# Highly Efficient Privacy-Preserving Key Agreement for Wireless Body Area Networks

Haibat Khan, Benjamin Dowling, Keith M. Martin
Information Security Group
Royal Holloway, University of London

***Abstract*—In 2012, the IEEE introduced IEEE Std 802.15.6 as the communication standard for Wireless Body Area Networks (WBANs). All key agreement protocols offered by this standard have been shown to exhibit grave security weaknesses. However, to date, no key agreement protocol has been proposed which fulfills all the requisite security and privacy objectives for deployment in a resource constrained WBAN environment. In this paper, based upon symmetric cryptographic primitives only, a key agreement protocol is presented which, in addition to good performance also offers the desirable privacy attributes of *node anonymity* and *session unlinkability*. The protocol is also suitable for post-quantum deployment scenarios as it is independent of any public key based operations.**

***Index Terms*—Anonymity, authenticated key agreement, energy-efficiency, forward-secrecy, unlinkability.**

## I. Introduction

Wireless Body Area Networks (WBANs) consist of miniaturized computing devices which can be fitted inside or around the human body [1]. Through use of short range communication technologies, these devices talk to a designated centralized node (Hub) which further communicates with external networks via a Gateway [2]. The general layout of a typical WBAN is illustrated in Fig 1. Mindful of the peculiarities of communicating in and around the human body, the IEEE published IEEE Std 802.15.6 [3] for WBAN communications in 2012. As high power transmissions are harmful to humans and nodes in a WBAN are energy constrained, this standard provisioned an optional two-hop communication architecture to enable resource-constrained nodes to minimize transmissions when communicating with the Hub.

In addition to conventional security guarantees, privacy is of utmost importance for typical target application areas such as healthcare and the military [4]. The session key agreement methods of IEEE Std 802.15.6 have been shown to have security weaknesses [5], but also do not provide the privacy features that should be expected of a WBAN [6]. In this paper, we present a key agreement protocol which renders comprehensive range of security and privacy properties considered essential [6] for WBANs.

The remainder of this paper is organized as follows. Section II discusses requisite security and privacy attributes of a key agreement protocol for WBANs. Section III, provides an overview and analysis of a WBAN key agreement scheme proposed in [7]. The new protocol is detailed in Section IV. Section V provides analysis of the proposed protocol while Section VI provides future research directions and concludes the paper.

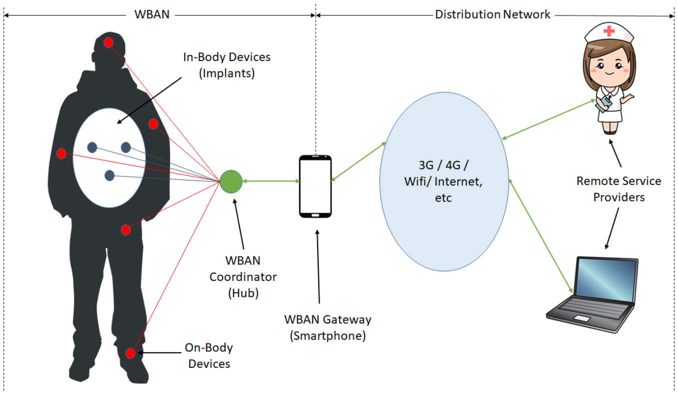


Fig. 1: Generic architecture of a typical WBAN

## II. Setting the Scene

In this section we present a network and adversary model for WBAN key agreement and elaborate upon the desired security, privacy and functional objectives.

### A. System Model

We begin by describing a system model suitable for the deployment scenarios of WBANs. In this model, a System Administrator ($SA$) initializes the network. The network is composed of three types of nodes; a Hub Node ($HN$), Intermediary Nodes ($IN$) and Normal Nodes ($N$). As the $HN$ is usually a resourceful device with better hardware protection mechanisms in place, we assume it to be trusted and its secret *Master Key* to be protected. Normal nodes $N$ are resource constrained and their transmission range is assumed to be limited; in particular, they are not always able to communicate directly with $HN$. Intermediary nodes $IN$ are also located in and around the body but, at a particular time instance, are in direct communication with both $N$ and $HN$, thus acting as intermediary nodes for the purpose of relaying traffic between $HN$ and $N$ when required.

### B. Objectives

The security of traffic in IEEE Std 802.15.6 is protected using authenticated encryption, which requires the establishment of symmetric session keys. The procedure for agreeing these keys is thus critical to the overall security and privacy of a WBAN. Keeping the previously defined model in mind, a *Privacy-Preserving Key Agreement (PPKA)* protocol, to be executed between a node $N$ and $HN$, should have the following properties:

*1) Security Properties:*

**Mutual Entity Authentication** [8] between $N$ and $HN$.

**Mutual "Implicit" Key Authentication** [8] between $N$ and $HN$.

**Known Key Security**, meaning that compromising a session key in one session should not impose any threat to the session key security in any other sessions.

**Key Randomness**, meaning that any successful key agreement should output a uniformly distributed session key amongst the set of all possible session keys [9].

**Replay Prevention**. An adversary should not be able to successfully replay previously captured copies of legitimate messages between the protocol participants.

**Desynchronization Resistance.** If the authentication parameters get updated during the protocol execution, then usually the participants need to have the same updated values at the end of a protocol run. Otherwise, they will not authenticate each other in later sessions and we say they have been desynchronized. In a desynchronization attack, the adversary forces the protocol participants to update their authentication parameters to different values. A PPKA needs to be resistant to these types of attacks.

*2) Privacy Properties:* We focus on two privacy aspects:

**Node Anonymity.** An adversary $\mathcal{A}$, who is observing all communications, should not be able to learn the identity of any node $N$ who is participating in a PPKA protocol with $HN$. The privacy attribute of anonymity is a necessity for typical application scenarios of WBANs, like healthcare and military.

**Session Unlinkability.** An adversary $\mathcal{A}$ , who is observing communications, should not be able to link one successfully executed PPKA session of node $N$ to another successfully completed session of the same node. Session unlinkability is imperative in addition to anonymity. Although, the PPKA sessions could be anonymous, if the adversary is able to link various PPKA sessions and group them together then $\mathcal{A}$ would be able to attribute a group to a particular node with high probability, due to his knowledge of the operations of the WBAN. For example, consider a medical WBAN in which a pacemaker is supposed to communicate with the remote healthcare providers every five minutes, while the body temperature sensor communicates only three times per day.

*3) Functional Requirements:*

**Support for Multi-Hop Communication.** As discussed in Section I, depending upon the network topology, nodes would either be communicating directly with the Hub Node $HN$ or via an Intermediary Node $IN$. Therefore, the PPKA protocol should be designed to be suitable for both single-hop and two-hop communication modes of [3].

**Energy Consumption.** As nodes in WBAN are severely energy constrained, the PPKA protocol needs to be minimalistic in terms of computation, communication and storage overhead. Energy consumption in WBANs is dominated by radio communications [10], which mainly depends on the number of bits to be transmitted within the network. Consequently, the PPKA protocol should be designed such that the number of bits to be exchanged between the protocol participants and the computational overhead for nodes $N$ should be minimal.

TABLE I: Notations used in [7]

| Symbol | Description |
|---|---|
| $h(.)$ | Cryptographic hash function |
| $(a, b)$ | Concatenation of $a$ and $b$ |
| $\oplus$ | Bitwise XOR operation $k$ |
| $SA$ | System Administrator |
| $N$ | Normal Node |
| $HN$ | Hub Node |
| $IN$ | Intermediary Node |
| $id_N$ | Long term secret/identity of node $N$ |
| $id'_{IN}$ | Relay identity of node $IN$ |
| $tid_N$ | Temporary identity of node $N$ |
| $k_{HN}$ | Master secret key of $HN$ |
| $k_N, f_N$ | Temporary secret parameters chosen by $HN$ |
| $r_N$ | Temporary secret parameter chosen by $N$ |
| $a_N, b_N$ | Authentication parameters stored in $N$ |
| $x_N, y_N$ | Auxiliary authentication parameters |
| $\alpha, \beta, \gamma, \eta, \mu$ | Authentication parameters computed by $HN$ |
| $k_S$ | Shared session key |
| $t_N$ | Timestamp generated by node $N$ |
| $X \rightarrow Y : Z$ | Entity $X$ sends message $Z$ to entity $Y$ |

**Stateless $HN$.** The network topology in WBANs is dynamic, some nodes go in to "sleep mode" for energy conservation purposes while others may be removed from the system upon completion of their useful life. However, the $HN$ is the consistent nucleus of the network, its non-accessibility to other nodes potentially devastating on the overall functionality of the WBAN. After the network initialization we can not expect it to remain inaccessible to the network, even temporarily, for maintenance activities i.e. updation of security parameters, updation of list of nodes in the network, etc. Consequently, an important functional requirement is that $HN$ should be independent of the network dynamism and ideally no states about the network nodes need to be maintained by it.

## C. Related Work

Toorani [5] discovered various security weaknesses in the key agreement methods of IEEE Std 802.15.6. Wang and Zhang [11] proposed a key agreement scheme for WBANs that claimed to provide anonymity and unlinkability in addition to the requisite security guarantees. However, Jiang et al. [12] demonstrated that [11] is vulnerable to client impersonation attack and thus lacks mutual authentication. They proposed an authenticated key agreement scheme which rectified this flaw. However, their scheme was based on computing bilinear pairings; which is not suitable for deployment in resource-constrained WBANs. To avoid the overhead of managing public-key certificates, He et al. proposed a certificateless authentication scheme [13], which provides anonymity and unlinkability. However, the computation and communication overheads associated with their scheme also render it un-

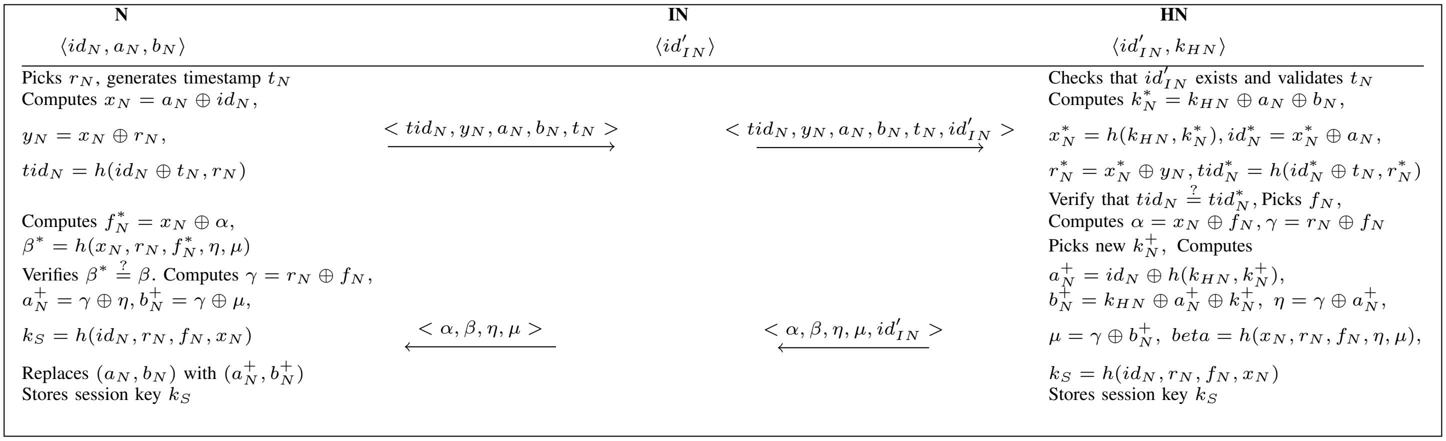

N
IN
HN
$\langle id_N, a_N, b_N \rangle$
$\langle id'_{IN} \rangle$
$\langle id'_{IN}, k_{HN} \rangle$
Picks $r_N$, generates timestamp $t_N$
Computes $x_N = a_N \oplus id_N$,
$y_N = x_N \oplus r_N$,
$tid_N = h(id_N \oplus t_N, r_N)$
$< tid_N, y_N, a_N, b_N, t_N >$
$< tid_N, y_N, a_N, b_N, t_N, id'_{IN} >$
Checks that $id'_{IN}$ exists and validates $t_N$
Computes $k^*_N = k_{HN} \oplus a_N \oplus b_N$,
$x^*_N = h(k_{HN}, k^*_N), id^*_N = x^*_N \oplus a_N$,
$r^*_N = x^*_N \oplus y_N, tid^*_N = h(id^*_N \oplus t_N, r^*_N)$
Verify that $tid_N \overset{?}{=} tid^*_N$, Picks $f_N$,
Computes $\alpha = x_N \oplus f_N, \gamma = r_N \oplus f_N$
Picks new $k^+_N$, Computes
$a^+_N = id_N \oplus h(k_{HN}, k^+_N)$,
$b^+_N = k_{HN} \oplus a^+_N \oplus k^+_N,\ \eta = \gamma \oplus a^+_N$,
$\mu = \gamma \oplus b^+_N,\ beta = h(x_N, r_N, f_N, \eta, \mu)$,
$k_S = h(id_N, r_N, f_N, x_N)$
Stores session key $k_S$
$< \alpha, \beta, \eta, \mu, id'_{IN} >$
$< \alpha, \beta, \eta, \mu >$
Computes $f^*_N = x_N \oplus \alpha$,
$\beta^* = h(x_N, r_N, f^*_N, \eta, \mu)$
Verifies $\beta^* \overset{?}{=} \beta$. Computes $\gamma = r_N \oplus f_N$,
$a^+_N = \gamma \oplus \eta, b^+_N = \gamma \oplus \mu$,
$k_S = h(id_N, r_N, f_N, x_N)$
Replaces $(a_N, b_N)$ with $(a^+_N, b^+_N)$
Stores session key $k_S$

Fig. 2: Li et al.'s Protocol

suitable for WBAN deployment. Very recently, Li et al. [7] presented an authenticated key agreement scheme suitable for WBANs based only upon symmetric cryptographic primitives. This is an attractive proposal, since there is no requirement of any additional infrastructure, and the associated computation and communication overheads are negligible. The authors claim that this scheme achieves almost all of the security and privacy objectives defined in Section II-B.

### D. Our Contributions

The contributions of this paper are as below:

- We analyse the scheme described in [7] which shows that the proposed scheme does not provide session unlinkability and forward secrecy. We further highlight additional flaws in this scheme, which hinder its functionality.
- We propose a key agreement protocol that improve upon [7] and provisions requisite security and privacy properties, while preserving the efficiency offered by the original scheme.

## III. Li et al.'s Scheme

In this section we present an overview and analysis of Li et al.'s scheme [7]. For ease of comparison we use the same notation (details in Table I) as in [7].

### A. The Key Agreement Protocol

Li et al.'s PPKA protocol between the Hub node $(HN)$ and a node $(N)$ consists of three phases. For a pictorial overview of the protocol the reader is referred to Fig. 2.

*1) Initialization Phase:* The $(SA)$ generates a master secret key $k_{HN}$ and stores it in $HN$.

*2) Registration Phase:* The $SA$ generates a unique secret identity $id_N$ for node $N$. It then randomly chooses the temporary secret parameter $k_N$ and calculates $a_N = id_N \oplus h(k_{HN}, k_N)$ and $b_N = k_{HN} \oplus a_N \oplus k_N$. A unique $id'_{IN}$ for the intermediary node $(IN)$ is chosen and the parameters $\langle id_N, a_N, b_N \rangle$ and $\langle id'_{IN}, id_N, a_N, b_N \rangle$ are stored in $N$ and $IN$ respectively, while $id'_{IN}$ is stored by $HN$ as the identity of $IN$ when communicating in relay mode.

*3) Authentication Phase:* We can think of the authentication phase of Li et al.'s scheme as a two-pass protocol. The individual steps are outlined below:

**Step 1:** $N \rightarrow IN : \langle tid_N, y_N, a_N, b_N, t_N \rangle$. $N$ picks a random $r_N$ and creates timestamp $t_N$. Then it computes $x_N = a_N \oplus id_N$, $y_N = x_N \oplus r_N$ and $tid_N = h(id_N \oplus t_N, r_N)$ and forwards the tuple $\langle tid_N, y_N, a_N, b_N, t_N \rangle$ to $IN$.

**Step 2:** $IN \rightarrow HN : \langle tid_N, y_N, a_N, b_N, t_N, id'_{IN} \rangle$. $IN$ adds its relay identity $id'_{IN}$ to the tuple and forwards it to $HN$.

**Step 3:** $HN \rightarrow IN : \langle \alpha, \beta, \eta, \mu, id'_{IN} \rangle$. After receiving the parameters from $IN$, $HN$ verifies the relay identity $id'_{IN}$ from its database and substantiates the validity of the timestamp $t_N$. Upon success of these checks, it computes $k^*_N = k_{HN} \oplus a_N \oplus b_N,\ x^*_N = h(k_{HN}, k^*_N),\ id^*_N = x^*_N \oplus a_N,\ r^*_N = x^*_N \oplus y_N$ and $tid^*_N = h(id^*_N \oplus t_N, r^*_N)$. It then verifies whether $tid_N \overset{?}{=} tid^*_N$. Then, a random $f_N$ is chosen and $\alpha = x_N \oplus f_N$ and $\gamma = r_N \oplus f_N$ are computed. Then a new $k^+_N$ is picked and $a^+_N = id_N \oplus h(k_{HN}, k^+_N),\ b^+_N = k_{HN} \oplus a^+_N \oplus k^+_N,\ \eta = \gamma \oplus a^+_N,\ \mu = \gamma \oplus b^+_N,\ \beta = h(x_N, r_N, f_N, \eta, \mu)$ are computed. The shared session key is computed as $k_S = h(id_N, r_N, f_N, x_N)$ and is stored in memory. Finally, $HN$ forwards the tuple $\langle \alpha, \beta, \eta, \mu, id'_{IN} \rangle$ to $IN$.

**Step 4:** $IN \rightarrow N : \langle \alpha, \beta, \eta, \mu \rangle$. $IN$ removes the relay identity $id'_{IN}$ from the received tuple and forwards $\langle \alpha, \beta, \eta, \mu \rangle$ to $N$.

**Step 5:** Upon receipt of the response from $IN$, $N$ computes $f^*_N = x_N \oplus \alpha$ and $\beta^* = h(x_N, r_N, f^*_N, \eta, \mu)$ and verifies that $\beta^* \overset{?}{=} \beta$. If true, $N$ computes $\gamma = r_N \oplus f_N$, $a^+_N = \gamma \oplus \eta$ and $b^+_N = \gamma \oplus \mu$. The shared session key $k_S$ is computed as $h(id_N, r_N, f_N, x_N)$ and the authentication parameters $(a_N, b_N)$ are replaced with $(a^+_N, b^+_N)$.

### B. Analysis of the Li et al.'s Scheme

*1) Security Analysis:* In addition to provisioning of mutual "direct" authentication [14], Li et al.'s scheme fulfills all the security criteria as defined in Section II-B. Moreover, the scheme also protects the master secret $(k_{HN})$ in the event of compromise of various nodes of the WBAN. For sake of brevity, we will restrict our security analysis to highlight only the vulnerabilities of Li et al.'s scheme.

**Discussion about Forward Secrecy.** Li et al. claimed a forward security property of their scheme. Their definition of forward secrecy varies from the generally accepted one. According to Li et al. the goal of forward secrecy is to protect other (past / future) session keys in the event of compromise of the current session key $k_S$. However, the conventional definition of forward secrecy states that in the event of compromise of the long term secrets of the protocol participant(s), an adversary should not be able to obtain any of the past session keys [15]. While Li et al.'s scheme is forward secure according to their own definition, it is not forward secure in a conventional sense.

*2) Privacy Analysis:*

**The Anonymity Dilemma.** It is known apriori to the attacker that all nodes ultimately communicate with $HN$. As the node identifier $id_N$ is always masked (by taking an XOR of it with a fresh random value) in Li et al.'s protocol, *anonymity* in Li et al.'s protocol is preserved from "direct" privacy attacks. However, now consider the situation depicted in Fig. 3, where an intermediary node $IN$ is providing the relaying service to various nodes $N$. In the second pass of Li et al.'s scheme, it is not clear how the intermediary node $IN$ would be able to identify the original node $N$ out of the "anonymity set" [16] for onward forwarding of the tuple $\langle \alpha, \beta, \eta, \mu \rangle$ received from $HN$. One naive way to resolve this is to allow $IN$ to broadcast the second pass of protocol for all nodes. However, this approach is unsuitable for already energy-constrained WBAN nodes as they will need to perform additional communication (radio reception) and computational steps for each and every transmission. This is a privacy dilemma from which Li et al.'s scheme suffers.

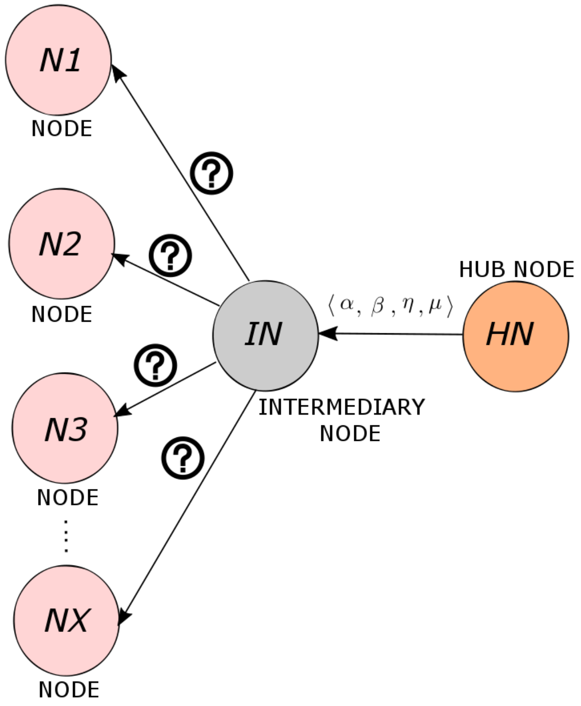


Fig. 3: The privacy dilemma of Li et al.'s scheme

**Session Unlinkability.** While Li et al. claim their scheme provides session unlinkability, we show this to be untrue. We highlight a weakness in Li et al.'s key agreement protocol, which allows a passive attacker to easily link two or more sessions of the same node $N$. The attack proceeds as follows:

Session # 1. Suppose that a run of Li et al.'s key agreement protocol is carried out between node $N$ and $HN$. A passive attacker $\mathcal{A}$ observes the contents of the messages being exchanged. From Step 1 of Section III-A3, $\mathcal{A}$ records the value $y_N = x_N \oplus r_N$. Then, from Step 3 of Sec III-A3, $\mathcal{A}$ records $\alpha = x_N \oplus f_N$. Now, $\mathcal{A}$ obtains the value $\gamma = r_N \oplus f_N = \alpha \oplus y_N$. Further, $\mathcal{A}$ records the values $\eta$ and $\mu$ from Step 3 of Section III-A3 and uses $\gamma$ to compute:

$$a_N^+ = \gamma \oplus \eta; \quad b_N^+ = \gamma \oplus \mu.$$

Session # 2. Now, $\mathcal{A}$ observes key exchange protocol sessions between various nodes and $HN$. $\mathcal{A}$ compares the values of the parameters $a_N$ and $b_N$ from Step 1 of the protocol with the saved values of $a_N^+$ and $b_N^+$. When $\mathcal{A}$ finds a match, $\mathcal{A}$ concludes with almost certainty that another key exchange session has been initiated by the same node $N$. This is correct because node $N$ uses the updated authentication parameters $a_N^+$ and $b_N^+$ in its next run of the protocol. In this way, $\mathcal{A}$ can track and link sessions of node $N$, demonstrating that Li et al.'s scheme does not achieve session unlinkability.

*3) Functional Requirements:* Li et al.'s scheme can be easily adapted for direct communication between $N$ and $HN$ without the involvement of $IN$. Since this scheme employs only symmetric cryptographic primitives, it is extremely efficient from a computation, communication and storage overhead perspective and there is no requirement of any additional network infrastructure. Assuming a hash function with a digest length of $B$ bits and 16 bit intermediary node IDs (i.e. $id'_{IN}$); Table II highlights the communication, computation and storage overhead of Li et al.'s scheme. In this table, $h$ denotes one hash operation, $\oplus$ denotes an XOR operation and $m$ denotes the number of intermediary nodes in the WBAN. Note that, contrary to the assumption made by Li et al. in Section 5.4 [7] about the arbitrary length of the timestamp field, it is implicitly the same length as of the hash function digest because, as described earlier in Section III-A3, $tid_N = h(id_N \oplus t_N, r_N)$. This is not commensurate with the length of the timestamp field as defined in IEEE Std 802.15.6, which is three octets or 24 bits. Regarding state maintenance by $HN$, in case of [7], $HN$ needs to maintain states concerning the relay nodes $IN$, which is an undesirable feature as already explained earlier in Section II-B.

## IV. Our PPKA Protocol

In this section we propose a PPKA protocol which rectify the problems highlighted in Section III-B. While devising this protocol, we have tried to preserve the original elegance, simplicity and efficiency of the scheme in [7]. The protocol

TABLE II: Overheads associated with Li et al.'s scheme

| Index | Node $N$ | Hub Node $HN$ |
|---|---|---|
| Computation Overhead | $3h + 7\oplus$ | $5h + 12\oplus$ |
| Communication Overhead | $5B$ bits | $4B + 16$ bits |
| Storage Overhead | $3B$ bits | $(B + 16m)$ bits |

TABLE III: Detail of additional symbols

| Symbol | Description |
|---|---|
| $id'_N$ | Session identity chosen randomly by $N$ |
| $\mathsf{Enc}(k, m)$ | Encryption of message $m$ under symmetric key $k$ |
| $\mathsf{Dec}(k, c)$ | Decryption of ciphertext $c$ under symmetric key $k$ |

addresses the privacy flaws present in Li et al.'s scheme. Detail of additional symbols used in our PPKA protocols is given in Table III.The phases of our PPKA Protocol are described as follows:

*1) Initialization Phase:* Same as [7].

*2) Registration Phase:* The intermediary node $(IN)$ is not provided with a relay identity $id'_{IN}$. Parameters $\langle id_N, a_N, b_N\rangle$ get stored in $N$.

*3) Authentication Phase:* The various steps of the authentication phase are depicted in Fig. 4 and are as follows:

**Step 1:** $N \rightarrow IN : \langle tid_N, y_N, a_N, b_N, t_N, id'_N\rangle$. $N$ picks a random $r_N$ and creates timestamp $t_N$. It then computes $x_N = a_N \oplus id_N$, $y_N = x_N \oplus r_N$. It further picks a random pseudonym $id'_N$ to be used as a temporary identifier for this session only, and calculates $tid_N = h(id_N, id'_N, t_N, r_N)$ and sets the "Relay Field" of the underlying "MAC Header" to value 1, according to sub-clause 6.10 of [3].

**Step 2:** $IN \rightarrow HN : \langle tid_N, y_N, a_N, b_N, t_N, id'_N\rangle$. $IN$ checks the value of "Relay Field" and forwards the tuple to $HN$.

**Step 3:** $HN \rightarrow IN : \langle \alpha, \beta, \eta, \mu, id'_N\rangle$. After receipt of the tuple from $IN$, $HN$ verifies the validity of the timestamp $t_N$. Upon success of this check, it computes $k^*_N = k_{HN} \oplus a_N \oplus b_N$, $x^*_N = h(k_{HN}, k^*_N)$, $id^*_N = x^*_N \oplus a_N$, $r^*_N = x^*_N \oplus y_N$ and $tid^*_N = h(id^*_N, id'_N, t_N, r^*_N)$. It then verifies whether $tid_N \overset{?}{=} tid^*_N$. Then, a random $f_N$ is chosen and $\alpha = x_N \oplus f_N$, $\gamma = r_N \oplus f_N \oplus h(id_N, t_N)$ and $\gamma' = r_N \oplus f_N \oplus h(id_N, t_N, r_N, id'_N)$ are computed. Then a new $k^+_N$ is picked and $a^+_N = id_N \oplus h(k_{HN}, k^+_N)$, $b^+_N = k_{HN} \oplus a^+_N \oplus k^+_N$, $\eta = \gamma \oplus a^+_N$, $\mu = \gamma' \oplus b^+_N$, $\beta = h(x_N, r_N, f_N, \eta, \mu, id'_N)$ are computed. Finally, the shared session key $k_S = h(id_N, r_N, f_N, x_N)$ is computed and stored in memory, and the value of the underlying "Relay Field" is set to 1.

**Step 4:** $IN \rightarrow N : \langle \alpha, \beta, \eta, \mu, id'_N\rangle$. $IN$ checks the "Relay Field" of the message received from the Hub node. If "Relay Field" value is set to 1, then it notes the identifier $id'_N$ received in the tuple for onward forwarding of the tuple to node $N$.

**Step 5:** Upon receiving a response from $IN$, $N$ computes $f^*_N = x_N \oplus \alpha$ and $\beta^* = h(x_N, r_N, f^*_N, \eta, \mu, id'_N)$ and verifies that $\beta^* \overset{?}{=} \beta$. If so, $N$ computes $\gamma = r_N \oplus f_N \oplus h(id_N, t_N)$, $\gamma' = r_N \oplus f_N \oplus h(id_N, t_N, r_N, id'_N)$, $a^+_N = \gamma \oplus \eta$ and $b^+_N = \gamma' \oplus \mu$. The shared session key $k_S$ is computed as $h(id_N, r_N, f_N, x_N)$, and the authentication parameters $(a_N, b_N)$ are updated by being replaced with $(a^+_N, b^+_N)$.

TABLE IV: Overheads associated with PPKA Protocol

| Index | Node $N$ | Hub Node $HN$ |
|---|---|---|
| Computation Overhead | $5h + 9\oplus$ | $7h + 14\oplus$ |
| Communication Overhead | $5B + 16$ bits | $4B + 16$ bits |
| Storage Overhead | $3B$ bits | $B$ bits |

## V. Analysis of the proposed PPKA Protocol

### *A. Security and Privacy Analysis*

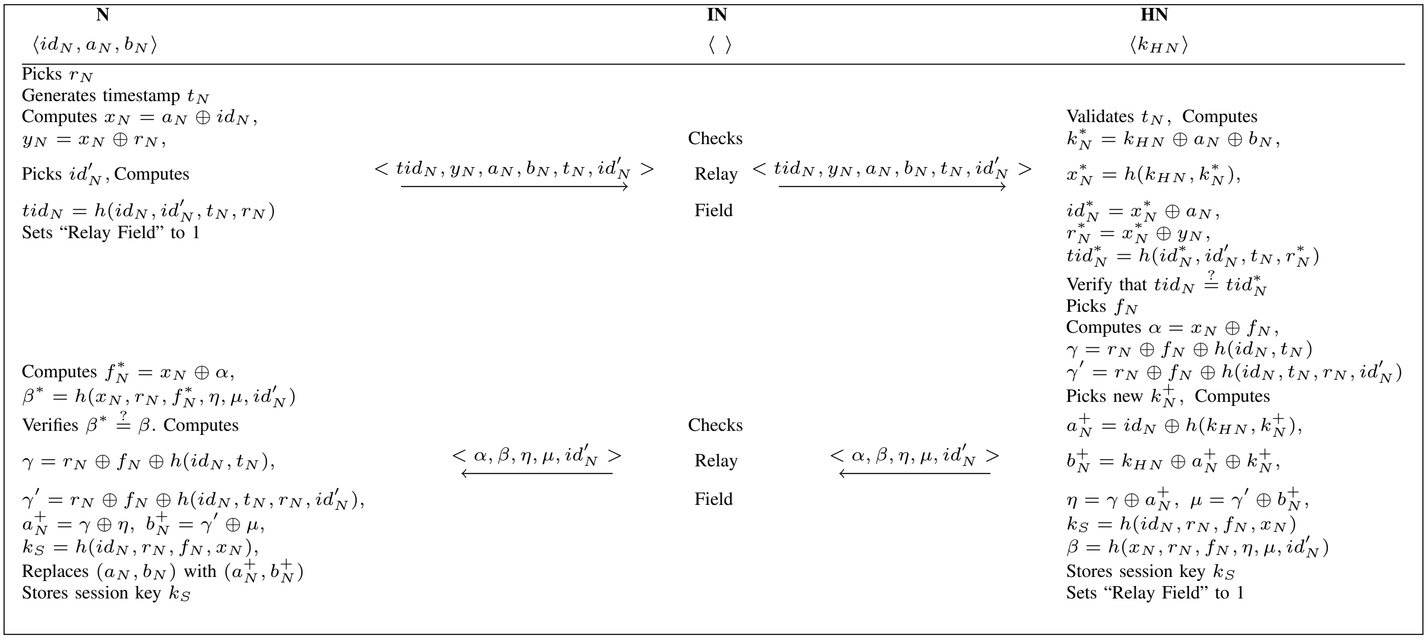
Our PPKA protocol preserves all the security properties offered by Li et al's scheme as all the measures ensuring various security attributes in [7] remain intact in our PPKA proposal too. Moreover, the protocol also achieves the anonymity objective of keeping the long term identity $id_N$ of the node $N$ secret. The PPKA protocol resolves the privacy dilemma (See Section III-B2) of [7] through the use of pseudonym $id'_N$. The inclusion of this pseudonym in all messages enables an intermediary node $IN$ to identify its communicating peers for that particular run of the protocol. Also, as these pseudonyms are changed in every other run of the protocol, the anonymity of node $N$ is preserved. In Li et al's scheme, an adversary was able to link two sessions to the same node $N$ because of the unmasking of the updated authentication parameters $(a^+_N, b^+_N)$ which in turn was due to the adversary being capable of calculating the mask $\gamma$, as explained in Section III-B2. However in our PPKA protocol, due to the inclusion of the additional masking parameters $h(id_N, t_N)$ and $h(id_N, t_N, r_N, id'_N)$ , the adversary is now unable to unmask the updated authentication parameters $(a^+_N, b^+_N)$. Therefore, the modified schemes provide the desirable privacy attribute of session unlinkability.

### *B. Functional Requirements*

The proposed PPKA protocol can be easily adapted for direct communication between $N$ and $HN$ by removal of Steps 2 and 4 out of the *Authentication Phase*. As our PPKA protocol is also based on symmetric cryptographic primitives, it preserves the efficiency of the original scheme from a computation, communication and storage perspective without the aid of any additional network infrastructure. Moreover, in our protocol the timestamp field can be of any arbitrary length to suit the underlying protocol layers unlike [7]. Assuming a $B$ bit hash digest and 16 bit pseudo identity $id'_N$ for node $N$, Table IV depicts the various overheads associated with PPKA Protocol. In this table, $h$ denotes an instance of a hash operation and $\oplus$ denotes an XOR operation. From a computational perspective, single instances of hash operation and encryption operation have been considered equal [17].

## VI. Conclusion and Future Research Directions

We proposed an authenticated key agreement protocol suitable for WBANs. The protocol is based upon symmetric cryptographic components only and thus is highly efficient



**N**

$\langle id_N, a_N, b_N \rangle$

Picks $r_N$
Generates timestamp $t_N$
Computes $x_N = a_N \oplus id_N$,
$y_N = x_N \oplus r_N$,
Picks $id'_N$, Computes
$tid_N = h(id_N, id'_N, t_N, r_N)$
Sets "Relay Field" to 1

$\xrightarrow{< tid_N, y_N, a_N, b_N, t_N, id'_N >}$

**IN**

$\langle \ \rangle$

Checks
Relay
Field

$\xrightarrow{< tid_N, y_N, a_N, b_N, t_N, id'_N >}$

**HN**

$\langle k_{HN} \rangle$

Validates $t_N$, Computes
$k^*_N = k_{HN} \oplus a_N \oplus b_N$,
$x^*_N = h(k_{HN}, k^*_N)$,
$id^*_N = x^*_N \oplus a_N$,
$r^*_N = x^*_N \oplus y_N$,
$tid^*_N = h(id^*_N, id'_N, t_N, r^*_N)$
Verify that $tid_N \overset{?}{=} tid^*_N$
Picks $f_N$
Computes $\alpha = x_N \oplus f_N$,
$\gamma = r_N \oplus f_N \oplus h(id_N, t_N)$
$\gamma' = r_N \oplus f_N \oplus h(id_N, t_N, r_N, id'_N)$
Picks new $k^+_N$, Computes
$a^+_N = id_N \oplus h(k_{HN}, k^+_N)$,
$b^+_N = k_{HN} \oplus a^+_N \oplus k^+_N$,
$\eta = \gamma \oplus a^+_N$, $\mu = \gamma' \oplus b^+_N$,
$k_S = h(id_N, r_N, f_N, x_N)$
$\beta = h(x_N, r_N, f_N, \eta, \mu, id'_N)$
Stores session key $k_S$
Sets "Relay Field" to 1

$\xleftarrow{< \alpha, \beta, \eta, \mu, id'_N >}$

Checks
Relay
Field

$\xleftarrow{< \alpha, \beta, \eta, \mu, id'_N >}$

Computes $f^*_N = x_N \oplus \alpha$,
$\beta^* = h(x_N, r_N, f^*_N, \eta, \mu, id'_N)$
Verifies $\beta^* \overset{?}{=} \beta$. Computes
$\gamma = r_N \oplus f_N \oplus h(id_N, t_N)$,
$\gamma' = r_N \oplus f_N \oplus h(id_N, t_N, r_N, id'_N)$,
$a^+_N = \gamma \oplus \eta$, $b^+_N = \gamma' \oplus \mu$,
$k_S = h(id_N, r_N, f_N, x_N)$,
Replaces $(a_N, b_N)$ with $(a^+_N, b^+_N)$
Stores session key $k_S$

Fig. 4: PPKA Protocol

and avoids the additional burden of deploying and managing an associated public key infrastructure. In fact, our protocol is suitable for every application scenario where efficiency is of essence and the network can be initialized by a *System Administrator*. In addition to the requisite security guarantees, the proposed protocol also offers appropriate privacy attributes suitable for a wide variety of application scenarios. The proposed protocol emerges as an attractive alternate for the current key exchange methods described in the IEEE 802.15.6 standard, which are based upon legacy public key based primitives and do not offer any privacy features. It would be interesting to investigate whether future research can yield a scheme which would be based on symmetric primitives and still offers forward secrecy and KCI resilience.

## References

[1] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1635–1657, 2014.

[2] S. Movassaghi, M. Abolhasan, J. Lipman, D. B. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[3] "IEEE Standard for Local and Metropolitan Area Networks - Part 15.6: Wireless Body Area Networks," *IEEE Std 802.15.6-2012*, pp. 1–271, Feb 2012, doi: 10.1109/IEEESTD.2012.6161600.

[4] S. Ullah, H. Higgins, B. Braem, B. Latré, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks - on phy, mac, and network layers solutions," *J. Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[5] M. Toorani, "On vulnerabilities of the security association in the IEEE 802.15.6 standard," in *Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*, ser. Lecture Notes in Computer Science, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds., vol. 8976. Springer, 2015, pp. 245–260.

[6] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, 2010.

[7] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[8] H. C. A. van Tilborg and S. Jajodia, Eds., *Encyclopedia of Cryptography and Security, 2nd Ed.* Springer, 2011.

[9] Q. Tang, "Key establishment protocols and timed-release encryption schemes," Ph.D. dissertation, Department of Mathematics, Royal Holloway, University of London, Royal Holloway Research Online, 10 2007.

[10] K. S. Deepak and A. V. Babu, "Energy efficiency analysis of IEEE 802.15.6 based wireless body area networks in scheduled access mode," *Wireless Networks*, vol. 22, no. 5, pp. 1441–1459, 2016.

[11] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *J. Medical Systems*, vol. 39, no. 11, pp. 136:1–136:8, 2015.

[12] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mhealth," *J. Medical Systems*, vol. 40, no. 11, pp. 231:1–231:10, 2016.

[13] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2016.

[14] W. Diffie, P. C. van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Des. Codes Cryptography*, vol. 2, no. 2, pp. 107–125, 1992.

[15] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[16] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[17] "Crypto++ 5.6.5 Benchmarks," https://www.cryptopp.com/benchmarks.html, [Online; accessed 25-August-2017].