# Securing the Communications of Home Health Care Systems based on RFID Sensor Networks

Wiem Tounsi, Joaquin Garcia-Alfaro, Nora Cuppens-Boulahia, Frédéric Cuppens

Institut Télécom, Télécom Bretagne
LUSSI Department, 2 rue de la Châtaigneraie,
CS 17607, 35576 Cesson Sévigné, France

E-mail: {FirstName.SurName}@telecom-bretagne.eu

## Abstract

*We address security solutions to protect the communication of the wireless components of a home health care system. We analyze especially the problem of exchanging secrets to satisfy authentication of entities. We outline some important aspects that must be guaranteed given the existence of low-cost and resource-constrained RFID components. Appropriate solutions must, therefore, enable several nodes, with different computing and communicating capabilities, to securely interact and communicate.*

**Key words**: Network Security; Wireless Security; RFID; Sensor Networks; Cryptographic Protocols.

## 1 Introduction

Sensor networks are a specific kind of ad hoc networks, which are highly decentralized and without infrastructure. In the same context, Radio Frequency IDentification (RFID) appears as a low-cost technology based on battery-less devices, and acclaimed as the successor of today's omnipresent bar codes. Over the last years, substantial progress has been made to integrate these two technologies into context-aware applications that combine the advantages of RFID with those of wireless sensor networks [4]. A promising scenario is the use of these two technologies to implement home health care systems [34, 27]. Securing the different components of these systems becomes both essential and challenging. Indeed, the integrity and availability of the information collected by such systems must be guaranteed for all the components, and the leakage of any sensitive information must be prevented [12]. The use of appropriate cryptographic schemes and, therefore, the establishment of secret keys among the system components is necessary to address these problems[6].

We survey in this paper some existing solutions that may allow the deployment of secure communications among the heterogeneous nodes of such aforementioned combination of technologies. We analyze and discuss the applicability of each reviewed solution in order to guarantee the security requirements of systems especially adapted to the surveillance of elder care. We focus our discussion on approaches that successfully satisfy the complexity imposed by the existence of nodes with different computing and communicating capabilities.

**Organization of the paper —** Section 2 provides further details of our motivation scenario and related works. Section 3 reviews a selected set of solutions and discusses the pertinence of each solution. Section 4 closes the paper.

## 2 Motivation and Related Works

The aging of our societies is an inescapable fact. According to a study made at U.S. Office of Censorship in 2000 [8]: *the net balance of the world's elderly population has increased by more than 750.000 per month; Two decades from now, the increase will likely be 2 millions per month*. In addition, elder patients, suffering from chronic disorders, represent a large number of admissions to home health services [3]. These services may highly benefit from the use of new technologies. These technologies allow daily activities of patients to be supervised without the necessity of imposing them to leave their homes or to be permanently supervised by a real presence of nurses or close relatives.

Some systems based on the use of wireless sensor nodes with other elements, such as surveillance cameras, exist in the literature (cf., references [11, 37] and citations thereof). These systems aim at improving the quality of traditional surveillance programs, as well as reducing the response time for decision-making situations. But, these solutions represent a high cost. In this sense, the combination of existent wireless sensor nodes and RFID systems can help to drastically reduce the deployment costs of surveillance systems for elder health care [33, 34, 21]. We can imagine a number of tags attached to patient clothing and medications, ready

to respond to the interrogations of associated sensor readers. The aggregation of tag identifiers, locations, timestamps, and sensed data, allows the health care operators to infer relevant information such as the elderly patients falling down, forgetting to take the medications, or having wrong drugs. However, these systems present challenging security requirements. Indeed, wireless technologies are, in general, very vulnerable to eavesdropping and spoofing attacks [5]. The use of sensor nodes and RFID tags (highly constrained in terms of computation, memory, storage, and energy) increases the likelihood of these threats [18]. To avoid privacy violations, all the data must be, moreover, properly protected [36].

Cryptography is a key solution to address most of these threats. The use of traditional cryptography on these systems is considered a very challenging problem because of strong constraints, such as production costs, power consumption, time of response, and regulations compliance. A brief list of solutions such as on-board encryption, password-based protocols, and rotation of pseudonym lists is surveyed in recent literature [19]. The use of low-overhead procedures becomes the main approach to solve these challenging problems in which traditional cryptography cannot fit. A vast number of low-cost solutions for key assignment on wireless sensor networks can be found in the literature (e.g., [7, 10]). Most of these approaches imposes conditions that would also apply for our motivation scenario. For example, not to assign the same key to multiple pairs of nodes within a certain location area, and not to use the same keys for long periods of time. In addition, the security and privacy requirements of health care applications may introduce more complex designs [36].

When nodes are required to collect information from human bodies, they can benefit from unique environmental data (e.g., unique biometrics gathered from the human bodies). The use of secure environmental data has been proposed for the distribution of secrets between body sensor nodes on health care components and has been reported in references like [35, 39]. These solutions allow the system to authenticate the sensors by using inherent data inferred from the wearer's body that is holding the set of sensors. Some important limitations, exposed later in Section 3.2.1, discourage us to use these solutions. The use of Elliptic Curve Cryptography (ECC) and well established key exchange schemes such as Diffie-Hellman [28], is presented in [37, 38], in the form of multi-server key establishment protocols, to address some of the previous limitations. These new solutions deal with security aspects between body sensor and other surveillance components of a home health care system, such as cameras and PDAs. Their complexity costs are, however, too high for the passive RFID components expected in our motivation scenario [20]. We analyze in the sequel some more appropriate protocols to establish keys between resource-constrained devices, while guaranteeing the same security properties.

# 3 Evaluation of Key Exchange Protocols for Resource-Constrained Devices

## 3.1 Evaluation Criteria

In order to rank the set of protocols by order of suitability, we consider in our analysis the following evaluation criteria:

- **Computation costs**: The computation costs are estimated by identifying expensive and time-critical operations. Operations which have to be performed sequentially are expensive compared to some computations that can be pre-performed before protocol run or that are computed when the system is idle.
- **Communication costs**: The communication costs clearly depend on the topology and properties of the network and the communication system used. We include here some general costs, such as:
  - **Number of operations**: This may affect communication delays. As the number of operations increases, the communication delay and the probability of message loss or corruption also increase.
  - **Number of messages**: The probability of message loss or corruption increases with the increase of messages number. The delay also depends on messages number.

These evaluation criteria are used to guide us to decide on the capacity of some selected protocols to respect the limited costs incurred by the set of nodes in our scenario. These authentication protocols have to answer, besides, two essential constraints, namely the *communication asymmetry* and the *intermittence of interrogations* imposed by the use of the passive RFID labels. The asymmetry constraint is required with the use of battery-less labels that can only be initiated by harvesting energy received from interrogators. To satisfy the second constraint, i.e., intermittence of interrogations, the protocols must guarantee that acknowledgments and rejections are properly handled to avoid desynchronization while the components are still within the range.

Therefore, a protocol compliant to the passive RFID labels of our scenario has to meet these two challenges. It must ensure that computing and communication costs for authentication are bearable by all the system nodes, while respecting the asymmetry constraint and the intermittent communication between the two sides. For standard operations such as inventory management, where nodes simply transmit their identifiers, these criteria are sufficiently met. However, more complex operations such as key exchange for distributing secrets that must be updated over time require more computing capacity and energy. And the more the operations are complex, the more they tend to introduce security flaws. We analyze in the sequel three protocols that handle the asymmetry and intermittence constraints, and discuss about their suitability in our motivation scenario.

### 3.2 Key Exchange Protocols for Resource-Constrained Devices

We survey in this section a representative set of protocols designed to address constrained devices such as those presented in our motivation scenario. For a more complete set of solutions, we refer the reader to [19] and citations thereof.

#### 3.2.1 Combination of Secure Environmental Values

We start our evaluation by analyzing a key exchange protocol that benefits from the use of secure environmental data for the distribution of secrets between constrained devices. It summarizes the main concepts presented in protocols like [35, 39]. We denote as Initiator the device in charge of initiating the refreshment of keys (e.g., an active RFID reader); and Responder the resource-constrained device in charge of accepting the new key and acknowledging the process (e.g., a passive RFID tag).

---

**Protocol 1** *SEV-based Key Exchange*

1. *Initiator generates a new random symmetric key, denoted as k*
2. *Initiator and Responder derive two new secure environmental values, denoted as $v_i$ and $v_r$*
3. *Initiator hashes k, denoted as $hash(k)$*
4. *Initiator blinds the contents of k by computing $e \leftarrow k \oplus v_i$*
5. *Initiator sends the message $\{hash(k), e\}$ to Responder*
6. *Responder computes $k' \leftarrow v_r \oplus e$*
7. *If $hash(k) = hash(k')$, responder accepts k, updates its symmetric key, and acknowledges the proper reception*
8. *Otherwise, Responder refuses k and notifies the rejection*

---

The devices involved in Protocol 1 successfully establish a new symmetric key $k$ by agreeing on a common environmental value that is used as a one-time pad. Inter-Pulse Intervals (IPI) [35] or Heart Rate Variance (HRV) [1] are appropriate examples of secure environmental values proposed in the literature. The value of $v$ must independently be derived from both devices. This value is then used to blind the content of $k$ and to send it over an insecure communication channel. The use of a one-way hash function to compute $hash(k)$ allows the Responder device to verify the integrity of the message. If satisfied, it decides the acceptance or rejection of $k$. Table 1 summarizes our evaluation of the protocol, regarding the criteria defined in Section 3.1.

| | | |
|---|---|---|
| **Computation costs** | – Generation of random sequences<br>– Generation of SEV sequences<br>– One-way hashing<br>– XORing ($\oplus$) | |
| **Number of operations** | Initiator | 5 operations |
| | Responder | 5 operations |
| **Number of messages** | Initiator | 1 message |
| | Responder | 1 message |

**Table 1. Evaluation of Protocol 1.**

From a hardware point-of-view, the most expensive operations in Protocol 1 are performed in Steps 3 and 7, involving one-way hash functions. Indeed, the implementation of robust hash functions in the constrained environment of low-cost RFID labels (e.g., EPC Gen2 labels [16]) is very challenging and probably unrealistic for our motivation scenario. This condition leads us towards less expensive schemes (in terms of computation costs) based uniquely on the single use of on-tag pseudo-randomness and simple arithmetic operations [20].

The use of appropriate Pseudo-Random Number Generators (PRNGs) on low-cost RFID devices has also been questioned in the literature [32]. Indeed, the complexity of implementing robust PRNGs is equivalent to the complexity of implementing robust one-way hash-functions or equivalent encryption engines [28]. However, since the ratification of the EPCglobal standard EPC Class-1 Generation-2 (Gen2 for short) [16] and ISO standards ISO/IEC 18000-6C [23] for the usage of on-tag PRNGs on low-cost RFID devices, the number of single PRNG-based solutions has increased in the industry and academia research [29]. Standard RFID devices, like the Electronic Product Code (EPC) technology [16], already require the use of PRNGs to guarantee the correctness of their local operations, such as singulation[1] of tags for inventorying process (e.g., scanning of tagged objects, potentially hundreds). The implementation of appropriate pseudo-random numbers generators and *aloha*-like protocols [24] is therefore paramount to guarantee the efficiency of EPC applications.

Some other limitations in Protocol 1 must be pointed out. Although SEV-based solutions may allow system devices attached to human bodies to infer secure environmental data, the impossibility of interaction between bod-

[1] Singulation is the method by which RFID interrogators isolate a specific RFID tag from a population of tags within range of the interrogators. This operation is crucial, since multiple labels responding at the same query will overlap their responses one over each other.

ies and tagged RFID objects, and the possibility of successfully compromising the secrets by simply compromising the bearer's data discourages us from the use of these solutions. Notice, moreover, that most tagged objects would not be able to produce environmental data with the cryptographic properties required by this type of protocols. The use of biometrics, furthermore, is still being debated in some countries [30] due to privacy violations that it can produce.

Protocol 1 also lacks mutual authentication among Initiators and Responders. Rogue Interrogators, able to generate appropriate SEV values, can contact the Responders to send bogus secrets in order to damage the integrity of the system (e.g., denial-of-service by desynchronizing the devices' keys). Authors in [37, 38] try to solve these limitations by proposing an extended version of Protocol 1, improved by combining the use of Secure Environmental Values and traditional cryptography, such as the Diffie-Hellman key exchange protocol and Elliptic Curve Cryptography (ECC) [28]. The authors propose a complete set of operations in order to guarantee authentication, key freshness and key confirmation. In the Diffie-Hellman based scheme, initiators and responders must independently execute their Diffie-Hellman components and derive new keys. Instead of using traditional secrets (like passwords or PINs) involved in Diffie-Hellman-like schemes, the authors propose the use of Independent SEV values. In the ECC-based scheme, initiators start the processes by selecting SEVs that are encrypted using responders' public keys.

Despite the drawbacks of Protocol 1, it is still considered as suitable for constrained devices, compared with protocols based on traditional cryptography like those presented in [37, 38]. These protocols add, indeed, new performance overheads (much more than those presented in the evaluation of Table 1). They require more CPU-intensive operations such as exponentiation, which cannot be afforded by highly CPU-constrained devices such as RFID tags. Even if implementations of traditional cryptosystems adapted to resource-constrained devices exist in the literature (e.g., [2]), their use is discouraged for our motivation scenario [4] because of the design considered still complex for batteryless devices [40].

We analyze in the sequel a more appropriate strategy that solves some of the drawbacks of Protocol 1 while keeping low the overhead of the process.

#### 3.2.2 Evolving Pre-distributed Secrets

The use of low-overhead procedures becomes the main approach to solve those challenging problems where traditional cryptography cannot fit. Lightweight cryptography, using little memory and relatively simple operations such as XORing and modular algebra (basically addition, shifting, and multiplication), may still provide security in scenarios like those presented in Section 2 because of the specificity of the adversary model. While traditional cryptography aims at providing provable security against, e.g., plain-text attacks [28], our motivation scenario has a different adversary with much worst powers and whose attacks are not always applicable to resource-constrained systems like those used on RFID sensor networks [15, 4]. Based on a low-overhead security model, Initiators (e.g., RFID readers and active sensors) are in charge of updating the system's keys, while Responders (e.g., RFID passive tags or sensors) rely on the Initiators to obtain the keys in each communication session.

In this sense, and based on a mutual authentication protocol presented in [25], Protocol 2 summarizes an alternative version of Protocol 1. This second protocol is based on modular algebra operations, such as multiplication[2] of vectors and matrices modulo $p$. It relies on the single use of onboard generated pseudo-random sequences instead of environmental or biometrics-based secure values. The protocol assumes that both the Initiator and the Responder share two $p \times p$ square matrices.

---

**Protocol 2** *Mutually Authenticated Key Exchange*

1. *Initiator contacts Responder*
2. *Responder computes* $X \leftarrow k \cdot M_1$ *and sends message* $\{X\}$ *to Initiator*
3. *Initiator authenticates the Responder by computing* $k' \leftarrow X \cdot M_1^{-1}$ *and verifies* $k = k'$. *If* $k \neq k'$ *Initiator aborts the process; Otherwise, Initiator authenticates the Responder and continues the process*
4. *Initiator computes a new fresh key vector* $k_{new}$ *at random, generates* $Y \leftarrow k \cdot M_2$ *and* $Z \leftarrow k_{new} \cdot M_2$, *and sends message* $\{Y, Z\}$ *to Responder*
5. *Responder computes* $k'' \leftarrow Y \cdot M_2^{-1}$ *and verifies* $k'' = k$. *If the verification fails, Responder aborts the process; Otherwise, it authenticates the Initiator, acknowledges the process, computes* $k'_{new} \leftarrow Z \cdot M_2^{-1}$, *and updates its key vector* $k$ *to the values of* $k_{new}$

---

Initiator maintains matrices $M_1$ and $M_2^{-1}$. Responder maintains matrices $M_2$ and $M_1^{-1}$. The matrices $M_1^{-1}$ and $M_2^{-1}$ are, respectively, the inverse matrices of $M_1$ and $M_2$. Initiator and Responder must also share an initial key $k$, defined as a vector of size $q$, where $q = rp$, and $r$ is an integer factor known by both Initiator and Responder. All the parameters, matrices, and the initial key are generated at random during an initial trusted setup performed by the system operators. Notice that the Initiator and the Responder both

[2] All the operations performed by Protocol 2 (e.g., multiplication of vectors and matrices) are in modular algebra.

authenticate each other and update their shared symmetric key secrets. In an early stage, the Responder challenges the Initiator by sending a blinded sequence $X$ computed as $k \cdot M_1$. The Initiator uses the inverse of $M_1$ to unblind $k$ from $X$. If the verification is satisfied, the Initiator responds to the challenge and sends a new vector key $k_{new}$ protected as $Z \leftarrow k_{new} \cdot M_2$. The challenge's response contains, in turn, a new blinded version of $k$ computed as $Y \leftarrow k \cdot M_2$. The Responder unblinds $k$ from $Y$ by using $M_2^{-1}$ and verifies the identity of the Initiator. If this new verification is also satisfied, the Responder acknowledges the process and updates its key vector to $k_{new} \leftarrow Z \cdot M_2^{-1}$.

| | | |
|---|---|---|
| **Computation costs** | – Generation of random sequences<br>– Matrix-vector modular multiplication | |
| **Number of operations** | Initiator | 7 operations |
| | Responder | 5 operations |
| **Number of messages** | Initiator | 2 messages |
| | Responder | 2 messages |

**Table 2. Evaluation of Protocol 2.**

Table 2 summarizes the evaluation of the protocol, by following the criteria we defined in Section 3.1. We can observe that, compared to Protocol 1, this new scheme increases by one the number of messages of both the Initiator and the Responder. It also adds two more operations to the Initiator (cf. Table 1). The computational costs of these operations are, however, much lower. Instead of using hash functions, public key cryptography, or any other traditional cryptosystem, it only uses common operations supported by highly-constrained devices like EPC labels.

The security of the protocol relies on the difficulty of recovering the operands used on both sides to synchronize the secret. Authors in [9] show that, under some special circumstances, the protocol is vulnerable to denial-of-service, tracing, and replay attacks. Indeed, if a rogue Interrogator succeeds to inject arbitrary information to the Responder, this leaves the Responder and the legitimate Interrogator unable to communicate. More specifically, and since the Responder does not properly authenticate the value that is given by the Interrogator in Step 4, the scheme is vulnerable to rogue interrogators providing previously accepted values. This opens the possibility of applying replay attacks and eventually to wrong updates. If these attacks succeed, the secrets on both sides get desynchronized. Based on the same vulnerability, it is also possible to exploit the security of the protocol by recording all the transmitted data generated in several sessions. This allows tracing the devices and, therefore, violating the privacy of the application.

#### 3.2.3 Proactive Evolution of Keys

An alternative solution that addresses the security flaws of Protocol 2 is presented in this section. The solution is based on an existing authentication protocol presented in [13, 14]. The Initiator and the Responder share now a square $p \times p$ matrix $M$, a PRNG $P$, a symmetric key $k$, and a vector $t$ of size $q$. It is also assumed here that all the operations performed in the protocol are based on modular algebra.

---

**Protocol 3** *Proactive Evolution of Keys*

1. *Initiator generates, at random, a vector $v$ of size $p$ and seed $\leftarrow (m_{p1} \oplus m_{p2} \ldots \oplus m_{pp})$, where $m_{p*}$ is the $p^{th}$ row vector of matrix $M$*
2. *Initiator generates a vector $w$ of size $(p+q)$ from $P(seed)$ and computes vector $x \leftarrow w \oplus (v||t)$, where $||$ stands for concatenation, and sends message $\{x\}$ to Responder*
3. *Responder computes seed $\leftarrow (m_{p1} \oplus m_{p2} \ldots \oplus m_{pp})$, vector $w$ from $P(seed)$, and $y \leftarrow x \oplus w$*
4. *Responder verifies if $y_{\{p+1,q\}} = t$, where $y_{\{p+1,q\}}$ is a vector of size $q$ derived from vector $y$. If verification fails, it aborts the process; otherwise, it acknowledges the process and refreshes secrets $M$ and $k$ as follows:*
   (a) *Shift all row vectors of $M$ down one position (i.e., $M_{p*}$ becomes $M_{1*}$, $M_{p-1*}$ becomes $M_{p*}$, and so on).*
   (b) *$M_{1*} \leftarrow y_{\{1,p\}}$ (e.g., substitute first row of $M$ by the first $p$ elements of vector $y$)*
   (c) *Shift all the column vectors of $M$ all over to the right (i.e., $M_{*p}$ becomes $M_{*1}$, $M_{*p-1}$ becomes $M_{*p}$, and so on)*
   (d) *$k \leftarrow y_{\{1,p\}}$*
5. *Initiator, if acknowledged by the Responder, also refreshes its shared secrets $M$ and $k$ with same steps of Responder; but replaces $y_{\{1,p\}}$, used in step 4, by the row vector $v$.*

---

Protocol 3 relies on the repeated communication sessions between an Interrogator (e.g., an active sensor) and a Responder (e.g., a passive RFID label) to proactively refresh a set of shared secrets (vector $k$ and matrix $M$). This protocol uses the entries of a new vector that is randomly chosen by the Initiator (less resource-constrained) and protects it by simply XORing such a vector with a shared random sequence generated by both the Initiator and the Responder. To allow this previous operation, both parties must synchronize the generation of the random sequence by agreeing on a

common seed value and a common pseudo-random number generator (denoted as $P$ in the protocol). The concatenation of the new sequence with a verification token $t$ shared between the two parties protects the scheme against injecting bogus information from a rogue Initiator. The remaining operations of the protocol are simply the shifting of columns and rows of $M$, and the addition of the new sequences into the shared matrix $M$.

| | | |
|---|---|---|
| **Computation costs** | – Generation of random sequences<br>– Matrix-vector shifting<br>– Concatenation (\|\|)<br>– XORing ($\oplus$) | |
| **Number of operations** | Initiator | 7 operations |
| | Responder | 7 operations |
| **Number of messages** | Initiator | 1 message |
| | Responder | 1 message |

**Table 3. Evaluation of Protocol 3.**

Table 3 summarizes the evaluation of Protocol 3, regarding the criteria defined in Section 3.1. Compared to Protocol 1, this new protocol increases to seven the number of operations of both the Initiator and the Responder, but does not increase the number of messages to exchange between the two sides. The computation costs of the operations of Protocol 3 (i.e., XORing, concatenation, and matrix shifts) are, moreover, much lower. No vulnerabilities or weaknesses regarding the security of the scheme used in the protocol have been presented in the literature. The scheme ensures that the refreshment of secrets between the Initiator and the Responder remains secure even if a malicious adversary is listening to all the session exchanges.

### 3.3 Summary and Discussion

We highlighted in the previous section three recent trends reported in the literature that we consider relevant (cf., Section 3.1) for securing the communications between the wireless components of a home health care system. We assumed that all the devices in the system are already holding an initial set of shared secrets. These secrets can be, for instance, the sources of secure environmental values, pass-phrases, or symmetric matrices. We also stated that the protocols must satisfy the following two constraints: *communication asymmetry* and *intermittence of interrogations*. Concerning the first constraint, we suppose that less constrained devices, in terms of computation and energy resources (e.g., active sensor or RFID reader), must initiate the communication of a second component that is much more resource-constrained (e.g., passive sensor or RFID tag). This second component expects, moreover, to be initiated with the energy collected from the active device. Our motivation scenario assumes, indeed, the existence of passive devices that expect the reception of new fresh symmetric keys. These keys later allow to secure their communications with the rest of components in the system. Regarding the second constraint, we assume that protocols properly handle the desynchronization threat in our scenario. Indeed, and due to the movement or the power intermittence of the active devices, the protocol must guarantee that it does not affect the update or the exchange of secrets [4]. All three approaches that we presented satisfy these two requirements.

We then analyzed the computation and communication costs of the three approaches. In this way, we can show the adequacy of the selected protocols in order to address the aforementioned constraints. Moreover, this analysis allowed us to extract some further elements to guide our future work. For instance, we have seen that using one-way hash functions and biometrics, as proposed in approaches presented in [35, 39] (and summarized here as Protocol 1), cannot always fit in our proposed scenario. On the one hand, previous studies [18, 31] discourage the use of one-way hash function in protocols applied to low-cost RFID technologies, such as the EPC technology [16]. On the other hand, the use of unique environmental values may sometimes be difficult when sensors are placed on inanimate objects instead of human bodies. In fact, even if such values can be derived from human bodies, this can generate several concerns regarding privacy violation. From a legal perspective, the use of biometrics as identifiers in pervasive applications, such as health care systems, has been reported by European institutions as worrying [30]. The other limitation we noticed in the use of environmental values is a lack of strong authentication. In fact, recent solutions in the literature propose to complement these approaches with traditional cryptography. For example, the authors in [37, 38] propose to establish strong authentication procedures based on Diffie-Hellman key exchanges and Elliptic Curve Cryptography. These improvement exceed, however, the hardware constraints that we assume in our work (e.g., use of EPC labels to identify objects).

We see in the use of mutual and proactive evolving predistributed secret schemes (e.g., approaches presented in [25, 13]) the most promising candidate for our motivation scenario. These solutions, which mainly rely on the use of on-board pseudo-random number generators, relax the drawbacks detected on the use of hashing functions and environmental values. Special care must be taken to ensure that these approaches handle desynchronization of secrets. A proper example is the set of vulnerabilities presented in [9]. The authors show, indeed, the possibility of a denial-of-service in the strategy presented in [25], and summarized as Protocol 2. An alternative solution, presented in [13], and summarized in Protocol 3, has been reported as computationally secure while still lightweight enough for being implemented in resource-constrained RFID labels.

## 4 Conclusions

We surveyed some state-of-the-art solutions for deploying secure communications between resource-constrained wireless components of home health care systems. We discussed and evaluated the pertinence of each approach to guarantee requirements such as performance and security. We especially outlined approaches that take into account the heterogeneity of the system components, assuming the existence of passive RFID based nodes with highly constrained computing and communicating capabilities. The analysis allowed us to extract some relevant properties about the expected procedures to be executed in our motivation scenario. These properties will be the subject of our future works.

**Acknowledgments —** The authors graciously acknowledge the financial support received from Institut TELECOM through its *Future et Rupture* program; and from the TSI2007-65406-C03-03 E-AEGIS, and CONSOLIDER CSD2007-00004 "ARES" projects.

## References

[1] S. D. Bao, Y. T. Zhang, and L.F. Shen. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. *27th Annual International Conference of the Engineering in Medicine and Biology Society*, pp. 2455–2458, 2005.

[2] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for RFID-tags Cryptology ePrint Archive, Report 2006/227, IACR, 2006.

[3] C. Boult, M. Altmann, D.Gilbertson, et al. Decreasing disability in the 21st century: the future effects of controlling six fatal and nonfatal conditions. *Am J Public Health*, pp. 86(10):1388-1393, 1996.

[4] M. Buettner, B. Greenstein, A. Sample, J. Smith, and D. Wetherall. Revisiting Smart Dust with RFID Sensor Networks. *7th ACM Workshop on Hot Topics in Networks (HotNets-VII)*, 2008.

[5] L. Buttyan and J. P. Hubaux. Security and Cooperation in Wireless Networks. *Cambridge University Press*. 496 pages. 2007. ISBN-13: 9780521873710.

[6] H. J. Chae, D. J. Yeager, J. R. Smith, K. Fu. Maximalist Cryptography and Computation on the WISP UHF RFID Tag. *Conference on RFID Security (RFIDSEC 2007)*, 2007.

[7] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. *IEEE Symposium on Security and Privacy*, pp. 197–215, 2003.

[8] Commission on Behavioral and Social Sciences and Education (CBASSE). Preparing for an Aging World:The Case for Cross-National Research. *National Academy Press -Washington, D.C.*, p. 31, 2001

[9] H. Chien and C. Chen. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. *Computers Standards and Interfaces*, 29(2), pp 254-259, 2007.

[10] S. A. Çamtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 15(2):346–358, 2007.

[11] S. Consolvo, P. Roessler, B. Shelton, A. LaMarca, B. Schilit, S. Bly. Technology for Care Networks of Elders. *IEEE Pervasive Computing*, 3(2):22-29. April-June 2004.

[12] A. Czeskis, K. Koscher, J. R. Smith, T. Kohno. RFIDs and Secret Handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications. *15th ACM conference on Computer and Communications Security*, 479–490, 2008.

[13] S. Dolev and M. Kopeetsky. Secure communication for RFIDs proactive information security within computational security. In *8th Int'l Symposium on Stabilization, Safety, and Security of Distributed Systems*, LNCS, 4280, pages 290–303. 2006. Springer.

[14] S. Dolev, M. Kopeetsky, and Adi Shamir. RFID Authentication Efficient Proactive Information Security within Computational Security. Tech. rep., Department of Computer Science, Ben-Gurion University, July 2007.

[15] S. Dolev, M. Kopeetsky, T. Clouser, and M. Nesterenko. Low Overhead RFID Security. In chapter 32 of S. A. Ahson and M. Ilyas, editors,*RFID Handbook: Applications, Technology, Security, and Privacy*, pages 589–602, CRC Press, 2008.

[16] EPCglobal. EPC Radio-frequency identity protocols Class-1 Generation-2. Technical report, http://www.epcglobalinc.org/standards/, January 2005.

[17] G. Gaubatz, J. P. Kaps, and B. Sunar. Public key cryptography in sensor networks. *European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, 2004.

[18] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. Analysis of Threats to the Security of EPC Networks. *6th Annual Communication Networks and Services Research (CNSR) Conference*, IEEE Communications Society, Halifax, Nova Scotia, Canada, May 2008.

[19] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. Handling Security Threats to the RFID System of EPC Networks. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Auerbach Publications, Taylor & Francis Group, 2010.

[20] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. Security Threat Mitigation Trends in Low-cost RFID Systems. *2nd International Workshop on Autonomous and Spontaneous Security (SETOP 2009)*, Springer, LNCS 5939, 193–207, January 2010.

[21] L. Ho, M. Moh, Z. Walker, T. Hamada, C. F. Su. A prototype on RFID and sensor networks for elder healthcare: progress report. *ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, 70–75, 2005.

[22] Q. Huang, J. Cukier, H. Kobayashi, B.Liu, and J.Zhang. Fast Authenticated Key Establishment protocols for Self-organizing Sensor Networks. *2nd ACM international conference on Wireless Sensor Networks and Applications*, 2003.

[23] ISO/IEC 18000-6:2004/amd:2006. Technical report, http://www.iso.org/, 2006.

[24] F. Kuo. The ALOHA system. *Computer Networks*, Prentice-Hall, pp. 501–518, 1973.

[25] S. Karthikeyan and M. Nesterenko. RFID Security without Extensive Cryptography. *3rd ACM workshop on security of ad hoc and sensor networks (SASN)*, pp. 63–67, New York, 2005.

[26] D. Malan, M. Welsh, and M. Smith. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. *First IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON04)*, 2004.

[27] M. Moh, L. Ho, Z. Walker, T. S. Moh. A Prototype on RFID and Sensor Networks for Elder Health Care. *RFID Handbook: Applications, Technology, Security, and Privacy*, CRC press, pp. 311–328, 2008.

[28] A. Menezes, P. Van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[29] J. Melia-Segui, J. Garcia-Alfaro, J. Herrera-Joancomarti. Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags. *Financial Cryptography and Data Security*, LNCS, Springer, January, 2010.

[30] A. Liberatore. Balancing Security and Democracy: the Politics of Biometric Identification in the European Union, European Univerity Institute. *EUI Working Paper RSCAS*, Robert Shuman Centre for Advanced Studies, 2005.

[31] P. Peris-Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. LAMED - A PRNG for EPC Class-1 Generation-2 RFID specification. *Journal of Computer Standards & Interfaces*, 2008

[32] P. Peris-Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks. *Emerging Directions in Embedded and Ubiquitous Computing*, LNCS, vol. 4809, pp. 781–794, 2007.

[33] M. Philipose, K. Fishkin, M. Perkowitz, D. Patterson, D. Fox, H. Kautz, and D. Hahnel. Inferring Activities from Interactions with Objects. *IEEE Pervasive Computing. 3(4):50-57.*, October-December 2004.

[34] M. Philipose, J. R. Smith, B. Jiang, A. Mamishev, S. Roy, K. Sundara-Rajan. Battery-free wireless identification and sensing. *IEEE Pervasive Computing.*, January-March 2005.

[35] C. C. Y. Poon, Y. T. Zhang, and S. D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73-81, 2006.

[36] J. J. Shen, L. F. Samson, E.L. Washington, P. Johnson, C. Edwards, and A. Malone. Barriers of HIPAA regulation to implementation of health services research. *Journal of Medical Systems*, 30(1):65–69, Springer, 2006.

[37] K. Singh and V. Muthukkumarasamy. Authenticated Key Establishment Protocols for a Home Health Care System. *Third International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 353–358, 2007.

[38] K. Singh and V. Muthukkumarasamy. Implementation and Analysis of Sensor Security Protocols in a Home Health Care System. *Third International Conference on Network and System Security*, 137–142, 2009.

[39] K. K. Venkatasubramanian and S. K. S. Gupta. Security for pervasive health monitoring sensor applications. *4th International Conference on Intelligent Sensing and Information Processing (ICISIP)*, 197–202, 2006.

[40] J. Wolkerstorfer. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? *Ecrypt Workshop on RFID and Lightweight Crypto*, Graz, Austria, July 2005.