2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems

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*—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. 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 [16], 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 [25], respectively.**

I. Introduction

Recent advances in wearable and implementable of wireless sensors in health domain attracted the attention of the research community ranging from theory to practice. These tiny devices with low computing power and limited life, deployed in/on or around a human body, are able to detect and collect the physiological phenomena of the human body (such as: EEG, ECG, SpO2, lactic acid, etc.), and further transmit this information to a collector point that will process it, take decisions, alert or record.

To address the increasing use of sensors in this area, a new technology called WBAN (Wireless Body Area Networks) has emerged in response to the various disadvantages associated with wired sensors commonly used to monitor patients in hospitals and emergency rooms. The mess of wires attached to a patient is not only uncomfortable for patients, leading to a very limited mobility and making patients anxious, but it is also difficult to manage for staff. Voluntary or involuntary disconnections of sensors are very common and reintegrating these sensors properly is difficult if not impossible. WBAN is a promising technology for various applications, and it shall be increasingly necessary for monitoring, diagnosing and treating populations. Recent medical reports predict that the number of people using home health technologies will enormously increase from 14.3 to 78 million consumers from 2014 to 2020 [1], respectively. Additionally, body sensors shipments will hit 3.1 million units every year.

WBANs could hence represent a true advance in digital patient care. Thus, the communication between the different wireless nodes deployed in a compact spatial region (in/on or around a human body) can be single-hop or multi-hop. Previous research [18], confirms that the multi-hop communication is considered as the most appropriate for WBAN networks due to the absorption nature of energy by the human body, entail a very low Signal-to-Noise-Ratio (SNR).

Since in the WBANs, the stored data related to a patient plays a critical role in medical diagnosis and treatment, ensuring the security of pertinent information and the privacy of patients is a crucial task. If not securely protected, an adversary may eavesdrops the patient related data and reveal them to social networks (i.e. facebook, twitter) or to insurance companies.

However, the WBAN characteristics such as, multi-hop communication, wireless medium, and low SNR expose information to multiple types of security and privacy attacks (i.e. eavesdropping, modification, loss, injection), and make the possibility of these attacks more likely to appear than in the traditional wireless sensor networks.

Unfortunately, the existing security mechanisms such as asymmetric cryptography used in wireless networks cannot be applied in WBANs given the limitations in terms of power budget, memory capacity, communication and computational ability of body sensors. To establish a trust relationship among the WBAN sensors and to ensure a secure forwarding of collected data from different nodes of the network to a collection point, a lightweight authentication mechanism must be implemented.

*This work is fully supported by SMARTBAN project http://www.smart-labex.fr/SMART-BAN.html

2155-6814/16 $31.00 © 2016 IEEE
DOI 10.1109/MASS.2016.62

Our contribution: In this paper, we present and prove the correctness of BANZKP, a novel ZKP-based solution. It allows two entities to verify their mutual identities with the low computational requirement of a local Zero Knowledge Proof scheme. Zero Knowledge Proof schemes, when used alone, are vulnerable to replay attack [5], which can permit an adversary to inject false data once he successfully performed a replay attack. To cope with this problem, BANZKP uses another cryptographic tool: a Commitment Scheme (CS) that allows one party to commit the message and reveal the secret later. our solution is based on the following hard to solve problem: it is infeasible to solve computationally the discrete logarithms for hundreds of bits numbers [16].

The security and efficiency performance of our scheme are then evaluated in the OMNET++ simulator, by implementing BANZKP as an add-on to the convergecast routing protocol. We also implemented in OMNET++ (using the same simulation bases as for BANZKP) TinyZKP [16] (the comparative alternative for BAN),and W-ECDSA [25]. Compared to TinyZKP [16] and W-ECDSA [25], BANZKP reduces the energy requirement by 94,11% and 80% and runs 17 and 5 times faster, respectively.

II. Related Work

The primary focus of TinySec [8], a popular secure link-layer protocol, is to ensure a secure communication between sensor nodes. It is designed to be easy to use, to consume little energy and to require a minimal amount of memory. Unfortunately, there is no restriction on selecting keying techniques. Therefore, an adversary can pollute the entire network by compromising only one single node [29].

To deal with this problem, Luk et al. have proposed an efficient architecture in MiniSec [15], where each pair of nodes shares two secret keys, one for each direction of communication. An internal counter for each direction is used as a nonce and incremented at each use of the associated key. The counters must be synchronized on both sides and only the last bits are included in the packet to minimize the transmission energy. Two drawbacks can be seen by this proposition. Firstly, every node should keep a counter for each of its neighbors, which are possible senders, resulting in high memory overhead. Secondly, the counter can be unsynchronized, making the resynchronization of counters a very expensive operation.

In a similar work, authors in μTesla [20] have used the commitment scheme to sign a messages and then broadcast it without disclosing the key. A short time later, the sender broadcasts the key that will not be used in the future. Time synchronization is necessary between the involved nodes [28], which increases authentication delay [16].

The commitment scheme used in μTesla requires approximately 1000 times less computational resources than ECDSA [6]. Hence, the number of packet that should be stored in each node until the disclosure of the keys may require large memory, since the key disclosure is independent from the packets broadcast, but tied to time intervals.

Moreover, the TinyPK scheme, described in [26], is based on the use of the public key cryptography using RSA, and different Diffie-Hellman key exchanges to ensure the authenticity of the sink. However, this process increases authentication delay. Also, the evaluation of the scheme shows that the nodes spend much time realizing public and private key operations. Compared to the RSA crytposystems, systems based on elliptic curve digital signature algorithm (ECDSA) described in [27], are more efficient since they are capable to maintain the same security level with shorter key sizes. However, an additional power and memory consumption is required, during the transmission and verification phase.

Another authentication scheme based on elliptic curve cryptography were described in [25]. The main objective of W-ECDSA [25] is to insure the same level of security as RSA (1024 bits key length), by only 160 bits key length using elliptic curve cryptography. This difference in length affects certainly the performance of the network and makes the use of ECC much more preferable than RSA. However, the authentication scheme in [25] is based on the PKC security scheme, that needs to integrate a certification authority, and require additional power consumption to verify the public key certificates, since the node must be approved by a list of secure nodes before reaching the destination.

Li et al. have proposed a secure sensor association and key management scheme for WBAN, called group device pairing (GDP) [12], by using an out of band authentication technique. They assume the existence of auxiliary channels and require the users to visually inspect simultaneous LED blinking patterns, in order to achieve a good level of authentication. However, such human aided verification may not be intuitive to use, and it is unlikely to be appropriate for emergency scenarios [22].

A distributed prediction based secure and reliable renting framework (PSR) has been proposed in [14] for wireless body area networks. In this scheme, each node maintains a matrix, in which it stores the link quality measurements between itself and all other nodes in the network during the last p past time slots. They also proposed an authentication scheme that requires computational resources and hence an additional energy consumption.

To achieve an efficient CPU and energy, Eschenauer et al [3] proposed a probabilistic key management scheme(RKP). Firstly, the service provider registers a key ring of K keys, selected randomly from a set of S keys in each node. Then, if two nodes shared the same key, they proceed of computing of their session secret key. However, this scheme requires a large memory. Additionally, if one node is corrupted, then the number of the discovered key will be important.

To cope with the above mentioned constraints, Goldwasser et al. [5] have developed an efficient cryptographic protocol (Zero Knowledge Proof) with small computational requirement and less energy consumption. ZKP can be used in both: key exchange, and authentication mechanisms.

To the best of our knowledge, the first use of Zero Knowledge Protocol in WBAN was presented in [16]. This scheme, called TinyZKP, allows a receiver R to verify that a piece of data originates from a sender S without leaking any secret information. Results in [16] have demonstrated that TinyZKP achieves a good performance specifically in terms of time execution, memory, and energy requirements. However, TinyZKP uses a large pre-distributed set of keys, 20 private keys, and 20 public keys for each node, used only to obscure the shared secret between the node and the sink, and they are not used in any case for encrypting the network data. Thus, it requires memory in the nodes and complicates the registration phase. The service provider has to register the public keys of every sensor node (e.g. 120 public keys for 6 nodes) into the base station (sink). Furthermore, to sign a message, TinyZKP used ECDSA algorithm [6] in which the shortest possible signature size is 320 bits, which requires non negligible computational resources.

III. System model

This section defines the network and the threat models.

A. Network model

To the best of our knowledge the only realistic channel model has been provided in [17]. In [2] the authors implemented it in MiXim project [9], that joins and extends several existing simulation frameworks developed for wireless and mobile simulations in Omnet++ [24]. The work of [17] models an on-body $2.4\,GHz$ channel between 7 nodes, that belong to the same WBAN, using small directional antennas modeled as if they were $1.5cm$ away from the body. Nodes are assumed to be attached to the human body on the head, chest, upper arm, wrist, navel, thigh, and ankle. Therefore, in our work we consider a network consisting of 7 nodes deployed on the human body, each human body represent a WBAN, and for each WBAN sensors are used to automatically collect physiological data and transmit them to the sink.

B. Threat model

As previously mentioned, an adversary may initiate only external attacks by using computationally powerful devices such as personal computers. For example he/she can eavesdrop all the traffic between the different nodes and the sink, inject arbitrary messages, replay old ones, and spoof node identities.

Note that an external adversary can launch denial of service (DoS) attacks, such as the black-hole attack, in which the attacker discards all received data (these security attacks type is out from the scope of this paper). We make no assumption about the number or the localization of the adversaries.

IV. Background

A. Security and privacy

The main goal of our work is to ensure a trust relationship among the WBAN nodes, and ensure a secure and privacy-protecting forwarding process of the collected medical data. This solution must take into account the nodes constraints resources in terms of energy and computation requirement. The secure term can indeed cover many security features, that are explained in the following:

1) WBAN Security requirements: Security is commonly referrer to the following parameters [11], [10], [23]:

Data Confidentiality: Patient related data contain personal and vital information that should be kept private. Therefore, protecting them from being leaked to external networks is primordial. Thus, encryption and access control methods must be used.

Authentication: Any user aiming to access patient-related data needs his identity to be identified in order to prevent attacks such as Denial of Service (DOS) or data injection from outside the BAN. Therefore, message authentication is used in order to prove the legitimacy of the patients that sent them.

Data Integrity: Information related to the patients health being vital, any possible modification, deletion or addition on it can have catastrophic results. Thus, these information must not be altered illegally. This can be prevented by dynamically checking it and alerting the user in advance in case any attempt of corruption is detected.

Data Freshness: To prevent data from being altered and facing attacks, it is necessary to use as fresh data as possible. Data freshness aims to ensure the received data is fresh, which guarantees it has not been captured in transit and replayed later by an adversary in order to confuse the coordinator. Two types of freshness may be used; weak freshness for ordering partial data frames without guaranteeing the delay and strong freshness, which ensures both frames ordering and delay.

Secure Management: WBAN security involves secure management in the coordinator since it provides key encryption for the BNs in order to enable encryption and decryption operation. In case of association or dissociation, the coordinator safely adds or removes the nodes.

Availability: An attacker could target an ECG node that contains a fragment of patient-related data before it arrives to the physician by capturing or enabling it; given that this information is vital, its loss may cause the patients' death. Ensuring the availability of information in the BAN is a necessity even under DOS attacks.

Dependability: In the case of data erasure or a node failure, patient information must absolutely be recoverable.

Revocability: The moment a WBAN node or user acts maliciously or try to carry out unauthorized actions; its privileges must be deprived immediately, before any harm could be done.

Accountability: Any user trying to act maliciously or cause harms to nodes containing patient related data should be identified and held accountable of his actions.

Non-repudiation: In order to avoid any eventual denial of the origin of a node by the source that generated it, non repudiation is required to assure that the attacker will be taken accountable for performing harmful activities.

In BANZKP, we focus on the following three main properties: *d*ata confidentiality, *data authenticity*, and *data integrity*, as most other properties derive from these ones.

2) WBAN Privacy requirements: Privacy task was always mitigated with security. Yet, very hard to define. In the literature we find: on one hand, those who consider it as one of the security parameters [21]; on the other hand, those who consider it as a fully fledged domain [7]. From our point of view, although the privacy inherits the majority of the security parameters, and one often follows the other, we consider them as two different research area. As mentioned in [7], security concerns the secure forwarding and storage of data. While, privacy concerns the rejection of any unauthorized entities to access to this data, and the appropriate use of them by an authorized party, Li et al. [13] have outlined a good and explicit taxonomy of privacy in traditional WSN (that can be heavily borrowed to WBAN), by dividing it into two principal axes: data-oriented privacy and context-oriented privacy. *D*ata-oriented privacy concerns the data created or transmitted within the network. In contrast, *Context-oriented privacy* concerns the contextual information such as the location of a node/network, or the timing of traffic flows.
Thus, to ensure a good level of privacy, the two axes should be well studied and secured.
In BANZKP, we first focus on *d*ata privacy by ensuring that in the case of multi-hop communication, only the emitter and the sink are able to have access to the unencrypted patient-related data. The motivation for the study of these problems in the multi-hop networks has been extensively discussed in section I.

B. Cryptographic tools

In order to overcome attacks that can target the WBAN, and to achieve the expected security and privacy level, BANZKP combines two cryptographic tools: a Zero Knowledge Proof scheme and a Commitment Scheme that are described hereafter.

Zero Knowledge Proof (ZKP): The main objective of ZKP schemes is to let two parties (a sender and a verifier), to verify the identity of their peer. Both nodes exchange a few challenge/response messages without disclosing any information about a shared secret to the other party and henceforth to any eavesdropper. The author in [19] proved that ZKP schemes have the following four main properties:

1) The verifier cannot guess any information from the exchanged messages during the challenge/response phase.
2) The sender cannot cheat the verifier.
3) The verifier cannot cheat the sender.
4) The verifier cannot cheat another party by pretending to be the sender.

Commitment Scheme (CS): Commitment schemes [12], are cryptographic primitives used to prevent eavesdropping by letting a sender to transmit an encrypted message to a receiver which does not possess the decryption key yet. The key must be transmitted later, when the sender receives a signal from the receiver. If used with classical additional techniques, it has the following properties:

1) A receiver cannot cheat and replay the message or use it to make its own calculation;
2) The sender cannot cheat by changing the message after committing it.

V. BANZKP Authentication scheme

Due to the high computational and energy requirement of asymmetric key cryptography, which is not favorable for resources limitation of body sensor nodes, the proposed BANZKP uses symmetric cryptography to ensure data confidentiality. Beside, to avoid sending data to a forge sink, a sensor node must be sure about the identity of the sink without nevertheless consuming a lot of energy. In this paper, we present a lightweight solution (BANZKP), that uses the challenge-response mechanism of a ZKP protocol as well as a commitment scheme to let the sensors authenticate the sink node, and vice versa. Several type of attacks have been countered by combining these two approaches, and will be detailed in the next section.

Notation: Table I contains a list of notations used throughout the rest of the paper

A. Parameters and Assumptions

We consider a network composed by 7 nodes, numbered from 0 to 6, deployed around or on a human body. BANZKP makes the following assumptions, which are the same as TinyZKP:

1) The nodes and the sink are assumed to be protected from physical compromises and trustworthy. This assumption is reasonable because the different nodes and the sink are handled by a patient and can be protected in secure location. Besides, the nodes can be equipped with anti-tampering mechanisms. Therefore, we can limit protection to external attacks only.

Table I: Main notations

Notation	Description
ID_i	The node ID of sensor node i
$K_{x,y}$	The symmetric session key between x and y
K_{CS}	The commitment scheme key
$V_{0,N}$	Secret information shared between the sink and N
$p_{N,0}$	The random value chooses by N
$q_{0,N}$	The random value chooses by the sink
E(K[M])	Encryption message M with the session key K
RI	Random interval
L(X)	Length of X
||	Concatenation operator

2) Due to the constrained resources of the sensor nodes, computationally expensive and energy intensive operations must be avoided to calculate and transmit keys. Therefore, keys and parameters used by BANZKP should be uploaded by an operator in the nodes before deployment of the wireless body sensor network.
3) To register a new node as a member of a WBAN network, or to replace a dead nodes, the sink must be accessible by the operator in order to register the new node, i.e. to upload in the sink shared parameters specific to this node. The use of close-range pairing mechanisms could be effective at this stage.

Under the previous assumptions, for each sensor node N, BANZKP uses and maintains the following values:

1) Each N shares with the sink (node 0) a session key $K_{0,N}$, N=$\{1, ..., 6\}$. The values of $K_{0,N}$ are different for each node, uploaded manually at the node registration phase and should kept secret.
2) Each N shares with the sink a number $V_{0,N}$, n=$\{1, ..., 6\}$ used for authentication. The values of $V_{0,N}$ are different for each node, uploaded manually at the node registration phase and should be kept secret.
3) Each N chooses a random number $p_{N,0}$, N=$\{1, ..., 6\}$ used for authentication with the sink.
4) The sink chooses randomly one different random number for each sensor node N : $q_{0,N}$, N=$\{1, ..., 6\}$, while each number must be used with a single node (i.e. $q_{0,1}$ will be used only with node 1).

B. BANZKP protocol

BANZKP is composed of two phases: a registration phase in which an operator physically pairs the nodes and the sink and an online authentication phase, both described below.

Registration Phase: In this phase, an operator (service provider) registers nodes with the sink by uploading each secret number $\{V_{0,1}, V_{0,2},..., V_{0,6}\}$ into the sink (considered as the authentication center), as well as the different shared keys, $\{K_{0,1}, K_{0,2},..., K_{0,6}\}$. These keys, shared between the sink and sensor nodes, allow sensors to communicate with the sink and ensure a secure data forwarding. Then the group of body sensor nodes must be uniquely and securely associated to the patient they will serve for.

Authentication Phase: We suppose that the sensors are deployed at designated places (on the human body), and that the system initialization is finished. When a node N has data to send, it starts the authentication mechanism. Authentication is mutual, which means that the node must prove its identity to the sink and verify that the sink is the expected one. Our approach is based on the strength of the zero knowledge proof algorithm, and the communication between the sensor node *N* and the sink *0* can be decomposed in the five following steps (as shown in figure 1) :

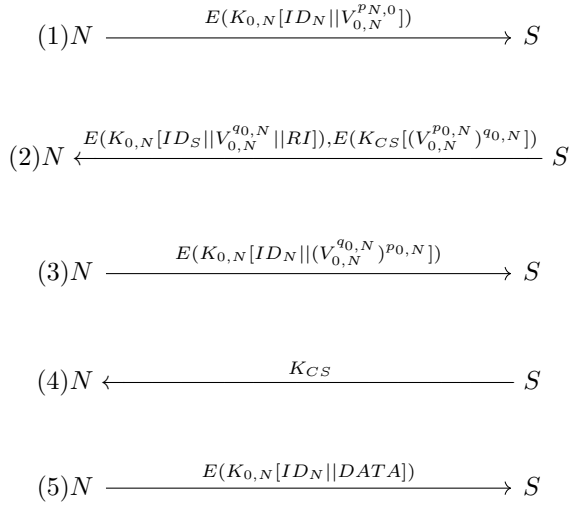

Figure 1: The authentication and data sending scheme

1) *Sensor node* $\rightarrow$ *sink*: $E\left(K_{0,N}\left[ID_N||V_{0,N}^{p_{N,0}}\right]\right)$

   The node N draws $p_{N,0}$, calculates $V_{0,N}^{p_{N,0}}$, concatenates it to its identifier ID_N, encrypts it with its session key $K_{0,N}$ and sends the entire resulting message to the sink.
2) *sink* $\rightarrow$ *sensor node*:
   $E\left(K_{0,N}\left[ID_0||V_{0,N}^{q_{0,N}}||RI\right]\right)$,
   $E\left(K_{CS}\left[\left(V_{0,N}^{p_{N,0}}\right)^{q_{0,N}}\right]\right)$

   Upon reception of the initial message, the sink decrypts it and then proceeds its calculations; it firstly calculates $V_{0,N}^{q_{0,N}}$ and encrypts it with the session key $K_{0,N}$, and then calculates $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$, which has minimum size of 1096 bits. Then, it chooses a random

interval such as the size of this latter must be 200 bits, and encrypts it with the commitment scheme key K_{CS} (chosen randomly and used only one time). The beginning of the interval *RI* is encrypted with the session key $K_{0,N}$.
The encrypted message, which includes the identifier, ID_0, $V_{0,N}^{q_{N,0}}$, RI and $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$ interval value, is sent to the sensor node N.

3) *Sensor node* $\rightarrow$ *sink*:
$E\left(K_{0,N}\left[ID_N||\left(V_{0,N}^{q_{0,N}}\right)^{p_{N,0}}\right]\right)$
When it receives the message from the sink, the sensor node *N* stores the received commitment message as it is, decrypts the other part of the message and calculates $(V_{0,N}^{q_{0,N}})^{p_{N,0}}$ from the received value $V_{0,N}^{q_{0,N}}$, and then extracts the beginning of the interval *RI* from the received message to send the same size of interval (starting from *RI*) from the calculated value. Then, it concatenates ID_N and $(V_{0,N}^{q_{0,N}})^{p_{N,0}}$, encrypts it with the shared session key and sends the message to the sink.
4) *sink* $\rightarrow$ *sensor node*: K_{CS}
In this step, the sink verifies the authenticity of the node as follows: if the interval of bits received in the message after decrypting is equal to the interval calculated by the sink in step 2, which means that $(V_{0,N}^{p_{N,0}})^{q_{0,N}} = (V_{0,N}^{q_{0,N}})^{p_{N,0}}$, then the sink sends the key K_{CS} (used to commit the 200 bits in the second step to the node *N*).
Otherwise, the sink stops the authentication mechanism and rejects all the data coming from this sensor node, until its authentication succeed.
5) *Sensor node* $\rightarrow$ *sink*: E($K_{0,N}[ID_N$ ||DATA])
If the authentication of the node *N* is successfully done in step 4, the node receives the key commitment scheme K_{CS} from the sink, which will enable it to decrypt the interval value of $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$, and checks the authenticity of the sink. The node *N* encrypts thereafter the DATA and the ID_N and sends the message to the sink. Otherwise, the node *N* denies the sink *S* and sends no data.

VI. Security and efficiency Analysis

In this section we discuss the performance of our solution in term of security, communication and computational cost efficiency.

A. Security and Privacy Analysis

We present in the following, the attacks that can be countered by our solution.

Forge node: In this attack, the attacker acts as a legitimate node which can result in an additional consumption of energy, not only of the sink but of the entire network since the used communication is a multi-hop broadcast, leading after that an attacker to inject false data. In our solution, before sending the data, the node must be authenticated to the sink. If the challenge imposed by the sink is not successfully done by the node, the sink will ignore all data coming from the node.

Forge sink: In this attack, the attacker acts as a legitimate sink to collect the pertinent data coming from different nodes. As our authentication scheme is mutual, the node, must be sure of the identity of the sink before sending any data. In addition, the data sent by the nodes are encoded with a key shared only between the legitimate sink and the relevant node.

Replay attack: In this attack, the attacker tries to maliciously or fraudulently replay the $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$ interval values to make the sink thinks that it is one of the legitimate nodes in order to gain admission to the network, which can easily overrule the authentication mechanism. To prevent this attack, the sink commits the message and reveal the key later (i.e. commitment scheme principal). By that, we ensure not only the security of our network from this kind of attack, but also, we prevent the data injection attack that may result by making a successfully replay of the $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$ interval value.

Injection attack: As previously mentioned, this attack can be introduced after passing the replay attack. In this attack, the attacker will try to inject false data into the network. The main goal of this attack can be to circulate false information, to consume the resources of a node, or just saturate (overload) the network. It can also cause a bad decision that can have catastrophic consequences, especially when it comes to life or death of a human being.

Man in the Middle Attack: In this attack, the attacker tries to get in between the legitimate node and the sink. The main goal of this attack is to control the entire conversation in order to sniff and intercept messages. Then, he/she tries to recover the secret or gains access to sensitive information, and performs malicious activities. However, in our solution, no information about the secret is disclosed, also the data sent to the sink are encrypted and no information about the key is sent over the communication channel.

Guessing Attack: In this attack, the attacker tries to guess the key or the secret information by collecting several messages exchanged between the different nodes and the sink. Our proposed authentication protocol is effectively resisting to this attack, since there is no secret information transmitted in BANZKP scheme. Even if in our scheme the Commitment Scheme key (K_{CS}) is sent in plain text, this latter gets changed with every communication, and only 200 random interval from $(V_{0,N}^{p_{N,0}})^{q_{0,N}}$ is sent (this interval also gets changed with every communication) , thereby rendering the task of guessing shared values very difficult. Moreover, the nodes also generates a random values (p and q) with every communication. Consequently, these values are also randomly changed.

Attack on privacy: Privacy preservation of sensitive data in Body Area Networks is particularly a difficult challenge. One of the most common and easiest form of attack on data privacy is eavesdropping and passive monitoring. If the messages are not protected, the attacker can easily understand and guess the disease that the patient suffer from. In our solution the messages are protected by cryptographic mechanism.

B. Efficiency Analysis

In this subsection, we compare the communication and computational requirement of our protocol with respect to TinyZKP [16].

Communication cost Analysis: To better analyze our mutual authentication and data sending process, we present the communication cost of our authentication scheme that can be achieved by four messages exchange and evaluated as follows:
$2 * L(V^{p/q}) + 2 * L((V_{0,n}^{q_{0,n}})^{p_{n,0}}) + L(K_{CS})$ = 1300 bits. While for TinyZKP, the communication cost is at least: $L(M_{chall}) + L(ECDSA(M_{chall})) + L(SHA-1(X_m)) + L(Y_m)$ = 1710 bits. For W-ECDSA, the communication cost depends on the number of the selected secure nodes used to endorse the sender. During the implementation of W-ECDSA, we chose only 2 secure nodes and the communication cost is: $L(al_0||C_0) + 2 * L(z_n l_n R_0) + L(al_A||l_r) + L(K_{h2(VA)}(al_0||query))$ = 2182 bits.

Computational cost Analysis: Since in our solution the different keys are pre-distributed, the computational cost (in term of keys' generation) is hence equal to zero. According to the literature [4], to generate or verify an identity, *T*(k+2)/2* represents the needed average of the used modular multiplications in TinyZKP, where T is the number of times we recalculate the modular multiplication, and k is the number of times we calculate a modular multiplication. Therefore, the computational cost in TinyZKP is 1*(20+2)/2=11, which requires not only additional computational resources but also a large memory in each node, especially for the sink node, that should hold the different public keys of each node (i.e. 120 public key for a 6 node network). These public keys are only used to verify the identity of the sender, and not to encrypt the network data.

VII. Simulation settings and performance results

A. Simulation settings

We evaluate BANZKP, TinyZKP [16] and W-ECDSA [25] schemes by implementing them as an add-on to the convergecast routing protocol through the MiXiM project [9], that joins and extends several existing simulation frameworks developed for wireless and mobile simulations in Omnet++ [24]. For evaluation, we used the convergecast routing protocol provided by Omnet++, which works in two simple and generic phases. First, to establish the routes, the sink broadcasts a Route-Flood message to every node in the network. This message is used by each node to choose a parent towards the sink and build a collection tree. The metric to compare routes can be any additive metric and nodes only maintain a single path towards the sink that will be used in the data transmission phase. Nodes do not know each other and cannot communicate together directly. Our WBAN consists of 7 sensor nodes deployed in a compact spatial region. The sensor node that acts as the sink is the one deployed on the chest. The rest of the sensor nodes send a challenge/response messages with the sink until the approval of the identity of each one. The sensor nodes, considered in our simulation have the following characteristics: 2.4 GHZ, 3.3 V Voltage, and the current draw is 10 mAh.

The performance of our protocol in terms of execution time requirement, and energy and memory consumption are evaluated by simulation, and compared to the ones achieved by W-EXDSA and TinyZKP (which is to the best of our knowledge the only ZKP-based scheme defined for WBAN).

B. Performance results

1) Execution Time: In some sensing application (i.e. emergency Applications), execution time is extremely important, not only to achieve a maximum network lifetime, but also to insure a fast interception of medical staff. Thus, insure a tradeoff, between a secure collect of patient medical data and a response time delay, is of crucial issue. As shown in figure 2, BANZKP has the lowest execution time compared to TinyZKP and W-ECDSA, and runs 17 and 5 times faster, respectively while ensuring a resistance to a broad class of attacks detailed inVI.
This difference in execution time, can be explained by the use of modular multiplications in TinyZKP which are considered as the most consumers in term of computation. While in W-ECDSA, this difference is due to the number of verification of PKC, imposing the use of multiple secure nodes to endorse the sender before reaching its destination.

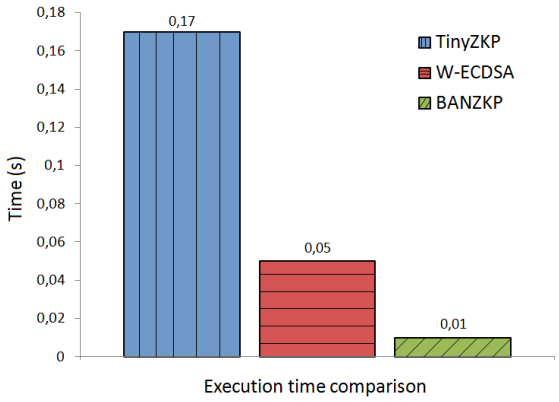

Figure 2: Execution time comparison

2) Energy Consumption: As shown in Figure 3. Our authentication scheme consumes less energy compared to TinyZKP and W-ECDSA, since in our proposed protocol we used the Commitment Scheme that requires 1000 times less computational resources than ECDSA [6], and hence induces a lower energy consumption. Additionally, in TinyZKP, the authors used a multiplicative modular operation to generate the public keys (used to obscure the shared secret between the node and the sink, and not to encrypt data), which also consumes energy, in contrast to our solution that obscure the shared secret, based on one of the hard to solve problem that constitutes the cryptography strength of ZKP, which is the infeasibility to computationally solve the discrete logarithms for hundreds of bits numbers. Furthermore, even if the number of data exchanges in TinyZKP is lower than in BANZKP, the communication cost has an important impact in terms of energy consumption and also in this case our proposed protocol consumes less energy than TinyZKP. Concerning W-ECDSA this difference can be simply explained by the additional energy consumed during the verification of the certificates on each intermediate secure node. And more the number of secure nodes increases, more the need in terms of energy is important.

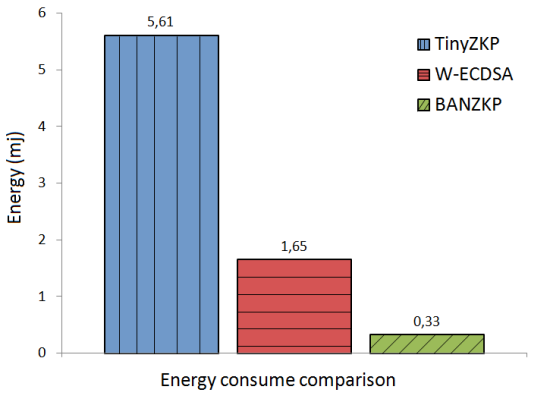

Figure 3: Energy consume comparison

3) Memory Consumption: The required memory of the TinyZKP, W-ECDSA and BANZKP authentication protocols is given in Figure4. BANZKP consumes 56.13% less memory than TinyZKP. Since in TinyZKP, a big number of keys must be held in each node (20 public key and 20 private keys), especially in the sink node that must hold 120 public keys (in case of 6 nodes), plus 6 session keys for the authentication phase and 6 other keys for the data transmission. Furthermore, the ECDSA and SHA-1 signature and verifications require additional memory resources. In contrast, our protocol uses a Commitment Scheme instead of ECDSA algorithm, and makes an efficient and simple comparison to verify the identity of the second party. Additionally, the number of keys used in our protocol is much lower than in TinyZKP.

Figure4 shows also that there is a minor difference between W-ECDSA and our proposed scheme and this difference is of 4.77%, which can be explained by the fact that the W-ECDSA requires little handling compared to TinyZKP and BANZKP since all necessary parameters are pre-computed by the certification authority and pre-loaded before deployment. BANZKP does not need this expensive precomputing phase which makes it interesting for scalable and reconfigurable systems.

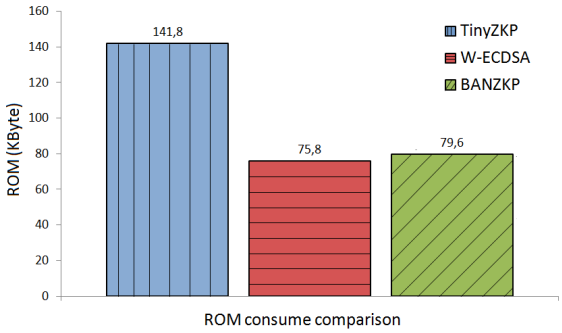

Figure 4: Memory Consumption

VIII. Conclusions

In this paper we have proposed and analyzed the efficiency of a new lightweight authentication scheme for WBAN, BANZKP. Our scheme allows two nodes to make sure about the identity of each other, and hence establish a trust relationship among the WBAN sensors. The main goal of the proposed scheme is to protect the subsequent wireless multi-hop communication, throughout a low computational and memory requirement. We implemented the three authentication scheme BANZKP, TinyZKP [16] (to the best of our knowledge the only ZKP scheme defined for WBAN) and W-ECDSA [25], as an add-on to the convergecast routing protocol, through the MiXiM project, using the Omnet++ simulator. Then, we evaluated them in terms of security and privacy, as well as in terms of efficiency. The analysis shows that our protocol effectively resists to a variety of security and privacy attacks, such as the replay and data injection attacks. Simulation results prove that our authentication scheme BANZKP requires 56% less memory compared to TinyZKP [16], is the most efficient in execution time and runs 17 and 5 times faster, and uses 94.11% and 80% less energy compared to TinyZKP and W-ECDSA, respectively.

References

[1] Tractica.com. *More than 78 Million Consumers Will Utilize Home Health Technologies by 2020* — tractica. [online] available at: https://www.tractica.com/newsroom/press-releases/more-than-78-million-consumers-will-utilize-home-health-technologies-by-2020. 2015.

[2] W. Badreddine, C. Chaudet, F. Petruzzi, and M. Potop-Butucaru. Broadcast strategies in wireless body area networks. In *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM 2015*, pages 83–90. ACM, 2015.

[3] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47. ACM, 2002.

[4] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in CryptologyCRYPTO86*, pages 186–194. Springer, 1987.

[5] 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.

[6] 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.

[7] S. S. Javadi and M. Razzaque. Security and privacy in wireless body area networks for health care applications. In *Wireless Networks and Security*, pages 165–187. Springer, 2013.

[8] 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.

[9] 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, 2008.

[10] R. Kumar and R. Mukesh. State of the art: Security in wireless body area networks. *International Journal of Computer Science & Engineering Technology (IJCSET) Vol*, 4:622–630, 2013.

[11] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *Wireless Communications, IEEE*, 17(1):51–58, 2010.

[12] 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.

[13] 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.

[14] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang. Exploiting prediction to enable secure and reliable routing in wireless body area networks. In *INFOCOM, 2012 Proceedings IEEE*, pages 388–396. IEEE, 2012.

[15] 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.

[16] 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.

[17] J.-i. Naganawa, K. Wangchuk, M. Kim, T. Aoyagi, and J.-i. Takada. Simulation-based scenario-specific channel modeling for wban cooperative transmission schemes. *IEEE Journal of Biomedical and Health Informatics*, PP(99), May 2014.

[18] 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.

[19] 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.

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

[21] A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57, 2004.

[22] 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.

[23] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak. A comprehensive survey of wireless body area networks. *Journal of medical systems*, 36(3):1065–1094, 2012.

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

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

[26] 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.

[27] 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.* IEEE, 2009.

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

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