journal homepage: www.intl.elsevierhealth.com/journals/ijmi

A comprehensive RFID solution to enhance inpatient medication safety

Pedro Peris-Lopez[a,*], *Agustin Orfila*[a,b], *Aikaterini Mitrokotsa*[a], *Jan C.A. van der Lubbe*[a]

[a] *Delft University of Technology (TU-Delft), Faculty of Electrical Engineering, Mathematics, and Computer Science (EEMCS), Information Security & Privacy Lab, P.O. Box 5031, 2600 GA, Delft, The Netherlands*
[b] *Department of Computer Science, Carlos III University of Madrid, Leganes, Madrid 28911, Spain*

ARTICLE INFO

Article history:
Received 8 December 2009
Received in revised form
13 September 2010
Accepted 6 October 2010

Keywords:
Inpatient safety
Medication error
Nursing informatics
Information technology
RFID security
Grouping-proof protocols

ABSTRACT

Errors involving medication administration can be costly, both in financial and in human terms. Indeed, there is much potential for errors due to the complexity of the medication administration process. Nurses are often singled out as the only responsible of these errors because they are in charge of drug administration. Nevertheless, the interventions of every actor involved in the process and the system design itself contribute to errors (Wakefield et al. (1998) [23]). Proper inpatient medication safety systems can help to reduce such errors in hospitals. In this paper, we review in depth two recent proposals (Chien et al. (2010) [7]; Huang and Ku (2009) [12]) that pursue the aforementioned objective. Unfortunately, they fail in their attempt mainly due to their security faults but interesting ideas can be drawn from both. These security faults refer to impersonation and replay attacks that could produce the generation of a forged proof stating that certain medication was administered to an inpatient when it was not. We propose a leading-edge solution to enhance inpatient medication safety based on RFID technology that overcomes these weaknesses. Our solution, named Inpatient Safety RFID system (IS-RFID), takes into account the Information Technology (IT) infrastructure of a hospital and covers every phase of the drug administration process. From a practical perspective, our system can be easily integrated within hospital IT infrastructures, has a moderate cost, is very ease to use and deals with security aspects as a key point.

1. Introduction

A medication error is a failure in the treatment process that may harm a patient [2]. It can be produced during different phases: prescribing, manufacturing or dispensing the formulation, administering the treatment and monitoring the therapy. Although medication errors are almost inevitable, patient safety can be improved by means of proper Information Technology (IT) systems. For instance, failure due to a misinterpretation of a hand-written prescription can be easily avoided with IT tools. Drug and patient identification systems can automate certain processes to guarantee that the appropriate prescription is given to each patient. According to [2], there are two possible kinds of errors when carrying out a correct plan: action based errors (slips) and memory based errors (lapses). An example of a slip is picking up a bottle containing "diazepam" from the pharmacy shelf when intending to

* *Corresponding author*. Tel.: +31 (0)15 27 83878.
E-mail address: P.PerisLopez@tudelft.nl (P. Peris-Lopez).
1386-5056/$ – see front matter © 2010 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.ijmedinf.2010.10.008

pick up "dilitiazem" instead. A simple example of a lapse is the administration of penicillin to a patient who is actually known to be allergic. Possible known preventive mechanisms for these errors are cross-checking, avoiding distractions and labeling medicines clearly.

According to international studies, medication errors occur predominantly with medication orders (49–56%) or administering medication (26–34%) [13]. A research, made by Peijas Hospital (Finland) [15], supports these international reports: 33.6% of all medication errors were related to documentation, 31.1% were related to medication administration, and 19.5% were linked to medication prescription. Effective nursing is defined as a "five-right" method [3,23]: treating the right patient, with the right drug, in the right dose, in the correct way and at the right time. However, nurses are working under a lot of pressure and the nursing shortage nowadays is a major concern for the healthcare providers [8,18]. Radio Frequency Identification (RFID) technology may help to reduce nurses' workload and decrease their slips and lapses. The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) placed "Improve the accuracy of patient identification" at the top of its list of National Patient Safety Goals (NPSG) again for 2010 [19], a position it has held for years.

1.1. *Background*

This paper uses RFID technology to enhance the medication safety of inpatients. RFID is a technology for identification using radio waves. Its main components are a tag, a reader and a data system for handling the information. An RFID tag includes an antenna and a chip for computation and information storage purposes. The content of the chip can be read and written with an RFID reader. The technology may be comparable to the barcode identification system, where a barcode scanner reads the information from a printed barcode. One of the main differences is that RFID identification systems do not need a line of sight to read or write tags. The information of RFID tags can be rewritten and an RFID reader can read hundreds of tags per second. In addition, RFID tags have computational power, more storage capacity and are more resistant to harsh environmental conditions compared to barcodes. Security mechanisms can also be incorporated into RFID systems providing authentication, non-repudiation, integrity or privacy services.

In 2005, Wu et al. [24] proposed the idea of applying RFID technology to improve drug safety for inpatients. Later, Sun et al. [22] proposed a specific system that uses RFID for inpatient identification and barcodes for unit-dose medication identification. In their system, once a prescription is ordered by the physician, the Hospital Information System (HIS) informs the pharmacy to start the drug package procedure. When the unit-dose (*UD*) is prepared it is labeled with a barcode. The information stored on it (i.e. the drugs making up the unit-dose) is also stored in the database. In order to perform a drug dispatch procedure, a nurse brings a *UD* cart, carrying a PC and a Personal Digital Assistant (PDA), to the inpatient's bedside. Then, the PDA is used as an RFID reader to scan the barcodes on the drug package and the RFID wristband carried by the inpatient. Sun et al. assume that the information needed for matching the barcode identifier with the patient identifier is stored in the PC. The main drawbacks of their proposal are the need to move a PC during the drug administration procedure and the use of barcodes for unit-dose identification instead of low-cost RFID tags. Although their work is very interesting, it lacks important technical details such as a description of the protocol involved in the identification process.

Huang and Ku [12] proposed an RFID grouping proof protocol for the medication safety of inpatients. A grouping proof protocol provides evidence for the simultaneous reading of a group of RFID tags [14,21]. This evidence is created by an RFID reader and can be checked for validity by a verifier. Huang and Ku pursued to create a proof of the simultaneous presence of the inpatient (pallet in their notation) and the drugs corresponding to her prescription. They assumed that every inpatient has a bracelet or wristband with an RFID embedded tag and that every pill container is also identified by an RFID tag. Although it is a good idea to use a grouping-proof to link inpatients with their prescription, the protocol they present has two problems. The first is that, although the proposed grouping-proof protocol is assumed to be executed online (i.e. the reader acts as a verifier in real time) in reality the generated evidence should be verified offline. If an online verifier is available, it is better to use an authentication protocol instead of a grouping-proof protocol, since it is usually more efficient and easier to design [7]. In that case, the design of an online grouping-proof is based on limiting the time span to authenticate each tag. Secondly, Huang and Ku's protocol has some serious security flaws. Chien et al. [7] pointed out some of these flaws and proposed two new protocols: an online authentication protocol and an offline grouping-proof. Unfortunately, both schemes [7,12] are also vulnerable to certain attacks as we will show in Section 2. It is important to note that Huang and Ku's and Chien et al.'s protocols use low-cost tags conforming to EPC Class-1 Generation-2 standard (EPC Gen-2) and that they do not provide anonymous identification. Therefore, an eavesdropper would be able to know the prescription of an inpatient easily.

1.2. *Motivation*

An offline grouping-proof provides evidence for auditing errors but it does not prevent them in real time. An online grouping-proof (i.e. an authentication protocol with time span restriction) demands access to the Hospital Information System (HIS) to verify the proof online. Therefore, it needs some kind of wireless infrastructure to connect PDAs (readers) with the HIS (verifier). We think this approach is expensive and so could be inoperative due to the overload or complete unavailability of the wireless network. Thus, we propose an approach which can be used to verify that an inpatient and her bedside prescription are matched correctly, without using any wireless infrastructure or any other permanent connection to the HIS. Furthermore, our system creates an evidence (offline grouping-proof) establishing that the right unit-dose has been administered to the right inpatient at the right time. Additionally, it enables tracking the identity of the nurses that administered each treatment. Our proposal automates the "five-right" method, thus minimizing errors. It also audits the whole process and allows further investigations on slips and

lapses. The main difference with previous work is that we consider the complete process, from the prescription phase to the monitoring of the therapy phase. Furthermore, we include the technical details of the proposed protocols.

The remainder of this paper is organized as follows. Section 2 exposes our attacks on Chien et al.'s and Huang and Ku's protocols. Then, Section 3 exposes our framework to enhance inpatient safety that focus on security, cost-effectiveness and ease of use. Section 4 analyses the security and the performance of our proposal and finally Section 5 concludes the paper.

2. Attacks on recent protocols for inpatient medication safety

In this section we reveal several security pitfalls in RFID grouping-proofs that aim to enhance inpatient medication safety. Two of the analyzed protocols are online and the last is offline. First, we show how the online protocols [7,12] leak private information in the messages transmitted over the insecure radio channel. This weakness is critical, since it allows the easy impersonation of tags. Then, we describe a replay attack on grouping-proofs that allows the generation of fake proofs. Specifically, a rogue reader can generate a proof that links a subset of simultaneously read legitimate tags to any other legitimate tag. Several grouping protocols such as [7,21] fall into this flaw. We will give details about this fault concentrating on the protocol proposed in [7]. We use the following methodology to describe the proposed attacks. First, the protocol is presented and then the attack and its consequences are exposed.

2.1. *Huang's and Ku's online protocol for medication safety of inpatient*

Huang and Ku [12] proposed an online grouping-proof compatible to Gen-2 standard (EPC Class-1 Generation-2 [10]; ISO/IEC 18006-C [1]), which is one of the most relevant standards for low-cost RFID tags. Unlike previous proposals that use a Message Authentication Code (MAC) and hash functions, operations supported on EPC Gen-2 tags are limited to a 16-bit Pseudo-Random Number Generation (PRNG) function, bitwise operations (e.g. exclusive OR (XOR)), and a Cyclic Redundancy Check (CRC) function. Additionally, these tags have two passwords of 32 bits each: (1) an access password (*PIN*) which controls the access to the reserved memory; (2) a kill password which upon reception irreversibly deactivates the tag.

The authors proposed a scheme to generate an evidence that $\{Tag_1, Tag_2, \ldots, Tag_n, Pallet\ Tag\}$ are scanned simultaneously (see Fig. 1). Tag_i represents a specific drug and the *Pallet Tag* corresponds to the inpatient. For a detailed description of the protocol, the reader is urged to consult [12]. We now focus on the messages received/transmited by one of the participating tags (e.g. Tag_i):

1.0. The reader sends to Tag_i the authentication message m_{i-1} computed by Tag_{i-1}.
2.0. Tag_i computes its response (r_i) and updates its PIN_i:
  2.1. Tag_i inserts m_{i-1} and PIN_i into its PRNG function to generate $r_i = PRNG(m_{i-1})$ and $c_i = PRNG(PIN_i)$, respectively.
  2.2. The tag concatenates the Electronic Product Code (EPC_i) and c_i and computes its *CRC*.
  2.3. The bitwise XOR operation between the above result, c_i and r_i is calculated ($m_i = CRC(EPC||c_i) \oplus c_i \oplus r_i$).
  2.4. The tuple $\{EPC_i, m_i\}$ is sent to the reader and the tag updates its access password ($PIN_i = c_i$).

2.1.1. *Forgery attack on Huang's and Ku's protocol*

Contrary to the author's assumption [12], a CRC is not a secure hash function. Consequently, an attacker may obtain information from the messages transmitted over the channel. CRC functions are based on polynomial arithmetic in F_2. Computing a CRC value for a given binary stream is performed by dividing the polynomial associated with this stream by another fixed polynomial (generator polynomial) and obtaining a remainder. Due to linearity, CRCs have the following properties [11,20]:

$$CRC(A \oplus B) = CRC(A) \oplus CRC(B) \tag{1}$$

$$CRC(A||B) = CRC(A \ll n) \oplus CRC(B) \tag{2}$$

where A and B represent arbitrary values and n is the bit-length of B. An attacker can exploit the above properties to obtain private information linked to the target tag and impersonate this tag in a future grouping-proof protocol. The attacker follows the phases described below.

Phase 1. Acquiring private information:

1.0. The adversary sends to Tag_i an arbitrary value a.
1.1. Tag_i computes its response (r_i) and updates its PIN_i:
  1.1.1. Tag_i first inserts a and PIN_i into its PRNG to generate $r_i = PRNG(a)$ and $c_i = PRNG(PIN_i)$, respectively.
  1.1.2. The tag concatenates EPC_i and c_i and computes its *CRC*. Third, the bitwise XOR operation between the above result, c_i and r_i is calculated ($m_i = CRC(EPC||c_i) \oplus c_i \oplus r_i$).
  1.1.3. The pair $\{EPC_i, m_i\}$ is sent to the adversary and the tag updates its access password ($PIN_i = c_i$).
1.2. The adversary knows value r_i since the known seed a takes part in its generation. The static identifier of the tag (EPC_i) is transmitted in clear over the channel and thus can be easily revealed to the adversary. Taking advantage of this knowledge and the properties of CRC functions, the adversary can disclose certain private information linked to the tag:

$$m_i = CRC(EPC_i||c_i) \oplus c_i \oplus r_i = CRC(EPC_i \ll n) \oplus CRC(c_i) \oplus c_i \oplus r_i \tag{3}$$

More precisely, the adversary obtains $S_i = CRC(c_i) \oplus c_i$, which is a value linked to the target tag univocally. According to the Gen-2 standard c_i's bit-length is 16. Therefore, $n = 16$ in Eq. (2). The reader should note that only public messages are used for

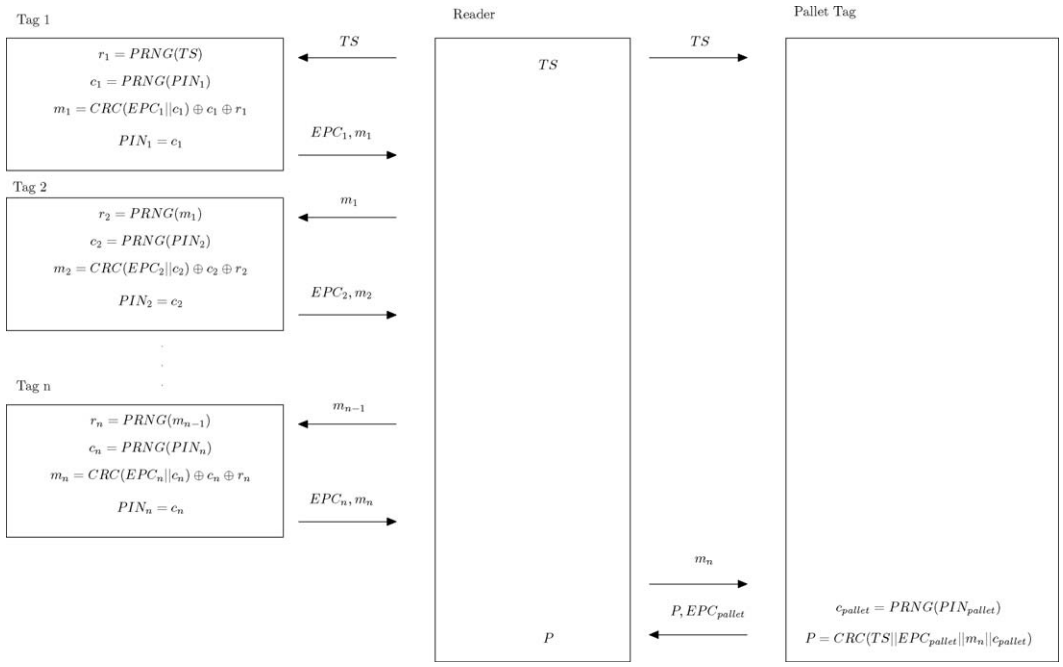

Fig. 1 – Huang's and Ku's online protocol [12] for medication safety of inpatient.

this computation.

$$S_i = CRC(c_i) \oplus c_i = m_i \oplus CRC(EPC_i \ll 16) \oplus r_i \quad (4)$$

Phase 2. Generation of a forged proof:

2.0. The legitimate reader sends to the adversary – impersonating Tag_i – the authentication message m'_{i-1} computed by Tag_{i-1}.
2.1. The adversary inserts m'_{i-1} into its PRNG function and generates $r'_i = PRNG(m'_{i-1})$. Then, the message authentication m'_i is computed by means of Eq. (4), $m'_i = S_i \oplus r'_i \oplus CRC(EPC_i \ll 16)$.

Thus, the adversary can deceive the reader/verifier to think that Tag_i is involved in the proof when it is absent. It is important to note that S_i is closely related to PIN_i. The impact of this attack depends on when it will be launched. In the protocol, the target tag updates its PIN just after the interrogation by the adversary. However, the updating is not performed by the verifier, as this entity is not aware that the tag has been read. That is, the reader and the tag will have lost their synchronization after the tag is read by the adversary. This fact is very advantageous for an adversary since the adversary has an indefinite time window at her disposal to impersonate the tags. After tag impersonation, the corresponding legitimate tag and the verifier are resynchronized, and the whole attack – phases 1 and 2 – must be repeated in order to supplant the legitimate tag again. Thus, updating the secret information (PIN) is an appropriate method, as it reduces the consequence of leaked private information on the channel. However, updates are performed even if there is no confirmation that interrogation comes from a legitimate reader. An adversary can exploit this weakness to conduct a very simple denial-of-service attack: if a fake request is sent to a tag, the tag and the verifier will become unsynchronized. Additionally, Chien et al. [7] show that Huang and Ku [12] scheme is vulnerable to replay attacks.

The consequences of such an attack are very serious in a medical application scenario. Anyone with a device able to simulate a tag (e.g. mobile phone) at her disposal, may generate a forged grouping-proof stating that certain medication was present while it was not. Consequently, a nurse could not refuse any false accusations of negligence or abuse. Regarding the denial of service attack, anyone under the aforementioned conditions may stop the system and prevent the generation of grouping-proofs.

2.2. *Chien et al.'s online protocol to enhance inpatient medication safety*

Chien et al. [7] proposed an authentication protocol conforming to the Gen-2 standard [10]. The operations on the tags are limited to a 16-bit PRNG function and a bitwise XOR operation. Additionally, the verifier and each tag share a secret PIN_i while the tags store into their memory a static identifier (EPC_i). As the verifier (reader) is online, any RFID authentication protocol may be used. Specifically, the following scheme was proposed (see Fig. 2):

0.0. The reader starts the timer.
1.0. The reader generates a random number N_R as a challenge to all the tags in its range.
The following procedure is repeated for all the tags:
2.0. The tag generates a random number N_i, and computes a pseudo-random message authentication code:

$$MAC_i = PRNG(EPC_i \oplus PRNG(PIN_i) \oplus PRNG(N_R) \oplus PRNG(N_i)) \quad (5)$$

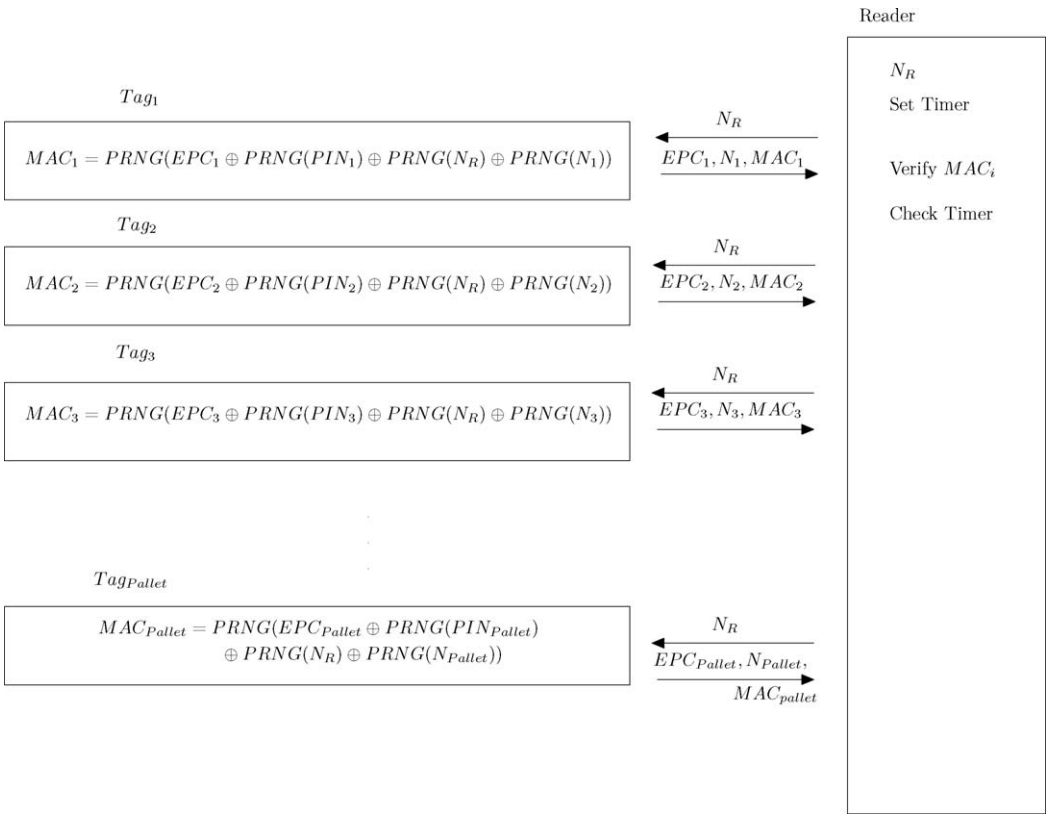

Fig. 2 – Chien et al.'s online protocol [7] to enhance inpatient medication safety.

The tag sends to the reader the tuple $\{EPC_i, N_i, MAC_i\}$.

2.1. The reader stops the timer and checks the correctness of MAC_i for each tag. If MAC_i is correct, the tags $\{Tag_1, Tag_2, \ldots, Tag_n, Tag_{Pallet}\}$ are associated. Otherwise the protocol is aborted. Finally, the reader verifies that all the tags' answers are within a predefined time window.

2.2.1. *Forgery attack on Chien et al.'s protocol*

We now show why the above protocol [7] is vulnerable to a passive attack. Basically, an adversary after eavesdropping several grouping-proof sessions can impersonate a target tag indefinitely. We focus our analysis on a specific Tag_i but it is straightforward to perform the attack in parallel for a set of tags. Suppose that the adversary is eavesdropping the messages exchanged between Tag_i and a legitimate reader. If the adversary detects that the random numbers generated by these two entities are equal (i.e. $N_R = N_i$), then she may intercept the corresponding MAC_i and store it for future use. In such a case, the MAC_i is independent of any random number and becomes a constant value, S_i, as shown in the following equation.

$$\begin{aligned} S_i &= PRNG(EPC_i \oplus PRNG(PIN_i) \oplus PRNG(N_R) \oplus PRNG(N_i)) \\ &= PRNG(EPC_i \oplus PRNG(PIN_i) \oplus PRNG(N_R) \oplus PRNG(N_R)) \\ &= PRNG(EPC_i \oplus PRNG(PIN_i)) \end{aligned} \quad (6)$$

As a consequence, the adversary can impersonate the target Tag_i as described below:

1.0 The reader generates a random number N'_R as challenge to the adversary.

2.0 The adversary sends to the reader the tuple $\{EPC_i, N'_R, S_i\}$.

The adversary – impersonating Tag_i – is thus authenticated by the reader and the attack succeeds. The adversary exploits the linearity of bitwise operations to perform this attack. It is important to note that this attack can be launched at any time.

The remaining question is how many grouping-proof sessions have to be eavesdropped by the adversary to detect a session where $N_R = N_i$. The reader should note here that the random challenges have a length of 16 bits as required by the Gen-2 standard. Therefore, and due to the birthday paradox [4], the adversary has to eavesdrop approximately $\sqrt{(\pi/2)2^{16}} \simeq 286$ sessions to find a collision. In summary, the adversary needs to eavesdrop a small number of sessions to impersonate the target tag and generate a forged grouping-proof.

The impact of such an attack is similar to that described in Section 2.1.1. A nurse could be falsely accused of negligence or abuse, since a forged electronic proof stating that an inappropriate drug was present (and probably administered to an inpatient).

2.3. *Chien et al.'s offline protocol to enhance inpatient medication safety*

Chien et al.'s offline protocol [7] is focused on proving that a specific group of drugs are indeed given to specific inpatients.

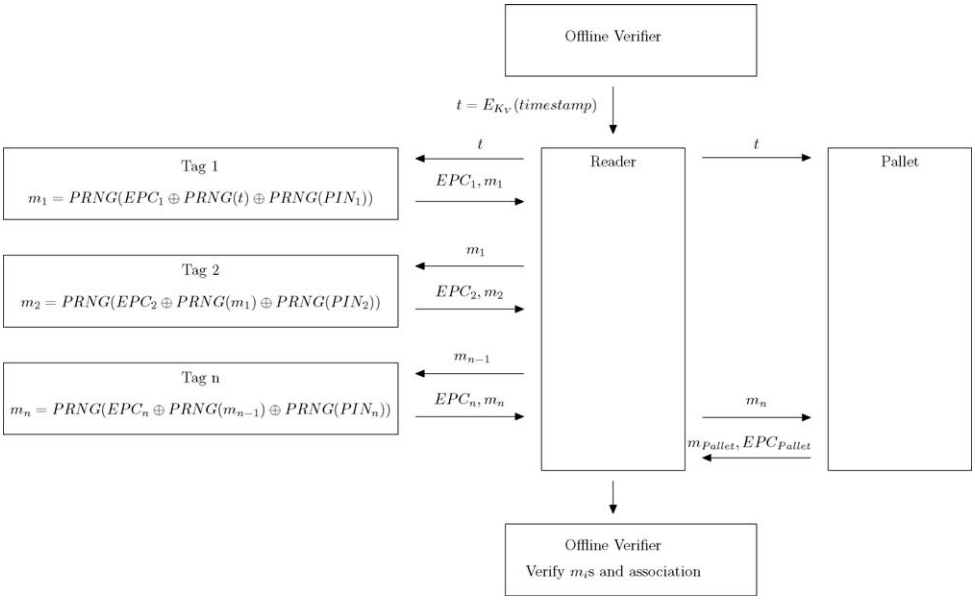

Fig. 3 – Chien et al.'s offline protocol [7] to enhance inpatient medication safety.

Accordingly, the offline verifier knows in advance which drugs correspond to each inpatient (i.e. the prescription). Thus, each drug is associated with a tag and a special tag refers to an inpatient (*Pallet*). In their notation, EPC_i is the tag identifier of Tag_i and EPC_{Pallet} is the tag identifier of the inpatient (*Pallet*). The steps of the protocol, represented in Fig. 3, are the following:

1. *Verifier* → *Reader*: $t = E_{K_V}(timestamp)$
   First, the reader gets an encrypted timestamp $t = E_{K_V}(timestamp)$ from the verifier, where $E_{K_V}(timestamp)$ denotes an encryption of the current timestamp using verifier's secret key K_V.
2. *Reader* → Tag_1, *Pallet*: t
   The reader sends the encrypted timestamp to Tag_1 and the inpatient (*Pallet*).
3. For $i = 1, \ldots, n-1$
   3.1. Tag_i → *Reader*: EPC_i, m_i
   If $i = 1$, then let $m_0 = t$;
   Tag_i computes $m_i = PRNG(EPC_i \oplus PRNG(m_{i-1}) \oplus PRNG(PIN_i))$ and then sends the pair $\{EPC_i, m_i\}$ to the reader.
   3.2. *Reader* → Tag_{i+1}: m_i
   The reader forwards m_i to the next tag Tag_{i+1}.
4. Tag_n and *Pallet*
   4.1. Tag_n → *Reader*: EPC_n, m_n
   Tag_n computes $m_n = PRNG(EPC_n \oplus PRNG(m_{n-1}) \oplus PRNG(PIN_n))$ and then sends the pair $\{EPC_n, m_n\}$ to the reader.
   4.2. *Reader* → *Pallet*: m_n
   The reader forwards m_n to the inpatient (*Pallet*).
   4.3. *Pallet* → *Reader*: EPC_{Pallet}, m_{Pallet}
   Upon receiving m_n, the inpatient (*Pallet*) computes $m_{Pallet} = PRNG(EPC_{Pallet} \oplus PRNG(m_n) \oplus PRNG(PIN_{Pallet}))$ and sends both EPC_{Pallet} and m_{Pallet} to the reader.
5. *Reader* → *Verifier*: $(t, EPC_1, m_1, \ldots, EPC_n, m_n, EPC_{Pallet}, m_{Pallet})$
   The reader collects the evidence $(t, EPC_1, m_1, \ldots, EPC_n, m_n, EPC_{Pallet}, m_{Pallet})$ and forwards it to the verifier.
6. The verifier checks:
   6.1. whether the association $(EPC_1, \ldots, EPC_n, EPC_{Pallet})$ holds for the prescription.
   6.2. whether the evidence $(m_1, .., m_n, m_{Pallet})$ holds.
   6.3. that the decrypted timestamp $D_{K_V}(t)$ is within a reasonable time span.

If all three conditions hold, the grouping-proof succeeds.

2.3.1. *Replay attacks on Chien et al.'s offline protocol*

Chien et al.'s protocol [7] assumes that the verifier knows in advance what the prescription for each inpatient is. Let us suppose that the prescription of inpatient *A* is a subset of the prescription of inpatient *B*. In these conditions, it is possible to generate a proof that inpatient *A* has received her prescription just by eavesdropping the messages exchanged while generating the proof for inpatient *B*. For instance, let inpatient *A*'s ($Pallet_A$) prescription be "ibuprofen" (Tag_1) and "penicillin" (Tag_2) and let inpatient B's ($Pallet_B$) prescription be "ibuprofen" (Tag_1), "penicillin" (Tag_2) and "morphine" (Tag_3). Once the messages corresponding to the grouping-proof for inpatient *B* $(t, EPC_1, m_1, EPC_2, m_2, EPC_{Pallet_B}, EPC_3, m_3, m_{Pallet_B})$ have been eavesdropped, a rogue reader can replay m_2 to inpatient *A* ($Pallet_A$) and generate the corresponding fake proof with the response $(t, EPC_1, m_1, EPC_2, m_2, EPC_{Pallet_A}, m_{Pallet_A})$.

This attack has a severe impact when a nurse forgets to administer the appropriate treatment to an inpatient. In that case she could easily generate a forged proof stating that the treatment was administered while it was not. In the aforementioned example, given that the nurse has administered the proper treatment to inpatient *B* at the right time, she could also generate an out-of-time proof and claim that she has also administered the appropriate treatment to inpatient *A*.

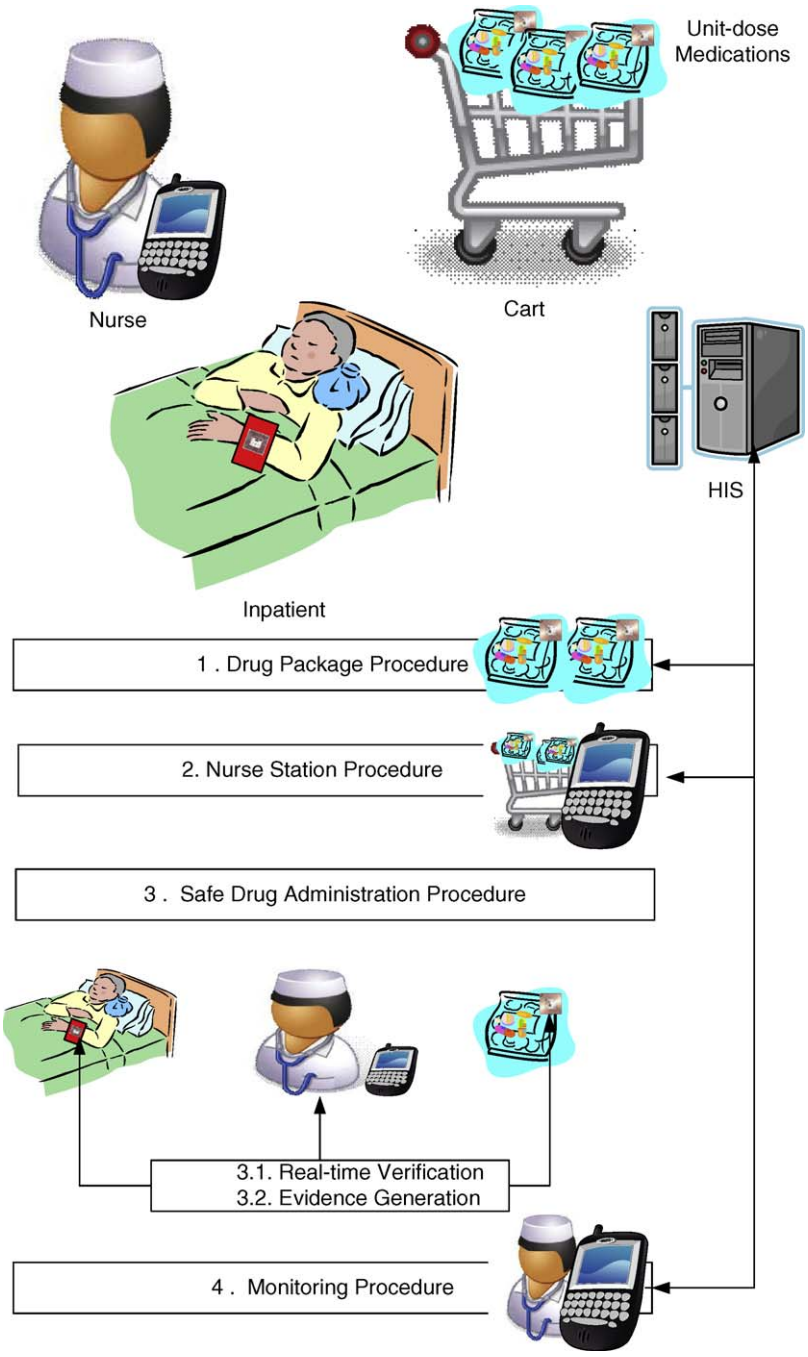

Fig. 4 – Phases of IS-RFID system.

3. IS-RFID system

In this section, we propose an innovative solution to enhance medication safety based on RFID technology. We name our solution Inpatient Safety RFID system (IS-RFID). While previous proposals [7,12] focus on an specific problem such as the grouping-proof protocol, our solution is designed to take into account the complete IT infrastructure of a modern hospital [16]. Although barcodes are a mature identification technology, we favor the use of RFID technology, since the latter has significant advantages.

In our proposed system, RFID tags are linked to the inpatients (e.g. wristbands) and to the unit-dose medications (e.g. labeled plastic packages) that need to be identified. RFID readers obtain the static identifier of each tag, which may then be used as a search index in a database to retrieve all the information linked to the labeled item. The reader must be connected to the back-end database via a secure (i.e. authenticated and encrypted) channel in order to access the aforementioned information. This is a usual assumption in RFID systems. We assume that the used tags conform the EPC Gen-2 standard and thus are passive, have a 32-bit password and support an on-board 16-bit PRNG function.

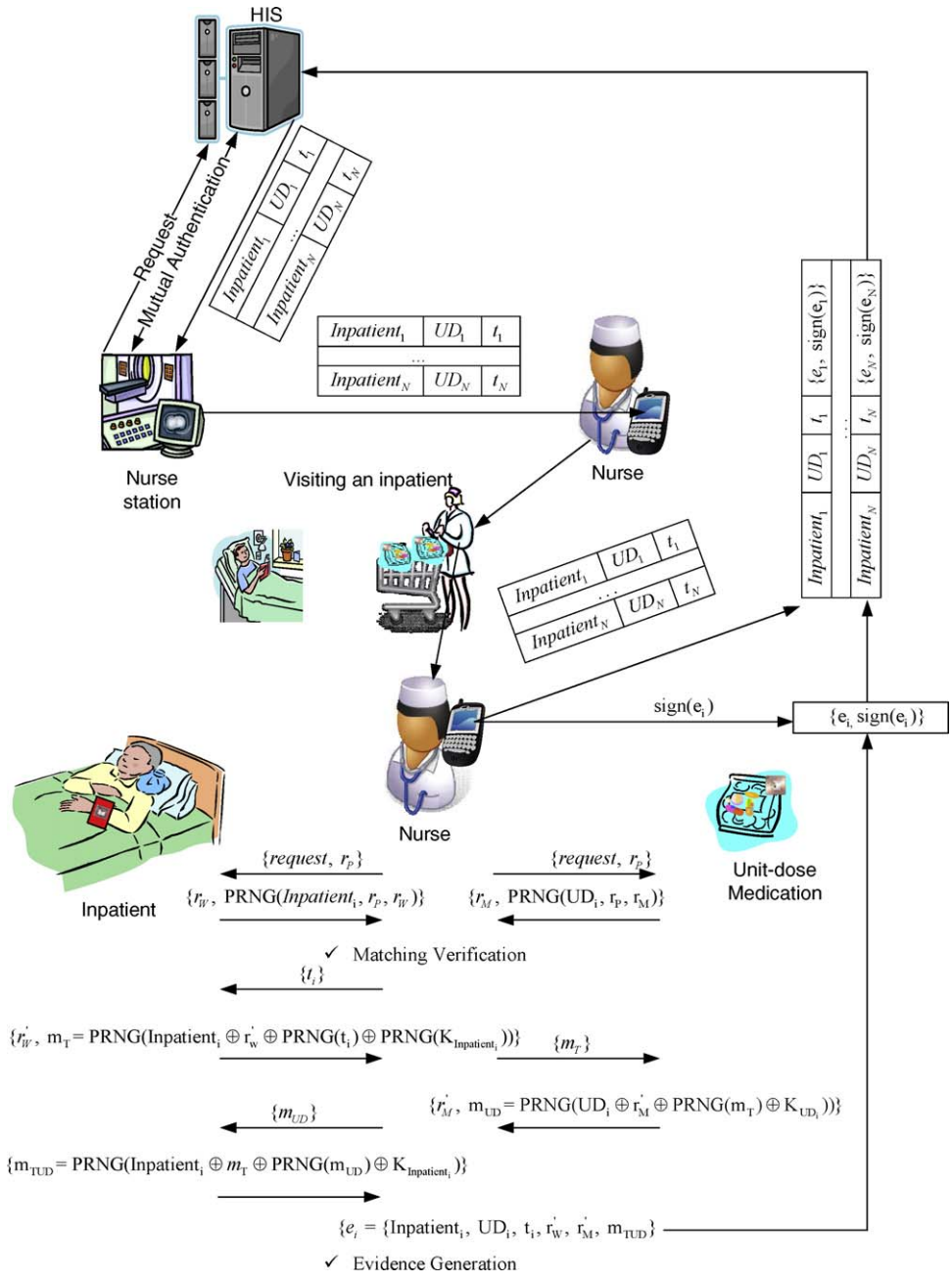

Fig. 5 – IS-RFID protocol.

We now describe how the proposed system works within the framework of a hospital IT infrastructure where it is crucial to avoid errors in the administration of drugs. Specifically, four procedures should be followed to guarantee the safety in the administration of the physician's orders (see Figs. 4 and 5):

Drug package procedure: A physician visits an inpatient to diagnose her. First, the physician reads the RFID tag attached to her wristband by using a PDA that includes an RFID reader. A static identifier ($Inpatient_i$) is obtained from this reading and the inpatient is univocally identified. After the examination of the inpatient, he issues a new prescription (i.e. a list of medications). Once the physician has visited his inpatients, he goes to his office and connects the PDA to his PC to register the prescriptions to the Hospital Information System (HIS). Then, the HIS informs the pharmacy to start the drug package procedure. In the pharmacy, the Automatic Medication Dispenser (AMD) prepares the unit-doses according to the orders received. Basically, the AMD picks up each drug included in each prescription and introduces them in a plastic package. During this process, a grouping-proof such as the one described in [17] may be used to generate an evidence that these drugs were indeed introduced simultaneously in the corresponding package. Then, the AMD generates an identifier (UD_i) to this unit-dose and writes this information on a passive tag, which is finally attached to the packet. The AMD informs the HIS about the completion of the process and the

unit-dose identifier is registered in the HIS. Thus, at this point, the HIS has the following record linked to the inpatient.

$Inpatient_i$	UD_i	$Additional\_Information_i$

The additional information field may include the time interval for unit-dose administration, the right route and the right dose or even a link to the electronic patient record.

Nurse station procedure: The nurse station receives a cart from the pharmacy with the unit-dose medications for the inpatients in floor *F*. A nurse – using a PC station – is logged into the system and gets access to the HIS. Then, she sends an information request about the drugs that have to be dispatched in the floor *F* at the current administration period. Consequently, the HIS sends the tuples $\{Inpatient_i, UD_i, t_i, Additional\_Information_i\}_{i=1}^{i=N}$, assuming that a group of *N* inpatients are in floor *F*. The third element t_i represents a timestamp that will be valid within a time window specified in advance and registered into the HIS. That is, the administration of the UD_i to the $Inpatient_i$ has to be carried out within this time window. Finally, the nurse transfers these records to her PDA and the administration round starts. This last step is crucial and facilitates the fact that the next step can be offline (i.e. no connection with the HIS needed). This represents a significant advantage over previous proposals such as [22] in which a permanent connection to the HIS database is required. Accordingly, the following information is stored in the nurse's PDA:

$Inpatient_1$	UD_1	t_1	$Additional\_Information_1$
		...	
$Inpatient_i$	UD_i	t_i	$Additional\_Information_i$
		...	
$Inpatient_N$	UD_N	t_N	$Additional\_Information_N$

Safe drug administration procedure: Each nurse is equipped with a PDA that functions as an RFID reader and as a local device. The nurse takes the PDA and the cart with the doses and visits the inpatients to administrate their treatments. The process is divided into two phases (see the bottom part of Fig. 5).

A: Verification process is executed just before administration in order to check the univocal correspondence between an inpatient and her unit-dose.
B: An evidence of drug administration to an inpatient is generated by the nurse.

By means of these procedures, we pursue to enhance medication safety for inpatients. Our automatic verification is incorporated into the drug administration process to prune human errors [6,9]. By a simple and transparent mechanism, the nurse can gain confidence of the matching between the inpatient at her side and the corresponding unit-dose medication. More precisely, the following procedure – depicted in Fig. 5 – is proposed.

Step A.1. The nurse's RFID reader generates a random number r_p and sends a request message $\{request, r_P\}$ to the tag attached to the inpatient wristband and to the tag linked to the drugs package.
Step A.2. Each of these two tags receives the request, computes and sends an anonymous identifier to the reader, where r_W and r_M represent random numbers generated by the inpatient's tag and unit-dose's tag, respectively.
- The inpatient's tag computes and sends $\{r_W, PRNG(Inpatient_i, r_P, r_W)\}$ to the reader.
- The unit-dose's tag computes and sends $\{r_M, PRNG(UD_i, r_P, r_M)\}$ to the reader.

Step A.3. The reader receives both values and a search process starts over the PDA stored records. The pair $\{Inpatient_1, UD_1\}$ is obtained and the PDA generates a local version of the anonymous identifiers: $\{PRNG(Inpatient_1, r_P, r_W), PRNG(UD_1, r_P, r_M)\}$. If these computed values equal the received values, a confirmation message is displayed in the screen of the PDA, a log is created, and the nurse can safely administer the drugs to the inpatient. Otherwise, the process is repeated with the following record $\{Patient_2, UD_2\}$ in the PDA until a match is found or there are no more records. If no match is found, the nurse stops the administration procedure and investigates the problem.

Once the inpatient and the unit-dose medication are matched the nurse administers the treatment. In addition, she can generate an evidence of the correct administration of treatment by simultaneously scanning both tags within the time window specified by the HIS. Considering that the proposed approach uses passive RFID tags, the effectiveness of the protocol depends on the reader's reliable function who activates the tags (i.e. passive backscatter or inductive coupling). The inpatient's and the unit-dose's tags store an identifier and a key in their memory: that is, $\{Inpatient_i, K_{Inpatient_i}\}$ and $\{UD_i, K_{UD_i}\}$, respectively. The messages exchanged between the three involved entities are described below (see Fig. 5):

Step B.1. The nurse's RFID reader queries the inpatient's tag by using the timestamp $\{t_i\}$ stored in the corresponding record of the PDA.
Step B.2. The inpatient's tag generates a random number r'_W and computes $m_T = PRNG(Inpatient_i \oplus r'_W \oplus PRNG(t_i) \oplus PRNG(K_{Inpatient_i}))$. The tag sends $\{r'_W, m_T\}$ to the reader.
Step B.3. The reader stores r'_W and submits m_T to the unit-dose tag.
Step B.4. The unit-dose tag generates a random number r'_M and computes $m_{UD} = PRNG(UD_i \oplus r'_M \oplus PRNG(m_T) \oplus K_{UD_i})$. The tag sends $\{r'_M, m_{UD}\}$ to the reader.
Step B.5. The reader stores r'_M and submits m_{UD} to the inpatient tag.
Step B.6. The inpatient tag computes $m_{TUD} = PRNG(Inpatient_i \oplus m_T \oplus PRNG(m_{UD}) \oplus K_{Inpatient_i})$ and sends the result to the reader.
Step B.7. The reader generates the evidence, $e_i = \{Inpatient_i, UD_i, t_i, r'_W, r'_M, m_{TUD}\}$.

Step B.8. The intervention of the nurse (e.g. password authentication) is required to generate a digital signature of the evidence ($sign(e_i)$). Finally, the evidence and the signature $\{e_i, sign(e_i)\}$ are stored in the corresponding PDA record.

As a consequence, the following information is stored in the nurse's PDA after the completion of her round:

$Inpatient_1$	UD_1	t_1	$\{e_1, sign(e_1)\}$	$Additional\_Information_1$
			...	
$Inpatient_i$	UD_i	t_i	$\{e_i, sign(e_i)\}$	$Additional\_Information_i$
			...	
$Inpatient_N$	UD_N	t_N	$\{e_N, sign(e_N)\}$	$Additional\_Information_N$

Monitoring procedure: The nurse comes back to her station. She logs into the system – using a PC station – and informs the HIS about the unit-dose administration process. Specifically, she transfers the records stored in the PDA ($\{Inpatient_i, UD_i, t_i, \{e_i, sign(e_i)\}, Additional\_Information_i\}_{i=1}^{i=N}$) to the HIS database. The HIS checks the validity of the received evidence and also examines that they were generated within the specified time window. If an error is detected, an alarm is generated and an error drug administration procedure is triggered. Furthermore, if an inpatient later suffers a complication, the HIS is able to analyze the evidence. It is also important to note that the proposed system renders the auditing procedure easy.

4. Security, performance and cost analysis

RFID is a relatively heterogeneous technology with a significant number of connected standards. Within these standards, one of the most relevant is the EPC Gen-2 specification [10]. This standard can be considered as a "universal" specification for low-cost RFID tags. In this paper, we pursue to design an RFID solution compatible with Gen-2 specification. The use of low-cost tags and standardized solutions results in a moderate-cost investment. We assert that the numerous benefits of RFID technology compensate for the slightly higher price of individual tags as compared to printed barcodes.

It is well-known that the Gen-2 standard offers low-level security [20]. Particularly, privacy protection is not a main concern of this specification and tags indiscriminately transmit their static identifier over the insecure radio channel. To the best of our knowledge, this undesirable property is inherited by every RFID grouping-proof protocol conforming to the standard [7,12]. In the application scenario of inpatient medication, confidential information such as the patient treatment may be compromised by simple eavesdropping on the radio channel. Our proposal is designed in such a way to take into consideration the main security concerns (i.e. privacy, authentication, integrity) for the intended medical application and requires only very slight modification of the EPC Gen-2 specification. In fact, it is possible to reach a trade-off between designing a reasonably secure system and being compatible with Gen-2 standard. IS-RFID tags use a PRNG function and perform bitwise XOR operations as dictated by the specification. The probability of having a successful brute-force attack in the real-time check process (phase A) and the evidence generation process (phase B) is bounded by $1/2^{16}$. That is because the PRNG function supported by the employed tags has a length of 16 bits. Thus, the probability of having a successful brute-force attack in the whole protocol is bounded by $1/2^{32}$ since each process (phases A and B) is independent from the other. The use of strong cryptographic primitives instead of a simple 16-bit PRNG function would increase the security level but also lead to stronger hardware requirements (i.e. circuit area, memory and power consumption), and thus to more expensive tags.

In our design, the verification check (phase A) and the evidence generation (phase B) are completely independent. An improvement of the proposed scheme is to link the two processes (i.e. the output of phase A, $\{v_T, v_{UD}\} = \{PRNG(Inpatient_i, r_P, r_W), PRNG(UD_i, r_P, r_M)\}$, could be used as input, in phase B). This way, we would guarantee causality: phase A must be completed before the execution of phase B. A straightforward solution could be the replacement of phase's B input (i.e. the timestamp $\{t_i\}$) – sent at the start of the evidence generation – by the value $\{PRNG(t_i \oplus v_T \oplus v_{UD})\}$.

An important aspect of our proposal is its efficiency. Solutions based on the use of pseudonyms – anonymized versions of the static identifiers – present the drawback of needing an exhaustive search in the back-end database [5]. However, our approach does not suffer from this disadvantage, since we have the advantage of knowing in advance which specific tags (i.e. the inpatients and their corresponding medications) are involved in the identification process. Due to this fact, the search is limited to a reduced number of tags and so the efficiency of our system is increased.

As previously shown, the system can be considered secure and efficient because of the security mechanisms used. Next, we propose a procedure to test the effectiveness of IS-RFID system in real environments. Let us consider a hospital where floor A uses IS-RFID system and floor B continues using the old system. The new system should be tested during a certain period of time (e.g. 6 months). During this period, the following activities should be done: (1) check correspondence in HIS (logs) between what is expected to happen and what really happened (i.e. errors in a) patient identification; (b) administration of drugs; (c) dose, etc.); (2) report nurses comments regarding usability and performance; (3) report inpatient comments about safety. After the completion of the trial period, compare the results in floor A with results in floor B: (1) compare the number of errors (inpatient safety); (2) compare times of nursing rounds (efficiency and usability).

The necessary investment is affordable due to IS-RFID system fits into the existing HIS and takes into account the most modern process in the management of drugs (i.e. AMD). More precisely, the cost of deploying the system can be computed adding up the price of the low-cost tags multiplied by the number of inpatients and unit-doses. Let us consider a floor with 5000 inpatients/year and 3 unit-dose/day and a cost of \$0.5/tag – including the plastic package of each unit-dose. This means \$20.55/day or \$7500/year. Every nurse should be also equipped with a PDA in which a software of inpatient medication safety is installed (∼\$300). In the aforementioned example, we can assume that each floor is attended by 3 nurses (4.5 inpatient/nurse). Finally, an average hospital with 8 floors would

Table 1 – Advantages and weaknesses of IS-RFID system.

Advantages	Weaknesses
√ Effectiveness on "five-right" method	× Initial investment on new technology
√ ROI in inpatient medication safety	× Learning process
√ Integration with HIS and AMD	× Excessive confidence on technology
√ Automatic verification	
√ Generation of evidences	
√ Audit and alarm process	
√ Increased efficiency	

have to cover a total investment of around $70,000/year. Note that the cost of HIS and AMD are excluded of this count since these systems are already included in the overall costs of the hospital.

Finally, we assume that our system is not perfect and it may possess certain weak points. In fact, the weaknesses of IS-RFID are those related to deploy a new technology. A learning process by healthcare personnel is needed and new procedures have to be applied. Although there is a cost for deploying the new technology, the system offers a definite ROI in the inpatient medication safety. The most serious risk is that nurses might rely on this new technology in such a way that they relax and do not check possible human errors manually. For instance, there can be an error when introducing the prescription in the HIS database. In a such a case, the Automatic Medication Dispenser (AMD) would prepare an erroneous unit-dose for the inpatient. Furthermore, errors can occur if technology is not used appropriately by personnel. For example, a nurse who has not administered a unit-dose to an inpatient could create an evidence of having done it. The positive point here is that every event is logged into the system and audit processes could detect these bad practices. We emphasize that future improvements in healthcare will come both from better medicine and from improved systems engineering. In Table 1, we summarize the positive and negative points of IS-RFID.

5. Conclusion

The safe medication care is based on the "five-right" principles [3], namely: treating the right inpatient, with the right drug, in the right dose, in the right way and at the right time. IS-RFID has been designed to fulfill all of them. Our proposed system covers the procedures in which medication errors occur predominantly, that is medication orders and administering treatment. Thus, handwritten prescriptions are substituted with electronic orders that are stored in the HIS and sent to the pharmacy. Human slips such as taking an incorrect pill with a similar name are drastically reduced, automating the identification process of drugs and unit-doses (collection of drugs linked to inpatient treatment). Lapses are also reduced, since nurses perform two checks: a human and an electronic one. Thanks to IS-RFID, if the drugs administered to an inpatient do not match her prescription, the administration process is stopped. Furthermore, even if an error happens post-medication procedures can be quickly implemented when the HIS checks the evidences that proves the simultaneous presence of the unit-doses and the inpatients within a specified time window.

Not only the inpatient safety is enhanced but audit procedures become more accurate and easier to perform. In this context, liability is cryptographically supported because the evidences are digitally signed providing the non-repudiation property. Therefore, the investigation of errors can be done quickly and the mechanisms to avoid their repetition can be developed rapidly.

IS-RFID also increases the efficiency of the healthcare personnel. Automation facilitates the work of nurses, physicians and pharmacists. Nurses do not need to spend time decoding handwritten prescriptions or preparing unit-doses any longer. The matching between the unit-dose and the inpatient is done electronically so nurses can focus on the inpatient care. Furthermore, the evidence of proper administration that the system generates allows the nurses to defend their good professional practices.

It is important to note that our proposal is cost-effective and takes into account the general hospital infrastructure: HIS, AMD and nurse stations. The only additional demand is to equip nurses with a PDA that incorporates an RFID reader. Other approaches [22] require portable PCs to visit the inpatients or a wireless infrastructure. IS-RFID system only needs an online connection to the HIS database at the nurses' stations. In addition, the RFID tags are not attached to single items (pills) but to unit-doses. The security properties that RFID tags support in comparison to barcodes as well as the more general benefits of RFID identification justify the investment.

Summary points

What was already known before this article

- Errors involving medication administration can be costly, both in financial and in human terms.
- Proper inpatient medication safety systems can help to reduce errors in hospitals.
- RFID grouping-proof protocols provide evidence generation at bedside of the simultaneous presence of an inpatient and the drugs corresponding to her prescription.

What this article added

- The security faults on previous RFID grouping-proof protocols for inpatient medication safety.
- A leading-edge solution, IS-RFID, to enhance inpatient medication safety based on RFID technology, that covers every phase of the drug administration process and takes into account the Information Technology infrastructure of a hospital.
- IS-RFID fulfills the "five-right" principles for reducing medication errors: treating the right inpatient, with the right drug, in the right dose, in the right way and at the right time.
- IS-RFID system makes audit procedures accurate and easy to perform.

Authors contributions

Medication errors (PPL, AO), RFID solution to enhance inpatient medica-tion safety (PPL, AO), IT Hospital Infrastructure (AM, JL), IS-RFID System-design and analysis- (PPL, AO, AM, JL).

Conflict of interest

All authors declare that we have no conflicts of interest in relation to this manuscript.

Acknowledgements

We would like to thank Christos Dimitrakakis for additional proofreading. This work was partially supported by the Netherlands Organization for Scientific Research (NWO) under the RUBICON grant "Intrusion Detection in Ubiquitous Computing Technologies" awarded to Aikaterini Mitrokotsa.

Contributions: Medication errors (PPL, AO), RFID solution to enhance inpatient medication safety (PPL, AO), IT Hospital Infrastructure (AM, JL), IS-RFID System design and analysis (PPL, AO, AM, JL).

REFERENCES

[1] ISO/IEC 18006-C, Information technology – radio frequency identification for item management – part 6: parameters for air interface communications at 860 MHz to 960 MHz, 2005. Available from: http://www.iso.org.
[2] J.K. Aronson, Medication errors: what they are, how they happen, and how to avoid them, QJM: An International Journal of Medicine 102 (8) (2009) 513–521.
[3] D.M. Benjamin, Reducing medication errors and increasing patient safety: case studies in clinical pharmacology, Journal of Clinical Pharmacology 43 (7) (2003) 768–783.
[4] D. Blomm, A birthday problem, American Mathematical Monthly 80 (1973) 1141–1142.
[5] L. Buttyan, T. Holczer, V. F Istvan, Optimal key-trees for tree-based private authentication, in: Workshop on Privacy Enhancing Technologies – PET 2006, Cambridge, UK, June, 2006.
[6] M.R Chassin, E.C. Becher, The wrong patient, Annals of Internal Medicine 136 (11) (2002) 826–833.
[7] H.-Y. Chien, C.-C. Yang, T.-C. Wu, C.-F. Lee, Two RFID-based solutions to enhance inpatient medication safety, Journal of Medical Systems (2010).
[8] J.W. Cooper, Adverse drug reaction-related hospitalizations of nursing facility patients: a 4-year study, Southern Medical Journal 92 (5) (1999) 485–490.
[9] B. Van de Castle, J. Kim, M.L.G. Pedreira, A. Paiva, W. Goossen, D.W. Bates, Information technology and patient safety in nursing practice: an international perspective, International Journal of Medical Informatics 73 (7–8) (2004) 607–614.
[10] EPC Class-1 Generation-2 Class-1 Generation 2 UHF Air Interface Protocol Standard Version 1.2.0: "Gen-2", 2008. Available from: http://www.epcglobalinc.org/standards/.
[11] D. Han, D. Kwon, Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards, Computer Standards & Interfaces 31 (4) (2009) 648–652.
[12] H.-H. Huang, C.-Y. Ku, A RFID grouping proof protocol for medication safety of inpatient, Journal of Medical Systems 33 (6 (December)) (2009) 467–474.
[13] R.G. Hughes, E. Ortiz, Medication errors: why they happen, and how they can be prevented, American Journal of Nursing 105 (3 Suppl.) (2005) 14–24.
[14] A. Juels, "Yoking-Proofs" for RFID tags, in: R. Sandhu, R. Thomas (Eds.), International Workshop on Pervasive Computing and Communication Security – PerSec 2004, Orlando, Florida, USA, March 2004, IEEE, IEEE Computer Society, pp. 138–143.
[15] V. Jylh, K. Saranto, Electronic documentation in medication reconciliation – a challenge for health care professionals, Applied Nursing Research 21 (4) (2008) 237–239.
[16] A. Lahtela, M. Hassinen, Requirements for radio frequency identification in healthcare, in: Medical Informatics in a United and Healthy Europe – Proceedings of MIE 2009, The XXIInd International Congress of the European Federation for Medical Informatics, Studies in Health Technology and Informatics, vol. 150, 2009.
[17] Y. Lien, X. Leng, K. Mayes, J.-H. Chiu, Reading order independent grouping proof for RFID tags, in: IEEE International Conference on Intelligence and Security Informatics, ISI 2008, Taipei, Taiwan, June, IEEE, 2008, pp. 128–136.
[18] L. Lotas, C. McCahon, J. Kavanagh, M. Dumpe, M. Talty, K. Knittel, C. O'Malley, The other nursing shortage: a regional collaboration to address the shortage of nursing faculty, Policy, Politics, and Nursing Practice 9 (4) (2008) 257–263.
[19] The Joint Commission on Accreditation of Healthcare Organizations, 2010 National Patient Safety Goals (NPSGs), 2009. Available from: http://www. jointcommission. org/PatientSafety/NationalPatientSafetyGoals.
[20] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard, Computer Standards & Interfaces 31 (2) (2009) 372–380.
[21] J. Saito, K. Sakurai, Grouping proof for RFID tags, in: Conference on Advanced Information Networking and Applications – AINA, vol. 2, Taiwan, March 2005, IEEE, pp. 621–624.
[22] P.R. Sun, B.H. Wang, F. Wu, A new method to guard inpatient medication safety by the implementation of RFID, Journal of Medical Systems 32 (4) (2008) 327–332.
[23] B.J. Wakefield, D.S. Wakefield, T. Uden-Holman, M.A. Blegen, Nurses' perceptions of why medication administration errors occur, MedSurg Nursing 7 (1 (February)) (1998) 39–44.
[24] F. Wu, F. Kuo, L.-W. Liu, The application of RFID on drug safety of inpatient nursing healthcare, in: ICEC '05: Proceedings of the 7th International Conference on Electronic Commerce, New York, NY, USA, ACM, 2005, pp. 85–92.