BANZKP: a Secure Authentication Scheme Using Zero Knowledge Proof for WBANs

Nesrine KHERNANE
Franche Comte University
FEMTO-ST
CNRS UMR 6174
nesrine.khernane@univ-fcomte.fr

MARIA POTOP-BUTUCARU
Sorbonne Universities
UPMC Paris 06
CNRS LIP6 UMR 7606
maria.potop-butucaru@lip6.fr

Claude CHAUDET
LTCI, CNRS UMR 5141
Telecom ParisTech
Universite Paris-Saclay
claude.chaudet@telecom-paristech.fr

***Abstract*—Advances in wearable and implementable of wireless sensors have enable the development of tiny and intelligent sensors called body sensors. Monitoring the vital body parameters in real-time using wireless body area network (WBAN) has shown great potential in improving healthcare quality not only for patients but also for medical staff. However, security and privacy are still an important issue in WBANs especially in multi-hop architectures. Considering the constraints of the body sensors (namely energy, memory, computational power, etc.). In this paper, we propose and present the design and the evaluation of a secure lightweight and energy efficient authentication scheme BANZKP based on an efficient cryptographic protocol, Zero Knowledge Proof (ZKP) and a commitment scheme. ZKP is used to confirm the identify of the sensor nodes, with small computational requirement, which is favorable for body sensors given their limited resources, while the commitment scheme is used to deal with replay attacks and hence the injection attacks by committing a message and revealing the key later. BANZKP reduces the memory requirement by 56,13% compared to TinyZKP [10], the comparable alternative so far for Body Area Networks. Also, the simulation results demonstrate that our proposed scheme is 17 and 5 times more efficient in term of execution time, and uses 94.11% and 80% less energy compared to TinyZKP and W-ECDSA [16], respectively.**

I. Introduction

L'utilisation des capteurs dans le domaine médical a pu attirer l'attention de la communauté de recherche, commençant par des recherches théoriques et allant à des applications pratiques. Ces minuscules dispositifs, à faible puissance de calcul et à une durée de vie limitée, sont capables de détecter et de collecter les phénomènes physiologiques du corps humain (tel que: EEG, ECG, SpO2, Acide lactique, etc.), et de les transmettre vers un point de collecte qui va les traiter, prendre des décisions, alerter, les enregistrer, etc.

Pour aborder l'utilisation croissante de capteurs dans ce domaine, une nouvelle technologie appelée WBAN (Wireless Body Area Networks) a émergé, permettant la résolution de divers inconvénients associés au capteurs câblés qui sont couramment utilisés dans les hôpitaux et les salles durgence pour surveiller les patients. Le désordre trop familier des fils attachés à un patient n'est pas seulement inconfortable pour les patients (conduisant à une mobilité très réduite et rendant les patients anxieux), mais il est aussi difficile à gérer pour le personnel. Très fréquentes sont les déconnexions volontaires de capteurs par les patients et les échecs pour réinsérer ces derniers correctement.

Ainsi, la communication entre les nœuds déployés sur, autour ou dans un corps humain peut être uni-saut ou multi-saut. Notons que la communication multi-saut est considérée comme la plus adéquate pour les réseaux WBAN dû à l'absorption de l'énergie par le corps humain, imposant ainsi l'utilisation d'un faible rapport signal/bruit [11].

Cependant, la communication multi-saut ainsi que le sans fil expose les informations à de multiples types d'attaques, rendant la sécurité dans ces réseaux une tâche incontournable. Malheureusement, les mécanismes de sécurité utilisés dans les réseaux sans fil traditionnels ne peuvent être appliqué en vigueur dans ce type de réseau vu les limitations en terme de ressources des noeuds capteur.

Dans cet article nous présentons une nouvelle solution, BANZKP, qui permet une authentification mutuelle des capteurs d'un réseau WBAN, en se basant sur le principe du Zero Knowledge Proof (ZKP). Bien que le protocole ZKP assure une authentification mutuelle entre l'émetteur et le récepteur, il est vulnérable à l'attaque par rejeu. Afin de contourner ce problème, nous avons utilisé un schéma cryptographique Commitment Sheme (CS) qui permet de mettre en gage un message, et de révéler la clé après un certain temps. Nous avons comparé, via les simulations, BANZKP, W-ECDSA [16], et TinyZKP [10] (la seule solution basée sur le schéma ZKP proposée jusqu'à présent pour les BANs) en prenant comme étude de cas le protocole de convergecast fourni par le projet MiXiM, intégré dans Omnet++. Les résultats de simulation montrent que BANZKP réduit le besoin en terme de mémoire de 56,13% comparer à TinyZKP, la consommation énergétique de 80% et 94.11%, ainsi que le temps d'execution de notre solution est 5 et 17 fois plus rapide comparer à W-ECDSA et TinyZKP, respectivement.

Cet article est organisé comme suit: Section II présente les travaux antécédents. Dans la section III, on présente les fonctionnalités principales des deux outils de sécurité: Zero Knowledge Proof et Commitment Scheme, ainsi qu'un petit rappel sur la sécurité et la protection de la vie privée. Ensuite, dans la section IV nous présentons notre réseau, et le schéma d'authentification de BANZKP. La section V, discute les performances de notre solution en termes de sécurité et

978-1-5090-3426-0/16/$31.00 ©2016 IEEE

d'efficacité. Finalement, la section VI présente les résultats de simulation des troix schéma d'authentification BANZKP, TinyZKP, et W-ECDSA.

II. Travaux connexes

L'objectif principal de TinySec [5], un protocole de sécurité de la couche liaison, est d'assurer une communication sécurisée entre les nœuds capteurs. Conçu pour faciliter son utilisation, pour consommer peu d'énergie et nécéssitant un besoin minime de mémoire. Malheureusement, il n'y a aucune restriction sur la méthode de chiffrement, et une seule paire de clés est sélectionnée pour l'ensemble du réseau, ce qui permet à un adversaire de polluer tous le réseau en compromettant uniquement un seul nœud [20].

Pour faire face à ce problème, Luk et al. ont proposé une solution efficace appelée MiniSec [9], dans laquelle chaque paire de noeuds partagent deux clés secrètes, une pour chaque sens de communication. Un compteur interne (pour chaque sens de communication) est utilisé en tant que nonce à usage unique, et est incrémenté à chaque utilisation de la clé associée. Les compteurs doivent être synchronisés sur les deux côtés et seuls les derniers bits sont inclus dans le paquet afin de minimiser l'énergie de transmission. L'inconvénient est que chaque nœud doit garder un compteur pour chacun de ses voisins, qui sont les expéditeurs possibles, résultant un grand besoin en terme de mémoire. En outre, l'opération de resynchronisation peut être très coûteuse, vu que les compteurs peuvent être désynchronisés.

L'idée de base derrière la conception du μTesla [13], est de résoudre certaines difficultés du standard Tesla dans les réseaux de capteurs, afin d'atteindre l'efficacité de la cryptographie asymétrique via la divulgation tardive des clés symétriques. Un expéditeur signe le message et le diffuse sans révéler la clé. Peu de temps plus tard, l'expéditeur diffuse la clé qui ne sera plus d'actualité. Cependant, la synchronisation de l'heure est nécessaire entre les nœuds concernés [19], ce qui nécéssite un temps supplémentaire pour l'authentification [10]. Même si le commitment scheme utilisé dans μTesla nécessite environ 1000 fois moins de ressources computationnelles que ECDSA [4], le nombre de paquets qui doivent être stockés dans chaque nœud jusqu'à la divulgation des clés peut nécessiter une grande mémoire, tant que la divulgation de clés est indépendante du nombre de paquets diffusés, mais liée à des intervalles de temps.

Dans des travaux similaires, Le schéma TinyPK décrit dans [17], se base principalement sur l'utilisation de la cryptographie à clé publique RSA, et sur différents échanges de clés Diffie-Hellman pour assurer l'authenticité du sink. Cependant, ce processus augmente le délai d'authentification. De plus, les évaluations montrent que les noeuds passent beaucoup de temps dans les opérations de conception de clés publiques et privées. En outre, Das et al [1], ont prouvé que TinyPK est vulnérabilité à l'attaque de mascarade.

Comparer aux crytpo-systèmes RSA, les systèmes basés sur les algorithmes de courbe elliptique à signature numérique (ECDSA) présentés dans [18], sont plus efficaces vu leurs capabilité de maintenir le même niveau de sécurité avec des tailles de clés réduite. Cependant, un besoin supplémentaire en terme d'énergie et de mémoire est nécéssaire durant la phase de transmission et de récéption.

Un autre schéma d'authentification basé sur l'utilisation de la courbe elliptique a été présenté dans [16]. l'objectif principal de W-ECDSA [16] est d'assurer le même niveau de sécurité que RSA (RSA avec une clé de taille 1024 bits), avec une clé de taille 160 bits seulement. cette différence de taille affecte certainement les performances du réseau, et permet au ECC (Elliptic curve cryptography) d'être un choix beaucoup plus préférable que RSA. Cependant, le schéma d'authentification utilisé dans W-ECDSA est basé sur les PKCs (public key cryptograpgy), qui nécéssite l'intégration d'une authorité de certification, ainsi qu'un besoin supplémentaire en terme d'énergie afin de vérifier les certificats, vu que chaque noeud doit être approuvé par une liste de noeuds (considérés comme sécurisés) pour qu'il puisse atteindre sa destination.

Li et al. ont proposé une association sécurisée de capteurs et un système de gestion de clés pour WBAN, appelé Group Device Pairing (GDP) [7], en utilisant une technique d'authentification hors-bande. Ils supposent l'existence de canaux auxiliaires et nécessitent l'intervention des utilisateurs afin d'effectuer une inspection visuelle et simultanée des LED clignotant, pour atteindre un bon niveau d'authentification. Une telle vérification humaine ne peut être intuitif à utiliser, et il est peu probable qu'elle soit approprier pour le scénario d'urgence [14].

Pour faire face aux contraintes de ressources liées aux noeuds capteurs, Zero Knowledge Proof (ZKP), un protocole cryptographique efficace, semble être un meilleur choix pour ce type de réseau. ZKP a été développé par Goldwasser et al. [3], afin d'assurer une authentification mutuelle avec un besoin minime en terme de puissance de calcul et de consommation énergétique. ZKP peut être également utilisé dans les échanges de clés.

À notre connaissance, la première utilisation du protocole Zero Knowledge Proof dans les WBAN a été présentée dans [10]. Ce schéma, appelé TinyZKP, permet à un récepteur R de vérifier que les données reçues proviennent d'un expéditeur S sans aucune divulgation d'informations secrètes. Les résultats dans [10] démontrent que TinyZKP atteint un bon niveau de performance en termes de: temps d'exécution, mémoire, et de consommation d'énergie. Cependant TinyZKP utilise un grand nombre de clés pré-distribué, 20 clés privées, et 20 clés publiques pour chaque nœud. Par conséquent, Il requiert un besoin supplémentaire en terme de mémoire dans les nœuds et complique la phase d'enregistrement. Le fournisseur de services doit enregistrer les clés publiques de chaque nœud de capteur (i.e. 120 clés publiques pour 6 nœuds) dans la station de base (puits). Notons que ces clés publiques sont utilisées uniquement pour vérifier l'authenticité de l'émetteur et du sink, et ne sont utilisées en aucun cas pour le chiffrement des données transitant le réseau. De plus, pour signer un message TinyZKP utilise l'algorithme ECDSA [4],

978-1-5090-3426-0/16/$31.00 ©2016 IEEE

qui résulte en une signature de 320 bits au minimum, et nécessite des ressources computationnelles non négligeable.

III. Background

l'objectif principal de notre schéma d'authentification est d'assurer la sécurité des données transitant le réseau, ainsi que de protéger ces dernières contre tout accès non autorisé, tout en prenant en considération les ressources limitées des nœuds capteur. Cependant, le terme sécurité engendre plusieurs paramètres tel que: la confidentialité, l'intégrité, l'authentification, la responsabilisation, la non-répudiation, la fraicheur de données, etc.

Dans BANZKP, on se base principalement sur les trois principaux axes: la confidentialité, l'intégrité ainsi que l'authenticité.

Concernant la protection de la vie privée, Li et al. [8] ont en présenté une taxonomie détaillée pour les réseaux de capteurs traditionnels RCSF, en divisant la protection de la vie privée en deux principaux axes: Protection de la vie privée *Orientée-Données*, qui concerne la création et la transmission des données via le réseau sans fil. Ainsi que, la protection de la vie privée *Orientée-Contexte*, qui concerne les informations contextuelles tel que la localisation du nœud/réseau, ainsi que le temps du traffic.

Dans BANZKP, on se base dans un premier temps sur la protection de la vie privée en assurant que seulement l'émetteur et le sink ont la capabilité de déchiffrer les données des patients.

Afin d'atteindre ces objectifs, BANZKP combine deux outils cryptographique présentés dans ce qui suit:

Zero Knowledge Proof (ZKP): Le schéma ZKP permet à un émetteur de vérifier l'authenticité du vérificateur et vice versa, en se basant sur un échange de messages de type challenge/réponse, sans toutefois divulguer aucune information sur le secret partagé. Le schéma ZKP a les trois propriétées[12] suivantes:

1) Le vérificateur ne peut pas trahir l'émetteur durant la phase d'échange de messages de type challenge/réponse.
2) L'émetteur ne peut pas trahir le vérificateur.
3) Le vérificateur ne peut pas trahir un autre parti en prétendant être l'émetteur.

Commitment Scheme (CS): Est une primitive cryptographique utilisée pour contrer l'écoute non autorisé. L'émetteur crypte le message en question et l'envoie vers la destination qui ne possède pas encore la clé de déchiffrement. La clé doit être transmise après avoir reçu un signal de la part du récepteur. CS a les propriétées suivantes:

1) Le récepteur ne peut pas trahir et rejouer le message, ou l'utiliser afin de faire ses propres calculs.
2) L'émetteur ne peut pas déjouer le message après le chiffrement.

IV. Le schéma d'authentification proposé

Afin de faire face aux différents types d'attaques, tout en prenant en considération les ressources limitées des capteurs, nous présentons une solution qui se base principalement sur le mécanisme "challenge-response" du protocole ZKP ainsi que sur la technique Comitmment Scheme.

A. Les paramètres du système

Comme le montre la figure 1, notre réseau est constitué de 7 nœuds numérotés de 0 à 6 déployés sur un corps humain.

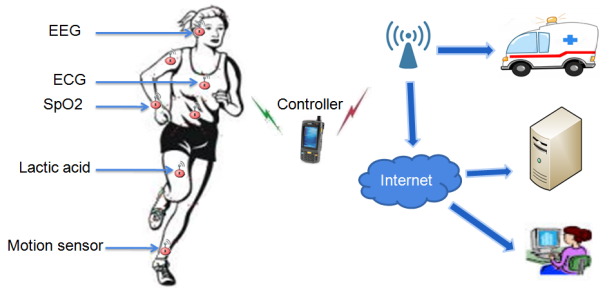

Figure 1: Architecture du réseau de capteur corporel dans les applications médicales

Chaque nœud du réseau partage avec le sink deux valeurs $K_{0,N}$ et $V_{0,N}$, N=1,...,6, tel que: $K_{0,N}$ est la clé de session, tandis que $V_{0,N}$ est le secret partagé entre chacun des nœuds et le sink. Ces valeurs sont différentes les unes des autres et doivent rester secrètes. Chaque nœud du réseau choisi aléatoirement un nombre $p_{N,0}$. Le sink doit choisir N nombres aléatoires $q_{0,N}$, N=1,...,6, tel que chaque nombre va être utilisé avec un seul nœud.

Le fournisseur de service doit introduire les paramètres $K_{0,N}$ et $V_{0,N}$ de chaque nœud dans le sink.

a) Notation: Table I contient la liste des notations utilisées dans ce papier.

Table I: Notations

Notation	Description
ID_i	L'ID du noeud i
$K_{x,y}$	La clé de session symétrique entre x et y
K_{CS}	La clé Commitment Scheme
$V_{0,N}$	Le secret partagé entre le sink et N
$p_{N,0}$	La valeur aléatoire choisi par N
$q_{0,N}$	La valeur aléatoire choisi par le sink
$E_K[M]$	Le message M chiffré par la clé K
RI	Intervalle aléatoire
L(X)	Taille de X
||	Operateur de concaténation

B. Les étapes d'authentification

Après l'initialisation des paramètres, quand un capteur, N, a des données à envoyer au sink, S, il déclenche le mécanisme d'authentification décrit par les étapes présentées dans la figure 2:

978-1-5090-3426-0/16/$31.00 ©2016 IEEE

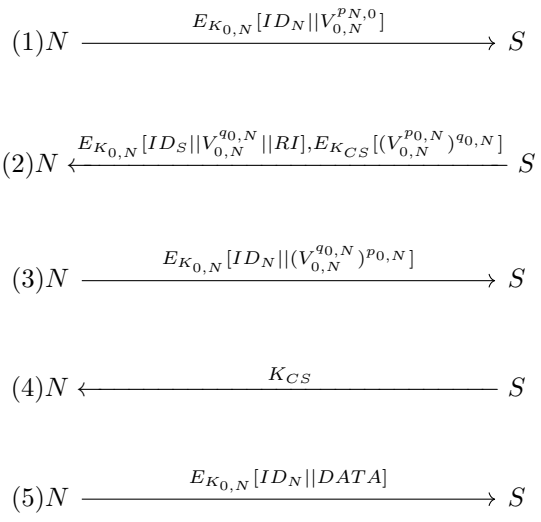

Figure 2: le schéma d'authentification et d'énvoie de données

1) *N* ——> *S*: $E_{K_{0,N}}[ID_N \mid\mid V_{0,N}^{p_{N,0}}]$
Le nœud N calcule $V_{0,N}^{p_{N,0}}$, chiffre le résultat avec la clé de session $K_{0,N}$, et envoie le tout au sink.
2) *S* ——> *N*: $E_{K_{0,N}}[ID_S \mid\mid V_{0,N}^{q_{0,N}} \mid\mid$ RI] , $E_{K_{CS}}[(V_{0,N}^{p_{0,N}})^{q_{0,N}}]$
A la réception du message, le sink le déchiffre, calcule $V_{0,N}^{q_{N,0}}$, et chiffre le résultat avec la clé de session $K_{0,N}$. Le sink calcule $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$ et choisit aléatoirement un intervalle de 200 bits du résultat, et le chiffre à l'aide de la clé "commitment scheme" K_{CS}(choisie aléatoirement). Le début de l'intervalle *RI* est chiffré avec la clé de session $K_{0,N}$, et la totalité du message chiffré est envoyée au nœud *N*.
3) *N* ——> *S*: $E_{K_{0,N}}[ID_N \mid\mid (V_{0,N}^{q_{0,N}})^{p_{0,N}}]$
A la réception du message, le capteur *N* garde le message mis en gage tel qu'il est, déchiffre l'autre partie du message et calcule $(V_{0,N}^{q_{0,N}})^{p_{N,0}}$, ensuite extrait le début de l'intervalle *RI* afin d'envoyer au sink le même intervalle de bits. A la fin, *N* chiffre l'ID_N avec l'intervalle de bits et envoie le message chiffré au sink.
4) *S* ——> *N*: K_{CS}
Dans cette étape, le sink vérifie l'authenticité du nœud comme suit : si l'intervalle de bits reçu est le même que celui calculé à l'étape 2, alors le sink envoie la clé K_{CS} au nœud *N*. Sinon le sink interrompt le mécanisme d'authentification et ignore tout message venant de ce dernier.
5) *N* ——> *S*: $E_{K_{0,N}}[ID_N \mid\mid$ DATA]
Si l'authentification du nœud a réussi, le nœud reçoit la clé K_{CS} qui va lui permettre de déchiffrer l'intervalle de bits de $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$, ainsi que de vérifier l'authenticité du sink. Le nœud chiffre les données pertinentes et envoie ces dernières au sink. Sinon, il ignore le sink et n'envoie aucune donnée.

V. Analyse de la sécurité et de l'efficacité

Dans cette section nous discutons les performances de notre solution en termes de sécurité et d'efficacité. On rappelle que notre solution repose principalement sur le protocole ZKP, cependant, l'utilisation de cette technique seule ne permet pas de faire face aux attaques de rejeu et d'injection de données. Pour palier ce problème nous avons utilisé la technique du "Comitment Scheme".

A. Analyse de la sécurité

Nous présentons en ce qui suit les différentes attaques tolérées par notre solution.

L'attaque des faux noeuds : L'attaquant se fait passer par un nœud légitime ce qui peut entrainer une consommation supplémentaire d'énergie ainsi qu'une injection de fausses données. Dans notre solution, avant d'envoyer ses données, un nœud doit s'authentifier auprès du sink. Si "le challenge" imposé par le sink n'a pas été réussi par le nœud alors le sink ignorera toutes les données venant de ce dernier.

L'attaque du faux sink : L'attaquant se fait passer par le sink afin de récupérer les données pertinentes venant des nœuds légitimes. Vu que notre schéma d'authentification est mutuel, le nœud, à son tour, doit être sûr de l'identité du sink avant d'envoyer ses données. De plus, les données sont cryptées avec une clé partagée uniquement entre le sink et le nœud en question.

L'attaque par rejeu : L'attaquant va essayer de rejouer la valeur $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$ pour faire croire au sink que c'est l'un des nœuds légitimes. Afin d'éviter cette attaque le principe du Commitment Scheme a été utilisé, permettant de mettre en gage un message et de le révéler plus tard, ce qui a permis d'éviter cette attaque ainsi que l'attaque d'injection de données.

L'attaque d'injection : Cette attaque peut être introduite après avoir réussi l'attaque par rejeu. L'attaquant va chercher à injecter de fausses données dans le réseau. Le but de cette attaque peut être de faire circuler de fausses informations, de consommer les ressources d'un nœud, ou tout simplement de saturer (surcharger) le réseau. Cette attaque peut également engendrer une mauvaise prise de décision intolérable dans un contexte médical. Afin d'éviter cette attaque nous avons utilisé le principe du Commitment Scheme qui permet de mettre en gage un message et de le révéler plus tard.

L'attaque "man in the middle" : L'attaquant se positionne entre le nœud légitime et le sink en établissant une connexion indépendante avec les deux et en essayant de récupérer le secret ou les données pertinentes envoyées vers le sink. Dans notre solution aucune information sur le secret n'est divulguée. En plus, les données envoyées vers le sink sont chiffrées et aucune information sur les clés n'est envoyée sur le canal de communication.

B. Analyse de l'éfficacité

Dans cette section, nous comparons les besoins en terme de communication et de puissance de calcul de notre BANZKP

978-1-5090-3426-0/16/$31.00 ©2016 IEEE

avec TinyZKP et W-ECDSA présentés dans [10], et [16], respectivement.

Analyse du coût de communication : Notre schéma d'authentification mutuelle se résume en quatre étapes d'échange de messages ayant besoin de 2*L($V^{p/q}$)+ 2*L($V_{0,n}^{q_{0,n}}$)$^{p_{n,0}}$)+ L(K_{CS})= 1300 bits. Le coût de la communication de TinyZKP est de : L(M_{chall})+ L(ECDSA(M_{chall}))+ L(SHA-1(X_m))+ L(Y_m)=1710 bits. Même si TinyZKP peut assurer un schéma d'authentification en seulement deux échanges, et même si on considère que l'ECDSA [4], utilisé dans TinyZKP, génère un minimum théorique de 320 bits pour la signature, le coût de communication de TinyZKP est plus important. Concernant W-ECDSA, le coût de la communication dépend du nombre de noeuds sécurisés choisi afin d'approuvé l'émetteur. durant l'implémentation du W-ECDSA, nous avons choisi uniquement deux noeuds sécurisés et le coût de la communication est: $L(al_0||C_0) + 2 * L(z_n l_n R_0) + L(al_A||l_r) + L(K_{h2(VA)}(al_0||query))$ = 2182 bits.

Analyse de la puissance de calcul : Dans notre solution le secret partagé est pré-distribué et les $p_{N,0}$ et les $q_{0,N}$ sont choisis aléatoirement. Il en résulte que le coût en puissance de calcul est zéro contrairement à TinyZKP où pour retrouver le secret partagé le besoin en terme de puissance de calcul n'est pas négligeable. Selon la littérature, [2], le nombre moyen de multiplications modulaires est de T*(k+2)/2, tel que T est le nombre de fois où la multiplication modulaire a été recalculée, et k est le nombre de fois où on a calculé la multiplication modulaire. Il en résulte que le coût de communication dans TinyZKP est de 1*(20+2)/2=11, ce qui nécessite non seulement des ressources en terme de puissance de calcul mais aussi en terme de mémoire.

VI. Résultats et évaluation

L'évaluation de notre schéma d'authentification et de communication a été réalisée en utilisant comme étude de cas le protocole de routage convergecast intégré dans Omnet++ [15] enrichi avec la plateforme MiXiM [6]. Dans nos simulations, le sink est positionné au niveau de la poitrine. Les autres nœuds du réseau échangent avec le sink les messages challenge/réponse jusqu'à la vérification de l'identité dans les deux sens, via une communication multi-sauts. Les performances de notre solution BANZKP, ainsi que celles de TinyZKP et W-ECDSA, en termes de temps d'exécution, de mémoire et d'énergie sont présentées en ce qui suit:

Temps d'exécution : Dans certains types d'application (tel que les applications d'urgence), le temps d'exécution joue un rôle primordiale, non seulement pour atteindre une durée de vie maximale du réseau, mais aussi afin d'assurer une intervention rapide du personnel. Pour ce, assurer un équilibre entre une collecte sécurisée des données et un temps de réponse minimale est un enjeu cruciale. Comme le montre la figure 3, BANZKP assure un temps d'exécution beaucoup plus petit comparer à TinyZKP et W-ECDSA, et s'exécute 17 et 5 fois plus rapidement, respectivement.

Cette différence, peut être expliqué par le fait que TinyZKP utilise la multiplication modulaire qui est considérée comme l'opération la plus gourmande en terme de computation. Tandis que pour W-ECDSA, cette différence est dû au nombre de vérification nécessaire du PKC afin d'approuver l'émetteur avant qu'il puisse atteindre sa destination.

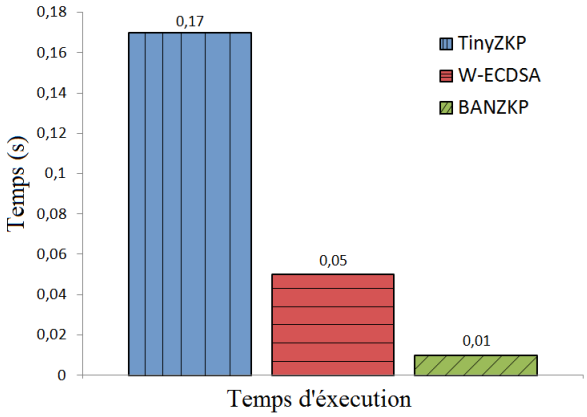

Figure 3: Comparaison du temps d'exécution

Coût énergétique **:** Les résultats présentés dans la figure 4 montrent que nous avons pu réduire la consommation énergétique de 80% et 94.11% comparé à W-ECDSA et TinyZKP, respectivement. Cette réduction est due notamment à l'utilisation du commitment scheme qui nécessite 1000 fois moins de ressources computationnelles comparé à ECDSA [4]. Concernant W-ECDSA, cette différence est due à la consommation énergétique supplémentaire pour la vérification des certificats par chaque noeuds intermédiaire. Notons que, plus le nombre de ces noeuds sécurisés est grand, plus le besoin en terme d'énergie est important.

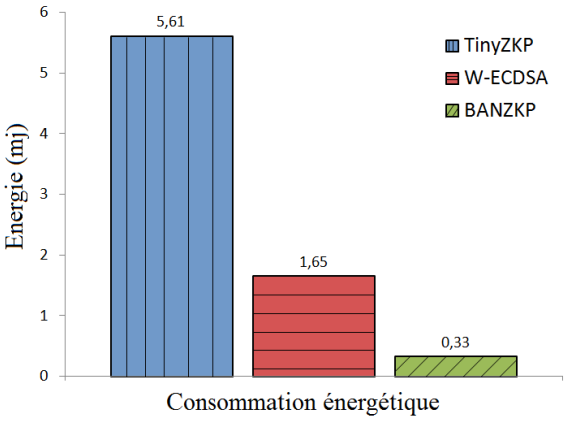

Figure 4: Comparaison de la consommation énergétique

Coût en mémoire **:**Les résultats présentés dans la figure 5, montrent que nous avons pu réduire le besoin en terme de mémoire de 56,13% comparé à TinyZKP. Les mauvaises performances de TinyZKP s'expliquent par le grand nombre de clés qui doivent être stockées dans chaque nœud du réseau

978-1-5090-3426-0/16/$31.00 ©2016 IEEE

(20 clés publiques et 20 clés privées), spécialement dans le sink qui doit maintenir dans sa mémoire non seulement les 6 clés de session, mais aussi les 120 clés publiques des nœuds du réseau (dans le cas de 6 nœuds). En outre, la signature et la vérification de la signature (ECDSA et SHA-1) utilisé dans TinyZKP, nécessite un besoin supplémentaire en terme de mémoire. Tandis que, dans BANZKP nous utilisons le principe du Commitment Scheme, ce qui nous a permis une vérification simple et efficace de l'identité de chaque entité.

La figure 5, montre une légère différence entre W-ECDSA et notre schéma qui se présente en 4.77%. Cette différence est due au fait que W-ECDSA nécessite une moindre manipulation comparé TinyZKP et BANZKP, vu que tous les paramètres nécessaire sont calculés au préalable par l'autorité de certification, et pré distribués avant le déploiement.

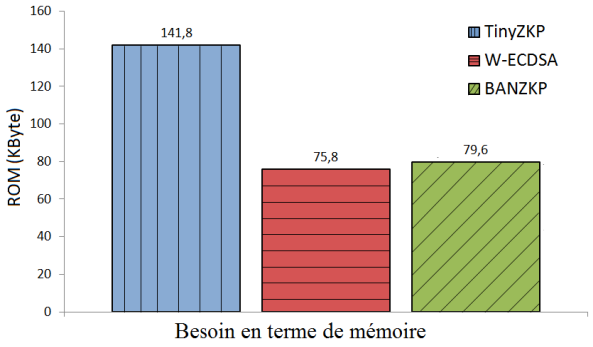

Figure 5: Comparaison de la mémoire ROM

VII. Conclusions

Les progrès réalisés ces dernières années dans les réseaux WBAN, montrent que ces derniers représentent une technologie du futur. Parmis les problèmes qui se posent dans ce contexte on trouve la sécurité comme une tâche incontournable. Afin de faire face aux différents types d'attaques et en se basant sur le principe du ZKP et de l'efficacité du Commitment Scheme, nous avons proposé une nouvelle solution, BANZKP, qui permet une authentification mutuelle entre l'émetteur et le récepteur, tout en prenant en considération les ressources limitées des capteurs. Notre solution a été comparée avec TinyZKP [10] (la seule solution ZKP proposée pour les réseaux WBANs) et W-ECDSA [16]. Les trois schémas d'authentification ont été implémenté en prenant comme étude de cas le protocole de routage convergecast fourni dans la distribution du projet MiXiM, intégré dans Omnet++. Les résultats de simulation montrent que notre schéma d'authentification réduit le besoin en terme de mémoire de 56,13% comparer à TinyZKP, le besoin en terme de consommation énergétique de 80% et 94.11%, ainsi que le temps d'execution de notre solution est 5 et 17 fois plus rapide comparer à W-ECDSA et TinyZKP, respectivement.

Acknowledgements

The authors are supported by the SMARTBAN project (http://www.smart-labex.fr/SMART-BAN.html).

References

[1] M. L. Das. Two-factor user authentication in wireless sensor networks. *Wireless Communications, IEEE Transactions on*, 8(3):1086–1090, 2009.

[2] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology-CRYPTO86*, pages 186–194. Springer, 1987.

[3] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304. ACM, 1985.

[4] Y.-C. Hu and K. P. Laberteaux. Strong vanet security on a budget. In *Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, volume 6, pages 1–9, 2006.

[5] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM, 2004.

[6] A. Köpke, M. Swigulski, K. Wessel, D. Willkomm, P. Haneveld, T. E. Parker, O. W. Visser, H. S. Lichte, and S. Valentin. Simulating wireless and mobile networks in omnet++ the mixim vision. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 71. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[7] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren. Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Transactions on sensor Networks (TOSN)*, 9(2):18, 2013.

[8] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Networks*, 7(8):1501–1514, 2009.

[9] M. Luk, G. Mezzour, A. Perrig, and V. Gligor. Minisec: a secure sensor network communication architecture. In *Proceedings of the 6th international conference on Information processing in sensor networks*, pages 479–488. ACM, 2007.

[10] L. Ma, Y. Ge, and Y. Zhu. Tinyzkp: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks. *Wireless personal communications*, 77(2):1077–1090, 2014.

[11] A. Natarajan, M. Motani, B. de Silva, K.-K. Yap, and K. C. Chua. Investigating network architectures for body sensor networks. In *Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments*, pages 19–24. ACM, 2007.

[12] V. Parbat, T. Manikrao, N. Tayade, and S. Aghav. Zero knowledge protocol to design security model for threats in wsn. *Int. J. Eng. Res. Appl.(IJERA)*, 2:1533–1537, 2012.

[13] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The tesla broadcast authentication protocol. *RSA CryptoBytes*, 5, 2005.

[14] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 524–539. IEEE, 2014.

[15] A. Varga et al. The omnet++ discrete event simulation system.

[16] H. Wang, B. Sheng, C. C. Tan, and Q. Li. Public-key based access control in sensornet. *Wireless Networks*, 17(5):1217–1234, 2011.

[17] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk: securing sensor networks with public key technology. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 59–64. ACM, 2004.

[18] W. Wei-hong, C. Yi-ling, and C. Tie-ming. Design and implementation of an ecdsa-based identity authentication protocol on wsn. In *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2009 3rd IEEE International Symposium on*, pages 1202–1205. IEEE, 2009.

[19] T. Winkler and B. Rinner. Security and privacy protection in visual sensor networks: A survey. *ACM Computing Surveys (CSUR)*, 47(1):2, 2014.

[20] J. Xing, C. Zhao, X.-l. Wang, and N. Xiang. Security analysis in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2014.

978-1-5090-3426-0/16/$31.00 ©2016 IEEE