LIRA: A New Key Deployment Scheme for Wireless Body Area Networks

Tonko Kovačević
University Department of Professional Studies in Split
University of Split, Croatia
tkovacev@oss.unist.hr

Toni Perković
FESB
University of Split, Croatia
toperkov@fesb.hr

Mario Čagalj
FESB
University of Split, Croatia
mcagalj@fesb.hr

Abstract— **A rapid development of the Wireless Body Area Network (WBAN) has become very important for applications in telemedicine and m-health. However, there is still a need to ensure a reliable and secure communication in these systems. In this paper we present a novel multi-channel key deployment scheme for wireless body sensor networks. The proposed key deployment scheme requires no public key cryptography and therefore is suitable for CPU-constrained sensor nodes. The solution is implemented on commercially available wireless sensor nodes while the performance of the system is shown through the experiments with users.**

Keywords— Wireless body area networks, Key deployment, Visible light channel, Initializiation, Authentication

I. INTRODUCTION

Wireless Sensor Networks (WSN) are increasingly being accepted by the upcoming concept of the Internet of Things (IoT) [1, 2]. Their growing use and simultaneous miniaturization have empowered the development of specialized sensor networks, namely Wireless Body Area Networks (WBAN). These networks are used in hospitals, emergency rooms or even at patient's homes and comprise of small low-powered wireless devices attached in or around a human body to monitor the patient's essential life functions (e.g., ECG, blood pressure, blood oxygen saturation, etc.) [3]. Though the data transmitted over a wireless channel need to be kept private, these communication channels can be easily eavesdropped and manipulated. Hence it presents a challenge to secure the communication over these channels, i.e., to establish secret keys on devices that lack traditional interfaces like USB or network ports, keyboards and screens [6].

A number of key pre-distribution based schemes have been proposed for bootstrapping key agreement [10, 11]. All these solutions assume that nodes are preloaded with some secret before their initial use. However, these solutions cannot always be applied to WBANs due to the following limitations: users might not trust the keys preloaded by the manufacturer, existing public key techniques might be expensive for sensor devices due to the limited computation resources, nodes supplied by different manufactures would require the existence of a global Public Key Infrastructure (PKI), etc. Therefore, an important task is to find both a secure and user-friendly solution that initializes a relatively large number of low-power WBAN devices (up to 20 devices) compatible with constrained interfaces.

Some proposed solutions rely on the availability of a specialized hardware (e.g., Faraday cage) [23, 24] or auxiliary out-of-band (OOB) channels (e.g., a visible light) [25, 26, 27], which makes them difficult and expensive to use. Moreover, the human-implemented OOB channel can only tolerate up to 10 sensor devices and the involvement of end users is quite significant what makes these solutions inappropriate for WBANs with a larger number of sensor nodes [26, 27]. Recently there has been an increased interest in bootstrapping security for WBANs using physical layer channel characteristics [28, 29].

In this paper we propose a new multi-channel [24, 25] key deployment scheme for WBAN in which information is transmitted over both a light channel and a radio channel. We named our scheme LIRA because we use *Light* channel for sensor *Initialization* and *Radio* channel for *Authentication*. In our protocol, each sensor node (*SN*) establishes a unique secret key with a body control unit (*C*). The body control unit (*C*) is a device that collects information from all sensors (*SN*), informs the user (e.g., a patient, a nurse) and conveys the data gathered from the sensors (e.g., ECG, SpO_2 levels etc.) to the central telemedicine system (e.g., a server). In the first phase of the protocol, a light source unit (*LS*) transmits secret keys over a protected visible light channel (VLC) to the body control unit (*C*) and each sensor node (*SN*). In the second phase, the body control unit (*C*) runs key verification with each sensor node (*SN*). After the successful key verification the body control unit (*C*) establishes a security association with each sensor node (*SN*).

In the proposed protocol the light source unit (*LS*) consists of a multi-touch screen that runs an appropriate program responsible for generating secret keys and transmitting them by flashing light (using on-off keying modulation) to the body control unit (*C*) and sensor nodes (*SN*) all equipped with a light detector (e.g. a photodiode). Since light is easier to block than radio waves (by covering the screen with a sensor), a potential attacker cannot get the secret information easily.

The main motivation to use VLC as an OOB channel for bootstrapping security information was inspired by the rapid development of VLC communication and multi-touch screen technology (smartphones and tablets) and their future vision for applications in offices and homes [4, 5, 6, 7, 8]. The VLC channel [9] can be used not only as a safe OOB channel for secure key transmission, but also as a mediate device for users to interact with resource-constrained wireless sensor devices after they have been initialized. For example, with the multi-touch screen we could assign multiple accounts to the same group of sensor devices. This way, many patients could use the same group of sensor devices (e.g. a family or patients in a hospital) and collect sensor data only while they are using the WBAN. Moreover, we could assign different account levels for different users (e.g., a doctor, a nurse and/or a patient) that have different permissions (e.g., reading the data from all users, changing the keys). Furthermore, we could easily assign different roles to certain sensors or even establish a logical key hierarchy between sensor devices (e.g. by circling the sensors).

Compared to some other proposed solutions (e.g., Message-in-a-Bottle [23] or KALWEN [24]) our solution does not require any specialized equipment. LIRA is applicable to various WBAN applications as opposed to the schemes based on biometrics derived from the human body and therefore applicable only to sensors that measure the same physiological signals [20, 21, 22]. LIRA scheme requires no Public Key Cryptography (PKC) and therefore can be applied onto sensor nodes with very limited computational power and memory resources as well. Furthermore, in our solution the user involvement is minimized - the user places the sensor nodes on *LS* and waits until the process is automatically executed. This is opposite to some proposed solutions [26, 27] that require a much greater involvement of the user. Indeed, we demonstrate the feasibility of our solution via a preliminary evaluation with 26 users. Although some other solutions also do not require the presence of the user during the initialization (e.g., ASK-BAN [28]), the key generation rate is higher in our solution than the solution [28].

The rest of this paper is organized as follows. Section 2 contains a description of related work. Section 3 describes our scheme in details and in Section 4 we analyze the security of our solution. In Section 5 the implementation and usability of the solution is described and Section 6 is the conclusion.

II. Related Work

WBANs can inherit many mechanisms applied in WSNs because they consist of sensor nodes. Perrig et al. [10] present a set of protocols for achieving security requirements for sensor networks, SPINS. This set of security protocols has two secure building blocks: (i) SNEP (Secure Network Encryption Protocol) provides data confidentiality, two-party data authentication, and data freshness, with low overheads; and (ii) TESLA (the “micro” version of the Timed, Efficient, Streaming, and Loss-tolerant Authentication Protocol) provides authenticated streaming broadcast. Du et al. [11] present a scalable and flexible pairwise key pre-distribution scheme for WSNs. These solutions assume that sensor devices are loaded with some secret before their initial use. Also, these solutions are suitable for application in WSNs and not suitable for resource constrained WBANs.

Undercoffer et al. [12] present a novel scenario defining perimeter protection as an application class of sensor networks. They identify threats to this application class and propose and implement a new security protocol that operates in the base station mode of sensor communication. The main drawback of the proposed scheme is the need for using routing tables and for packet synchronization when a new node is added to the network.

Shaikh [13] et al.’s key management scheme requires the base station to provide public keys to the communicating nodes and the main drawback is frequent communication with the cluster head node which generates significant communication overheads.

Peak et al. [14] and Zhu et al. [15, 16] also propose key management scheme for WSNs. Common drawbacks of these solutions is their assumption that the network is safe during some initial time period and they are not designed for a scenario in which all nodes are in communication range of each other.

SHELL [17] and MUQAMI+ [18] are lightweight solutions for resource constrained sensor networks and they also avoid single point of failure in sensor networks. They are based on combinatorics and Exclusion Basis System (EBS) matrix [19]. Both these schemes are designed for large sensor networks and when applied to small body senor networks, their performances drop considerably.

Cherukuri et al. [20] present a scheme based on biometrics derived from human body itself for securing the keying material used for achieving security objectives. Miao et al. [21] propose a mixed mode of AES based biometrics cryptosystem for Body Area Sensor Network (BASN). The keys in the cryptosystem are generated from physiological signals and transmitted in a secure way. SEKES scheme [22] exploits physiological signal to address security issues in WBANs and manages the generation and distribution of symmetric cryptographic keys to constituent sensors in a WBAN and protects the privacy. The main drawback of these solutions is that they are applicable only to sensors that measure the same physiological signals.

Message-In-a-Bottle (MIB) enables a sensor network to establish a secret with a new node in the absence of prior shared secrets between the two parties [23]. MIB relies solely on the wireless communication interface, ensuring that this approach is applicable to any commodity wireless sensor node. Law et al. [24] propose a new practical and interoperable key management scheme for BSN, KALwEN. KALwEN is user-friendly in the sense that it requires no expert knowledge from a user, and instead only requires a user to follow a simple set of instructions when bootstrapping or extending a network. The main drawback of these solutions is that they need additional equipment as Smart Faraday Cage.

Perkovic et al. [26] propose a solution that allows an unaided user to initialize a relatively large number of wireless devices. The proposed solution is based on a multichannel Group message Authentication Protocol (GAP) in which information is transmitted over both a radio and Visible Light Channel (VLC). Li et al. [27] propose a lightweight scheme for secure sensor association and key management in BAN. A group of sensor nodes, having no prior shared secrets before they meet, establish initial trust through group device pairing (GDP), which is an authenticated group key agreement protocol where the legitimacy of each member node can be visually verified by a human.

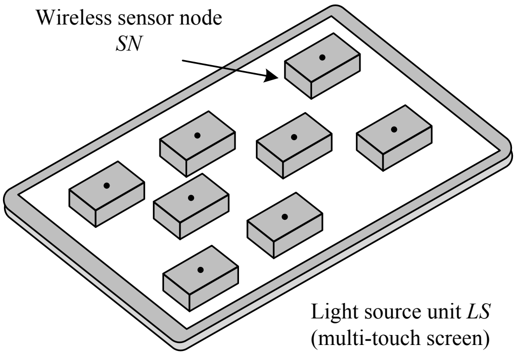

Fig. 1. Placing the sensor nodes on the multi-touch screen

Shi et al. [28] propose ASK-BAN, a lightweight fast authenticated secret key extraction scheme for intra-BAN communication. This scheme neither introduces any advanced hardware nor relies on out-of-band channels. To perform device authentication and fast secret key extraction at the same time, they exploit the heterogeneous channel characteristics among the collection of on-body channels during body motion. ASK-BAN utilizes the relatively static channels for device authentication and the dynamic ones for secret key generation and achieves authentication through multi-hop stable channels, which greatly reduces the false positive rate as compared to the existing work.

III. Scheme Overview

In this section we describe how our key deployment scheme can be used to distribute symmetric keys to the sensor nodes. LIRA scheme allows establishment of shared keys between sensor nodes *in a safe and user-friendly way* without any pre-shared secrets. In our protocol the light channel is used to transfer the keys and the radio channel to confirm their correct reception, and later for secure communications. Our key transmission and verification protocol is based on ISO/IEC 9798-2 three-pass mutual authentication protocol [30]. This protocol is modified to include the communication over a light channel.

A. Key transmission over a visible light channel

Key transmission process over a visible light channel is described below. The user places the sensors nodes on the screen (*LS*) and powers them on so that they can measure the screen intensity with their light sensor (Fig. 1). The multi-touch screen during this process determines the position of the sensor nodes on the screen and their total number. The sensor initialization process is shown in Fig. 2. After sensor recognition process *LS* generates the master secret key K_C by using a pseudorandom number generator (PRG). Then pseudorandom function (*PRF*) is applied to K_C to derive the keys $K_1,K_2,...,K_i,...,K_n$ for all sensor nodes, Fig. 3 (a).

Deriving the internal key for the sensor node SN_i from the master key is implemented as $K_i = PRF(K_C,ID_i)$. All keys derived in this manner are computationally independent since *PRF* function has strong one-way properties (e.g. MAC) [10]. Even if an attacker captures one sensor node *j* and finds its key K_j, that would not help him to determine the master secret key K_C or any other key $K_i \neq K_j$.

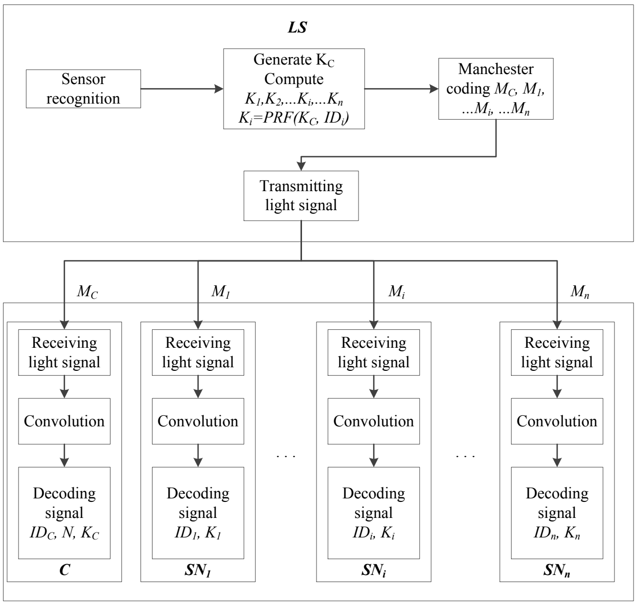
LS
Sensor recognition
Generate K_C Compute K_1,K_2,...K_i,...K_n K_i=PRF(K_C, ID_i)
Manchester coding M_C, M_1, ...M_i, ...M_n
Transmitting light signal
M_C
M_1
M_i
M_n
Receiving light signal
Convolution
Decoding signal ID_C, N, K_C
C
Receiving light signal
Convolution
Decoding signal ID_1, K_1
SN_1
. . .
Receiving light signal
Convolution
Decoding signal ID_i, K_i
SN_i
. . .
Receiving light signal
Convolution
Decoding signal ID_n, K_n
SN_n

Fig. 2. Transmission of messages over a visible light channel

When the key generation process is finished the screen emits messages $M_C,M_1,M_2,...,M_i,...M_n$ via light signals under each sensor node $C,SN_1,SN_2,...,SN_i,...SN_n$, respectively. These light signals are coded in the form of small white squares representing bit "1" and black squares representing bit "0" (on-off keying modulation).

A message M_C which is transmitted to body control unit *C* has the following format, as illustrated in Fig. 3(b): its identity ID_C, the number of nodes in the network *N* and 128-bit master key K_C. Fig. 3(c) also shows the format of messages transmitted to other sensor nodes and consists of three fields: the sensor node identity ID_i, *C*'s identity ID_C and 128-bit sensor node key K_i that is derived from K_C. The messages transmitted over light channel are formed as logical "zeros" and "ones" that are encoded using Manchester code where sequence "01" represents 0, and a sequence "10" represents 1.

Fig. 4 shows the main components of a sensor node used in our implementation. To receive the message, sensor nodes read the light levels (by photodiodes). Next, a convolution function is applied to the samples to recover the bits at the receiver. Finally the Manchester decoding is applied to get the original messages and extract relevant information ID_C, *N*, K_C and ID_i, ID_C, K_i , respectively.

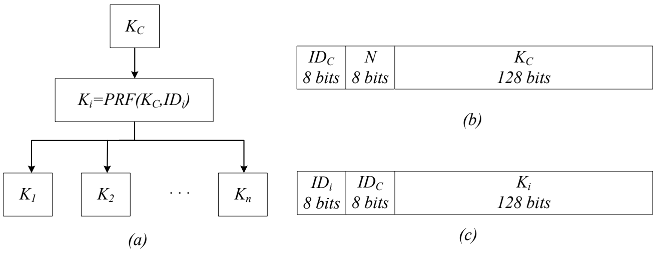

Fig. 3. Structure of (a) keys, (b) message M_C transmitted to the body control unit, (c) message M_i transmitted to the i-th sensor

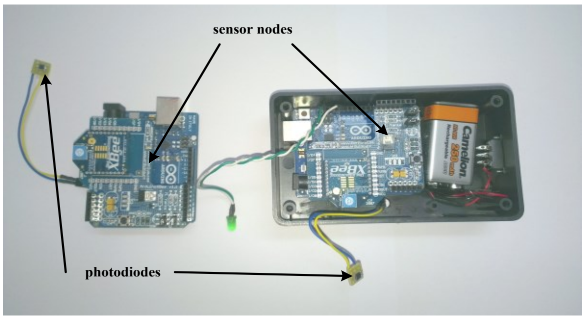

Fig. 4. Wireless sensor nodes used in our implementation

B. *Key verification over a radio channel*

The radio channel is used to confirm correct reception of the key because the light channel is unidirectional. For this reason ISO/IEC 9798-2 three-pass mutual authentication protocol is used, Fig. 5. Body control unit *C* generates a 128-bit pseudorandom number N_{Ai} and broadcasts a message consisting of the node identifier ID_i (starting from the smallest to the largest) and N_{Ai}.

The sensor nodes listen to the radio channel and when they receive the broadcast packet they check the message ID_i with their own *ID*. If these *IDs* match, i-th sensor node SN_i generates a 128-bit pseudorandom number N_{Bi}, and then sends message $m=N_{Bi},N_{Ai},ID_C$ together with $MAC_{Ki}(m)$ back to *C*.

On receipt, body control unit *C* computes the MAC from the message using K_i which is computed from the sensor node identifier ID_i and K_C. If *C* is able to correctly verify received $MAC_{Ki}(m)$, N_{Ai} and ID_C it knows that SN_i received correct key K_i. To inform sensor node SN_i that the key is correct *C* sends concatenation $N_{Ai},N_{Bi},MAC_{Ki}(N_{Ai},N_{Bi})$ to SN_i.

When the message is received sensor node SN_i computes the MAC. If sensor node SN_i is able to verify received $MAC_{Ki}(N_{Ai},N_{Bi})$ and N_{Bi}, sensor node SN_i knows that it shares a secret key with *C*. Body control unit *C* repeats this protocol with all sensor nodes in the network.

IV. Brief Security Analysis

To ensure security of the overall system WBAN must be protected, e.g., against eavesdropping, injection and modification of packets, and physical attack. During the sensor initialization process each area of the screen which emits light signal is covered by a sensor node to prevent simple attacks like the attacker looking at the screen and getting the key. Also to prevent this attack around each area of the screen there is a larger area that emits random light signal (noise). The case when an attacker captures and analyzes side channels, e. g., RF signals from video card, is out of scope in this paper because we assume the initialization process takes place in a controlled environment (in our model it is very difficult to perform this attack).

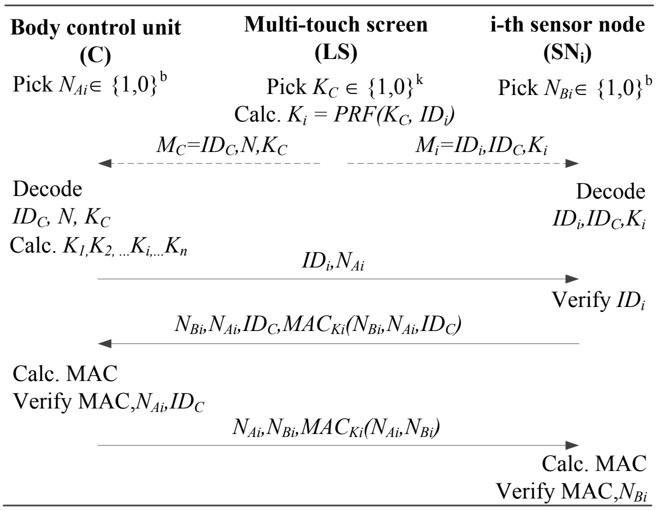
Body control unit (C)
Multi-touch screen (LS)
i-th sensor node (SN_i)
Pick $N_{Ai} \in \{1,0\}^b$
Pick $K_C \in \{1,0\}^k$
Calc. $K_i = PRF(K_C, ID_i)$
Pick $N_{Bi} \in \{1,0\}^b$
$M_C=ID_C,N,K_C$
$M_i=ID_i,ID_C,K_i$
Decode
ID_C, N, K_C
Calc. $K_1,K_2,\dots K_i,\dots K_n$
Decode
ID_i,ID_C,K_i
ID_i,N_{Ai}
Verify ID_i
$N_{Bi},N_{Ai},ID_C,MAC_{Ki}(N_{Bi},N_{Ai},ID_C)$
Calc. MAC
Verify MAC,N_{Ai},ID_C
$N_{Ai},N_{Bi},MAC_{Ki}(N_{Ai},N_{Bi})$
Calc. MAC
Verify MAC,N_{Bi}

Fig. 5. Complete key deployment scheme. The dashed arrow indicates a transmission over the secure light channel.

Protection against eavesdropping of the radio channel can be easily achieved by encrypting messages with the established keys. Therefore an adversary may capture the information, but they are encrypted. To perform an active attack, attackers can inject their own packets in the radio channel, but the data sent to some of the nodes would be invalid, and the node discards them. If an attacker has come into possession of an initialized sensor node, it opens up the possibility of a physical attack. The secret key is stored somewhere in the memory of the sensor nodes and if the attacker has sophisticated equipment, this key can be withdrawn from the memory. Against this type of attack there is not a completely secure solution. However if the attacker has come into possession of one sensor node, the other nodes are not threatened because of the properties that each node has a different encryption key. This means that the damage from this kind of the attack is minimal. We have to state that the body control unit is specially protected (tamper-resistant) because compromising the body control unit can render entire sensor network unsecured and useless (if this happens an attacker can find out the keys of all sensor devices in the network).

V. Implementation And Usability Tests

Implementation details. The body control unit and sensor nodes in our solution are implemented on commercially available Arduino Uno platform based on: ATmega328, 32 KB flash memory, 2 KB SRAM, 1 KB EEPROM and 16 MHz clock speed. Also we use ZigBee radio (Xbee S2 module), BPW34 photodiodes and RGB LEDs, Fig. 4. In our experiments we emulate a multi-touch screen monitor using an 22-inch LCD screen, a camera that is connected to the computer and located above the screen for screen monitoring and sensor detection, the application that is responsible for keys generation to each node and their broadcast in the form of the light.

For the transmission through the light channel bit rate is limited by the screen frame rate (16.66 milliseconds per frame for a standard 60 Hz LCD screen). In our implementation we use 20 bps Manchester encoded to avoid errors. The message sizes are 288 Manchester encoded bits for both the body control unit (M_C) and for regular sensor nodes (M_i). This means that it takes 14.4 seconds to transfer a message over the light channel.

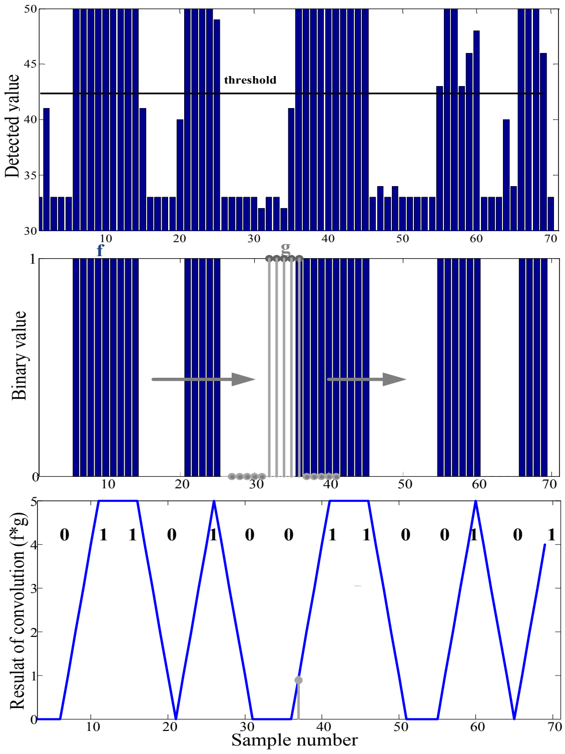

Fig. 6. Received light signal and the result of applying convolution

At the reception side, sensor nodes read light levels every 10 milliseconds. Since every bit lasts 50 milliseconds it means that there are 5 samples for every bit transmitted through the light channel. Fig. 6 shows an example of the received light signal. We set a threshold above which each received sample is converted into a binary 1 and below as a binary 0. To detect the received bits a convolution function is applied over the newly formed series (*f*) of “zeros” and “ones” and the delimiter (*g*) with mask {0,0,0,0,0,1,1,1,1,1,0,0,0,0,0} [31]. Upon applying this function data arrays containing values ranging from 0 to 5 are obtained, where elements with extremes 0 and 5 are decoded as bits 0 and 1, respectively. Plateaus areas are decoded as double 0s and 1s, depending on their values (0 or 5). Finally the Manchester decoding is applied to get the original bit-stream. Due to the Manchester encoding our solution is highly robust to de-synchronization effects and also frame loss during transmission via VLC does not affect correct bit recognition in any way.

Please note that the time required to initialize a certain number of sensor nodes over a light channel is fixed. This time does not depend on the number of sensor nodes to be initialized and is only determined by the characteristics of the screen. The key verification process through the radio channel scales linearly with the number of sensor nodes.

Usability test. To check the usability goals of our solution we have run the following tests. Besides LIRA solution we prepared another one in which the wireless sensor devices are initialized using an USB cable (the "cable" solution). In LIRA solution, the user’s task was to place the sensor nodes on *LS*. Then the user had to start the sensor initialization process and wait for the end of the process, which was signaled by LED lights. When testing the "cable" solution, WBAN was initialized by connecting the sensor nodes with the base station using an USB cable and loading them with the secret information. We evaluated both the users’ ability to complete the test procedures for WBAN initialization and their satisfaction. A total of 26 participants took part in the usability tests. Each tester performed tests 3 times with a group of 3 and 9 sensor devices for both solutions. A total number of 312 test cases was performed (3 x 26 x 2 x 2 = 312).

TABLE I. THE TESTERS’ INFO

Age		Sex		Using SP or TS devices		Familiar with TS technology (years)			
18-25	>25	M	F	Yes	No	0-1	1-2	2-3	>3
15	11	19	7	26	0	2	5	8	11

Using SP or TS devices (hours/week)				Familiar with the VLC concept		Have you ever used device pairing?	
0-5	5-20	20-30	>30	Yes	No	Yes	No
8	6	6	6	5	21	23	3

SP – Smartphone TS – Touchscreen

TABLE I summarizes the testers’ demographic info as well as information about using smart phones and touchscreen devices. The testers were given a short introduction which involved the description of our solution, possible applications and a video showing set-up procedure for our test cases.

Fig. 7 shows completion time in seconds for our test cases. On the basis of the measured time we calculated the total average time required for the successful initialization of 3 and 9 sensor devices for both solutions. It was 29.87 (std. = 4.25) and 51.21 (std. = 7.62) seconds for LIRA and 37.00 (std. = 8.93) and 98.72 (std. = 13.22) seconds for the "cable" solution. This average time was calculated for all 78 test cases per each group of the sensor devices. The increase in time required to initialize a certain group of the sensor nodes (3 and 9 sensor devices) relates purely to manipulation costs - the user should place all the sensor devices on *LS* or connect the cable into them. These results also show that the process of WBAN initialization with a large number of sensor devices is much faster using LIRA solution than the "cable" solution.

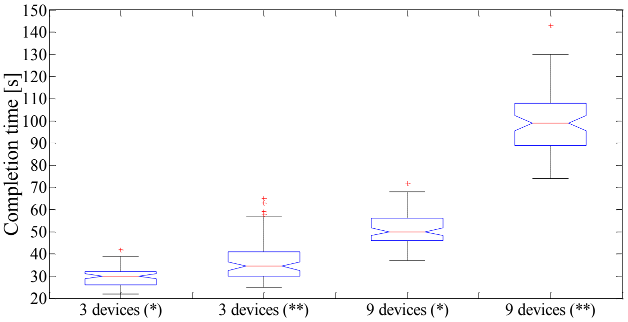

Fig. 7. Time-to-completion for successful WBAN initialization; (*) – LIRA solution, (**) – the "cable" solution

At the end of the usability tests the users were asked to fill in the post-test questionnaires for both solutions. For the global assessments of our solutions usability we used the System Usability Scale [32] questionnaires. The SU-scores were 87.05 for LIRA and 70.68 for the "cable" solution. These results show that the users prefer LIRA solution and that it was very easy to use. More thorough tests are underway.

VI. Conclusion

In this work we designed and implemented a key deployment system for WBANs that is very practical and easy to use. Our key deployment scheme requires no public key cryptography and requires almost no computation from the sensor node with very little involvement of the end user.

The scheme was implemented in Arduino Uno platform and we have shown through experiments that our solution has a good performance, scales linearly with the number of sensor nodes in the network and is easy to use.

The main part of our future work will be in the implementation of public key cryptography to deploy the initial key in the presence of a very strong attacker.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Technical Report CLOUDS-TR-2012-2, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, 29 June 2012.

[2] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, “Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?,” 1st International Workshop on the Security of the Internet of Things (SecIoT'10), Tokyo, 2010.

[3] L. Benoit, B. Braem, I. Moerman, C. Blondia, and P. Demeester, “A Survey on Wireless Body Area Networks,” Wireless Networks, pp. 1–18, 2011.

[4] Future Vision. http://www.microsoft.com/office/vision/, last access, July, 2013.

[5] Interactive kitchen worktops, screens that take up entire walls and touchscreens as desks: Microsoft reveals what the home and office of the future will look like. http://www.dailymail.co.uk/sciencetech/article-2289770/Microsoft-reveals-home-office-future-like.html, last access, July, 2013.

[6] Today’s Phones and Tablets Will Die Out Like the PC. www.technologyreview.com/view/516486/todays-phones-and-tablets-will-die-out-like-the-pc/, last access, July, 2013.

[7] D. Nowacka, K. Ladha, N. Y. Hammerla, D. Jackson, C. Ladha, E. Rukzio, P. Olivier, “Touchbugs: Actuated Tangibles on Multi-Touch Tables,” CHI 2013, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 759-762

[8] T. Vu, A. Baid, S. Gao, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, J. Walling, “Distinguishing Users With Capacitive Touch Communication,” Mobicom '12 August 22-26, 2012, Istanbul.

[9] Visible Light Communication: Tutorial, doc.: IEEE 802.15-<08/0114-02>, http://ieee802.org/802_tutorials/2008-03/15-08-0114-02-0000-VLC_Tutorial_MCO_Samsung-VLCC-Oxford_2008-03-17.pdf

[10] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, “SPINS: Security Protocols for Sensor Networks,” In Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001; pp. 189-199.

[11] W. Du, J. Deng, Y. S. Han, and P. Varshney, “A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks,” In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS’03), pp. 42–51, 2003.

[12] J. Undercoffer, S. Avancha, A. Joshi and J. Pinkston, “Security for Sensor Networks,” In Proc. of CADIP Research Symposium, 2002.

[13] R. Shaikh, S. Lee, M. Khan, Y. Song, “LSec: Lightweight Security Protocol for Distributed Wireless Ssensor Networks,” In Proceedings of the 11th IFIP International Conference on Personal Wireless Communications (PWC’06), Albacete, Spain, September 20–22, 2006; Volume 4217, pp. 367–377.

[14] K.J. Paek, J. Kim, C. S. Hwang, U. S. Song, “An Energy-Efficient Key Management Protocol For Large-Scale Wireless Sensor Networks,” In Proceedings of the 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE’07), Seoul, Korea, April 26-28, 2007, pp. 201–206.

[15] S. Zhu, S. Setia, S. Jajodia, “LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” ACM Trans. Sen. Netw. 2006, 2, pp. 500–528.

[16] S. Zhu, S. Setia, and S. Jajodia. “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Nnetworks,” In CCS 2003: Proceedings of the 10th ACM conference on Computer and communications security, pp. 62-72, October 27-30 2003. ACM.

[17] M.F. Younis, K. Ghumman, M. Eltoweissy, “Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks,” IEEE Trans. Parallel Distrib. Syst. 2006, 17, pp. 865–882.

[18] S.M.K. Raazi, H. Lee, S. Lee, Y.K. Lee, “MUQAMI+: A Scalable and Locally Distributed Key Management Scheme for Clustered Sensor Networks,” Annals Telecommun. 2010, 65, 101–116.

[19] M. Eltoweissy, M. H. Heydari, L. Morales, I. H. Sudborough, “Combinatorial Optimization of Group Key Management,” Journal of Network and Systems Management, Vol. 12, No. 1, March 2004.

[20] S. Cherukuri, K. K. Venkatasubramanian, S. K. S. Gupta, “BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body,” Proceedings of the 2003 International Conference on Parallel Processing Workshops, ICPPW 2003.

[21] F. Miao, L. Jiang, Y. Li, Y. Zhang, “AES based Biometrics Security Solution for Body Area Sensor Networks,” Bulletin of Advanced Technology Research, Vol. 3 No.4 / Apr. 2009.

[22] M. Mana, M. Feham and B. A. Bensaber, “SEKES (Secure and Efficient Key Exchange Scheme for wireless Body Area Network),” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, pp. 305 – 314, November 2009.

[23] C. Kuo, M. Luk, R.Negi, A. Perrig, “Message-In-a-Bottle: User-Friendly and Secure Key Deployment for Sensor Nodes,” Proceedings of the ACM Conference on Embedded Networked Sensor System (SenSys) 2007

[24] Y. Law, G. Moniava, Z. Gong, P. Hartel, and M. Palaniswami, “Kalwen: A New Practical and Interoperable Key Management Scheme for Body Sensor Networks,” In BodyNets ’09, April 1-3 2009.

[25] F. L. Wong, F. Stajano, “Multi-channel Protocols for Group Key Agreement in Arbitrary Topologies,” Pervasive Computing and Communications Workshops, 2006.

[26] T. Perković, M. Čagalj, T. Mastelić, N. Saxena, and D. Begušić, “Secure Initialization of Multiple Constrained Wireless Devices for an Unaided User,” IEEE Transactions on Mobile Computing 2012.

[27] M. Li, S. Yu, W. Lou, K. Ren, “Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks,” IEEE INFOCOM ’10, Mar. 14-19 2010, pp. 1–9

[28] L. Shi, J. Yuan, S. Yu, M. Li, “ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area -Networks,” WiSec ’13, April 17-19, 2013, Budapest, Hungary, pp. 155-166

[29] Y. Hou, M. Li, and J. D. Guttman, “Chorus: Scalable In-band Trust Establishment for Multiple Constrained Devices over the Insecure Wireless Channel,” WiSec ’13, April 17-19, 2013, Budapest, Hungary.

[30] C. Boyd, A. Mathuria, “Protocols for Authentication and Key Establishment,” Springer, 2003.

[31] T. Perković, “User Friendly Authentication Mechanisms in User-to-Device and Device-to-Device Interactions,” Doctoral Thesis, Split 2013.

[32] J. Brooke, “SUS: A Quick and Dirty Usability Scale,” In Usability Evaluation in Industry, London 1996.