Sécuriser les communications dans les systèmes de surveillance médicale basés sur les étiquettes RFID

Protocoles appliqués aux étiquettes à faible coût.

Wiem Tounsi* — **Joaquin Garcia-Alfaro*** — **Nora Cuppens-Boulahia*** — **Frédéric Cuppens***

* *TELECOM-Bretagne, 02, rue de la Châtaigneraie,*
35576 Cesson Sévigné - France

{wiem.tounsi, joaquin.garcia, nora.cuppens, frederic.cuppens}@telecom-bretagne.eu

RÉSUMÉ. *Nous nous intéressons aux solutions de sécurité visant à protéger la communication des composants sans fil dans un système de surveillance médicale à domicile. Nous analysons particulièrement le problème d'authentification et d'échange de secrets entre des entités ayant des capacités de calculs et de communications différentes. Nous soulignons quelques propriétés importantes qui doivent être garanties en cas de présence de capteurs passifs du type RFID à faible coût. L'analyse des différentes approches existantes dans la littérature nous a permis de dériver une approche robuste pour répondre au contexte de cette étude. Cette approche se base sur la technique du masque jetable.*

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 having different computing and communicating capabilities. We outline some important properties that must be guaranteed given the existence of low-cost and resource-constrained RFID components. The analysis of existing approaches reveals a robust technique based on one-time pads.*

MOTS-CLÉS : *Sécurité des réseaux, réseaux sans fil, donnée médicale, surveillance à distance, RFID, réseaux de capteurs, Protocoles cryptographiques, environnement pervasif*

KEYWORDS: *Network Security, Wireless Security, Medical data, Remote monitoring, RFID, Sensor Networks, Cryptographic Protocols, Pervasive environment*

1. Introduction

Les réseaux de capteurs représentent un type spécifique de réseaux ad hoc. Il s'agit d'une technologie sans infrastructure et hautement décentralisée. Dans le même contexte, Radio Frequency IDentification (RFID) représente une technologie à faible coût, sans batteries et un successeur des codes à barres omniprésents de nos jours. Au cours des dernières années, des progrès substantiels ont été réalisés pour intégrer ces deux technologies dans des applications sensibles combinant les avantages de la RFID avec ceux des réseaux de capteurs sans fil [BUE 08]. L'intégration de ces technologies dans les systèmes de soins et de surveillance médicale à distance est un scénario en cours d'exploitation [PHI 05, MOH 08]. Sécuriser l'information qui circule dans ces différents composants devient à la fois essentiel et complexe. En effet, l'intégrité et la disponibilité de l'information médicale, considérée sensible, doivent être garanties [CZE 08]. L'utilisation de schémas cryptographiques appropriés comme l'établissement de clés partagées, devient alors un besoin crucial [CHA 07].

Nous mettons en évidence dans le présent article certaines approches existantes qui permettraient une communication sécurisée entre les différents capteurs du système ; les capteurs étant la combinaison des technologies précitées. Nous analysons et discutons, par ailleurs les capacités de chaque solution à satisfaire les besoins de sécurité pour les systèmes de surveillance et de soins des personnes âgées. Nous identifions, suite à cette analyse, les approches qui répondent au mieux à la complexité imposée par la combinaison de composants différents en capacités de calcul et de communication.

Organisation de l'article — La section 2 motive le besoin de sécuriser les données médicales et présente les travaux connexes. La section 3 passe en revue un ensemble de solutions pour l'établissement de clé partagée et discute l'adéquation de chaque solution avec le domaine d'application auquel nous nous intéressons. Enfin, la section 4 conclut l'article et présente quelques perspectives.

2. Motivation et travaux connexes

Le vieillissement de la population au niveau mondial est un fait inéluctable. D'après une étude faite à *U.S. bureau of Censure* en l'an 2000 [Com 01], *le solde net de la population âgée du monde a augmenté de plus de 750.000 par mois. Dans deux décennies, l'augmentation sera probablement de 2 millions par mois.* Notons, par ailleurs, que les patients, en particulier les personnes âgés, souffrant de troubles chroniques sont les plus nombreux à solliciter des services de surveillance à domicile [BOU 96]. Ces services peuvent bénéficier de l'utilisation des nouvelles technologies qui permettraient de surveiller les activités quotidiennes des patients, sans imposer à ces derniers de quitter leurs foyers ou d'être accompagnés en permanence. Dans la littérature, certains systèmes de surveillance se

basent sur l'utilisation de nœuds de capteurs sans fil, en plus de la mise en place d'autres éléments comme la vidéo-surveillance [CON 04, SIN 07]. Ces systèmes visent à améliorer la qualité des programmes de surveillance traditionnels et à réduire le temps de réponse dans les situations de prise de décision. Mais ce type de solutions représente un coût élevé.

La combinaison des réseaux de capteurs actifs et passifs du type RFID a été proposée dans la littérature pour réduire les coûts de déploiement des systèmes de surveillance des personnes âgées [PHI 04, PHI 05, HO 05]. Nous pouvons imaginer, pour cela, des étiquettes collées aux vêtements et médicaments des patients répondant aux interrogations des lecteurs associés. L'agrégation des données d'identification des étiquettes permettrait aux exploitants de services de santé d'en déduire des informations pertinentes, telles que la chute des patients et l'oubli ou la prise erronée de médicaments. C'est dans un tel contexte que s'inscrit le scénario de motivation du présent article. La réponse aux exigences de la sécurité informatique dans ce scénario de motivation représente un défi. En effet, si les technologies sans fil sont en général très vulnérables à l'espionnage et aux attaques de type usurpation d'identité [BUT 07], les contraintes des nœuds de capteurs et particulièrement des étiquettes RFID (très limitées en termes de calcul, de mémoire, de stockage, et d'énergie) augmentent la probabilité d'occurrence de ces menaces [GAR 08].

La cryptographie est une solution clé pour résoudre la plupart de ces menaces. Un bref aperçu des solutions existantes, telles que les fonctions cryptographiques pour les radio-étiquettes et les protocoles basés sur le changement circulaire des listes de pseudonymes sont abordées dans des ouvrages récents comme [GAR 10]. L'utilisation de la cryptographie traditionnelle dans ces systèmes est un véritable défi à cause des contraintes matérielles comme le coût de production, la consommation d'energie, le temps de réponse et les règles de conformité. De ce fait, les procédures de type *low-overhead* représentent la principale approche pour résoudre les problèmes de capacité limitée. Il existe dans la littérature un grand nombre de solutions à faible coût pour l'affectation de clés dans les réseaux de capteurs sans fil [CHA 03, CAM 07]. La plupart de ces approches impose des conditions qui s'appliquent à notre scénario de motivation. Par exemple, la non-attribution d'une même clé à plusieurs paires de nœuds dans une même zone, la non-utilisation des mêmes clés par un nœud pendant des périodes précises. Cependant, les caractéristiques et les exigences de sécurité des applications de surveillance des malades nécessitent la définition de protocoles plus spécifiques.

Lorsque les nœuds sont tenus de recueillir des informations auprès du corps humain, ils peuvent bénéficier de données environnementales. L'utilisation de ce type de données (par exemple, des informations biométriques) a été proposée pour la répartition des clés entre les nœuds de capteurs. Ces capteurs sont collés sur le corps et représentent les composants de surveillance [POO 06, VEN 06]. De telles solutions permettent au système d'authentifier les capteurs en utilisant

les données inhérentes déduites du corps de l'utilisateur. Cependant, certaines limites extraites et présentées dans cet article (voir section 3.2.1) n'incitent pas à les utiliser dans le cadre de notre étude. La cryptographie à courbe elliptique (ECC) et les schémas d'établissement de clés d'échange comme celles de Diffie-Hellman [FER 03], présentent aussi de nouvelles solutions [SIN 07, SIN 09] pour renforcer la sécurité de l'accès aux composantes du réseau. Cependant, l'exigence d'utiliser des fonctions de hachage appropriées dans leurs schémas d'échange de clé ne permet pas de les utiliser dans notre scénario de motivation [GAR 09].

Nous présentons, dans la suite, des approches utilisées pour l'authentification des capteurs hétérogènes que nous avons résumés sous forme de protocoles d'établissement de clés entre les dispositifs du système. Nous analysons ensuite leur aptitude à garantir la sécurité et la performance dans un système de surveillance médicale.

3. Évaluation des protocoles d'échange de clés dans les dispositifs à ressources restreintes.

3.1. *Critères d'évaluation*

Afin de classer l'ensemble des protocoles par ordre de pertinence, nous tenons compte dans notre analyse des critères d'évaluation suivants :

– **Les coûts de calcul** : Ils sont estimés en identifiant les opérations critiques et coûteuses en temps. Par exemple, les opérations qui sont réalisées de manière séquentielle sont, plus coûteuses que les opérations effectuées quand le système est en repos.

– **Les coûts de communication** : Ils dépendent de la topologie, des propriétés du réseau et du système de communication. Nous pouvons les estimer en considérant les coûts suivants [LIA 05] :

- **Le nombre d'opérations** : Ceci peut affecter les délais de communication. Plus le nombre d'opérations augmente, plus le temps de communication et la probabilité de perte de messages ou de corruption augmentent.

- **Le nombre de messages** : Plus le nombre de messages augmente, plus la probabilité de perte ou de corruption augmente. Les délais augmentent aussi en fonction du nombre de messages.

Ces critères d'évaluation nous permettent de décider de la capacité des protocoles d'authentification sélectionnés à respecter les coûts supportés par les nœuds capteurs. Ces protocoles doivent, cependant, répondre à deux contraintes essentielles, à savoir *la communication asymétrique* et *l'intermittence*

des interrogations imposées par l'utilisation des étiquettes passives RFID. La communication asymétrique [BUE 08] est nécessaire avec l'utilisation des étiquettes sans batterie. Ces dernières ne peuvent être amorcées que par l'énergie recueillie à partir des interrogateurs tels que les lecteurs d'étiquettes. Si cette contrainte ne présente pas de problèmes dans l'échange d'identités, elle rend difficile le développement d'un protocole d'échange de clés pour la distribution des clés qui doivent changer dans le temps. La deuxième contrainte que les protocoles actuels doivent satisfaire, est l'intermittence des interrogations. Comme la communication entre les lecteurs et les étiquettes RFID doit être capable de gérer des interruptions [BUE 08], les protocoles, supportant cette contrainte, doivent alors garantir que les accusés de réception et les rejets sont correctement réalisés pour éviter la désynchronisation.

Les protocoles que nous retenons pour cette étude doivent alors relever des défits à double tranchant. Ils doivent garantir des coûts de calcul et de communication modérés tout en respectant le caractère asymétrique et intermittent des communications.

3.2. *Protocoles d'échange de clés pour des dispositifs à ressources restreintes*

Nous passons en revue, dans la suite, un ensemble représentatif de protocoles d'échange de clés conçus pour couvrir les contraintes présentées dans la section précédente.

3.2.1. *Combinaison des valeurs environnementales uniques*

Nous commençons l'évaluation par l'analyse d'un protocole d'échange de clés qui utilise des données environnementales uniques ou *Secure Environmental Value* : SEV (par exemple, des informations biométriques) pour la distribution des clés entre les équipements. Ce protocole résume les principaux concepts présentés dans des références telles que [POO 06, VEN 06]. Nous notons comme Initiateur l'équipement qui commence à rafraîchir les clés (e.g., un lecteur RFID actif) et comme Répondeur, le dispositif contraint, en charge d'accepter la nouvelle clé et d'accuser réception du processus (e.g., une étiquette RFID passive).

Les dispositifs impliqués dans le Protocole 1 établissent avec succès une nouvelle clé symétrique k en se mettant d'accord sur une valeur commune de l'environnement v, utilisée comme un masque jetable ou *one-time pad* pour masquer la clé k qui sera envoyée dans un canal faiblement protégé. Les intervalles entre les impulsions (nommés *Inter-Pulse Intervals (IPI)* [POO 06]) ou la variation de la fréquence cardiaque (dite *Heart Rate Variance (HRV)* [BAO 05]) sont des exemples appropriés de valeurs environnementales proposées dans la littérature. La valeur de v doit être définie de manière indépendante par les deux dispositifs. L'utilisation d'une fonction de hachage unidirectionnelle pour

---

Protocole 1 *Échange de clés basé sur SEV*

1) Initateur génère aléatoirement une nouvelle clé symétrique, notée k

2) Initiateur et Répondeur dérivent de nouvelles valeurs environnementales uniques, notées v_i et v_r

3) Initiateur réalise une fonction de hachage sur k, notée $hash(k)$

4) Initiateur masque le contenu de k en calculant $e \leftarrow k \oplus v_i$

5) Initiateur envoie le message $\{hash(k), e\}$ au Répondeur

6) Répondeur calcule $k' \leftarrow v_r \oplus e$

7) Si $hash(k) = hash(k')$, Répondeur accepte k, met à jour ses clés symétriques, et accuse la bonne réception

8) Si non, Répondeur refuse k et notifie le rejet de la communication

---

calculer $hash(k)$ permet à l'équipement Répondeur de vérifier l'intégrité du message et de décider de l'acceptation ou du rejet de k.

La Table 1 résume notre évaluation, en prenant en compte les critères définis dans la Section 3.1.

Coûts des calculs	– Génération de séquences aléatoires – Génération de séquences SEV – Hachage unidirectionnel – OU exclusif ($\oplus$)	
Nombre d'opérations	Initiateur	5 opérations
	Répondeur	5 opérations
Nombre de messages	Initiateur	1 message
	Répondeur	1 message

Table 1. *Évaluation du Protocole 1.*

D'un point de vue matériel, les opérations les plus coûteuses dans le Protocole 1 sont effectuées dans les étapes 3 et 7, impliquant une fonction de hachage à sens unique. La mise en œuvre des fonctions de hachage robustes dans l'environnement contraint des étiquettes RFID du type EPC [EPC 05], par exemple, représente un défi. Cette condition nous pousse à adapter le Protocole 1 à des schémas de capacités moins coûteuses (en terme de calculs) qui se basent sur des séquences pseudo-aléatoires pour masquer la clé et sur des opérations arithmétiques simples [GAR 09].

L'utilisation de générateurs de nombres pseudo-aléatoires (*Pseudo Random Number Generators* : PRNGs) appropriés sur les étiquettes RFID a été longuement discutée dans la littérature [PER 07]. En effet, la mise en œuvre de générateurs robustes PRNGs est équivalente à la complexité de la mise en œuvre de fonctions de hachage à sens unique ou de fonctions de chiffrement équivalentes implémentées dans les deux parties communicantes [FER 03]. Mais depuis la ratification du standard EPC Classe-1 Génération-2 (Electronic Product Code) [EPC 05] et des standards ISO/IEC 18000-6C [ISO 06] pour l'utilisation des PRNGs sur les étiquettes RFID, le nombre de solutions basées sur des générateurs PRNG a augmenté. Pour les radio-étiquettes standardisées avec la technologie EPC [EPC 05], ce standard exige déjà l'utilisation des générateurs PRNGs pour garantir la réalisation de leurs opérations locales, comme la singulation[1] des étiquettes pour inventorier un processus (e.g., le balayage d'une centaine d'objets étiquetés). La mise en œuvre de générateurs de nombres pseudo-aléatoires appropriés et les protocoles de type *aloha* [Kuo 73] est alors primordiale pour garantir l'efficacité des applications EPC.

Au delà des fonctions de calcul coûteuses proposées par le Protocole 1, d'autres contraintes doivent être précisées. Citons, pour notre scénario, l'impossibilité d'extraire des valeurs SEV à partir des étiquettes collées sur des objets et le problème d'utiliser la biométrie qui continue à susciter des débats dans certains pays [LIB 05] en raison de la violation de la vie privée qu'elle peut engendrer.

En définitif, même s'il existe dans la littérature des cryptosystèmes traditionnels adaptés aux dispositifs à ressources limitées [BAT 06], leur déploiement reste défavorable pour les technologies utilisées dans notre scénario de motivation [BUE 08]. Leur conception est, en effet, toujours complexe pour des dispositifs démunis de batteries [WOL 05]. Nous analysons, dans la suite, d'autres stratégies pour remédier aux inconvénients du Protocole 1 en maintenant un faible coût global de calcul.

3.2.2. *Évolution des secrets pré-distribués*

La cryptographie traditionnelle n'étant pas utilisée, la cryptographie légère ou *Lightweight cryptography*, utilisant peu de mémoire et des opérations relativement simples tels que le OU exclusif (XOR) et l'algèbre modulaire (essentiellement l'addition, le décalage et la multiplication) peut encore garantir la sécurité de certains scénarios où le modèle d'adversaire est spécifique. Alors que la cryptographie traditionnelle vise à assurer une sécurité robuste contre, par exemple, les attaques de type *plain-text* [FER 03], notre scénario de motivation profite d'un modèle d'adversaire différent, c'est à dire, ayant moins de pouvoir

1. La singulation , appelée aussi la séparation, est la méthode par laquelle des lecteurs RFID isolent une étiquette RFID spécifique d'une population d'étiquettes à la portée de leurs lecteurs. Cette opération est essentielle, car de multiples étiquettes répondant à la même requête peuvent se chevaucher dans leurs réponses.

et dont les attaques ne sont pas toujours réalisables vu la difficulté, pour l'attaquant, de suivre tous les échanges possibles entre les lecteurs et les étiquettes [DOL 08, BUE 08]. Basé sur le protocole d'authentification mutuelle présenté par Karthikeyan et Nesterenko [KAR 05], le Protocole 2 résume une version alternative du Protocole 1. Il se base sur des opérations de l'algèbre modulaire comme la multiplication[2] de vecteurs et de matrices modulo p et repose sur l'utilisation des séquences pseudo-aléatoires pour la génération des clés.

Le protocole suppose que l'Initiateur et le Répondeur partagent deux matrices carrées $p \times p$ de même taille. L'Initiateur maintient deux matrices M_1 et M_2^{-1}. Le Répondeur, de son côté, maintient les matrices M_2 et M_1^{-1}. Les matrices M_1^{-1} et M_2^{-1} sont, respectivement, l'inverse des matrices M_1 et M_2. L'Initiateur et le Répondeur doivent aussi partager une clé initiale k, définie comme un vecteur de taille q, où $q = rp$ et r est un facteur entier connu par l'Initiateur et le Répondeur. Les paramètres, les matrices et la clé initiale sont générés aléatoirement durant la configuration initiale (supposée de confiance) et effectuée par l'opérateur du système.

Protocole 2 *Authentification mutuelle des clés d'échange*

1) Initiateur contacte Répondeur

2) Répondeur calcule $X \leftarrow k \cdot M_1$ *et envoie le message* $\{X\}$ *à Initiateur*

3) Initiateur authentifie Répondeur en calculant $k' \leftarrow X \cdot M_1^{-1}$ *et en vérifiant* $k = k'$*. Si* $k \neq k'$ *Initiateur interrompt le processus ; Autrement, Initiateur authentifie le Répondeur et continue le processus*

4) Initiateur calcule un nouveau vecteur de clé k_{new} *au hasard, génère* $Y \leftarrow k \cdot M_2$ *et* $Z \leftarrow k_{new} \cdot M_2$*, et envoie le message* $\{Y, Z\}$ *au Répondeur*

5) Répondeur calcule $k'' \leftarrow Y \cdot M_2^{-1}$ *et vérifie* $k'' = k$*. Si la vérification échoue, Répondeur interrompt le processus ; Autrement, il authentifie l'Initiateur, accuse réception du processus, calcule* $k'_{new} \leftarrow Z \cdot M_2^{-1}$*, et met à jour son vecteur de clé* k *avec la valeur de* k_{new}

Notons que l'Initiateur et le Répondeur authentifient l'un l'autre et mettent à jour leur clé secrète partagée et symétrique. Dans une première phase, le Répondeur défie l'Initiateur en lui envoyant une séquence masquée X calculée comme $k \cdot M_1$. L'Initiateur utilise l'inverse de M_1 pour démasquer k à partir de X. Si la vérification est satisfaisante, l'Initiateur relève le défi et envoie une nouvelle version masquée de k calculée comme $Y \leftarrow k \cdot M_2$ et un nouveau vecteur de clé k_{new} protégé comme $Z \leftarrow k_{new} \cdot M_2$. Le Répondeur découvre k à partir de Y en utilisant M_2^{-1} et vérifie l'identité de l'Initiateur. Si cette nouvelle vérification est satisfaisante, le Répondeur accuse réception du processus et met

2. Toutes les opérations effectuées par le Protocole 2, telle que la multiplication de vecteurs et de matrices, sont en algèbre modulaire.

à jour son vecteur de clé $k_{new} \leftarrow Z \cdot M_2^{-1}$. La Table 2 résume notre évaluation du protocole en prenant en compte les critères définis dans la Section 3.1.

Coûts des calculs	– Génération des séquences aléatoires – Multiplication modulaire des vecteurs de la matrice	
Nombre d'opérations	Initiateur	7 opérations
	Répondeur	5 opérations
Nombre de messages	Initiateur	2 messages
	Répondeur	2 messages

Table 2. *Évaluation du Protocole 2.*

Le Protocole 2 augmente d'une unité le nombre de messages de l'Initiateur et du Répondeur et ajoute deux opérations de plus à l'Initiateur par rapport au Protocole 1. Cependant, les coûts de communication dans ce protocole sont beaucoup plus faibles. Au lieu d'utiliser les fonctions de hachage ou la cryptographie à clé publique ou tout autre cryptosystème traditionnel, ce schéma utilise uniquement les opérations communes supportées par les dispositifs fortement contraints comme ceux cités dans [EPC 05]. La sécurité du protocole s'appuie, en effet, sur la difficulté de récupérer les opérandes utilisés des deux côtés pour synchroniser les secrets partagés. Toutefois, certaines faiblesses sont signalées par Chien et al. [CHI 07] concernant la possibilité de réaliser des attaques de déni de service, de traçage et de relecture dans des circonstances particulières. Les auteurs montrent que si un Initiateur intrus réussit à injecter des informations arbitraires au Répondeur, cela rend le Répondeur et l'Initiateur légitime incapables de communiquer. Aussi, un Initiateur intrus peut, dans certaines circonstances, fournir des valeurs précédemment échangées entre l'Initiateur légitime et le Répondeur (en appliquant une attaque de relecture) sans se faire remarquer, ce qui conduit à de fausses mises à jour des clés et donc une désynchronisation de la communication. Cette faiblesse est due à l'utilisation de la même variable de protection de clé M dans chaque session.

Un exemple qui apporte une solution à ces faiblesses est présenté à travers le Protocole 3. Il se base sur les protocoles d'authentification de Dolev et al. dans [DOL 06, DOL 07]. L'Initiateur et le Répondeur maintiennent une matrice carrée $p \times p$, nommée M, une fonction PRNG P, une clé symétrique k, et un vecteur t de taille q. Il es supposé également que toutes les opérations effectuées dans le protocole sont basées sur l'algèbre modulaire.

Le Protocole 3 utilise comme relais les sessions de communication répétées entre l'Initiateur (e.g., un capteur actif) et le Répondeur (e.g., un capteur passif) pour actualiser de manière pro-active un ensemble de secrets partagés (le vecteur k et la matrice M). Ce protocole utilise les entrées d'un nouveau vecteur choisi au hasard par l'Initiateur (étant moins limité en ressources) et le

protège en lui appliquant un OU exclusif avec une séquence aléatoire générée par l'Initiateur et le Répondeur que nous appelons le masque jetale. Pour ce faire, les deux parties synchronisent la génération de cette deuxième séquence en convenant d'une valeur de départ commune *seed*, et en utilisant le même générateur de nombres pseudo-aléatoires P. La concaténation de la nouvelle séquence avec un jeton de contrôle commun t partagé entre les deux parties protège le schéma contre l'injection de fausses informations de la part d'un Initiateur intrus. Le reste des opérations du protocole se résume en un ensemble de décalages de colonnes et de lignes et d'ajout de nouvelles séquences dans la matrice partagée M.

Protocole 3 *Évolution proactive des clés*

1) Initiateur génère aléatoirement un vecteur v de taille p et seed $\leftarrow (m_{p1} \oplus m_{p2} \ldots \oplus m_{pp})$, où m_{p*} est le $p^{\text{ème}}$ vecteur ligne de la matrice M et $\oplus$ désigne l'opération OU exclusif

2) Initiateur génère un vecteur w de taille $(p+q)$ à partir de $P(seed)$ et calcule le vecteur $x \leftarrow w \oplus (v||t)$, où $||$ représente la concaténation, et envoie le message $\{x\}$ au Répondeur

3) Répondeur calcule seed $\leftarrow (m_{p1} \oplus m_{p2} \ldots \oplus m_{pp})$, le vecteur w à partir de $P(seed)$, et $y \leftarrow x \oplus w$

4) Répondeur vérifie si $y_{\{p+1,p+q\}} = t$, où $y_{\{p+1,p+q\}}$ est un vecteur de taille q dérivé du vecteur y. Si la vérification échoue, il interrompt le processus ; Autrement, il accuse réception du processus et rafraîchit les secrets M et k comme suit :

a) Décale tous les vecteurs lignes de M d'une position en bas (i.e., M_{p*} devient M_{1*}, M_{p-1*} devient M_{p*}, ainsi de suite).

b) $M_{1*} \leftarrow y_{\{1,p\}}$ (e.g., remplace la première ligne de M par les premiers p éléments du vecteur y)

c) Décale tous les vecteurs colonnes de M d'une position vers la droite (i.e., M_{*p} devient M_{*1}, M_{*p-1} devient M_{*p}, ainsi de suite)

d) $k \leftarrow y_{\{1,p\}}$

5) Initiateur, si reconnu par le Répondeur (par un accusé de réception), rafraîchit aussi ses secrets partagés M et k, en suivant le même ordre que l'étape 4 mais en utilisant le vecteur v à la place du vecteur $y_{\{1,p\}}$.

La Table 3 résume une évaluation du Protocole 3, en tenant en compte les critères définis dans la Section 3.1.

L'utilisation d'un masque jetable pour protéger la clé est l'avantage de ce protocole par rapport au précédent protocole présenté par Karthikeyan et Nesterenko [KAR 05].

Coûts des calculs	– Génération de séq. aléatoires – Décalage de vecteurs de matrice – Concaténation (||) – OU exclusif (XOR) ($\oplus$)	
Nombre d'opérations	Initiateur	7 opérations
	Répondeur	7 opérations
Nombre de messages	Initiateur	1 message
	Répondeur	1 message

Table 3. *Évaluation du Protocole 3.*

Actuellement, il n'existe pas de vulnérabilités ou de faiblesses décelées dans la littérature en ce qui concerne la technique utilisée dans le Protocole 3. Le schéma garantit que, même dans le cas où un adversaire malveillant est à l'écoute de tous les échanges de la session, le rafraîchissement des secrets entre l'Initiateur et le Répondeur demeure sécurisé.

3.3. *Résumé et discussion*

Nous avons traité dans la section précédente certaines approches récentes, que nous considérons appropriées pour assurer la communication entre les dispositifs actifs et passifs d'un système de surveillance de santé basé sur les réseaux de capteurs RFID [BUE 08]. Nous avons supposé que tous les périphériques du système sont déjà pré-configurés, avec des clés symétriques et des masques initialement identiques (par exemple, des valeurs environnementales uniques ou des matrices symétriques). Ces valeurs permettent, par la suite, la réalisation du processus d'authentification. Pour pouvoir les analyser, nous avons vérifié , également, que les trois protocoles répondent à deux exigences essentielles à savoir, *la communication asymétrique* et *l'intermittence des interrogations*. En ce qui concerne la première exigence, nous avons supposé dans toutes les approches que ce sont les nœuds moins contraints en terme de calcul et de ressources énergétiques (par exemple, les lecteurs d'étiquettes RFID ou les capteurs actifs) qui initient la communication avec une deuxième composante dont les ressources sont beaucoup plus limitées (par exemple, la radio-étiquette RFID passive) et qui doit être amorcée par l'énergie recueillie à partir des dispositifs actifs. Dans notre cas, l'étiquette passive reste en attente de la réception d'une nouvelle clé symétrique dès le début du processus. La seconde exigence vérifie si les protocoles traitent correctement les désynchronisations en raison de l'intermittence du signal envoyé par les dispositifs actifs [BUE 08]. Les approches que nous avons présentées satisfont, en effet, de telles exigences pour être utilisées dans l'échange de clés et le rafraîchissement des secrets.

Ensuite, une analyse des coûts de calculs et de communications a été réalisée pour pouvoir conclure l'adéquation des protocoles aux contraintes imposées par les capteurs passifs de notre schéma de motivation. Cette analyse nous a permis en effet, d'extraire des éléments qui orientent notre choix. Par exemple, l'utilisation d'une fonction de hachage à sens unique avec des éléments biométriques comme dans la solution présentée dans [POO 06, VEN 06] et résumée ici dans le Protocole 1, n'est pas appropriée à notre scénario de départ. D'une part, plusieurs études découragent l'utilisation des fonctions de hachage dans les protocoles appliqués sur les étiquettes RFID [GAR 08, PER 08]. D'autre part, l'utilisation de valeurs environnementales uniques n'est pas possible lorsque les capteurs sont placés sur des objets et non sur un corps humain. Et même si de telles valeurs peuvent être dérivées du corps humain, cela peut provoquer des préoccupations quant à la violation de la vie privée des porteurs de l'étiquette. D'ailleurs, d'un point de vue juridique, l'utilisation de la biométrie comme identifiant dans les applications omniprésentes, telles que celles des services médicaux, a été signalée par les institutions européennes comme solution inquiétante [LIB 05]. Enfin, le manque d'authentification forte est une autre limite relevée dans le Protocole 1. Pour cela, des solutions alternatives, comme celles présentées dans [SIN 07, SIN 09], consistent à ajouter des notions de la cryptographie traditionnelle pour compléter l'approche du Protocole 1. Ces solutions proposent l'utilisation des valeurs environnementales uniques avec des procédures d'authentification bien établies. Par exemple, l'authentification du type Diffie-Hellman avec un échange de clés basé sur la cryptographie à courbe elliptique. Malgré ces efforts, les principales insuffisances de cette solution par rapport à notre schéma de motivation se trouvent au niveau du matériel supportant son implémentation. En effet, en raison des coûts impliqués dans les implémentations de hachage et dans les algorithmes de chiffrement asymétriques proposés, ces solutions ne peuvent être appliquées sur des capteurs passifs du type EPC [EPC 05]. Compte tenu de ces inconvénients, nous nous sommes orientés vers les approches basées sur l'évolution des secrets prédistribués [KAR 05, DOL 06]. Ces approches s'appuient sur des générateurs de séquences pseudo-aléatoires implémentés dans les radio-étiquettes à la place des fonctions de hachage et des valeurs environnementales uniques pour protéger la clé. Nous avons résumé une première stratégie basée sur [KAR 05] dans le Protocole 2. La principale limite de cette nouvelle approche relève des problèmes de synchronisation qui peuvent conduire à des attaques de déni de service [CHI 07]. Une deuxième stratégie, qui résume les approches présentées dans [DOL 06], a été spécifiée en proposant le Protocole 3. Ce protocole garantit un échange hautement sécurisée, s'appuyant sur un seul masque pour chaque session. Notre évaluation montre, en plus, qu'il reste suffisamment léger pour être mis en œuvre dans des capteurs passifs dont les ressources sont limitées.

4. Conclusions et perspectives

Nous avons examiné des approches spécifiques pour sécuriser la communication des composants de surveillance médicales basés sur des capteurs RFID. Nous avons discuté et évalué la pertinence de chaque approche pour garantir certaines exigences telles que la sécurité et la performance. Nous avons particulièrement souligné les approches qui prennent en compte l'hétérogénéité des composants du système en supposant l'existence de nœuds avec des contraintes de calculs et de communications différentes. Notre analyse nous a permis d'extraire des propriétés nécessaires pour garantir l'échange sécurisé des clés entre les composants de notre scénario de motivation. La propriété retenue repose sur l'utilisation d'un masque jetable dans le processus d'envoi du message comportant la clé d'authentification. Cette propriété sera l'objet de nos futurs travaux.

Remerciements

Les auteurs remercient gracieusement le support financier reçu de l'Institut TELECOM grâce à son programme *Future et Rupture*.

5. Bibliographie

[BAO 05] Bao S., Zhang Y., Shen L., « 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*, 2005, p. 2455-2458.

[BAT 06] Batina L., Guajardo J., Kerins T., Mentens N., Tuyls P., Verbauwhede I., « An elliptic curve processor suitable for RFID-tags », *Report 2006/227, IACR*, 2006.

[BOU 96] Boult C., Altmann M., D.Gilbertson e. a., « Decreasing disability in the 21st century : the future effects of controlling six fatal and nonfatal conditions », Health A. J. P., Ed., *Am J Public Health*, vol. 86, 1996, p. 1388-1393.

[BUE 08] Buettner M., Greenstein B., Sample A., Smith J., Wetherall. D., « Revisiting Smart Dust with RFID Sensor Networks », *7th ACM Workshop on Hot Topics in Networks (HotNets-VII)*, 2008.

[BUT 07] Buttyan L., Hubaux. J. P., « Security and Cooperation in Wireless Networks », Cambridge University Press, 2007.

[CAM 07] Camtepe S. A., Yener B., « Combinatorial design of key distribution mechanisms for wireless sensor networks », *IEEE/ACM Transactions on Networking (TON)*, vol. 15, 2007, p. 346-358.

[CHA 03] Chan H., Perrig A., Song. D., « Random key predistribution schemes for sensor networks », *IEEE Symposium on Security and Privacy*, 2003, p. 197-215.

[CHA 07] Chae H. J., Yeager D. J., Smith J. R., Fu. K., « Maximalist Cryptography and Computation on the WISP UHF RFID Tag », *Conference on RFID Security (RFIDSEC)*, 2007.

[CHI 07] Chien H., Chen. C., « Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards », *Computers Standards and Interfaces*, vol. 29, 2007, p. 254-259.

[Com 01] Commission on Behavioral and Social Sciences and Education (CBASSE), « Preparing for an Aging World : The Case for Cross-National Research », rapport, 2001, National Academy Press -Washington, D.C.

[CON 04] Consolvo S., Roessler P., Shelton B., LaMarca A., Schilit B., Bly S., « Technology for Care Networks of Elders », *IEEE Pervasive Computing*, vol. 3, 2004, p. 22-29.

[CZE 08] Czeskis A., Koscher K., Smith J. R., Kohno T., « 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*, 2008, p. 479-490.

[DOL 06] Dolev S., Kopeetsky M., « Secure communication for RFIDs proactive information security within computational security. », Springer L., Ed., *8th Int'l Symposium on Stabilization, Safety, and Security of Distributed Systems*, vol. 4280, 2006, p. 290-303.

[DOL 07] Dolev S., Kopeetsky M., Shamir A., « RFID Authentication Efficient Proactive Information Security within Computational Security », rapport, 2007, Department of Computer Science, Ben-Gurion University.

[DOL 08] Dolev S., Kopeetsky M., Clouser T., Nesterenko M., « Low Overhead RFID Security », *RFID Handbook : Applications, Technology, Security, and Privacy. Ahson S., Mohammad, I. (Editors), CRC Press*, 2008, p. 589-602.

[EPC 05] EPC global, « EPC Radio-frequency identity protocols Class-1 Generation-2 », rapport, 2005, http ://www.epcglobalinc.org/standards/.

[FER 03] Ferguson N., Schneier B., *Practical Cryptography*, vol. 2, John Wiley & Sons, 2003.

[GAR 08] Garcia-Alfaro J., Barbeau M., Kranakis E., « Analysis of Threats to the Security of EPC Networks », *6th Annual Communication Networks and Services Research (CNSR) Conference, IEEE Communications Society*, 2008.

[GAR 09] Garcia-Alfaro J., Barbeau M., Kranakis E., « Security Threat Mitigation Trends in Low-cost RFID Systems », *2nd International Workshop on Autonomous and Spontaneous Security (SETOP 2009), LNCS*, vol. 5939, 2009, p. 193-207.

[GAR 10] Garcia-Alfaro J., Barbeau M., Kranakis E., « 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.

[HO 05] Ho L., Moh M., Walker Z., Hamada T., Su C. F., « A prototype on RFID and sensor networks for elder healthcare : progress report », *ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, 2005, p. 70-75.

[ISO 06] ISO/IEC, « 18000-6 :2004/amd :2006 », rapport, 2006, http ://www.iso.org/.

[KAR 05] Karthikeyan S., Nesterenko M., « RFID Security without Extensive Cryptography », *3rd ACM workshop on security of ad hoc and sensor networks (SASN)*, 2005, p. 63-67.

[Kuo 73] Kuo F., Abramson., « The ALOHA system », *Computer Communications Networks. Abramson, N. and Kuo, F. (Editors.)*, Prentice-Hall, 1973, p. 501-518.

[LIA 05] Liao L., « Group Key Agreement for Ad Hoc Networks », Master's thesis, Ruhr-University Bochum, 2005.

[LIB 05] Liberatore A., « Balancing Security and Democracy : the Politics of Biometric Identification in the European Union », rapport n° 30, 2005, European University Institute (EUI), Robert Schuman Centre of Advanced Studies (RSCAS).

[MOH 08] Moh M., Ho L., Walker Z., Moh T. S., « A prototype on RFID and Sensor Networks for Elder Health Care », RFID Handbook : Applications Technology S., Privacy, Eds., *CRC press*, 2008, p. 311-328.

[PER 07] Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J., Ribagorda A., « An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks », *Emerging Directions in Embedded and Ubiquitous Computing, LNCS*, vol. 4809, 2007, p. 781-794.

[PER 08] Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J., Ribagorda A., « LAMED - A PRNG for EPC Class-1 Generation-2 RFID specification », *Elsevier Science Publishers*, vol. 31, 2008.

[PHI 04] Philipose M., Fishkin K., Perkowitz M., Patterson D., D. Fox H. K., Hahnel. D., « Inferring Activities from Interactions with Objects », *IEEE Pervasive Computing*, vol. 3, 2004, p. 50-57.

[PHI 05] Philipose M., Smith J. R., Jiang B., Mamishev A., Roy S., Sundara-Rajan K., « Battery-free wireless identification and sensing », *IEEE Pervasive Computing*, 2005.

[POO 06] Poon C. C. Y., Zhang Y. T., Bao S. D., « A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health », *IEEE Communications Magazine*, vol. 44, n° 4, 2006, p. 73-81.

[SIN 07] Singh K., Muthukkumarasamy V., « Authenticated Key Establishment Protocols for a Home Health Care System », *Third International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2007, p. 353-358.

[SIN 09] Singh K., Muthukkumarasamy V., « Implementation and Analysis of Sensor Security Protocols in a Home Health Care System », *Third International Conference on Network and System Security*, 2009, p. 137-142.

[VEN 06] Venkatasubramanian K. K., Gupta S. K. S., « Security for pervasive health monitoring sensor applications », *4th International Conference on Intelligent Sensing and Information Processing (ICISIP)*, 2006, p. 197-202.

[WOL 05] Wolkerstorfer J., « Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags ? », *Ecrypt Workshop on RFID and Lightweight Crypto*, 2005.