A secure low-delay protocol for wireless body area networks

A Secure Low-Delay Protocol for Multi-hop Wireless Body Area Networks

Dave Singelée[1], Benoît Latré[2], Bart Braem[3], Michael Peeters[4], Marijke De Soete[4], Peter De Cleyn[3], Bart Preneel[1], Ingrid Moerman[2], and Chris Blondia[3]

[1] ESAT–SCD–COSIC, Katholieke Universiteit Leuven — IBBT,
Kasteelpark Arenberg 10, 3001 Heverlee-Leuven, Belgium,
dave.singelee@esat.kuleuven.be,
[2] IBCN, Dept. of Information Technology (INTEC), Ghent University — IBBT,
Gaston Crommenlaan 8, bus 201, 9050 Gent, Belgium,
[3] PATS, Dept. of Mathematics and Computer Sc., University of Antwerp — IBBT,
Middelheimlaan 1, B-2020, Antwerp, Belgium,
[4] NXP Semiconductors, Competence Center System Security & DRM,
A&I Innovation & Development Center Leuven,
Interleuvenlaan 74–82, 3001 Leuven, Belgium.

Abstract. The development of Wireless Body Area Networks (WBANs) for wireless sensing and monitoring of a person's vital functions, is an enabler in providing better personal health care whilst enhancing the quality of life. A critical factor in the acceptance of WBANs is providing appropriate security and privacy protection of the wireless communication. This paper first describes a general health care platform and pinpoints the security challenges and requirements. Further it proposes and analyzes the CICADA-S protocol, a secure cross-layer protocol for WBANs. It is an extension of CICADA, which is a cross-layer protocol that handles both medium access and the routing of data in WBANs. The CICADA-S protocol is the first integrated solution that copes with threats that occur in this mobile medical monitoring scenario. It is shown that the integration of key management and secure, privacy preserving communication techniques within the CICADA-S protocol has low impact on the power consumption and throughput.

1 Introduction

Recent progress in wireless sensing and monitoring, and the development of small wearable or implantable biosensors, have led to the use of Wireless Body Area Networks (WBANs). The research on communication within a WBAN is still in its early stages. Only few protocols designed specifically for multi-hop communication in WBANs exist. They try to minimize the thermal effects of the implanted devices by balancing the traffic over the network [1] or by forming clusters [2, 3] or a tree network [4].

Wireless Body Area Networks can be seen as an enabling technology for mobile health care [5]. Medical readings from sensors on the body are sent to

servers at the hospital or medical centers where the data can be analyzed by professionals. These systems reduce the enormous costs associated to ambulant patients in hospitals as monitoring can take place in real-time even at home and over a longer period.

The communication of health related information between sensors in a WBAN and over the Internet to servers is strictly private and confidential and should therefore be encrypted to protect the patient's privacy. Furthermore, the medical staff who collects the data must be confident that the data is not tampered with, and indeed originates from that patient. In this paper, we propose and analyze CICADA-S, a secure protocol for WBANs. It is based on an existing multi-hop protocol for WBANs, called CICADA [4]. This is a cross-layer protocol that sets up a data gathering tree in a reliable manner, offering low delay and high energy efficiency.

The CICADA-S protocol is designed within the scope of the IBBT IM3-project (Interactive Mobile Medical Monitoring), which focuses on the research and implementation of a wearable system for health monitoring [6]. Patient data is collected using a WBAN and analyzed at the gateway (also called medical hub) worn by the patient. If an event (e.g., heart rhythm problems) is detected, a signal is sent to a health care practitioner who can view and analyze the patient data remotely.

The remainder of this paper is organized as follows. Section 2 gives an overview of related work. The general architecture and the necessary security assumptions are described in section 3. A description of CICADA is given, followed by the integration of the security mechanisms in the protocol and a description of the key management aspects in section 4. The analysis of the integration in terms of performance overhead and the verification of the security claims are dealt with in section 5. Finally, section 6 provides a final conclusion on the paper.

2 Related Work

Security is essential for broad acceptance and further growth of Wireless Sensor Networks. These networks pose unique challenges as security techniques used in traditional networks cannot be directly applied. Indeed, to make sensor networks economically viable, sensor devices should be limited in their energy consumption, computation, and communication capabilities. Since most of the existing security mechanisms have major drawbacks in that respect, new ideas are needed to address these requirements in an appropriate way [7].

One of the most crucial components to support the security architecture of a Wireless Sensor Network is its key management. During the last years, a number of pairwise key establishment schemes have been proposed. Zhou and Haas propose to secure ad-hoc networks using asymmetric cryptography [8]. They use threshold cryptography to distribute trust among a set of servers. This scheme achieves a high level of security, but is too energy consuming to be used in practice in a Wireless Sensor Network. Eschenauer and Gligor introduce a key management scheme for distributed sensor networks [9]. It relies on probabilistic

key sharing among the nodes of a random graph. Perrig et al. present SPINS, a suite of security building blocks optimized for resource-constrained environments and wireless communication [10]. It has two secure building blocks: SNEP and μTESLA. SNEP provides data confidentiality, two-party data authentication and data freshness, while μTESLA offers authenticated broadcast in constrained environments.

The security mechanisms employed in Wireless Sensor Networks do generally not offer the best solutions to be used in Wireless Body Area Networks for the latter have specific features that should be taken into account when designing the security architecture. The number of sensors on the human body, and the range between the different nodes, is typically quite limited. Furthermore, the sensors deployed in a WBAN are under surveillance of the person carrying these devices. This means that it is difficult for an attacker to physically access the nodes without this being detected. When designing security protocols for WBANs, these characteristics should be taken into account in order to define optimized solutions with respect to the available resources in this specific environment. Although providing adequate security is a crucial factor in the acceptance of WBANs, little research has been done in this specific field. One of the most crucial components to support the security architecture is its key management. Further, security and privacy protection mechanisms use a significant part of the available resources and should therefore be energy efficient and lightweight.

The communication of critical data (e.g., health related information) between sensors in a WBAN has to comply with the following security requirements: *data confidentiality*, *data authenticity*, *data integrity* and *data freshness* [11]. Data confidentiality means that the transmitted information is secret and can only be accessed by certain entities. It is usually achieved by encrypting the information using a secret key. This encryption can be symmetric or asymmetric. Due to the restrictions on energy and computational power of devices in wireless networks, symmetric encryption is preferable. Data authenticity provides a means for making sure that the information originates from the claimed sender. To fulfill this requirement, one can compute a Message Authentication Code (MAC) using a shared secret key. Data integrity means that the received information has not been tampered with without this being noticed. This can be done by computing a MAC on the data. Data freshness guarantees that the received data is recent and not an old message being replayed (e.g., to cause disruption in the network). A frequently used technique is to add a counter to the message, which is increased in every communication round.

A solution for data integrity and freshness in WBANs was proposed by Balasubramanyn et al. in [12]. Their algorithm provides integrity based on the measurement of a permissible round trip time threshold and is computationally feasible. Authentication is done by calculating a MAC with a random sequence of numbers. This sequence is determined at the initialization phase.

Another promising solution for key management in WBANs is the use of biometrics. Biometrics is a technique commonly known as the automatic identification and verification of an individual by his or her physiological and/or

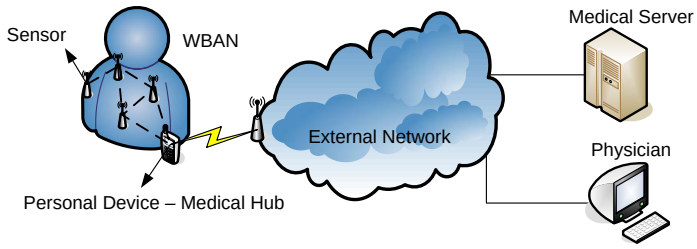


Fig. 1. General overview of the IM3 health care architecture.

behavioral characteristics [13]. Poon et al. [14] describe an algorithm based on biometric data that can be employed to ensure the authenticity, confidentiality and integrity of the data transmission between the personal device and all the other nodes. Bao et al. proposed an algorithm that uses the heartbeat [15].

In [16] body-coupled communication (BCC) is used to associate new sensors in a WBAN. As BCC is limited to the body, this techniques can be used to authenticate new sensors on the body.

The developers of WBANs will also have to take into account the privacy issues. After all, a WBAN can be considered as a potential threat to freedom, if the applications go beyond "secure" medical usage, leading to a Big Brother society. Social acceptance would be the key to this technology finding a wider application. Therefore, considerable effort should be put in securing the communication, protecting the privacy of the user in the WBAN, and making sure that only authorized persons can access the data traveling in the network.

None of the current protocols offer a solution where appropriate security mechanisms are incorporated into the communication protocol while addressing the life cycle of the sensors. Further, security and privacy protection mechanisms use a significant part of the available resources and should therefore be energy efficient and lightweight. The mechanisms proposed in this paper aim to cover these challenges.

3 Architecture

3.1 General Overview

Fig. 1 shows the health care architecture used by the IM3 project. There are three main components: the Wireless Body Area Network (WBAN), the external network and the back-end server. The WBAN contains several sensors that measure medical data such as ECG, body movement, temperature etc. These sensors are equipped with a radio interface and send their measurements wirelessly to a central device called the medical hub. This can be done either directly or via several intermediate hops. The medical hub is unique for each WBAN (and hence for every patient) and acts as a gateway between the WBAN and the external network. As it has more processing power than normal sensors, it can process the medical data and generate alarms if necessary. Each sensor shall only

send its recorded data to the unique gateway it is linked with and this needs to be enforced by specific security mechanisms. The external network can be any network providing a connection between the medical hub and the back-end server. In most cases, the communication between the external network and the medical hub will be wireless. The back-end server securely stores, processes and manages the huge amount of medical bio-data coming from all of the patients. This data can then be observed and analyzed by medical staff.

Although the architecture was originally designed for and is fully adapted to a medical environment, it may also be used in other applications. Indeed, as long as the (security) relations between the different devices remain valid, the protocol remains applicable. In the remainder of this paper, the medical scenario will be further used to explain the architecture and the secure cross-layer protocol for multi-hop WBANs.

3.2 Security Assumptions

This section aims to address the security of the entire system, and the WBAN in particular.

The most security critical device in the entire architecture is the back-end server. This server, which is managed by the hospital or medical center, will receive the medical data sent by all active WBANs. It is assumed that this server is physically protected (e.g., put in a secure place in the hospital where it can not be stolen or tampered with), and that an adequate access control system is implemented (i.e. only authorized medical personnel has (partial) access to the server through appropriate identification/authentication mechanisms). The back-end server is considered to be a trusted third party, which means that it is known and trusted by all other devices in the network after a successful authentication, it performs all tasks correctly and will not tamper with the data its receives.

Since potentially security critical data will be transferred through the external network, end-to-end security between the gateway and the back-end server is necessary. For efficiency reasons, it is assumed that both devices share a symmetric session key to secure their communication. This symmetric session key can be manually installed (e.g., pre-installed during manufacturing), or (preferably) established via a symmetric key establishment protocol. The description of such protocols can be found in the ISO 9798–2 standard, and is out of scope of this article. The symmetric session key is updated regularly. The end-to-end channel between gateway and back-end server should also be anonymized using temporary pseudonyms. This avoids privacy problems like (location) tracking. In the remainder of the paper, it is assumed that the secure end-to-end channel between gateway and back-end server is already established after a successful mutual authentication. As mentioned before, each gateway belongs to a specific WBAN (i.e. a patient, who is carrying this device). To enforce this, the gateway is registered in advance at the back-end server.

It is assumed that it is impossible to alter or read the memory of a (securely initialized) node that is put on the patient's body, or to modify the behavior of a

node without this being detected. This is not a very strong assumption, since the patient is carrying the nodes on its body, and an attacker is not able to access the nodes without this being detected. It is also assumed that the attacker has no access to the sensors that yet have to be securely initialized (e.g., because they are stored in a safe place). These assumptions limit the use case scenarios of the protocol we will propose in this paper. If one cannot avoid the attacker having physical access to nodes in the network (e.g., because the sensor is temporarily removed from the network when it is not measuring data), our proposed solution will not be secure. This problem can be avoided by making the sensors tamper resistant. This is however an expensive solution.

Despite these limitations, the attacker can still perform several attacks to the Wireless Body Area Network. He can put a malicious node in the presence of a WBAN, and try to join the network. He can also eavesdrop on all data transmitted in the WBAN, and insert/delete/modify (malicious) data into the network. The attacker is hence assumed to be active.

4 Protocol Design

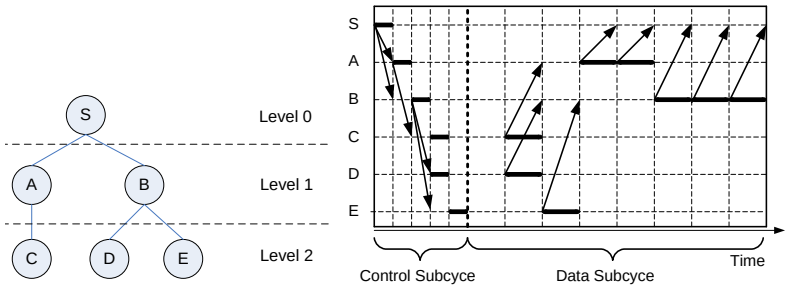
4.1 CICADA

CICADA is a low energy protocol designed for wireless, multi-hop Body Area Networks [4]. It is a cross-layer protocol as it handles both medium access and routing of data. Data gathering trees are autonomously set up and used to route data from the nodes towards the personal device or sink. The time axis is divided in slots in order to lower the interference and avoid idle listening. Slot assignment is done in a distributed manner where each node informs its children when they are allowed to send their data using a SCHEME.

In the following, we will use the small example network from Fig. 2 to explain the protocol. The tree is set up in such a way that communication is only possible between a child and its parent or between siblings.

Data transfer is defined by a sequence of cycles. At the beginning of each cycle, the slots in the remainder of the cycle are assigned. Each parent sends a SCHEME-message to all their children, containing their slot allocation scheme. A node calculates the scheme of its children based on the scheme it has received from its parent. Each cycle is divided in two parts: the control subcycle and the data subcycle. Each subcycle has its own slot allocation scheme: the control-scheme and the data-scheme respectively. These schemes are both sent in the control subcycle. When all nodes have received their schemes, the control subcycle has ended and the data subcycle starts. Thus, as can be seen in Fig. 2, control information is sent downwards from the sink to all nodes in the control subcycle. In the data subcycle, all data is sent upwards to the sink.

Each node is assigned one slot in the control subcycle. As slots in the control subcycle are only used to send the short scheme-messages, slots can be shorter. When a node has received such a scheme-message in a control slot, it can turn its radio off as no more packets will arrive in the control subcycle. The data subcycle



(a) Sample topology

(b) Packet streams in this network. Notice the down- and upstream traffic

Fig. 2. Communication in CICADA for a sample network of 5 nodes and a sink. The arrows indicate the transmission direction. The bold lines show when the node is transmitting.

is used to forward the data from the nodes to the sink. The first nodes to start sending data are the nodes at the bottom of the tree. Doing so, all data can be sent to the sink in one cycle. This lowers the end-to-end delay tremendously.

In the following, we will discuss the operation of the control and data subcycle.

Control Subcycle The control subcycle is used for transferring both schemes (i.e. the control scheme and the data scheme) to all nodes. At the start of the control subcycle, the sink sends the first message (i.e. its scheme-message). Table 1 shows which nodes are allowed to send in which slot for the example network. The assignment of the slots in the control subcycle is done using the control scheme.

Each control scheme contains the following information of the control subcycle:

- The control scheme indicates the order in which the children are allowed to send their control scheme;
- The total length of the control subcycle in slots T_{CC}, starting from the transmission of the control scheme of the sink. Stated otherwise, this is the total number of slots needed to allow all devices to send their scheme. In the example, the length is 5;
- The remaining number of slots in the control subcycle, including the slot in which the node is transmitting. This is needed to know when the data subcycle begins.

This information is used to calculate the exact slot in which the node can send.

For example, node S sends its scheme with the following information: control scheme AB, control subcycle length 5 and 5 remaining slots 5. Nodes A and B receive this information. Node A sees in the control scheme that it is allowed to

send first, so it will send its scheme-message containing the control scheme, the additional information and the data scheme in the following slot. Node B will send in the slot thereafter. However, as node C cannot send simultaneously with node B, node A will add a wait slot to its control scheme which becomes "$.C$". Node B will send the following: control scheme DE, control subcycle length 5 and 3 remaining slots. The remaining length indicates how many slots are left in the control subcycle and is thus used to know the start of the data subcycle.

Table 1. Control subcycle information of the nodes. NA indicates that no control scheme is available (i.e. the node has no children).

	S	**A**	**B**	**C**	**D**	**E**
send in slot number	1	2	3	4	4	5
remaining length	5	4	3	2	2	1
control scheme	AB	$.C$	DE	NA	NA	NA

Data Subcycle For the example network the data schemes of the nodes, or stated otherwise, the assignment of the slots in the data subcycle, can be seen in Fig. 2.

The data scheme consists of three parts: a *receiving period* (length α), a *waiting period* (length β) and a sending period. In the waiting period, the node must remain silent and should switch off its radio. In the receiving period, the node receives data from its children and in the sending period the node sends data to its parent. In the example, node B has a waiting period of 1 slot, a receiving period of 2 slots and a sending period of 3 slots. The data scheme determines when the child nodes are allowed to transmit in the receiving period. The last slot of each data scheme is a *contention slot* which is used to allow new children to join the network. This will be explained later on.

Each node maintains a table called ChildTable with the following information for each child i:

α_i The number of data slots needed to receive the data from node i
β_i The number of data slots node i needs to receive data from its children, i.e. the length of the waiting period of node i and 1 slot for contention.

Each child is granted the number of data slots indicated in the ChildTable (α_i). Each time a node n sends a data packet, a small amount of additional information is put in the data header: α_n and β_n. These values are calculated as follows.

$$\alpha_n = \sum_{i \in Ch_n} \alpha_i + \delta_n \tag{1}$$

$$\beta_n = \max_{i \in Ch_n} \beta_i + \sum_{i \in Ch_n} \alpha_i + 1 \tag{2}$$

In these formulas, Ch_n represents the set of node n's children and δ_n equals the number of data slots that is needed for node n to transmit its own generated data. The max function is needed as different branches of the tree are allowed to send simultaneously. When a parent receives a packet from its child, it will extract this information from the header and update its ChildTable. Each child has to send this additional information each data subcycle. If a child has no data packet to send or to forward, it will send a HELLO-message to its parent containing only that information. Doing so, the parent knows that the child is still connected to the tree. In Table 2, the ChildTables for nodes S, A and B are given. As nodes C, D and E have no children, their ChildTables are empty.

Table 2. ChildTables of nodes S, A and B for the network of Fig. 2

S

	α_i	β_i
A	2	3
B	3	4

A

	α_i	β_i
C	1	1

B

	α_i	β_i
D	1	1
E	1	1

Based on the information in the ChildTable, the node can calculate the data scheme as follows. First, it determines how long the child nodes have to wait until they can start sending by taking the maximum of the children's waiting period: $\max_{i \in Ch_n} \beta_i = \beta$. Doing so, the structure of the tree and the subsequent simultaneous transmissions are taken into account. Then each child node i is granted α_i slots, leading to a receiving period of $\alpha = \sum_{i \in Ch_n} \alpha_i$ slots. At the end, a contention slot is added.

As described above, a contention slot is included in each data subcycle so that nodes can join the tree. New children listen to the SCHEME messages of neighboring nodes. When one is received, a JOIN-REQUEST message is sent in the contention slot, preferably after a random delay within the contention slot to avoid contention of simultaneously sent JOIN-REQUEST messages. When the parent hears the JOIN-REQUEST message, it will include the node in the next cycle. Each node will send at least two packets per cycle: a data packet or HELLO packet (if no data is sent) and a SCHEME packet. If a parent does not receive a packet from a child for N or more consecutive cycles, the parent will consider the child to be lost. If a child does not receive packets from its parent for N or more consecutive cycles, the child will assume that the parent is gone and will try to join another node.

4.2 CICADA-S

The CICADA protocol, as described in the previous section, does not guarantee any form of security and privacy. Unauthorized nodes can easily join the WBAN, and all communication in the network is sent in plain text and is not integrity protected. The fixed identity of the sensors is not kept confidential, and can hence be used to track sensors (and patients carrying these sensors). To

counter these problems, appropriate security mechanisms have to be added to the CICADA protocol. The result is the CICADA-S, the secure version of the CICADA protocol.

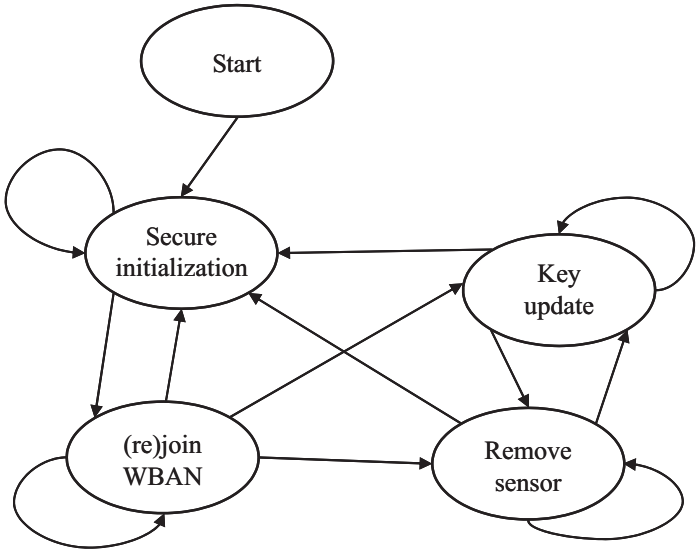


Fig. 3. FSM of a sensor in a WBAN.

From a security point of view, there are four main phases which take place during the lifetime of a sensor: the secure initialization phase, the sensor (re)joining the WBAN, a key update procedure in the WBAN, and the sensor leaving the WBAN. This is shown in Fig. 3. The security mechanisms used in these phases and their integration into the CICADA-S protocol, based on the results of the IM3 project [6], will now be described.

Secure initialization phase: Initially, each sensor has to be securely initialized by the back-end server before it can join the WBAN in a later stage. During this initialization phase, the sensor and the back-end server will agree on a shared symmetric key. This can be done via asymmetric cryptographic techniques, but this is typically too energy (and computation) consuming for a regular sensor. Another way of establishing a shared key, is by using a private and authentic out-of-band channel. Such a channel is typically cheap to set up. It has the interesting property that all data transmitted on the channel remains confidential for eavesdroppers, and that the integrity and authenticity is protected too. A private and authentic channel can be created in several ways, depending on the exact hardware and (physical) characteristics of the sensors. It can be established by connecting the sensor directly to the back-end server, via an extra electrical

contact available on both devices. Other techniques to create such a secure out-of-band channel is by employing distance bounding protocols, by having the user manually enter the data on both devices, etc. More information on these and other techniques to establish a private and authentic out-of-band channel can be found in literature [17–19].

Let us assume that sensor A has to be initialized. The data transfer via the secure out-of-band channel takes place in two steps. First, the sensor sends its fixed identity to the back-end server. This can be done explicitly or implicitly (the identity of the sensor can be implicitly known because of the specific characteristics of the out-of-band channel). In the second step of the protocol, the back-end server generates a random secret key (k_A), and sends this key securely to the sensor. The sensor and the back-end server store this secret key in their memory. The key is (conceptually) composed out of 2 subkeys: the encryption key k_{A_encr} and the integrity key k_{A_int}. Note that each new node is assigned a new and unique secret key.

Each sensor (A) is also assigned a unique counter (CTR_A), which is initialized to 0 and stored in the sensor's memory. The value of this counter is included in all key management messages, and is used to avoid replay attacks and assure freshness. Every time the counter is used, the value gets incremented by 1.

Sensor (re)joining the WBAN: After the initialization procedure, the sensor is ready to be put on the patient's body. It will detect the WBAN, and start the join procedure, which will now be discussed.

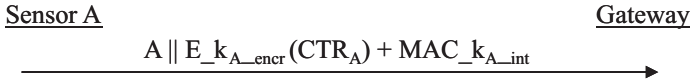


Fig. 4. Secure JOIN-REQUEST originating from sensor A.

When the sensor (with fixed identity A) hears the SCHEME of the desired parent, it sends a secure JOIN-REQUEST message, as shown in Fig. 4, in the contention slot. This message is forwarded to the gateway. It is basically a HELLO message containing the unique (global) identity of the sensor and the value of its unique counter CTR_A. The counter is encrypted for privacy reasons (since it is used in all key management messages). The gateway stores (and updates) this value of the counter. The integrity and authenticity of the entire secure JOIN-REQUEST message is protected by a message authentication code (MAC) [20], computed with the key k_{A_int}.

When the gateway receives the secure JOIN-REQUEST message of sensor A, it forwards this request to the back-end server via the secure end-to-end channel. This triggers a protocol in which the key k_A is securely transported from the back-end server to the gateway. More information on how to accomplish this, can

be found in the ISO 9798–2 standard [21]. In some scenarios, and this is often the case in a medical environment, it is known in advance (e.g., already during the initialization procedure) in which WBAN the sensor will be deployed. In this case, the back-end server can already transport the key k_A to the correct gateway, and does not have to wait until it receives the secure JOIN-REQUEST message. This makes the join procedure faster. In case a sensor leaves the network, and (not much) later rejoins it, the gateway may still have the key k_A in its memory and does not have to forward the request to the back-end server. From the moment the gateway has access to the key, it can check the validity of the JOIN-REQUEST by verifying the message authentication code, and in case of a rejoin, also the value of the counter CTR_A (the new value should be higher than the current value shared by sensor and gateway). If this verification is successful, the sensor is allowed to join the WBAN and is assigned a temporary identity $localID_A$. This temporary identity, which is chosen by the gateway, is established in order to preserve the privacy. It is only unique within the environment of the WBAN. Other networks can reuse the same identifier. Since the bitlength of such a local identifier can be smaller than the full identity of the sensor (A), it also improves the efficiency. A joining sensor in the WBAN is informed about its temporary identity during the key transport procedure, which takes place immediately after the approval of the secure JOIN-REQUEST message.

Key update procedure in the WBAN: Except for the key management messages, the data traveling in the WBAN consists of schemes sent during the control subcycle, and medical data sent during the data subcycle from the sensors to the gateway. The former is only integrity protected (to allow a new node to inform itself about the contention slot), while the latter is both integrity protected and encrypted. All these operations are performed by employing a secret group key s, that is shared between all the sensors in the WBAN. Every time a node joins or leaves the network, the group key is updated in order to avoid an attacker recovering the key. Even when the topology of the network remains constant for a long time, the group key should still be updated at regular intervals. The exact period is determined by the cryptographic strength of the encryption and integrity algorithms used to protect the data in the WBAN, and the length of the key. We will briefly come back to this in section. 5.1.

The update process works as follows. First, the gateway randomly generates a new group key s. Next, it performs a secure key transport procedure with all the nodes in the WBAN, as shown in Fig. 5. The gateway constructs a key update message, unique for every sensor, which contains the encrypted value of the updated group key s. For each node i, the message also contains the new value of the counter CTR_i (which is the current value of the counter incremented by 1), in order to avoid replay attacks, and the local identifier $localID_i$. The authenticity and the integrity of the message is protected by a message authentication code. Nodes that have been excluded from the WBAN, can not decrypt the key transport messages anymore, and are hence not able to obtain the new group key s.

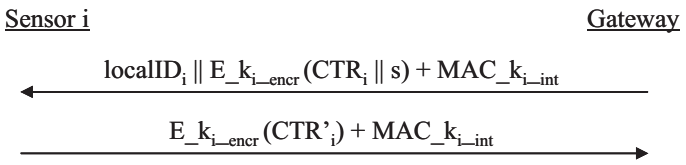


Fig. 5. Secure key transport to all the sensors in the WBAN.

The key update message is uniquely constructed for every sensor, and forwarded from the gateway to the correct node during the control subcycle. Each node takes the message containing its local identifier, checks the validity of the message (by verifying the value of the counter and the message authentication code) and decrypts the encrypted part in order to recover the new value of the group key s. It also forwards all other key update messages to its children, who perform the same procedure. A new joining node A does not yet know its local identifier $localID_A$, and therefore has to check the message authentication code (and the counter) of all the key update messages using its key k_{A_int} until the test succeeds. This only has to be done once, and is easily feasible since computing a message authentication code can be done very efficiently. The joining sensor stores its local identifier $localID_A$ in its memory, and recovers the group key s from the encrypted part of the key update message. Finally, all sensors send a secure acknowledgement back to the gateway during the next data subcycle, to inform that they received the key well. This key confirmation message only contains the encrypted value of the updated counter CTR_i, concatenated with a message authentication code. After having received the key confirmation message, the gateway knows it can definitively update the group key. When a node does not send its key confirmation message within a certain period, e.g., because it did not receive the new group key s due to packet loss, the gateway retransmits the key transport message to that particular node.

Sensor leaving the WBAN: When a node detects that a particular sensor A is not part anymore of the WBAN, it forwards this information to the gateway. This automatically triggers a group key update procedure. This has to be done to avoid that an attacker stealing a sensor from the network, would be able to read or modify the data in the WBAN. After a certain interval (or even immediately, depending on the policy), the gateway deletes the key k_A and the identifier $localID_A$ from its memory. If the medical staff removes sensor A from the patient, or if the sensor is reported lost or stolen, the key k_A should also be deleted from the memory of the back-end server. This way, the sensor cannot rejoin any network anymore in a later stage, until it has been securely reinitialized by the back-end server.

5 Analysis

5.1 Performance Evaluation

The addition of these security mechanisms to CICADA undoubtedly influences the performance as it leads to an increased overhead and higher delay. The exact impact strongly depends on the choice of the cryptographic algorithms that are deployed in the WBAN, and it is hence difficult to formulate results that are generally applicable. In practice, it is best to employ an efficient low-cost encryption and integrity algorithm. To have a brief idea of the overhead caused by the security mechanisms, we will do a worst case analysis and assume that a secure block cipher that is not optimized for low power, such as the Advanced Encryption Standard (AES) [22], is employed in an authenticated encryption mode (e.g., CCM or GCM mode of operation). The numbers used below are based on the guidelines of the National Institute of Standards and Technology (NIST) [23, 24].

The combined encryption and authentication algorithm uses a symmetric key of 16 bytes (the group key s or the shared key k_i). The output of this method are encrypted blocks of 16 bytes, and a message authentication code of at least 8 bytes. Furthermore, the unique hardware address of the sensor is assumed to be 6 bytes (e.g., as in Bluetooth), and a counter of 4 bytes is employed to avoid replay attacks. Note that encrypting the counter results in an encryption block of 16 bytes. Using these parameters offers a high level of security as long as the keys are updated regularly, which depends on the strength of the cryptographic algorithm that is being used. E.g., when AES is used in the GCM mode of operation, the group key s should be updated at least at every 2^{32}th invocation of the encryption algorithm [24]. In this section, we will now briefly discuss the (worst case) impact of the security mechanisms on the CICADA protocol, using the numbers stated above.

In the (re)joining phase, additional information is sent to the gateway in the JOIN-REQUEST message. The original CICADA-message only contains $localID_A$ and $localID_P$ (i.e. the local ID of node A joining the network and the local ID of the desired parent P respectively). The length of these IDs is 1 byte, which is sufficient for a WBAN. In CICADA-S the unique hardware address of the sensor is sent, together with the encrypted synchronized counter and a message authentication code. The length of the JOIN-REQUEST message thus is longer, but still only 30 bytes. As this information is sent in a contention slot with fixed size, this will not influence the throughput of the system. However, this secure JOIN-REQUEST message needs to be forwarded to the gateway. As the contention slot of a node is in the beginning of a data subcycle, the message can be sent to the gateway directly. E.g., the JOIN-REQUEST message can be piggybacked on a data packet that is sent to the gateway. As the length of the message is small, this may not influence the overall throughput significantly. The number of bytes that can be sent in one slot depends on the size of the slot and the raw bit rate of the radio technology used. If the number of bytes in the data packet and the secure JOIN-REQUEST message is too large, the slot size

will have to be altered. This will lower the throughput of the network. A better solution is to send the JOIN-REQUEST message in a separate data slot. This will hardly impact the throughput of the network. If the key is already present at the gateway, the gateway can immediately start the key update procedure. If not, the gateway has to wait for a response from the back-end server. This will add extra delay to the joining procedure.

In the key update procedure, the gateway sends a new key to all the nodes in the control subcycle. This message contains $localID_A$, the new key group key s concatenated with an increased counter (both encrypted), and a message authentication code. For each node, this is an additional 41 bytes. Due to the broadcast mechanism in the control subcycle, these messages all need to be broadcasted by every node sending its SCHEME in the control subcycle. This will lead to a larger slot length in the control subcycle, and subsequently a lower throughput. In CICADA, the slot length in the control subcycle is smaller than the data slot length as the SCHEME-messages sent in the control subcycle are very short. The slot length can be up to ten times smaller. This improves the energy throughput of CICADA. As the key is only updated after several cycles, we opt to change the control slot dynamically. When the key is updated, the control slot length has the same length as the data slot. At any other time, the control slot has its shorter length. When the key is about to be updated, the gateway broadcasts a warning in the previous cycle by setting a bit in the header. The nodes receive this warning and adapt their control slot lengths for one cycle.

When a node leaves the network or is no longer attached to it, the (former) parent node sends a message to the gateway. This can be added to a data packet and will not influence the throughput.

It is very important to note that the key management messages are sent rarely (only when a node (re)joins the network, or when the group key has to be updated), and hardly affect the global throughput in the network. Most data traveling in the WBAN is medical data, sent by the sensors to the gateway. These messages are protected by employing the group key s. The data is encrypted in blocks of 16 bytes, and a message authentication code of 8 bytes is added. The SCHEME packets sent during the control subcycle are not encrypted, but integrity protected. For both types of data, the length of the messages is hardly influenced. Overall, the security mechanisms will have a minor impact on the performance of CICADA-S.

5.2 Security Claims

The CICADA-S protocol has some interesting security properties. These will now be briefly discussed. It has to be stressed that the following statements are based on the assumptions stated in section 3.2, and that all devices in the network, including the attacker, are computationally bounded.

- One of the most important security requirements of the CICADA-S is the ability to exclude nodes from the Wireless Body Area Network. From the

moment a node is lost, compromised by an attacker or just not needed anymore, it should be removed from the network and is no longer able to read/modify/insert/delete data in the WBAN. This requirement is fulfilled, since the group key s is always updated if the topology of the network changes. Only nodes that are still part of the network receive a new group key, which is encapsulated in a secure key transport message. Other nodes do not get any information about the updated group key, and can only obtain the latter by decrypting the secure key transport message, without having the secret key. In other words, a node that is no longer (or never has been) part of the network does not have any advantage compared to an attacker.

- Since the group key is transported in an encrypted format from the gateway to the nodes in the WBAN, it is practically not feasible for an eavesdropper to recover the key. Only an attacker that can break the encryption scheme used to protect data in the WBAN, is able to find the group key s. Since we assume that the encryption scheme used in the WBAN has an appropriate security level, this attack is not feasible.
- Another important requirement is that only authorized nodes can join the WBAN. To technically enforce this, nodes first have to be securely initialized before they can join the network. After this secure initialization procedure, nodes share a symmetric key with the back-end server. This key is used to construct a valid secure JOIN-REQUEST message, which is needed to join the WBAN.
- A sensor that is a member of a WBAN cannot join another WBAN at the same time. The second secure JOIN-REQUEST message sent by this sensor will be refused by the back-end server, because it will detect that the sensor already belongs to another network.
- The CICADA-S protocol offers key confirmation, which is important for security and performance reasons. After receiving the new group key s via a secure key transport message, a node sends an authenticated key confirmation message to the gateway, to inform that the key was received well. This avoids certain Denial-of-Service attacks (in which an attacker blocks some key update messages, in order to disrupt the key update mechanism and cause these nodes to be unsynchronized). Due to packet loss and bit errors, key confirmation is also an important and necessary property of network protocols for wireless media (a key transport message can always be affected by noise).
- Nodes that are part of a particular WBAN, are not able to read encrypted data, neither modify, insert or delete data in other WBANs without this being detected, since these other networks do not share the same group key s. A node that is not part of a network has no advantage compared to an attacker, both do not possess information about the group key s that is currently being used in the network.
- Since the confidentiality and integrity of data transmitted in the WBAN is cryptographically protected, a device that does not possess the group key will not succeed in decrypting the enciphered communication, nor successfully modifying/inserting/deleting data into the network without this being

detected. This can only be done by breaking the encryption algorithm and/or the message authentication code (MAC) deployed in the WBAN. Since we assume that both algorithms have an appropriate security level, this attack is not feasible.

- Replay attacks are detected because of the use of the synchronized counter, that is shared between sensor and gateway. The other party will detect the replay attack because the value of the synchronized counter is lower or equal to a previous value, which is not allowed. Modifying the value of the counter without possessing the necessary secret key is not possible, since the counter is integrity protected by a MAC.
- Since the sensors that are going to perform the CICADA-S protocol will be put on a patient, location privacy is certainly an issue. Fortunately, this has been taken into account during the design of the protocol. Even more, the communication between gateway and back-end server is assumed to be completely secured (end-to-end) and anonymized (by employing pseudonyms). Let us now focus on the Wireless Body Area Network. The data that is transmitted in the WBAN by the sensors cannot be used to trace a patient, since it only contains local identifiers, and these are not unique across WBANs. Only in the first message of the join procedure, the exact identity of the sensor is exposed. This identity is however not used in the other key management messages. It is also not possible to link other (key management) messages to each other or to the initial key management message of the join procedure. The only common element in all key management messages is the synchronized counter. This value is however encrypted, and hence cannot be used by the attacker (which does not possess the secret key and cannot break the encryption scheme). All medical data that is sent by the sensors to the gateway, is encrypted with the group key. An attacker cannot decrypt this. The headers contain the local identifier of the sensors, which is meaningless outside the concept of a particular WBAN. So as a conclusion, location privacy can be guaranteed, and patients cannot be traced by the data that is transmitted in the network.

6 Conclusion

Wireless Body Area Networks are an enabling technology for mobile health care. These systems reduce the enormous costs associated to patients in hospitals as monitoring can take place in real-time even at home and over a longer period. A critical factor in the acceptance of WBANs is the provision of appropriate security and privacy protection of the wireless communication medium. The data traveling between the sensors should be kept confidential and integrity protected. Certainly in the mobile monitoring scenario, this is of uttermost importance.

In this paper we have presented CICADA-S, a security enabled cross-layer multi-hop protocol for Wireless Body Area Networks. It is a secure extension of the CICADA protocol, and was designed within the scope of the IM3-project (Interactive Mobile Medical Monitoring), which focuses on the research and im-

plementation of a wearable system for health monitoring. The CICADA-S protocol is the first integrated solution to cope with the threats of interactive mobile monitoring and the life cycle of the sensors. It combines key management and secure privacy preserving communication techniques. We have presented the main security claims of CICADA-S and have shown that the addition of security mechanisms to the CICADA-S protocol has low impact on the power consumption and throughput. The security mechanisms integrated in the protocol are simple, yet very effective. The CICADA-S protocol can be implemented on today's devices as it only requires minimal and low-cost hardware changes.

The authors strongly believe that adding sufficient security mechanisms to Wireless Body Area Networks will work as a trigger in the acceptance of this technology for health care purposes.

Acknowledgments. This work is partially funded by a research grant of the Katholieke Universiteit Leuven for D. Singelée, by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), by the Fund for Scientific Research — Flanders (F.W.O.-V.,Belgium) project G.0531.05 (FWO-BAN) and by the Flemish IBBT project IM3.

References

1. D. Takahashi, Y. Xiao, and F. Hu. LTRT: Least total-route temperature routing for embedded biomedical sensor networks. In *Proceedings of the 50th IEEE Global Telecommunications Conference, GLOBECOM '07*, November 2007.
2. M. Moh, B.J. Culpepper, D. Lan, M.Teng-Sheng, T. Hamada, and S. Ching-Fong. On data gathering protocols for in-body biomedical sensor networks. In *Proceedings of the 48th IEEE Global Telecommunications Conference, GLOBECOM '05*, November/December 2005.
3. A.G. Ruzzelli, R. Jurdak, G.M.P O'Hare, and P. Van Der Stok. Energy-efficient multi-hop medical sensor networking. In *Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, HealthNet '07*, pages 37–42, New York, NY, USA, 2007.
4. B. Latré, B. Braem, I. Moerman, C. Blondia, E. Reusens, W. Joseph, and P. Demeester. A low-delay protocol for multihop wireless body area networks. In *Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, Philadelphia, PA, USA, August 2007.
5. C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4):307–326, 2006.
6. IBBT IM3-project [online] http://projects.ibbt.be/im3.
7. A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57, June 2004.
8. L. Zhou and Z.J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, November/December 1999.
9. Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on*

Computer and communications security, pages 41–47, New York, NY, USA, 2002. ACM.

10. A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar. SPINS: Security protocols for sensor networks. In *Mobile Computing and Networking*, pages 189–199, 2001.
11. S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta. Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on*, pages 432–439, October 2003.
12. V. B. Balasubramanyn, G. Thamilarasu, and R. Sridhar. Security solution for data integrity inwireless biosensor networks. In *Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on*, pages 79–79, Toronto, Ont., June 2007.
13. M. Guennoun, M. Zandi, and K. El-Khatib. On the use of biometrics to secure wireless biosensor networks. In *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, pages 1–5, Damascus, April 2008.
14. C.C.Y. Poon, Z. Yuan-Ting, and B. Shu-Di. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, April 2006.
15. S.S.-D Bao, C.C.Y. Poon, Y.Y.-T. Zhang, and L.L.-F. Shen. Using the timing information of heartbeats as an entity identifier to secure body sensor network. *Information Technology in Biomedicine, IEEE Transactions on, Accepted for future publication*, 2008.
16. T. Falck, H. Baldus, J. Espina, and K. Klabunde. Plug 'n play simplicity for wireless medical body sensors. *Mobile Networks and Applications*, 12(2-3):143–153, 2007.
17. C. Gehrmann, C. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, 2004.
18. D. Singelée and B. Preneel. Key establishment using secure distance bounding protocols. In *Proceedings of the first Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems, SPEUCS '07*, Philadelphia, PA, USA, August 2007. IEEE.
19. F. Stajano and R. Anderson. The resurrecting duckling: Security issues in ad–hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–182. Springer-Verlag, 1999.
20. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
21. ISO/IEC 9798-2. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms, 1999.
22. J. Daemen and V. Rijmen. *The Design of Rijndael – AES – The Advanced Encryption Standard*. Springer-Verlag, 2002.
23. NIST Special Publication 800-38C. Recommendation for block cipher modes of operation – the CCM mode for authentication and confidentiality. U.S. DoC/NIST. Available at `http://csrc.nist.gov/publications/`, May 2004.
24. NIST Special Publication 800-38D. Recommendation for block cipher modes of operation – galois/counter mode (GCM) and GMAC. U.S. DoC/NIST. Available at `http://csrc.nist.gov/publications/`, November 2007.