A secure cross-layer protocol for multi-hop wireless body area networks

A Secure Cross-layer 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 even at home in real-time and over a longer period.

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 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.

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 short 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 security properties 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

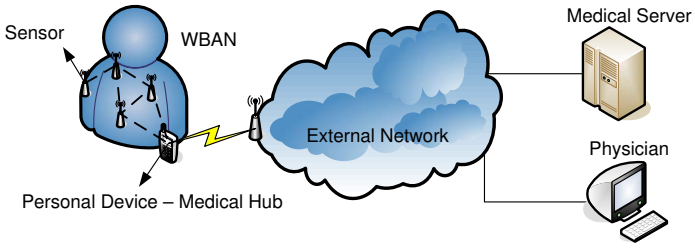


Fig. 1. General overview of the IM3 health care architecture.

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 [11]. In [12] an algorithm based on biometric data is described that can be employed to ensure the authenticity, confidentiality and integrity of the data transmission between the personal device and all the other nodes. Another method is presented in [13] where body-coupled communication (BCC) is used to associate new sensors in a WBAN.

None of the current protocols offer a solution where appropriate security mechanisms are incorporated into the communication protocol while addressing the lifecycle 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. In this scenario, the WBAN contains several sensors that measure medical data such as ECG, body movement etc. These sensors send their measurements, directly or via several hops, to the gateway. Each WBAN (and hence every patient) has its unique gateway. In other words, the sensors shall only send their data to the unique gateway they are linked with and this needs to be enforced by specific security mechanisms. The gateway processes the medical data, and sends the result via the external network to the back-end server at the hospital, where it can 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, which increases the generality of our solution. 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.

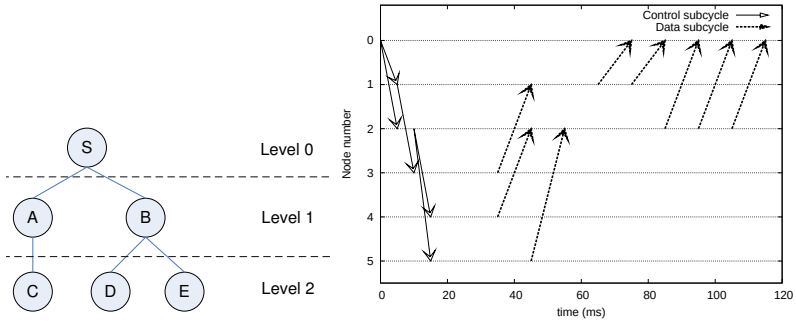
Since potentially security critical data will be transferred through the external network, end-to-end security between the gateway and the back-end server is required. For efficiency reasons, it is assumed that both devices share a symmetric session key to secure their communication. This symmetric session 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 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). However, an attacker 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 cross-layer protocol as it handles both medium access and the routing of data [4]. The protocol sets up a spanning tree in a distributed manner, which is subsequently used to guarantee collision free access to the medium and to route data toward the gateway. The time axis is divided in slots grouped in cycles, to lower the interference and avoid idle listening. Slot assignment is done in a distributed way where each node informs its children when they are allowed to send their data using a SCHEME. Slot synchronization is possible because a node knows the length of each cycle. During a cycle, a node is allowed to send all of its data to its parent node. CICADA is designed in such a way that all packets arrive at the source in only one cycle. Routing itself is not complicated in CICADA anyway as data packets are routed up the tree which is set up to control the medium access, no special control packets are needed.



(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

A cycle is divided in a control subcycle consisting of control slots, and a data subcycle consisting of data slots. The former is used to broadcast a SCHEME

message from parent to child, i.e. to let the children know when they are allowed to send in the data subcycle. In the data subcycle, data is forwarded from the nodes to the gateway. In each data subcycle, a contention slot is included to allow nodes to join the tree. New children hear the SCHEME message of the desired parent and send a JOIN-REQUEST message in the contention slot. 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. An example of communication in CICADA is given in Fig. 2, for a network of 5 nodes. The control and data subcycles can be seen clearly.

A node informs its parent node of the number of slots it needs to send its own data and forward data coming from its children, by calculating two parameters: α and β. The former gives the number of slots needed for sending data (including forwarded data) to its parent, the latter gives the number of slots the node has to wait until it has received all data from its children. Based on the α and β from its children, a node can calculate the slot allocation for the next cycle.

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 protocol, the secure version of the CICADA protocol.

From a security point of view, there are four main states 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. The security mechanisms used in these phases and their integration into the CICADA-S protocol, based on the results of [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 setup. 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 the literature [14–16].

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 i is also assigned a unique counter CTR_i, 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.

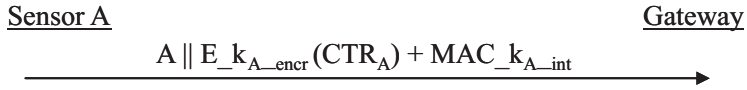


Fig. 3. Secure JOIN-REQUEST originating from sensor A.

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. 3, 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) [17], 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 [18]. 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 the 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. 4. 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.

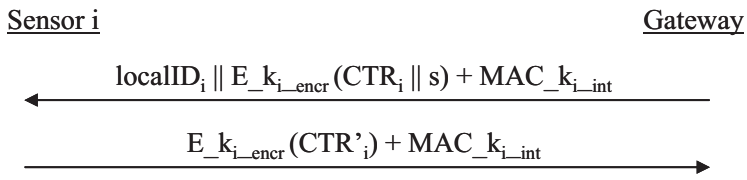


Fig. 4. Secure key transport to all the sensors in the WBAN.

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 in order 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 can not 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. That is why a worst case analysis will be given, in which we assume that a secure block cipher, such as the Advanced Encryption Standard (AES) [19], 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) [20,21]. In practice, it would be better to employ a low-cost encryption and integrity algorithm, which has a slightly lower security level, but is more efficient.

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 [21]. 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 Properties

One of the design goals of the CICADA-S protocol is to secure the wireless communication in the WBAN while preserving privacy. The most interesting security properties of our protocol will now be briefly discussed (without formal proof). 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.

- The CICADA-S protocol provides forward security. A node that leaves the network can not successfully read/modify/insert/delete data in the WBAN,

since the group key s is always updated in case the topology of the network changes.
- Nodes that are not securely initialized, can not join the WBAN. Only nodes that share a symmetric key with the back-end server, can construct a valid secure JOIN-REQUEST message, which is needed to join the WBAN.
- 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.
- The CICADA-S protocol offers key confirmation, which is important for security and performance reasons. After receiving the new group key s, a node sends a key confirmation message to the gateway, to inform that the key was received well. This avoids certain Denial-of-Service attacks (e.g., blocking key update messages). Due to packet loss and bit errors, key confirmation is also an important and necessary property of network protocols for wireless media.
- A sensor that is a member of a WBAN can not join another WBAN at the same time. The second secure JOIN-REQUEST message sent by the sensor will be refused by the back-end server, because this device will detect that the sensor already belongs to another network.
- Nodes that are part of a particular WBAN, are not able to read, modify, insert or delete encrypted data in other WBANs without this being detected, since these other networks do not share the same group key s.
- Since the confidentiality and integrity of data traveling 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.
- Replay attacks are detected because of the use of the synchronized counter, that is shared between sensor and gateway.
- Location privacy has been taken into account during the design of the CICADA-S protocol. The communication between gateway and back-end server is assumed to be completely secured (end-to-end) and anonymized. Using the data in the WBAN to trace a patient is not possible, because 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. It is however not used in the other key management messages. Neither is it possible to link other messages to the initial key management message of the join procedure (since the synchronized counter is encrypted). As a result, the data in the WBAN can not be used to trace patients.

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 even at home in real-time 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 implementation 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 properties of CICADA-S, and 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 low-cost and minimal 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. L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002*, November 2002.
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. H. Baldus, K. Klabunde, and G. Msch. Reliable set-up of medical body-sensor networks. In Holger Karl, Andreas Willig, and Adam Wolisz, editors, *Proceedings of the First European Workshop on Wireless Sensor Networks, EWSN '04*, volume 2920 of *Lecture Notes in Computer Science*, pages 353–363. Springer-Verlag, 2004.
12. 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.
13. 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.
14. C. Gehrmann, C. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, 2004.
15. 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.
16. 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.
17. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
18. ISO/IEC 9798-2. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms, 1999.
19. J. Daemen and V. Rijmen. *The Design of Rijndael – AES – The Advanced Encryption Standard*. Springer-Verlag, 2002.
20. 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.
21. 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.