2014

ISSN : 0974 - 7435

Volume 10 Issue 9

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(9), 2014 [3908-3917]

Security lightweight RFID protocol for U-healthcare system

Xiuqing Chen[1]*, Tianjie Cao[1]*, Jingxuan Zhai[1], Yu Guo[2]
[1]School of Computer, China University of Mining and Technology, Xuzhou, (CHINA)
[2]School of Materials Science and Engineering, China University of Mining and Technology, Xuzhou, (CHINA)
E-mail : xiuqingchen@126.com

ABSTRACT

Radio Frequency Identification systems have been extensively deployed in the ubiquitous healthcare domain. However, healthcare records of patients in database and mobile devices can be revealed by a malicious attacker, there are many privacy threats. In order to meet the practical requirements of hospital environment, this paper critically analyzes all the possible attacks on original protocol and proposes an improved low-cost lightweight RFID protocol conforming to EPC Class 1 Generation 2 standards in hospital scenarios. Therefore, the enhanced protocol is more secure and higher performance in terms of performance and security properties compared with other schemes.

KEYWORDS

Radio frequency identification; Ubiquitous healthcare; Low-cost lightweight RFID protocol; Provably security; Privacy property.

INTRODUCTION

Radio Frequency Identification (RFID) systems have been extensively deployed in the ubiquitous health care (U-healthcare) domain[1]. U-healthcare is an evolutionary service of healthcare applied by wireless networks, RFID mobile devices, wireless medical sensors and body area networks (BANs). To implement U-healthcare service, developing U-healthcare system in the healthcare industry is a significant tendency via traditional wired, mobile health (M-health) and ubiquitous sensor network (USN) technologies[2]. Adoption of the Health Information System (HIS) based on the wireless network infrastructure gives a lot of benefits. As a part of the U-healthcare system, many mobile devices have been employed in hospitals due to their outstanding mobility. Immediate access to the Electronic Medical Record (EMR) database (DB) offered with the mobile device can reduce the processing time to access and update EMR[3-5]. Healthcare information of mobile devices can be exposed, then there are many security problems occurred.

In order to monitor and track patients, automatic solutions based on RFID technology have been provided for the nursing staff[6] in U-healthcare environment.

On the one hand, USN is employed as a key factor to rapidly transmit medical information (biomedical signals) to the remote hospitals in previous health environments. On the other hand, patient monitoring medical information in real time can be analyzed by consultants. But there are many security issues and limitations for the patients' safety. In a passive scenario and an active scenario, the adversary monitors and traces the messages in insecurity channels, such as the channel between a genuine tag and a mobile reader (a reader and DB). There are U-healthcare scenarios where the adversary can initiate fake transactions between a tag (hold by a patient) and a mobile reader (hold by a nurse). The adversary can have an objective to reconstruct the genuine tag key and disturb the regular arrangement of the nurse.

The safety performance and low-cost is the task of designing a lightweight RFID scheme in U-healthcare. This is why U-healthcare should be as economic and widely available as possible. The doctor should obtain accurately the biological information of the patient from wireless medical sensors BANs (WMSBANs) and diagnose promptly the patient’s condition. The efficient U-healthcare system applications benefit from RFID technology, such as the patient traceability, ownership transfer procedures, medication administration and cost savings.

This paper is focused on acute diseases that are increasingly threatening the sustainability of health care systems due to rapidly-increasing incidence. The improved scheme requirements for better utilization of health care resources, and RFID technology can provide effective medical checkup in U-healthcare.

In order to manage effectively the related clinical processes, we develop a security lightweight RFID protocol for the multi-tags and multi-owners. Since it is common for RFID-tagged patients being owned by multi-owners, a patient is commonly managed by some nurses and doctors. The proposed protocol addresses the dynamic associated in the u-healthcare scenarios.

CRYPTANALYSIS OF MOHAMMADALI ET AL’S PROTOCOL

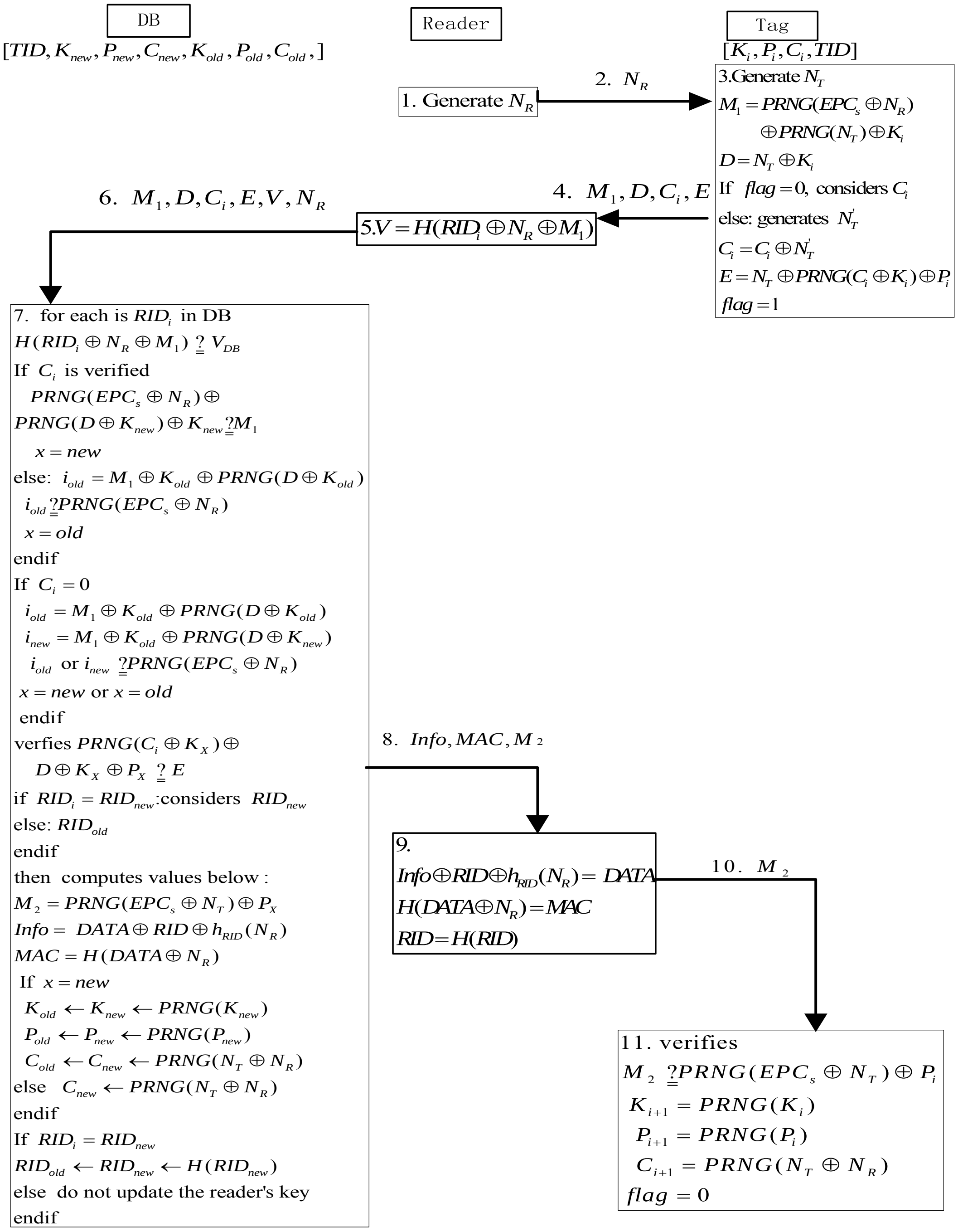
For simplicity, we use the notations of the original paper. These notations have been explained in TABLE 1.

TABLE 1 : The notations and descriptions.

Notations	Descriptions
EPC_s;$DATA$	Electronic Product Code; The tag’s record.
K_i (P_i)	key (access key) stored in the tag^i.
C_i; RID	The i-th tag’s index in DB; reader’s identifier.

RID	The reader identication number.
$H()$; $h_K()$	Hash function; Keyed hash function.

We analyze the security of Mohammadali et al's scheme in Figure.1 to find out various attacks. Then, we propose several types of attacks against this protocol, such as tag, reader, DB impersonation attack and tracing attack.



DB
$[TID, K_{new}, P_{new}, C_{new}, K_{old}, P_{old}, C_{old},]$
Reader
Tag
$[K_i, P_i, C_i, TID]$
1. Generate N_R
2. N_R
3.Generate N_T
$M_1 = PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$
$D = N_T \oplus K_i$
If $flag = 0$, considers C_i
else: generates N_T'
$C_i = C_i \oplus N_T'$
$E = N_T \oplus PRNG(C_i \oplus K_i) \oplus P_i$
$flag = 1$
4. M_1, D, C_i, E
5.$V = H(RID_i \oplus N_R \oplus M_1)$
6. M_1, D, C_i, E, V, N_R
7. for each is RID_i in DB
$H(RID_i \oplus N_R \oplus M_1) \overset{?}{=} V_{DB}$
If C_i is verified
$PRNG(EPC_s \oplus N_R) \oplus PRNG(D \oplus K_{new}) \oplus K_{new} \overset{?}{=} M_1$
$x = new$
else: $i_{old} = M_1 \oplus K_{old} \oplus PRNG(D \oplus K_{old})$
$i_{old} \overset{?}{=} PRNG(EPC_s \oplus N_R)$
$x = old$
endif
If $C_i = 0$
$i_{old} = M_1 \oplus K_{old} \oplus PRNG(D \oplus K_{old})$
$i_{new} = M_1 \oplus K_{old} \oplus PRNG(D \oplus K_{new})$
i_{old} or $i_{new} \overset{?}{=} PRNG(EPC_s \oplus N_R)$
$x = new$ or $x = old$
endif
verfies $PRNG(C_i \oplus K_X) \oplus D \oplus K_X \oplus P_X \overset{?}{=} E$
if $RID_i = RID_{new}$:considers RID_{new}
else: RID_{old}
endif
then computes values below :
$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$
$Info = DATA \oplus RID \oplus h_{RID}(N_R)$
$MAC = H(DATA \oplus N_R)$
If $x = new$
$K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new})$
$P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new})$
$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R)$
else $C_{new} \leftarrow PRNG(N_T \oplus N_R)$
endif
If $RID_i = RID_{new}$
$RID_{old} \leftarrow RID_{new} \leftarrow H(RID_{new})$
else do not update the reader's key
endif
8. $Info, MAC, M_2$
9.
$Info \oplus RID \oplus h_{RID}(N_R) = DATA$
$H(DATA \oplus N_R) = MAC$
$RID = H(RID)$
10. M_2
11. verifies
$M_2 \overset{?}{=} PRNG(EPC_s \oplus N_T) \oplus P_i$
$K_{i+1} = PRNG(K_i)$
$P_{i+1} = PRNG(P_i)$
$C_{i+1} = PRNG(N_T \oplus N_R)$
$flag = 0$

Figure 1 : Mohammadali et al’s protocol.

(1) Impersonation DB Attack

Phase 1 (Learning): The attacker *Adv* plays as a blocker and eavesdrops one successful run of protocol and blocks the Step 2, then stores the exchanged messages $\{M_1, D, C_i, E\}$, where:

Step 1. The R_i generates a nonce N_R and sends it to the T_i.

Step 2. The T_i generates N_T and computes M_1, D, C_i, E, then sends them to the R_i.

a. $M_1= PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$

b. $D = N_T \oplus K_i$

c. $C_i= C_i$ ($flag$=0)

d. $E= N_T \oplus PRNG(C_i \oplus K_i) \oplus P_i$

Step 3. The attacker *Adv* blocks and stores the information, then stops the session.

Phase 2 (Impersonation DB): To impersonate the DB, *Adv* initiates a new session of protocol, where:

Step 1. *Adv* replays the monitored nonce N_R to the T_i.

Step 2. The T_i produces N'_T and computes M'_1, D', C'_i, E', then sends them to the R_i. Their equations are calculated as follows.

a. $M'_1= PRNG(EPC_s \oplus N_R) \oplus PRNG(N'_T) \oplus K_i$

b. $D' = N'_T \oplus K_i$

c. $C'_i= C_i \oplus N''_T$ ($flag$=1)

d. $E' = N'_T \oplus PRNG(C'_i \oplus K_i) \oplus P_i$

Step 3. *Adv* blocks the messages $\{M'_1, D', C'_i, E'\}$ and modifies the transferred messages as follows:

a. $M_{1Adv}=PRNG(EPC_s \oplus N_R) \oplus PRNG(N'_T) \oplus K_i$

b. $D_{Adv} = D'=N'_T \oplus K_i$

c. $C_{iAdv}= C_i$

d. $E_{Adv}= E \oplus D \oplus D'=N'_T \oplus PRNG(C_i \oplus K_i) \oplus P_i$

Subsequently, *Adv* forwards the messages $\{M_{1Adv}, D_{Adv}, C_{iAdv}, E_{Adv}\}$ to the reader R_i.

Step 4. (R_i -DB)

The reader R_i computes $V=H(N_R \oplus RID \oplus M'_1)$ and sends $\{M_{1Adv}, D_{Adv}, C_{iAdv}, E_{Adv}, V, N_R\}$ to the DB.

Step 5. (DB verification)

DB picks up each stored *RID* sequentially to compute $H(RID \oplus N_R \oplus M'_{1Adv})$ with the same N_R, and compares the computed V_{DB} with the received V. If $V_{DB}= V$, the DB verifies the legitimate reader. On the other hand, the values $\{M_{1Adv}, D_{Adv}, C_{iAdv}, E_{Adv}, V, N_R\}$ are verified by the DB. The following equations are given to prove the computational process.

a. $V_{DB}= H(RID \oplus N_R \oplus M'_{1Adv})$

$=V= H(RID \oplus N_R \oplus M'_1)$

From the above compared result, the DB can authenticate the R_i.

b. The DB compares transferred message M_{1Adv} with the calculated M_{1DB} using the stored keys $\{EPC_s, K_i\}$ and the received messages $\{N_R, D_{Adv}\}$. Therefore, the DB verifies $M_{1DB} = M_{1Adv}$ using the following equation.

$M_{1DB}=PRNG(EPC_s \oplus N_R) \oplus PRNG(N'_T) \square K_i$

$= M_{1Adv}$

c. The DB compares transferred message E_{Adv} with the calculated E_{DB} using the following equation.

$E_{DB} =D_{Adv} \oplus K_i \oplus PRNG(C_{Adv} \oplus K_i) \oplus P_i$

$=N'_T \oplus PRNG(C_i \oplus K_i) \oplus P_i=E_{Adv}$

d. After the DB verifies successfully, it computes the messages $\{M_2, MAC, info\}$ as follows:

$M_2 = PRNG(EPC_s \oplus N'_T) \oplus P_i$

$Info= DATA \oplus RID \oplus h_{RID} (N_R)$

$MAC=H(DATA \oplus N_R)$

e. The DB renews the related secrets as follows:

$C_{i+1}= PRNG(N_R \oplus N'_T)$

The DB forwards the messages $\{M_2, MAC, info\}$ to the reader R_i.

Step 6. The reader R_i receives the messages $\{M_2, MAC, info\}$ and compares the computed value $MAC_R=H(DATA_R \oplus N_R)$ with the received MAC by extracting $DATA$ from $info$. If the received messages are authenticated by the reader R_i, M_2 is sent to the tag T_i.

Step 7. The tag veritifies $M_{2\text{tag}}$ using its current keys $\{EPC_s, P_i\}$ and the nonce N'_T. The private keys of the tag are updated as follows:

$C_{i+1}= PRNG(N_R \oplus N'_T)$

(2) Reader Impersonation Attack

Since the channel between the mobile reader and the DB is unsafety, and the adversary has manipulated the reader's outputs, the DB and the tag can authenticate the modified messages from the spoofed reader.

Phase 1 (Learning):

The reader transmits a nonce N_R to the tag, while the tag calculates as follows:

a. $M_1= PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i$

b. $D =N_T \oplus K_i$

c. $C_i= C_i \oplus N_T$

d. $E= N_T \oplus PRNG(C_i \oplus K_i) \oplus P_i$

Phase 2 (Impersonation Reader): To impersonate the reader, the spoofed attacker modifies the blocked messages, where:

Step 1. The spoofed attacker modifies the blocked messages from tag to reader, where:

$M_{1R} =PRNG(EPC_s \oplus N_R) \oplus PRNG(N_T) \oplus K_i \oplus N_R$

Step 2. The reader computes $V= H(RID \oplus N_R \oplus M_1 \oplus N_R)= H(RID \oplus M_1)$

Step 3. The spoofed attacker modifies the blocked messages from the reader to the DB, where:

a. $N_R=0$

b. $M_{1R}= M_1$

c. $V_R = H(RID \oplus M_1)= V$

Step 4. The DB computes and compares the computed V_{DB} with the received V_R.

$V_{DB}= H(RID \oplus N_R \oplus M_{1R})=H(RID \oplus 0 \oplus M_1)$

$= H(RID \oplus M_1)= V_R$

Therefore, the counterfeited reader is verified by the DB, the attack succeeds.

(3) Impersonation Tag Attack

Phase 1 (Learning): Adv eavesdropps the first successful run of protocol and blocks the Step 2, then stores the exchanged messages $\{M_1, D, C_i, E\}$, where:

Step 1. The R_i generates a nonce N_R and sends it to the T_i.

Step 2. The T_i generates N_T and computes M_1, D, C_i, E, then sends them to the R_i

a. $M_1=PRNG(EPC_s \oplus N_R) \oplus PRNG(\oplus N_T) \oplus K_i$

b. $D =N_T \oplus K_i$

c. $C_i= C_i$ ($flag$=0)

d. $E= N_T \oplus PRNG(C_i \oplus K_i) \oplus P_i$

Step 3. The R_i computes $V= H(RID_i \oplus M_1 \oplus N_R)$ and sends V to the DB.

Step 4. After the DB verifies successfully, it computes the messages $\{M_2, MAC, info\}$ as follows:

$M_2 = PRNG(EPC_s \oplus N_T) \oplus P_i$

$Info= DATA \oplus RID \oplus h_{RID} (N_R)$

$MAC=H(DATA \oplus N_R)$

The DB renews the related secrets as $C_{i+1}= PRNG(N_R \oplus N_T)$.

The attacker Adv blocks and stores these information M_2, then stops the session.

Phase 2 (Impersonation Tag): To impersonate the tag T_i, until the reader initiates a second session of protocol, where:

Step 1. the reader initiates a second run of protocol and replays the monitored nonce $N'_R=0$ to the T_i.

Step 2. The T_i produces N'_T and computes $\{M'_1, D', C'_i, E'\}$, then sends them to the R_i. The equations are calculated as follows.

a. $M'_1= PRNG(EPC_s \oplus N'_R \oplus N'_T) \oplus K_i$

b. $D' =N'_T \oplus K_i$

c. $C'_i= C_i \oplus N''_T\ (flag=1)$

d. $E'= N_T \oplus PRNG(C'_i \oplus K_i) \oplus P_i$

Step 3. *Adv* blocks the messages $\{M'_1 \oplus N_R, D', C'_i, E'\}$ from T_i to R_i.

Step 4. The R_i computes $V'= H(RID_i \oplus M'_1 \oplus N_R \oplus N_R) = H(RID_i \oplus M'_1)$ and sends V' to *Adv*.

Step 5. *Adv* modifies the transferred messages as follows:

a. $M_{1Adv}=M'_1 \oplus N_R$

$=PRNG(EPC_s \oplus N'_R \oplus N'_T) \oplus K_i$

b. $D_{Adv}= D'=N'_T \oplus K_i$

c. $C_{iAdv} = C_i$

d. $E_{Adv} = E \oplus D \oplus D'=N'_T \oplus PRNG(C_i \oplus K_i) \oplus P_i$

e. $V_{Adv} =V'= H(RID_i \oplus M'_1)$

f. $N'_R=0$

Subsequently, *Adv* forwards the messages $\{M_{1Adv}, D_{Adv}, C_{iAdv}, E_{Adv}, V_{Adv}, N'_R\}$ to the R_i.

Step 6. (DB authenticates the reader and tag)

From the following compared result, the DB can authenticate the R_i. If $V_{DB}= V_{Adv}$, DB compares transferred message $\{M_{1Adv}, E_{Adv}\}$ with the calculated $\{M_{1DB}, E_{DB}\}$ as following.

$V_{DB}= H(RID \oplus N'_R \oplus M_{1Adv})$

$= V_{Adv} = H(RID_i \oplus M'_1)$

From the above compared result, the DB can authenticate the counterfeited R_i.

b. If C_{iAdv} is not verified, the DB computes the calculated I_{old}.

$I_{old}=M_{1Adv} \oplus PRNG(D_{Adv} \oplus K_{old}) \oplus K_{old}$

$=PRNG(EPC_s \oplus N'_R)=PRNG(EPC_s)$

$X= old=i$

Therefore, the DB verifies that the state of the tag's keys is old.

c. $E_{DB}=D_{Adv} \oplus K_i \oplus PRNG(C_{iAdv} \oplus K_i)\square P_i$

$= D' \oplus K_i \oplus PRNG(C_i \oplus K_i) \oplus P_i$

$=N'_T \oplus PRNG(C_i \oplus K_i) \oplus P_i=E_{Adv}$

After DB verifies $E_{DB}=E_{Adv}$ successfully, it computes the messages $\{M'_2, MAC', info'\}$ as follows:

d. $M'_2 = PRNG(EPC_s \oplus N'_T) \oplus P_i$

$Info'= DATA \oplus RID \oplus h_{RID}\ (N'_R)$

$MAC'=H(DATA \oplus N'_R)$

e. The DB renews the related secrets as follows:

$C_{i+1}= PRNG(N_R \oplus N'_T)$

The tag impersonation attack succeeds.

(4) The Tag Tracing Attack

The attacker can calculate the xored value $D\square E=PRNG(C_i \oplus K_i) \oplus P_i$ using the monitored messages $\{D,E\}$. Therefore, *Adv* traces the target tag^{i} according to the fixed value $PRNG(C_i \oplus K_i) \oplus P_i$.

THE ENHANCED MOHAMMADALI ET AL.'S PROTOCOL

There is a wide variety of applications in a hospital where secure and efficient authentication mechanisms are demanded. For instance, RFID technology ensures the safety of transfusion patients, and creates the accurate and effective medical service for treatment. In order to avoid transfusion-handling errors, this process consists of two phases. First the identities of the patients and liquid medicine bags are confirmed (authentication protocol) and then the matching between both entities is checked (verification step). The process is sketched in Figure. 2 and an authentication protocol is at the core of this application.

Our authentication protocol are shown in Figure. 2 and described below:

Step 1: R →T: N_R. When the physician arrives at the bed, the reader's holder sends a query signal and a nonce N_R to the tag.

Step 2 :T →R: $\{M_1,E,F\}$. The tag generates a nonce N_T and computes the encrypted messages contained patient identifier, concrete disease and medication lists. The most common service in a hospital environment have patient data and medication lists, which call automatically at the display of mobile reader.

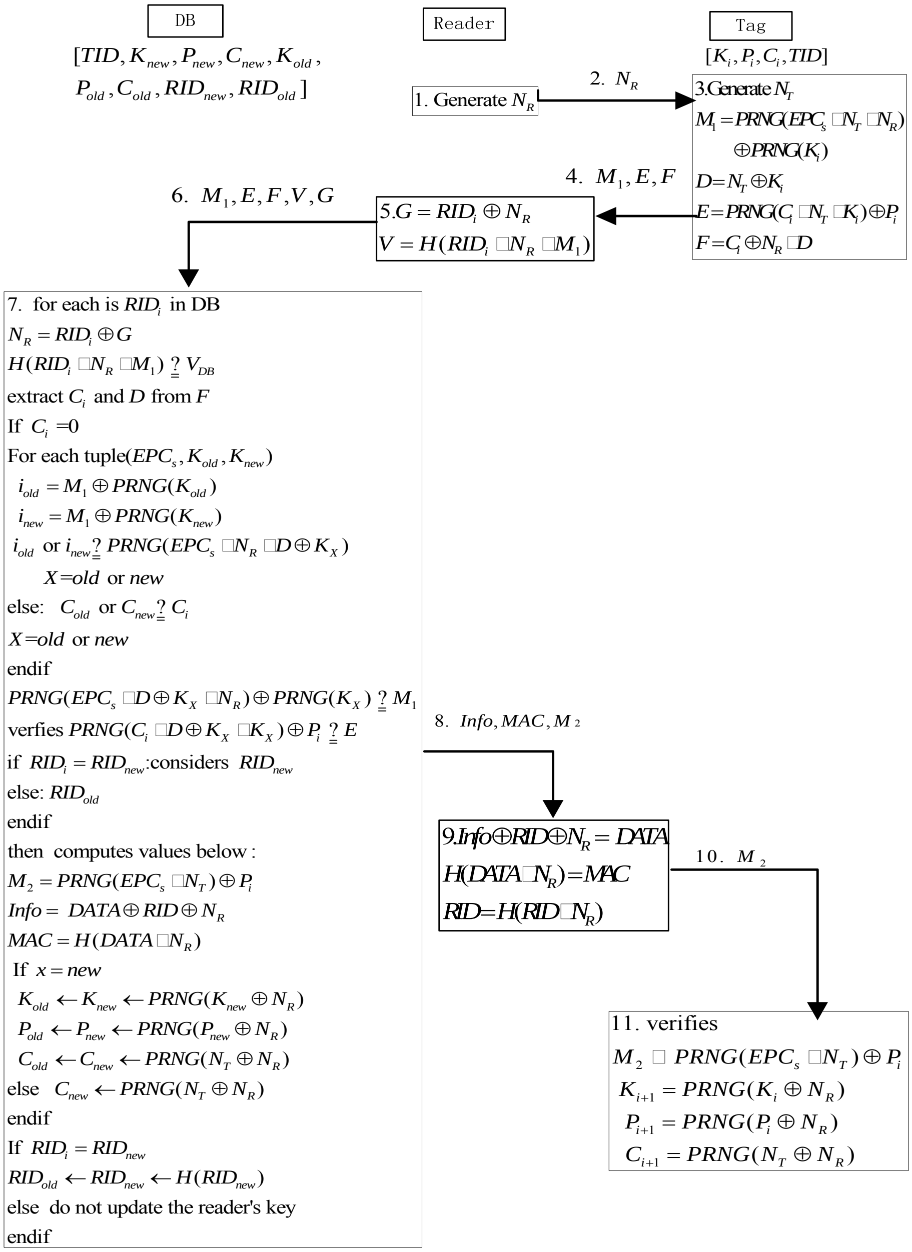

DB
Reader
Tag
$[TID, K_{new}, P_{new}, C_{new}, K_{old}, P_{old}, C_{old}, RID_{new}, RID_{old}]$
$[K_i, P_i, C_i, TID]$
1. Generate N_R
2. N_R
3.Generate N_T
$M_1 = PRNG(EPC_s □N_T □N_R) \oplus PRNG(K_i)$
$D = N_T \oplus K_i$
$E = PRNG(C_i □N_T □K_i) \oplus P_i$
$F = C_i \oplus N_R □D$
4. M_1, E, F
5.$G = RID_i \oplus N_R$
$V = H(RID_i □N_R □M_1)$
6. M_1, E, F, V, G
7. for each is RID_i in DB
$N_R = RID_i \oplus G$
$H(RID_i □N_R □M_1) \underset{=}{?} V_{DB}$
extract C_i and D from F
If C_i =0
For each tuple$(EPC_s, K_{old}, K_{new})$
$i_{old} = M_1 \oplus PRNG(K_{old})$
$i_{new} = M_1 \oplus PRNG(K_{new})$
i_{old} or $i_{new} \underset{=}{?} PRNG(EPC_s □N_R □D \oplus K_X)$
X=old or new
else: C_{old} or $C_{new} \underset{=}{?} C_i$
X=old or new
endif
$PRNG(EPC_s □D \oplus K_X □N_R) \oplus PRNG(K_X) \underset{=}{?} M_1$
verfies $PRNG(C_i □D \oplus K_X □K_X) \oplus P_i \underset{=}{?} E$
if $RID_i = RID_{new}$:considers RID_{new}
else: RID_{old}
endif
then computes values below :
$M_2 = PRNG(EPC_s □N_T) \oplus P_i$
$Info =$ $DATA \oplus RID \oplus N_R$
$MAC = H(DATA □N_R)$
If $x = new$
$K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new} \oplus N_R)$
$P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new} \oplus N_R)$
$C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R)$
else $C_{new} \leftarrow PRNG(N_T \oplus N_R)$
endif
If $RID_i = RID_{new}$
$RID_{old} \leftarrow RID_{new} \leftarrow H(RID_{new})$
else do not update the reader's key
endif
8. $Info, MAC, M_2$
9.$Info \oplus RID \oplus N_R = DATA$
$H(DATA □N_R) = MAC$
$RID = H(RID □N_R)$
10. M_2
11. verifies
M_2 □ $PRNG(EPC_s □N_T) \oplus P_i$
$K_{i+1} = PRNG(K_i \oplus N_R)$
$P_{i+1} = PRNG(P_i \oplus N_R)$
$C_{i+1} = PRNG(N_T \oplus N_R)$

Figure 2 : The improved protocol.

Step 3: R →DB : $\{M_1, E, F, V, G\}$. Upon receiving the messages, the reader computes V $=H(RID||N_R||M_1)$ and forwards (N_R, M_1, F, V, E) to the DB. The nurse or the doctor forwards the messages such as patient identifier, concrete disease and medication lists, to the DB.

Step 4: DB verification and computation

After receiving $\{M_1, E, F, V, G\}$, the DB performs the following operations:

a. The DB searches its look-up table for a value RID_i that satisfies $N_R=RID_i\oplus G$ and $V=H(RID_i||N_R||M_1)$. If the above equation is set up, the DB authenticates the reader of the holder is legal. Some patients need more care and regular checks. For example, if a patient needs a regular check three times a day, the RFID system should remind the responsible personnel. Therefore an automatic checklist can be created.

b. If $C_i= 0$, it stands for the first access. For each tuple $(K_{old},P_{old},C_{old},K_{new},P_{new},C_{new},EPC_s)$, the DB computes values $I_{old} =M_1\oplus PRNG(K_{old})$ and $I_{new}=M_1\oplus PRNG(K_{new})$ in its DB, and checks whether $I_{old}(I_{new})$ matches $PRNG(EPC_s||D\oplus EPC_s||N_R)$. The process is iteratively repeated for each entry until it finds authentication key (K_{new} or K_{old}).

c. When $C_i\neq 0$, the DB considers C_i as an index to find the related keys in the database. If $C_i =C_{old}$, the DB sets $X =old$, otherwise ($C_i =C_{new}$) $X=new$. Then the DB investigates whether M_1 is equal to the computed value $PRNG(EPC_s||D\oplus K_X||N_R)\oplus K_X$.

d. The DB uses K_X and D to obtain N_T, then checks whether the received E matches $PRNG(C_X||D\oplus K_X||K_X)\oplus P_X$ computed by the DB. If the two values match, the back-end server verifies the tag, otherwise terminates the session.

e. The DB computes $M_2 =PRNG(EPC_s||N_T)\oplus P_X$. When the next shift nurse knows which tasks have been done and which have not, another problem in hospitals is that ‘‘change of shift’’ report which includes the tasks that have been done. The checklist can be created automatically by this way. If $RID_i = RID_{new}$, the DB uses RID_{new} to compute $info$ and MAC; otherwise, $RID_i =RID_{old}$. If $X=old$, $info= DATA\oplus RID\oplus N_R$ and $MAC=H(DATA||N_R)$, then DB sends it to the reader. If $X=old$, the DB updates just $C_{i+1}= PRNG(N_T\oplus N_R)$. Otherwise, it updates the record by replacing K_{old} with K_{new},P_{old} with P_{new} and $C_{old} =C_{new}$. New values K_{new}, P_{new} and C_{new} are reset as $PRNG(K_{new}\oplus N_T)$, $PRNG(P_{new}\oplus N_T)$ and $C_{new}=PRNG(N_T\oplus N_R)$.

f. The reader updates secret values $RID_i=RID_{new}$, $RID_{new}=H(RID_{new}||N_R)$, when the received messages are verified successfully. Otherwise, the back-end server does not update the keys of the reader.

Step 5:DB→R:$\{M_2, MAC, info\}$

The DB forwards the messages $\{M_2, MAC, info\}$ to the reader.

Step 6: R→T:$\{M_2\}$

The reader obtains $DATA$, then checks whether the received MAC is equal to $H(DATA||N_R)$. If the message MAC is verified, the reader sends M_2 to the tag and updates secret value $RID=H(RID||N_R)$. After receiving M_2, the tag computes $PRNG(EPC_s||N_T) \oplus P_i$ based on the saved value (N_T, P, EPC_s), then compares the recieved value M_2 with the computed value. If the equations hold, the tag authenticates the reader and updates the its' keys as $K_{i+1}=PRNG(K_i\oplus N_R)$, $P_{i+1}=PRNG(P_i \oplus N_R)$ and $C_{i+1}=PRNG(N_T\oplus N_R)$.

Data acquisition equipments of RFID system and patient data measuring equipments of the clinical manifestation would perform data synchronous updating mechanism according to relevant application requirements. Moreover, the update mechanism that have important meaning towards control condition developing and reducing its harm in time.

THE SECURITY AND PERFORMANCE PROPERTIES ANALYSIS

(1) Tag Impersonation Resistance

In order to impersonate a tag, an adversary should have the forged messages $\{M_1, E,F\}$. In order to compute M_1, the Adv needs EPC_s,K_i and N_T that are unknown for Adv. On the other hand, the current value of E is independent of the value D. Adv can not find the relations from the messages $\{M_1,E,F\}$. Therefore, Adv can not impersonate the tag.

(2) DB Impersonation Resistance

The enhanced protocol is DB impersonation resistance. It is impossible for Adv to obtain $info$ and MAC. Even if the DB receives the replayed N_R in the DB'S verification process,the computations of

$\{M_1, D, E, M_2\}$ need check the integrity of N_T which is known for *Adv*. Therefore, it is impossible for *Adv* to reveal the tag's information.

(3) Reader Impersonation Resistance

It is clear that the forged value V cannot be identified by the DB which checks the integrity of N_R and M_1. Even if *Adv* compromises the current key RID_{cur}, the next key of the reader is updated using N_R which is not known for *Adv*.

(4) Tracing Attack Resistance

If *Adv* uses the monitored messages $\{M_1, E, F\}$ to analyze the tag's keys, we encrypt K_i and C_i using N_T and $PRNG$ (N_T) respectively in the improved protocol. Therefore, *Adv* can not obtain any other secret values and trace the tag.

TABLE 2 and TABLE 3 show the comparison of security and performance properties for the five protocols.

TABLE 2 : The comparison of security properties

Protocols	S1	S2	S3	S4
Protocol[8]	NO	NO	NO	NO
Protocol[9]	NO	NO	NO	NO
Protocol[10]	NO	NO	NO	NO
Protocol[7]	NO	NO	NO	YES
ours	YES	YES	YES	YES

S1 : Tag impersonation resistance; S2 : Server Impersonation Resistance; S3 : Reader Impersonation Resistance; S4 : Tracing Attack Resistance.

The protocol**[7]** shows that protocols**[8-10]** has some weaknesses including tracing attack, DB impersonation, tag impersonation and DATA forgery attack. Moreover, we also show that protocol**[7]** suffers from the reader impersonation, DB impersonation, tag impersonation attack and tracing attack. Since our scheme is more secure than other schemes.

TABLE 3. The comparison of performance properties

Protocols	T1	T2	T3	T4	T5
Protocol[8]	0	6 hash	1	4	NO
Protocol[9]	1hash	6PRNG	1	4	YES
Protocol[10]	0	6PRNG	1	4	YES
Protocol[7]	2hash	7PRNG	2	4	YES
ours	1hash	6PRNG	1	3	YES

T1 : Type and number of encryption functions on reader; T2 : Type and number of encryption functions on tag; T3 : Number of pseudo-random nonces on tag; T4 : Number of outputs on tag; T5: EPC C1G2 compliance.

In our protocol, the tags need not implement hash functions, so that the huge computational workloads can be reduced. Further, the tag computation is restricted to XOR operations and *PRNG*. Thus, performance properties of our scheme is superior to four protocols.

Thus, we see that our scheme provides the required security properties while at the same time conforming to EPC Class-1 Gen-2 standards in the u-healthcare system.

CONCLUSIONS

In our scheme, the tag computation is restricted to bitwise operations, concatenation calculations and pseudo random number generation. All the methods are within the capabilities of EPC Class-1 Gen2 tags. Further, since the tags need not implement hash functions, the huge computational workloads can be reduced. We have demonstrated that Mohammadali et al's protocol is vulnerable to various attacks. Subsequently, we have proposed a new RFID authentication protocol for u-healthcare environment.

As an alleviation, we claim that these enhanced protocols are secure against DB impersonation attack, tag impersonation attack, reader impersonation attack, and afford untraceability and forward secrecy based on the Vaudenay's formal privacy model. Apart from guaranteeing some essential security properties, the improved protocol claims to solve the trade-off between location privacy and low-cost in u-healthcare environment.

REFERENCES

[1] S.D.Kaul, A.K.Awasthi; RFID Authentication Protocol to Enhance Patient Medication Safety. Journal of medical systems, **37(6)**, 1-6 **(2013)**.

[2] J.T.Kim; Enhanced Secure Authentication for Mobile RFID Healthcare System in Wireless Sensor Networks [M]. Computer Applications for Database, Education, and Ubiquitous Computing. Springer. 190-197 **(2012)**.

[3] J.T.Kim; Privacy and Security Issues for RFID Healthcare System in Wireless Sensor Networks [M]. Convergence and Hybrid Information Technology. Springer, 594-601 **(2012)**.

[4] P.Picazo-Sanchez, N.Bagheri et al.; Two RFID Standard-based Security Protocols for Healthcare Environments. Journal of medical systems, **37(5)**, 1-12 **(2013)**.

[5] Y.Ren, R.W.N.Pazzi et al.; Monitoring patients via a secure and mobile healthcare system. Wireless Communications, IEEE, **17(1)**, 59-65 **(2010)**.

[6] A.Ropponen, M.Linnavuo et al.; A novel concept of a wearable information appliance using context-based human–computer interaction. Personal and Ubiquitous Computing, **17(1)**, 159-167 **(2013)**.

[7] A.Mohammadali, Z.Ahmadian et al.; Analysis and Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard. IACR Cryptology ePrint Archive, **(2013)**.

[8] R.H.E.Alakrut, A.Samsudin et al.; Provably Lightweight RFID Mutual Authentication Protocol. International Journal of Security & Its Applications, **7(4)**, **(2013)**.

[9] E.J.Yoon; Improvement of the securing rfid systems conforming to epc class 1 generation 2 standard. Expert Syst.Appl., **39(12)**, 1589–1594 **(2012)**.

[10] T.C.Yeh, Y.J.Wang, T.C.Kuo, S.S.Wang; Securing RFID systems conforming to EPC Class 1 Generation 2 standard, Expert Systems with Applications, Available online, **(2010)**.