A New Scheme Based Biometric to Protect Location Privacy in Wireless Body Area Networks

Mohammed MANA[1], Mohamed FEHAM[2] and Boucif AMAR BENSABER[3]

[1] University of Ain Temouchent
Ain Temouchent, 46000, Algeria

[2] STIC Lab., Department of telecommunications, University of Tlemcen
Tlemcen, Algeria

[3] Laboratoire de mathématiques et informatique appliquées LAMIA, Université du Québec à Trois-Rivières
C.P. 500 Trois-Rivières, Québec, Canada G9A 5H7

Abstract

The wireless body area network (WBAN) has emerged as a new technology for e-healthcare that allows real time monitoring of patients using small wearable and/or implantable sensors. The latest collect vital information of the patient and communicate them to a central unit using short-range wireless communication techniques. The security and privacy protection of the data collected from a WBAN is major preoccupation with challenges coming from stringent resource constraints of WBAN devices and the high demand for both security/privacy and practicality/usability. In this paper, we first categorize the type of eavesdroppers that threatening the privacy in WBAN, and then we propose a new scheme based biometric to protect location privacy in WBAN.

Keywords: *Wireless Body Area Networks, location privacy, Eavesdroppers, attack games, Biometrics*

1. Introduction

A wireless body area network WBAN consists of a set of wearable or implanted biosensors that collect vital signs from the person carrying these devices and transmit them wirelessly to a personal device or a base station to be analyzed as shown in figure 1 [1].

Due to the wireless nature of communication between the sensor nodes and the base station, the wireless body area network can be subject to many threats. For example, it is relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the sender or the receiver physically. To fight against this threat, location privacy must be protected.

Location privacy can be defined as the confidentiality of personal location information [2]. In wireless body area network, privacy may be classified into two categories [3]: *content privacy or data privacy* and *contextual privacy*.

Threats against content privacy occur due to the ability of adversaries to observe and manipulate the content of packets sent over the body area network. This type of threats is countered by encryption and authentication mechanisms. Protecting data privacy is not enough because an adversary can deduce sensitive information from a wireless body area network by eavesdropping the network traffic and analyzing the traffic patterns. In particular, the location information about senders/receivers may be derived based on the direction of wireless communications [3].

To deal with threats against sender/receiver location information, it is very important to protect contextual privacy in wireless body area network.

Traditional mechanisms employed to protect contextual privacy of communication parties in Internet and Ad-hoc networks are not appropriate for wireless body area networks because communicating devices are very resource constrained [4]. Also, the contextual privacy 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 following table gives the major differences between the wireless body area networks and the wireless sensor networks.

Tableau 1: Major differences between WBAN and WSN

Wireless body area network	Wireless sensor network
- Quite limited number of sensor nodes	- Large number of sensor nodes
- Small area interest	- Wide area interest
- Quite limited range between the different devices	- Large range between the different nodes
- Nodes under surveillance of the person carrying these devices	-hostile environment

It is very important to take into account these characteristics when designing location privacy protocols for WBAN in order to define optimized solutions with respect to the available resources in this specific environment [5].

In this paper, we aim to use biometrics to improve and to adapt the scheme proposed by Dave Singelée (show figure 3) to provide the source and the sink location privacy in Wireless Body Area Networks.

The remainder of this paper is organized as follows. In Section 2, we give the problem definition including network model, security assumptions, adversarial model and definition of the attack games. In Section 3, we present Dave Singelée Location Privacy Protocol and in section 4, we propose a novel scheme for source/sink location privacy. Section 5 is intended to analyze the degree of anonymity of our scheme according to each attack game. Finally, concluding remarks are given in Section 6.

2. Problem Definition

2.1 Network model

We consider that the wireless body area network contains several sensor nodes that measure medical information such as ECG, PPG, body movement, pressure …etc and communicate them to a central device called the base station as shown in figure1. These sensors are limited in terms of energy, memory space and computation capability.

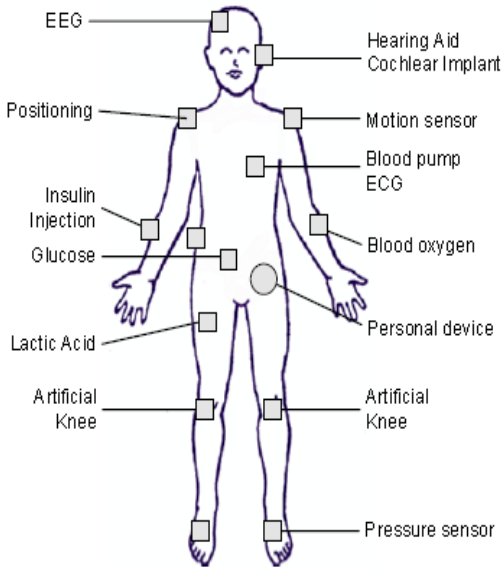

Fig.1 Wireless Body Area Network Architecture

Due to the limited range between the sensor nodes and the base station, we propose to adopt a star topology of our wireless body area network.

The following figure depicts our network model. All sensor nodes have the same level and can communicate directly with the sink. In the system there is also an adversary present who wants to track a particular user by the sensor nodes the latter is carrying.

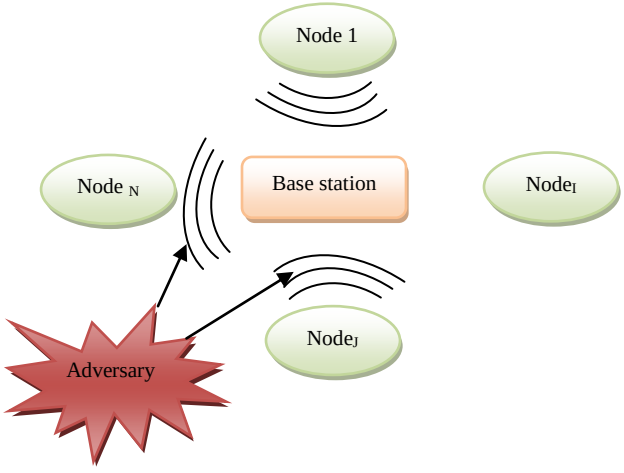

Fig.2 Our Network Model

2.2 Security Assumptions

We make only a unique assumption that is each sensor node is able to measure ECG signals.

2.3 Adversarial model

The model consists of the means of the adversary and his goals. The means of the adversary are represented using the following oracles [2]:

- Query Target: The adversary sends a message to the base station, and observes the response.
- Query node N_i: The adversary sends a message to the node N_i, and observes the response.
- Execute (N_i, Target): The adversary forces N_i and the base station to communicate between them and eavesdrops on the exchanged messages.

During an attack game, the adversary is allowed to make a particular number of queries to each (or some) of the oracles. We parameterize the number of Query Target messages by q_t, the number of Query node messages by q_r and the number of Execute messages by q_e. An adversary with these means is denoted by $A[q_t , q_r , q_e]$ in the rest of the paper.

2.4 Attack games

The goal of an adversary in an attack game is twofold, the first is to distinguish between a node and the base station of the WBAN and the other is to detect which node/base station belongs to a specific WBAN.

To analyze the security of the protocol used to identify the source and the destination of messages, authors in [6] assume that its security level can be parameterized by a security parameter k and in the definition of parameterizable attack games; they used the notation poly(k) to represent any polynomial function of degree k.

Following are defined two attack games. The first attack game aims to distinguish between a specific target T (the base station), chosen by the adversary, and another random node. The second attack game aims to detect that a certain node belongs to a specific WBAN in order to track the user carrying the wireless body area network.

2.4.1 Attack game 1

The attack game goes as follows:

- The adversary selects a specific node N_j = T from a particular wireless body area network. This will be the target node for the challenge.
- The adversary can query the three oracles (Query target T, Query node N_i, and Execute (N_i, T)). The numbers of allowed queries to these oracles are parameterized by q_t, q_r and q_e respectively.
- The adversary selects two nodes, T_0 and T_1. One of these nodes is equal to the target T, the other node is a random node N_x. The goal of the adversary is to indicate which one of these two nodes T_b is the target node T (the base station).
- The adversary can query the three oracles (Query target T_i, Query node N_i, and Execute (N_i, T)).
- The adversary has to decide which node of T_0 and T_1 is equal to the target T (the sink).

An identification protocol P executed in a WBAN with security parameter k is (q_t, q_r, q_e)-location private if:

$\forall A[q_t , q_r , q_e]$: Pr (A[q_t, q_r , q_e] wins attack game 1 by guessing b) $\leq$ (1\2)+(1\poly(k)) [2, 6]

2.4.2 Attack game 2

The game goes as follows:

- The adversary selects a particular WBAN. This last is the target of the adversary.
- The adversary can query the two oracles Query node N_i and Execute (N_i, T), as described previously. The numbers of allowed queries to these oracles are parameterized by q_r and q_e respectively.
- The adversary randomly selects one of the nodes N_i. This node is removed from the WBAN. The adversary also selects another node, which is not part of the same WBAN (and hence not known by the nodes N_i). These two nodes are randomly defined as T0 and T1. The goal of the adversary is to indicate which one of these two nodes T_b belongs to the particular WBAN (and is hence known by the other node N_i).
- The adversary can query the three oracles (Query Sink, Query node N_i, and Execute (N_i, T)). The numbers of allowed queries to these oracles are parameterized by q_s, q_r and q_e respectively.
- The adversary has to decide which node T_b (so T_0 or T_1) belongs to the WBAN formed by the nodes

N_i (the Sink is included). The adversary wins when his guess of the bit b was correct.

A protocol P executed in a WPAN with security parameter k is (q_t, q_r, q_e)-WBAN location private if:

$\forall A[q_t, q_r, q_e]$: Pr ($A[q_t, q_r, q_e]$ wins attack game 2 by guessing b) $\leq (1\backslash 2)+(1\backslash poly(k))$ [2, 6]

Next is given our protocol design which aims to provide location privacy in wireless body area network.

3. Dave Singelée Location Privacy Protocol

This section presents Dave Singelée location privacy protocol in wireless personal area networks.

To protect location privacy, author proposes to use temporary pseudonyms. As depicted in figure 3, author proposes to compute the new temporary pseudonym from a random nonce and the old pseudonym using a pseudo random function "*PRF(.)*" and a shared key "K".

$R_{New}=PRF_K(n|R_{Old})$

After each round of the protocol, the key "K" is updated.

$K'=h(K)$

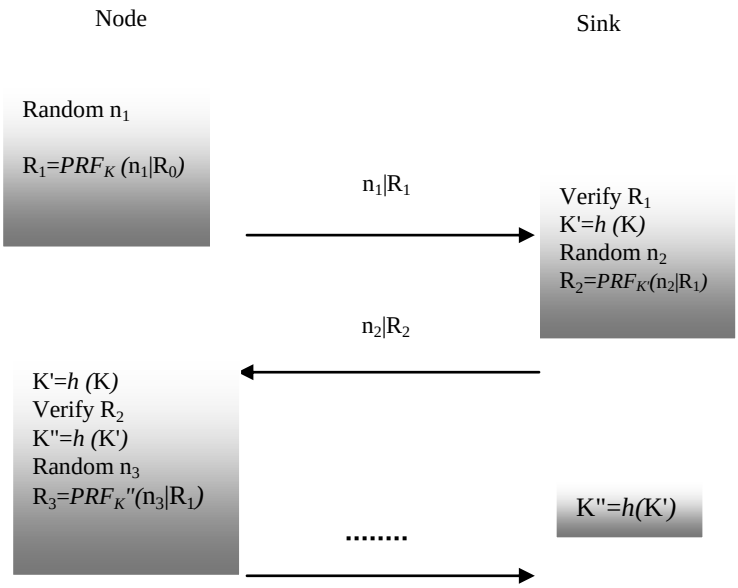

Fig.3 Dave Singelée Location Privacy Protocol [2, 6]

This scheme does not provide full protection against attack games because if a node and the sink use the same nonce, an adversary can win attack game 1 with a probability close to 100% by performing the following adversarial algorithm:

- The adversary selects a specific node N = T from a particular wireless personal area network. This will be the target node for the challenge.
- The adversary sends two queries to a node N_i, which shares an unknown key K with the target T. The current pseudonym shared by N_i and T is R. In the first query, the node N_i will reply with the pseudonym R. In the second query, the node N_i will reply with the pseudonym $PRF_K(R|n)$.
- The adversary selects two nodes, T_0 and T_1. One of these nodes is equal to the target T, the other node is a random node N_x.
- The adversary sends a query to the nodes T_0 and T_1. This target query contains the pseudonym R.
- One of the nodes will reply to this query with a message containing the pseudonym $PRF_K(R|n)$, the other node with a random message. The node that has replied with $PRF_K(R|n)$ is the target node T.

Also, an adversary can win attack game 2 with a probability close to 100% by performing the following adversarial algorithm:

- The adversary selects a particular wireless personal area network, formed by the group of nodes N_i. This group is the target of the adversary.
- The adversary randomly selects one of the nodes N_i. This node is removed from the network. The adversary also selects another node, which is not part of this particular network (and hence not known by the nodes N_i). These two nodes are randomly defined as T_0 and T_1.
- The adversary sends two queries to both the nodes T_0 and T_1. One of the nodes will reply with the pseudonym R in the first query, and with the pseudonym $PRF_K(R|n)$ in the second query. The other node will reply twice with a random message (denoted by X_1 and X_2).
- The adversary randomly selects one of the nodes T_b (T_0 or T_1), and sends the response of this node's first query (so R or X_1) in a query to each of the remaining (n − 1) nodes N_i of the particular wireless personal network.
- If one of the nodes Ni replies with the pseudonym $PRF_K(R|n)$, the node T_b is equal to the target node T. If all the

nodes Ni send a random reply back not equal to $PRF_K(R|n)$, node T_b is not part of the particular wireless personal area network and hence not the target node.

Next, is given our protocol design which aims to provide full protection against attack games. Our solution is based biometrics and it is designed to provide location privacy in wireless body area networks.

4. Our protocol design

This section shows our location privacy protocol. First, is given the different notation used in our protocol and then is presented the detail of our protocol.

4.1 Notation

We will use the following notation to illustrate different Primitives in our protocol design:

- *Req_Joint:* is a request to join the WBAN from a node to the base station
- *Req_Auc:* is an authentication request from the base station to a node
- *Res_Auc:* is an authentication response from a node to the base station
- *Conf_Auc:* is an authentication confirmation from the base station to a node
- *BioKey:* is a biometric key
- *Idt:* is a temporary pseudonym
- R_1, R_2… are examples of nonce
- $E_K(M)$: an encryption of a message M with a symmetric key K
- *h (m)*: a cryptographic hash function applied to the message *m.*
- *M1*|*M2*: is the concatenation of messages *M1* and *M2*

1.1 Protocol description

In this subsection, we present the different steps of our scheme based biometric to protect location privacy in wireless body area networks.

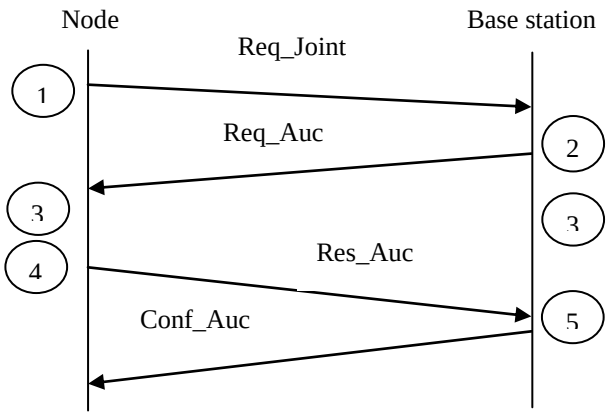

Fig.4 Connection Establishment between Node and the Base Station

Main steps
(1) The node aiming to join the WBAN sends a request "Req_Join" to the base station
(2) After receiving the request "Req_Join", the base station sends the authentication request "Req_Auc" to the node
(3) Both the base station and the node try to generate a biometric key "BioKey"
(4) The node encrypts an "Ok" message using "BioKey" and sends the encrypted message loaded in the packet "Res_Auc" to the base station
(5) The base station checks the "Res_Auc", if the check is successful then it generates two random numbers R_{N1}, R_{N2}, encrypts them with "BioKey". Finaly it sends the encrypted message loaded in the packet "Conf_Auc".

To provide location privacy in WBANs, nodes and the sink perform the following basic steps (as depicted in figure 5):

The node

Step 1: generates two nonces R_1 and R_2, (R_1, R_2) $\epsilon[R_{N1}, R_{N2}[.[R_{N1}, R_{N2}[$ is the interval of nonces shared between the sink and the node.
Step 2: Computes Idt= *h(BioKey|R1)*
Step 3: Encrypts R_1 and R_2 with "BioKey"
Step 4: Transmits $Idt|E_{BioKey}(R_1|R_2)$ to the Sink

The sink

Step 5: Decrypts $E_{BioKey}(R_1|R_2)$
Step 6: Computs $Idt'=h(BioKey|R_1)$
Step 7: Checks Idt= Idt'

- If the Sink wants to send a message to the node, it computes the new pseudonym from the received nonce R_2 using "BioKey" and the hash function *E(.)*
Computs Idt'=h (BioKey|R2)
- If the node wants to send a new message to the sink, it generates two new nonces R_3 and R_4/ (R_3, R_4) ϵ[R_{N1}, R_{N2}[and (R_3, R_4) ǂ (R_1, R_2). The new nonces are used to compute the new pseudonym.

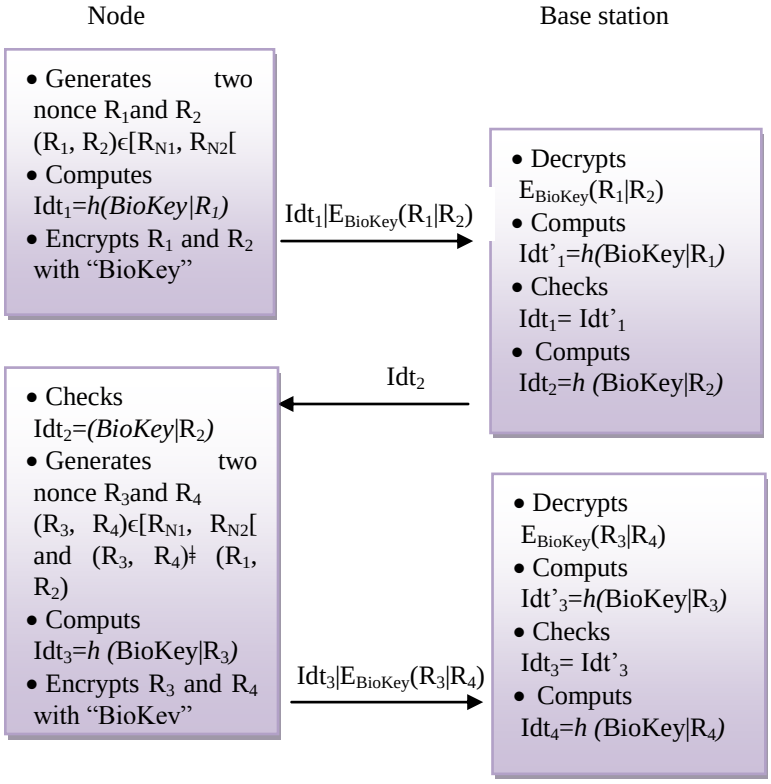

Fig.5 Temporary Identity Generation

5. Analysis of our location privacy protocol

First, we will examine and evaluate the efficiency of our location privacy protocol for WBANs against the two attack games presented in subsection 2.4. Then, we will analyze the energy needed for the execution of our proposed scheme.

5.1 Efficiency against attack game1

To track a node or the sink, an adversary performs the following steps as described above (subsection 2.4):

○ The adversary selects a specific node N_j = T from a particular WBAN. This will be the target node for the challenge.

○ The adversary sends two queries to a node N_i, which shares an unknown key K (BioKey) with the target T. The current pseudonym shared by N_i and T is Idt. In the first query, the node N_i will reply with the pseudonym Idt. In the second query, the node N_i will reply with the pseudonym Idt'=h(BioKey|R) where R is a random number and BioKey is the biometric key.

○ The adversary selects two nodes, T_0 and T_1. One of these nodes is equal to the target T, the other node is a random node N_x.

○ The adversary sends a query to the nodes T_0 and T_1. This target query contains the pseudonym Idt.

○ One of the nodes (the target T) will reply to this query with a message containing the pseudonym Idt"=h(BioKey|R'), the other node with a random message X containing the pseudonym Idt'".

Because the random responses of N_i, T_0 and T_1 which are respectively Idt', Idt" and Idt'", the adversary will not be able to detect which node is the target T.

The adversary is able to detect the target T if Idt"=Idt', but this will not be occur because the target and the nodes will never use the same nonces.

Our protocol is (q_s, q_r, q_e)-location private because:

$\forall A[q_t , q_r , q_e] : Pr (A[q_s, q_r , q_e])=0 \leq (1\backslash 2)+(1\backslash poly(k))$.

5.2 Efficiency against attack game2

To track a particular WBAN, an adversary performs the following steps as presented also in subsection 2.4.

○ The adversary selects a particular WBAN, formed by the group of nodes N_i. This group (WBAN) is the target of the adversary.

○ The adversary randomly selects one of the nodes N_i. This node is removed from the particular WBAN. The adversary also selects another node, which is not part of this particular WBAN (and hence not known by the nodes N_i). These two nodes are randomly defined as T_0 and T_1.

○ The adversary sends two queries to both the nodes T_0 and T_1. One of the nodes will reply with the pseudonym Idt in the first query, and with the pseudonym Idt'=h(BioKey|R') in the second query. The other node will reply twice with a random message (denoted by X_1 and X_2).

○ The adversary randomly selects one of the nodes T_b (T_0 or T_1), and sends the response of this node's first query (so Idt or X_1) in a query to each of the remaining (n −1) nodes N_i of the particular WBAN.

The adversary wins attack game if one of the nodes N_i replies with the pseudonym Idt' (the node T_b is equal to the target node T), but this not will be occurred because all the nodes N_i send a random reply back not equal to Idt'. The pseudonyms contained in the random replies are not equal to Idt' because the nodes do not use the same keys and the same nonces to compute their pseudonyms.

Our protocol is (q_s, q_r, q_e)-WBAN location private because:

$\forall A[q_t , q_r , q_e] : Pr (A[q_s, q_r , q_e])=0 \leq (1\backslash 2)+(1\backslash poly(k))$.

5.3 Energy consumption

Energy consumption is also taken into account. In our solution, we compute cryptographic hash values and use the result as an identifier (pseudonym). According to [7], the execution of cryptographic hash function requires 5,9µJ/Byte if the SHA-1 algorithm is used and the transmission and reception of a single byte of data requires 59, 2µJ and 28, 6µJ respectively.

Assuming that a 128-bit nonce and 128-bit BioKey are used, the cost of computing the pseudonym "Idt" is 188,8 µJ.

The cost of transmitting or receiving one 128-bits identifiers and two encrypted 128-bits nonce is 2841,6 µJ and 1372,8 µJ respectively.

Therefore the total energy cost is 4592 µJ.

6. Concluding Remarks

Wireless Body Area Networks (WBANs) 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 nodes should be kept confidential and integrity protected. Certainly in the mobile monitoring scenario, this is of uttermost importance.

In this paper, we have presented a light weight protocol to provide location privacy in wireless body area network. The basic idea of our solution consists on the use of temporary pseudonyms instead the use of hardware addresses to communicate in the wireless body area networks. This allows protecting the source and the destination of mobile devices in the WBANs.

Our solution is efficient and energy saving.

Acknowledgement

The research is developed in STIC Laboratory, Department of telecommunications, University of Tlemcen, Tlemcen, Algeria in collaboration and supervision of Professor Boucif Amar Bensaber, director of LAMIA Laboratory, Université du Québec à Trois-Rivières, Quebec, Canada.

This work was completed with the support of the natural sciences and engineering research council of Canada (nserc).

References

[1] Benoît Latré, Bart Braem, Ingrid Moerman, Chris Blondia, Piet Demeester: A survey on wireless body area networks. Wireless Networks 17(1): 1-18 (2011)

[2] Dave SINGELEE, thesis "Study and Design of a Security Architecture for Wireless Personal Area Networks", December 2008

[3] Ying Jian Shigang Chen Zhan Zhang Liang Zhang, "Protecting Receiver-Location Privacy in Wireless Sensor Networks", This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings

[4] Song-Woo Lee, Young-Hun Park, Ju-Hyung Son, Seung-Woo Seo, U Kang y, Ho-Kun Moony, and Myoung-Soo Leey, " Source-Location Privacy in Wireless Sensor Networks ", www.cs.cmu.edu/~ukang/200704_source_privacy.pdf
sensor networks," Proceedings of PerCom, pp. 324-328, 2005.

[5] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber, "Trust Key Management Scheme for Wireless Body Area Networks", International Journal of Network Security, Vol. 12, No. 2, PP. 75{83, Mar. 2011.

[6] Dave Singelée, Ford-Long Wong, Bart Preneel, and Frank Stajano, " A Theoretical Model for Location Privacy in Wireless Personal Area Networks"; www.cl.cam.ac.uk/~fms27/papers/2008-SingeleeWonPreETAL-**location**.pdf

[7] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," Proceedings of PerCom, pp. 324-328, 2005.