r_2 \in \{0, 1\}^l$ and computes an authentication factor $A_1$ and $A_2$, $A_1 = H(r_1) \oplus r_2$, $A_2 = H(r_1 \parallel r_2) \oplus k_i$, subsequently sends the request message ($A_1$, $A_2$) to the reader and saves $r_1$, $r_2$ in its memory.

(3)When receiving the message ($A_1$, $A_2$), the reader firstly verify the validity of time stamp T by checking $(T' - T) < \theta$ to judge the authentication request where T' is the current time of the reader. If it finds incorrect, the authentication request is rejected, else the reader sends ($r_1$, $A_1$, $A_2$, T') to the server.

(4)After receiving the message ($r_1$, $A_1$, $A_2$, T'), then the server firsly verify the validity of time stamp T' by verifying $(T'' - T') < \theta'$ to judge the authentication request. If it finds correct, then the server computes $r_2^* = A_1 \oplus H(r_1)$, $k_i^* = A_2 \oplus H(r_1 \parallel r_2^*)$.

The server should match whether there exists certain $k_i$ in column pair ($ID_i$, $k_i$) of the database or not directly, which could make $k_i = k_i^*$. If there exists such record, the tag would be considered as a legitimate tag, then the server should calculate $ID_i^{new} = H(ID_i \parallel r_1 \parallel r_2)$, $k_i^{new} = H(k_i \parallel r_1 \parallel r_2)$, $A_3 = H(ID_i \parallel r_1 \parallel r_2 \parallel k_i)$, then sends the mutual authentication factor $A_3$ to the reader, finally, the server updates pre-pair ($ID_i$, $k_i$) with pair ($ID_i$, $k_i$) and pair ($ID_i$, $k_i$) with pair ($ID_i^{new}$, $k_i^{new}$).

If there not exists certain $k_i$ in column pair ($ID_i$, $k_i$) of the database or not directly, which could make $k_i = k_i$*. The server would search whether there exists certain $k_i$ in column pre-pair ($ID_i$, $k_i$) of the database, which could make $k_i = k_i$*. If there exists such record, the tag would be considered as a legitimate tag, but in the last authentication access, the tag has not updated pair ($ID_i$, $k_i$) successfully for some reason, then the server should calculate $ID_i^{new} = H(ID_i \| r_1 \| r_2)$, $k_i^{new} = H(k_i \| r_1 \| r_2)$, $A_3 = H(ID_i \| r_1 \| r_2 \| k_i)$, then sends the mutual authentication factor $A_3$ to the reader, finally, the server updates pair ($ID_i$, $k_i$) with pair ($ID_i^{new}$, $k_i^{new}$), but keeps pre-pair ($ID_i$, $k_i$) unaltered.

If there not exists certain $k_i$ in column pair ($ID_i$, $k_i$) and column pre-pair ($ID_i$, $k_i$) of the database, the authentication is failed, F(failure information) would be sent to the reader.

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

(5)The reader directly sends $A_3$ to the tag. Finally, Tag verify the authenticity of received $A_3$ by the computed $A_3^* = H(ID_i \| r_1 \| r_2 \| k_i)$. If $A_3$ equals to $A_3^*$, then mutual authentication can be done.

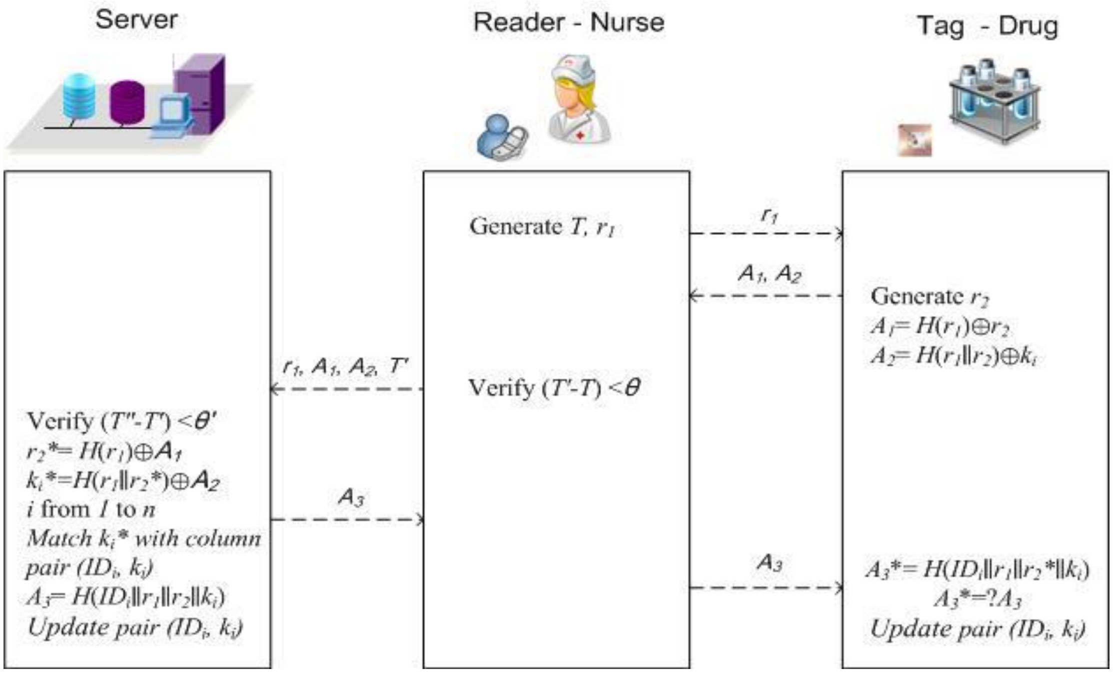

**Figure 2. Authentication Phase of New Proposed Protocol**

## 4. Security Analysis

In this section, we present the security analysis of our scheme. In addition to limited storage capacity, low computational and communicational cost, our protocol withstand against de-synchronization attack, impersonation attack, replay attack, parallel session attack, backward traceability, forward traceability, 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 $A_2$ and tag to server authentication is done by the message $A_3$. An adversary cannot modify the message $A_2$ and $A_3$ as both them are protected by one way hash function.

(2)Resist impersonation attack

To make the protocol secure from tag impersonation attack, both $A_1$ and $A_2$ are protected by secure one way hash function and any modification in request message ($A_1$, $A_2$) will be detected by the server by verifying $A_2$. The legitimate server reply the message $A_3$ to the tag in order to enable the tag to authenticate the reader or server. So, because the attacker has no way to find $ID_i$ and $k_i$ of the legitimate tag, he cannot form the same request message $A_3$, which makes our proposed protocol secure against server impersonation attack.

(3)Resist de-synchronization attack

As pair ($ID_i$, $k_i$) 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 dy-synchronization between the server and the tag, this protocol can solve this problem in the next authentication access by searching $k_i$ in column pre-pair ($ID_i$, $k_i$) and continuing the verification process. So this protocol can resist de-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 ($A_1$, $A_2$) 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 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 ($A_1$, $A_2$) 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 $r_2$ during each authentication access, and shields $r_2$ with $H(r_1)$ and $k_i$ with $H(r_1 \| r_2)$, so the adversary cannot determine which tag does the response from the message ($A_1$, $A_2$). So this protocol can meet tag untraceability.

(6)Resist backward and forward traceability

In our protocol, even when at the current time $t_0$ the secret information of tag is disclosed, an adversary is unable to identify the tag at the time t for all $t < t_0$ and also and adversary is unable to identify the tag at the time t for all $t > t_0$ which makes our protocol secure against backward and forward traceability. For the security of past and future communication, updation process not only involves secret pair ($ID_i$, $k_i$) and random numbers $r_1$ and $r_2$, but also involves one way hash function.

(7)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.

(8)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 Sonam Devgan Kaul et al's authentication scheme and our proposed scheme in terms of performance.

**Table 2. Comparison of Performance**

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

'*l'* denotes the length of ID, '*x'* denotes XOR function, '*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 Sonam Devgan Kaul et al's authentication scheme. Thus, we present a new dynamic ID based lightweight RFID authentication protocol, which is designed to enhance patient safety. Inspite 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, backward traceability, forward traceability, man in middle attack and cloning attack and achieve mutual authentication, tag untraceability which make our protocol secure and efficient for health care domain. The performance properties of our proposed schemes are analyzed as well by comparing with Sonam Devgan Kaul et al's authentication scheme.

## Acknowledgements

This work was fully supported by Scientific Research Fund No.12533002 of Heilongjiang Provincial Education Department

## 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] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador and A. Ribagorda, "Advances in Ultralightweight Cryptography for Low Cost RFID Tags: Gossamer Protocol", In Proceedings of WISA'08, vol. 5379, **(2008)**, pp. 56-68.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[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] F. Wu, F. Kuo, 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.

[11] 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, vol. 2, **(2009)**, pp. 58-61.

[12] 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.

[13] 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.

[14] N. W. Lo and K. H. Yeh, "Anonymous Coexistence Proofs for RFID Tags", Journal of Information Science & Engineering, vol. 26, no. 4, **(2010)**, pp. 1213-1230.

[15] D. Molnar, A. Soppera and D. Wagner, "A Scalable", Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags, Selected Areas in Cyptography, Lecture Notes in Computer Science Springer, SAC2005, vol. 3897, **(2006)**.

[16] M. M. Morshed, A. Atkins and H. Yu, "Secure Ubiquitous Authentication Protocols for RFID Systems", EURASIP Journal on Wireless Communications and Networking, **(2012)**, pp. 1-35.

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

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

[19] 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.

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

## Authors

**Xu Youjun**, was born in 1977, received the Master degree in computer application from Jilin University in 2005 and the PhD degree in computer software and theory from Jilin University in 2011. Now he is a lecturer at College of Computer Science and Information Technology, Daqing Normal University, China. His papers have been published in some well-known international Journals. His main interests include Automated Reasoning, Internet of Things.

**He Jialiang**, 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.

**Wang Jian**, was born in 1971, received the Master degree in software engineering from Jilin University in 2009. Now he is an associate professor at College of Computer Science and Information Technology, Daqing Normal University, China. His papers have been published in some well-known conferences. His main interests include Data Mining, Internet of Things.

**Wang Dongxing**, was born in 1977, received the Master degree in computer application from Xiamen University in 2005. Now she is an associate professor at College of Computer Science and Information Technology, Daqing Normal University, China. His papers have been published in some well-known conferences. Her main interests include SOC Architecture, Internet of Things.