CHAPTER

6.3

Trust Establishment in Wireless Body Area Networks

Shucheng Yu[1], *Ming Li*[2], *and Lu Shi*[1]

[1]**University of Arkansas at Little Rock, Little Rock, Arkansas, USA,**
[2]**Utah State University, Logan, Utah, USA**

1. INTRODUCTION

In recent years, WBAN technology has been increasingly applied in the healthcare domain. A number of medical devices, wearable or implantable, are integrated into WBANs to monitor patients' health status, treat patients with automatic therapies, and so on and so forth. Such WBAN devices include pacemakers, implantable cardioverter defibrillators (ICDs), implantable drug pumps, ECG/EMG/EEG monitoring devices, etc. Today there are over 3 million pacemakers and over 1.7 million ICDs in use according to recent research [1]. Other applications of WBAN extend to sports, military, or security. With the popularity of WBAN applications, however, great privacy and security risks about WBAN devices exist, which may hinder the wide adoption of WBAN technology in real life scenarios. These risks include the possibility of exposing sensitive personal information, wireless hijack attacks in which attackers manipulate physiological data or commands transmitted between legitimate devices, the vulnerability to physical device compromise attacks or replacement of WBAN devices, etc. In order to address these risks, fundamental security mechanisms shall be in place such that each WBAN device has the confidence that it is communicating with legitimate peers, and every physiological measurement or command is sent to authentic WBAN device(s) without being modified or overheard by unintended parties. To this end, it is important to design secure and practical security mechanisms that allow WBAN devices to authenticate each other (i.e., verify that each device is valid and trustworthy) and establish secret key(s) (i.e., generate shared cryptographic key(s)) for protecting the subsequent communications. Major challenges exist with establishing secure communications in WBAN mainly due to the following factors: 1) resource-constrained or heterogeneous WBAN; 2) users lacking the expertise to conduct complex operations for security bootstrapping; and 3) compatibility with billions of commercial-off-the-shelf WBAN devices that have been on the market already. This chapter reviews state-of-the-art techniques of WBAN security.

2. WBAN DEVICE AUTHENTICATION TECHNIQUES

Among various security measures, authentication is the fundamental step towards the initial trust establishment (e.g., key generation) and subsequent secure communications in WBANs. With effective authentication, attackers will fail to pretend to be valid sensor nodes and join the WBAN for private information-involved communication, thereby avoiding either wrong reports or false commands by attackers, which may put the patient's safety at risk. Unfortunately, WBAN devices are not designed with enough security considerations in current practices. The situation might be more severe for healthcare applications involving patient information in which the lack of security solutions has been shown to result in the possibility of fatal consequences. In [2], researchers utilized wireless access to steal personal information from a common cardiac defibrillator, and demonstrated that fatal heart rhythms can be induced. In [3,4], the dosage levels of an insulin pump were remotely adjusted by hackers with knowledge of the pump's serial number, which could kill the patient wearing the pump. Being aware of the data privacy or security risks, the FDA has begun to urge manufacturers to tighten security measures on wireless medical devices [5]. Therefore, an effective node-authentication mechanism is the key to WBAN's security and user safety.

Although great efforts have been made on authentication in wireless networks, the same issue remains a challenge in WBAN due to its unique features and stringent application-level requirements. Conventionally, authentication is achieved based on predistributed secret keys among sensor nodes in a network. Such key distribution in wireless sensor networks (WSNs) is extensively described in the literature [6−11]. However, if this method is directly applied to a WBAN, end-users are required to trust the entire chain of the distribution process, in which untrustworthy users may be involved to hamper the trust establishment or even launch attacks. In addition, general users of WBAN devices are expected to have little knowledge of the WBAN technology, implying that high usability, i.e., ideally "plug-and-play," is desired. To be specific, the authentication process should be simplified, automatic, and transparent to users. Thus, it is highly desirable that in WBANs node trustworthiness is established and evaluated without assuming any prior security context among nodes.

Since WBAN devices are ubiquitous, they are likely to be physically compromised. Consequently, pre-shared secret materials in the devices, e.g., keys, may be disclosed to attackers. This would allow attackers to disguise themselves as legitimate sensor nodes in the network and further render traditional cryptographic authentication mechanisms ineffective. From this aspect, node authentication mechanisms in WBAN should have minimal reliance on cryptography.

Finally, resources, such as hardware, energy, and user interfaces, are extremely limited for low-end WBAN sensor devices. This imposes additional requirements on authentication mechanisms in terms of communication and computation costs. Moreover, most of the existing non-cryptographic authentication mechanisms require advanced hardware such as multiple antennas [12], or significant modifications to the system software. It is important to note that hardware requirements should be minimized in the WBAN, not only because of extra cost but also due to compatibility with legacy systems.

The following sections review cryptographic and non-cryptographic authentication mechanisms in WBANs, respectively.

2.1 Cryptographic Authentication Mechanisms in WBAN

In this section, cryptographic authentication mechanisms in WBAN are investigated according to the type of cryptography. Existing crypto-based authentication schemes can be classified into the following categories: symmetric key-based (SKC-based) authentication and public key-based (PKC-based) authentication. While the high computational cost of asymmetric cryptography makes symmetric encryption the more viable option, key-distribution in symmetric encryption is challenging.

2.1.1 Symmetric Key-Based Authentication

As an efficient choice for distributed access control in WBANs, symmetric key-based authentication relies on the trust establishment by the prior security context [13–17]. By predistributing key materials, a pairwise key can be easily generated between the user and any authorized entity. And then authentication can be implemented by using the authentication key.

However, SKC-based authentication schemes suffer from several disadvantages [18]. First, since compromised nodes are harmful to the system, it is desirable to detect and revoke compromised nodes in a timely fashion. For most schemes, either high computational overhead or complex key management in the revocation of nodes is involved; therefore it is difficult to achieve fine-grained access control. Second, such schemes are subject to user collusion in which attackers collude to exchange and derive keys and other sensitive information, or exhibit agreed-upon behavior in the authentication process. Finally, if a WBAN device is compromised physically, the data and prior security context stored in it will possibly be exposed to unauthenticated users.

It is also noteworthy that there exist alternatives to SKC-based authentication that do not assume preshared secrets and additional hardware devices, while enjoying higher usability [19,20]. For example, the group device pairing in [19] allows a group of WBAN devices to establish a common group key based on symmetric key cryptography. Each device authenticates itself to the whole group as a valid member by visually human-aided verification. However, the group device pairing technique assumes the existence of an additional out-of-band (OOB) secure channel to facilitate human-aided verification, which may not be intuitive to use.

To avoid the above issues, [21] proposed lightweight source and data authentication schemes in a routing framework for WBANs by utilizing hash-chain techniques. Since source authentication requires decryption operations, it is much more costly than data authentication only with equality checks involved. Therefore, source authentication is disabled if the neighbor set is not changing based on the prediction results. However, according to [21], source authentication only achieves 70% accuracy in terms of filtering false requests.

2.1.2 Public Key-Based Authentication

Among public key-based authentication schemes, attribute-based encryption (ABE) and identity-based encryption (IBE) are the most common techniques.

ABE achieves flexible one-to-many encryption based on attributes. The decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext [22]. In this way, only a group of users satisfying a certain access protocol can read the ciphertext. A crucial security feature of ABE is collusion-resistance, so any user key cannot be derived by collusion. The features of ABE make it a good candidate for authentication in WBANs.

Ciphertext policy ABE was proposed in [23] to provide role-based access control on encrypted data in WBANs. The secret is split among secret key components belonging to different attributes owned by a user to provide collusion resistance. By employing ciphertext policy ABE, [24] proposes the primitive functions to implement a secret-sharing scheme, which provides message authenticity. In [25,26], ABE was exploited to secure the communications between a WBAN and its external users. While [26] achieved secure communication between the data controller and an external user by fuzzy ABE, [25] utilized the basic ABE to self-protect electronic medical records (EMRs) on mobile devices and offline communications.

Besides ABE, IBE has also been actively studied and widely applied in cryptography research in which the user's public key carries unique information about the user's identity in the form of an ASCII string. One common feature of the IBE-based schemes is that no prior trust/key predistribution is required between individual users. Conventional IBE primitives are computationally demanding and cannot be efficiently implemented on sensor devices in WBAN. To solve this problem, [27,28] proposed a lightweight IBE-based access control scheme to balance security and privacy in WBANs, which was built upon elliptic curve cryptography (ECC). The limitation of [27,28] is that the master secret key becomes vulnerable to compromise if more than a limited number of secret keys are released. The Boneh—Franklin IBE algorithm was applied in [29] to achieve a faster authenticated key establishment and encryption scheme for WBANs with less energy consumption and optimal memory requirement.

However, it is important to note that a trusted certificate authority, called the private key generator is involved with private key generation, and it is capable of decrypting messages without authorization. Therefore, the private key generator must be highly trusted. If the private key generator is compromised, all the messages protected by the public-private key pairs are also compromised, which makes the generator a target to attackers.

2.2 Non-Cryptographic Authentication Mechanisms in WBAN

From another perspective, non-cryptographic methods provide an alternative way of authentication without key predistribution and non-intuitive user participation. In addition, most non-cryptographic schemes have simpler protocols with less complicated computation. In general, current non-cryptographic authentication mechanisms are mainly divided into the following categories based on type of techniques: biometric-based authentication, channel-based authentication, proximity-based authentication, and a combination of authentication schemes.

2.2.1 Biometric-Based Authentication

Since security context in traditional authentication methods can be easily stolen, shared, or forged, biometric systems are explored to provide more reliable authentication with unique traits physically linked to the user. Common traits include anatomical traits such as fingerprint, iris, electrocardiogram (EEG), etc., and behavioral traits such as signature, gait, etc. To assist authentication, physiological values of a biometric trait are measured using appropriate sensors, and features are extracted from the measurements to create a template stored in the system database. When a user device is to be authenticated, its current corresponding physiological values are compared with the template to verify the identity [12,30]. Physiological values of the same biometric trait can also be collected and compared at sender and receiver sides located on different body parts. To achieve better security, instead of a static template, [31] extracted the time-variant features from the ECG signals, which then were used for message authentication. Common accelerometer data extracted from body motion was used for authentication in [32], but specialized sensing hardware was required for every sensor.

Although these methods do not rely on preshared secrets, biometric-based authentication is vulnerable in two aspects. First, it is hard for body sensors in different positions to measure the same physiological signal with the same accuracy. Second, a spoof attack may occur using a counterfeit biometric trait that is not obtained from a live person, e.g., a gummy finger, photograph, or mask of a face, or even a dismembered finger from a legitimate user.

2.2.2 Channel-Based Authentication

Recently, there has been an increasing interest in exploring received signal strength (RSS) measurements for authentication [33–35]. Generally, RSS values tend to vary over time due to mobility and channel environments. Channel-based solutions leverage such RSS variations to achieve authentication in a different way. Zeng et al. [36] proposed to compare the lists of temporal RSS variation to handle identity-based attacks, where an intruder trying to impersonate another user B that is communicating with A can be detected by A. To protect communication between two devices, the secure device-pairing scheme proposed in [35] utilizes differential RSS to perform proximity detection for limiting malicious senders by distance, but the proposed method required additional hardware – at least two receiver antennas. In addition, the use of RSS in authentication can be compromised by adversaries with array antennas that can launch a beam-forming attack to spoof location. In other words, by sending different signal strengths in the directions of different access points, an attacker attempts to appear similar to another node instead of its own actual location. Furthermore, a link's RSS can be eavesdropped.

In addition to utilizing RSS, other channel-based authentication schemes build a signature for each device's wireless channel. For example, the temporal link signature in [37] uses channel impulse response (CIR) information to uniquely identify the link between a transmitter and a receiver. Then, if an attacker at a different location pretends to be the transmitter, the change in the physical channel will be detected due to link distinction. It is also difficult to infer the link signature measurements from interactions between nodes. But this method requires a learning phase and advanced hardware platforms such as GNU radio.

2.2.3 *Proximity-Based Authentication*

Several proximity-based authentication schemes are based on co-location detection. Amigo in [38] extended the Diffie−Hellman key exchange with authentication of co-located devices. Specifically, after a shared secret is derived by Diffie−Hellman key exchange, both devices monitor the radio environment for a short period of time and exchange a signature including its RSS of that environment with the other device. Then at each device, similarity detection between the received signature and its own signature is performed independently to determine proximity. Ensemble technique [34] provides proximity-based authentication by monitoring the transmissions and analyzing RSS. Similarly, to securely pair wireless devices in proximity with one another, Mathur et al. [39] proposed a co-location based pairing scheme by exploiting shared time-varying environmental signals that were used to generate a common cryptographic key for the devices authenticating each other's physical proximity for further confidential communication. However, the main drawback of the methods in [34,38,39] is that the devices are required to be within a half wavelength distance of each other, which is restrictive for sensor devices deployed in a WBAN.

Other methods exploit secure ranging techniques, such as distance bounding [40], to determine a device's proximity. For example, in [41], based on ultrasonic distance bounding, an implanted medical device can limit access to its resources only to devices that are in its close proximity. But the common concern with the RF distance bounding technique is that specialized/advanced hardware must be involved; otherwise high accuracy cannot be achieved. Although [42] proposed the first design of RF distance bounding that can be realized fully using a wireless channel, it requires multi-radio capabilities and additional hardware, which may not be available on general WBAN devices, especially legacy devices.

2.2.4 *Other Authentication Schemes*

To distinguish legitimate WBAN devices on/near body from imposters, [43,44] propose a channel-based and proximity-based authentication scheme − BANA − based on the observation that an off-body attacker has obviously distinct RSS variation behavior with an on-body sensor. The advantage of BANA lies in the fact that it is simple, lightweight, and does not require any additional hardware, but still promises effectiveness, efficiency, and applicability in real-life scenarios. It is important to note that body movements are required in BANA to obtain unique channel characteristics for authentication.

2.3 Summary of Authentication Methods

Due to unique characteristics of WBANs, effective and efficient authentication techniques are required to guarantee security and privacy in WBAN applications.

Table 1 provides a summary of current authentication schemes in WBANs. Each cryptographic or non-cryptographic authentication scheme has its pros and cons, which also imply potential for improvement. Cryptographic authentication schemes may be best suited to the nature of self-deployable WBANs, but they generally suffer from extensive computation and rely on pre-shared secrets that may be disclosed to unauthorized users if

TABLE 1 Summary of current authentication methods in WBAN

	Comparison Criteria	**Cryptographic Authentication based on:**		**Non-Cryptographic Authentication based on:**		
		SKC	**PKC**	**Biometric**	**Channel**	**Proximity**
Security	Preshared Secrets	Yes	Partial	No	No	No
	Vulnerability	Key management, collusion, physically compromise	PKG must be highly trusted	Forging biometric trait	Beam forming attack, location spoof attack	
Usability	Human Interaction	Partial	No	Yes	Partial	Partial
Cost	Additional Hardware	No	No	Require specialized sensing hardware	May require	May require
	Other Requirements	May require OOB channel	N/A	Consistent physiological signal	Channel reciprocity	Within half wavelength distance

physically compromised. With the development of biometric techniques and comprehensive study of channel characteristics, authentication schemes based on non-cryptographic methods are substantially explored. Complex, but distinguishable, human body characteristics provide an ideal way for authentication, but they also raise user privacy concerns. Wireless channels are also complicated and difficult to predict, and greatly affected by environment interference, so the performance of channel based-authentication schemes is subject to channel conditions. In proximity based-authentication schemes, WBAN devices must be in close proximity to be authenticated, but location spoof by attackers could undermine security. While prior secret is no longer necessary in non-cryptographic solutions, there may exist extra requirements to implement them in real-life scenarios, such as advanced hardware, human involvement, etc.

Different levels of security should be considered in authentication schemes. For example, in healthcare applications, life-threatening requests shall be distinguished from others and given highest security priority. Appropriate privacy-protection measures are needed along with authentication.

3. SECRET KEY ESTABLISHMENT IN WBAN

In order to protect the physiological data and the command messages transmitted in WBAN, a secret key shall be established between WBAN devices. One straightforward approach for key establishment is to preload shared secret keys in the devices prior to WBAN deployment. In practice, however, this approach may fail due to the following factors: first, devices in the same WBAN can be made by different manufactures and preloading the same secret keys to these devices at the time of manufacturing is impractical; second, it is impractical for general WBAN users who may lack the necessary expertise to load secret keys to WBAN devices; third, WBAN devices may lack the necessary interface (such as USB) for loading the keys, especially for miniature devices; last but not least, preloading the same secret keys will put the entire WBAN under threat once one of the WBAN devices is compromised. Considering practical WBAN applications, a body of research has been focusing on establishing secret keys for WBAN on the fly based on various resources such as biometric signal of the patient, patient's body motion, wireless channel characteristics, etc.

3.1 Secret Key Establishment Based on Biometrics or Motion

Many schemes have been proposed to measure and compare physiological information collected by the sensors, such as electrocardiogram (ECG), photoplethysmogram (PPG), iris, and fingerprint, to assist authentication and key establishment without a priori distribution of keying material. For key generation combined with authentication, schemes in [45–48] establish physiological data-based keys between devices for verification. For example, [45] proposes to use a secure environmental value as the source of random secret key information. Specific examples of secure environmental value include physiological data such as inter-pulse-interval (IPI) and heart rate variability. Secret keys can be extracted from ECG data measured by on-body ECG sensors [48–50] or a combination of PPG and ECG signals [46]. Physiological variables such as blood glucose, blood pressure, temperature, etc., were considered in [47] to obfuscate an arbitrary secret key for securing data. Due to their uniqueness, randomness, and time-sensitiveness, physiological data can act as the dependable source for both device authentication and secret key extraction. The major drawback of biometric-based techniques, however, is that the biometrics derived from physiological features are usually accompanied with high degrees of noise and variability inherently present in the signals. It is also difficult to guarantee consistent physiological signal measurements with the same accuracy for sensors located in different positions on the human body. Moreover, not all the physiological parameters have the same level of entropy for key generation. According to [51], for example, heart rate is not a good choice because its level of entropy is not satisfactory.

Schemes in [32,52,53] exploited the movement patterns when shaking devices together for authentication, and generated shared secret keys based on the measured acceleration data in the shaking process. Similar to biometric-based methods, these schemes require specialized sensing hardware and human participation.

3.2 Secret Key Establishment Based on Wireless Channel Characteristics

Use of a wireless channel for authentication and/or key generation has been of great interest recently [54,55]. One of the key research topics in this area is improvement of the key generation rate. Lai et al. [56] exploited the random channels associated with relay nodes in the wireless network as additional random sources for the key generation between two nodes with one-hop relay nodes.

3.3 Authenticated Secret Key Establishment in WBAN

3.3.1 Challenges

While device authentication and secret key establishment are important for WBAN security, simultaneously achieving both of them is required in practical applications, i.e., WBAN devices need to establish shared secret keys with authenticated peers for secure communications. Many existing methods achieve this utilizing non-wireless channels and under constrained scenarios. For example, physiological data can be used for both device authentication and secret key extraction [45–48]. WBAN devices can be shaken together and take advantage of the same motion pattern measured by the devices for both authentication and secret key extraction [32,53]. However, these solutions are not able to support general commercial-off-the-shelf WBAN devices due to the additional hardware that is needed for measuring the biometric or motion data. An authenticated secret key extraction solution compatible with commercial off-the-shelf devices shall make minimal assumptions on device hardware and only utilize widely available resources such as wireless channel measurements. However, it is challenging to use wireless channels alone for simultaneously realizing authentication and key generation. In particular, the dilemma exists since authentication usually requires proximity, while fast key generation requires channel fading that proximity cannot provide.

3.3.2 ASK-BAN: Authenticated Secret Key Establishment Utilizing Channel Characteristics for Wireless BAN

To simultaneously achieve device authentication and fast secret key extraction, ASK-BAN takes advantage of the following characteristics for wireless channels among on-body devices:

1. On-Body channels exhibit obviously different variations (Figure 1, in which the control unit (CU) of the WBAN is deployed to the front of the body and in clear line-of-sight location to sensor nodes S1, S2, and S3).
2. Channels between LOS on-body devices tend to be much more stable than those in NLOS locations. For example, sensor S3 has more stable RSSs for its channel to sensor S4 than other nodes since S3 and S4 are both on the back of the subject and in close LOS locations to each other.

Based on these channel characteristics, ASK-BAN proposes a multi-hop authenticated secret key extraction solution between the CU and on-body sensors with the help of trusted sensors as relay nodes. For multi-hop authentication, ASK-BAN observes that trust relationship is transitive: if RSS variations between A-B and that between B-C are both stable, i.e., A trusts B and B trusts C, then A can trust C with high confidence, and A-B-C is a "trust path" between A and C. Therefore, to authenticate a node ASK-BAN looks for a multi-hop "trust path" between the CU and that node. For secret key extraction, the main challenge is to achieve a high key generation rate during the authentication process. To this end, between each on-body sensor and CU, ASK-BAN exploits possible multi-hop paths that exhibit relatively large RSS variations. Therefore, ASK-BAN adopts five steps for authenticated secret key extraction:

Step 1: Pairwise Key Generation and Initial Authentication. By letting each node broadcast a known message, each pair of nodes measure RSS for packets received from

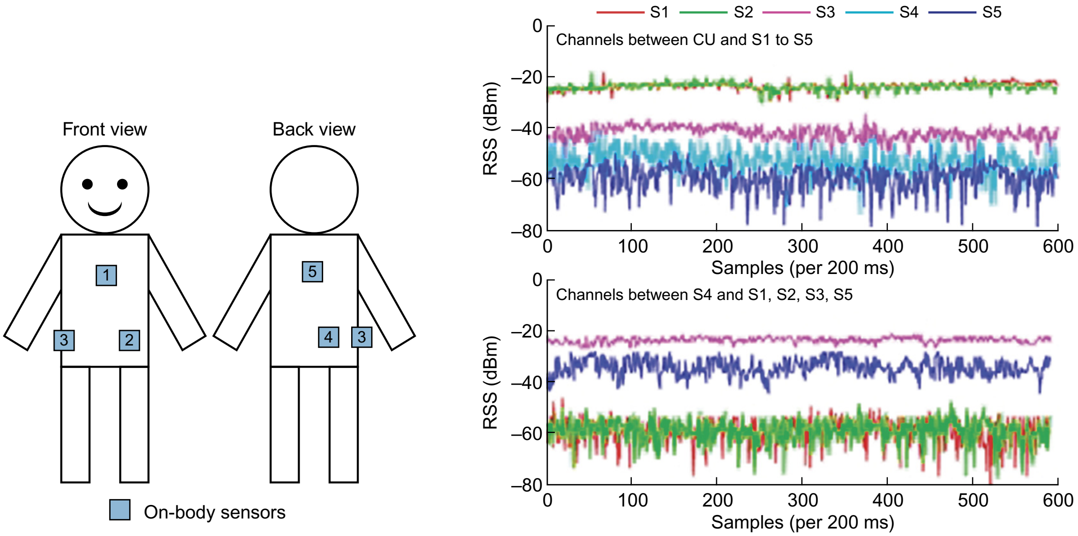

FIGURE 1 WBAN sensor deployment (left) and measured RSS values.

each other and obtain a shared secret key, the length of which is used as the estimation to the secrecy capacity of the channel between the pair. Meanwhile, each node uses the measured RSS values to authenticate all the other nodes with BANA [43,44].

Step 2: Broadcasting Authenticated Secrecy Capacity. During this step each node broadcasts the information regarding every other node *i*: a) trust value (Yes or No) for node *i*; b) the secrecy capacity for the channel between node *i* and itself.

Step 3: Discovering Multi-hop Trusted Paths with Maximum Multi-hop Secrecy Capacity. On receiving the broadcast message from all other nodes in step 2, each node obtains a weighted graph, with each edge indicating the trust relationship between the connected pair and the weight, meaning the secrecy capacity for the channel. By running the max-flow algorithm, each node is able to find multi-hop trusted paths between itself and CU that has the maximum secrecy capacity.

Step 4: Broadcasting Aggregated Secret Key. For each max-flow path, each node, if it is on the path, broadcasts the XORed value of secret keys (obtained in step 1) shared with its previous-hop and next-hop, respectively. After having collected all the XORed values for the max-flow paths, each node and CU are able to derive a shared secret key that has the maximum length.

3.4 Wireless In-Band Trust Establishment in WBAN

The ASK-BAN channel characteristic-based authentication approach assumes all the devices on/near the body are trusted. However, this may not hold in all cases. For example, a careful attacker may sneakily place a malicious sensor near the patient's body or attach another sensor onto the patient's body. In such scenarios, the malicious device can join the BAN easily. To deal with this, in addition to proving device proximity, we need to achieve a higher security goal – demonstrative identification. That is, the user/patient should be able to verify the devices forming the BAN are exactly those she designated to be. Here we assume the designated devices are all benign, because otherwise there is no way to protect the established secret keys. Moreover, the user can count the number of devices correctly.

3.4.1 Related Work

It is well known that the simple Diffie–Hellman key exchange over the wireless channel suffers from the man-in-the-middle attack, as the unprotected wireless signal is subjected to malicious modifications (such as bit flipping and message overshadowing [57]). Thus, in the past decade, various researchers have proposed secure channel-based approaches to work around this problem, which is usually called "secure device pairing" [58]. Secure device pairing relies on the security (authentication) properties of some auxiliary out-of-band (OOB) channel in one way or another. For example, well-known OOB channels include USB connections [59], infrared [60], visual [61], audio, faraday cage [62], etc. However, all these schemes require non-trivial human support, and the devices to be paired should possess common additional hardware such as USB ports, screens, keypads, LEDs, accelerometers, etc. This assumption is often strong and impractical, because all these schemes are often obtrusive to use and not scalable, and are against the global trend for device miniaturization. Moreover, it is commonly believed that human implemented OOB channels can only tolerate up to 10 devices [61]. The human-implemented OOB channel and requirement for advanced hardware have been major obstacles against the practical adoption of those protocols.

There is a growth of interest in using merely wireless in-band communication to achieve authentication and protect message integrity. The Integrity code (I-code) was proposed by Capkun et al. [57], and tamper-evident pairing was proposed by Gollakota et al. [63]. The I-code primitive protects the integrity of every message sent over the insecure wireless channel. It assumes the infeasibility of signal cancellation, and exploits unidirectional error detection codes to provide message tamper-evidence. The I-code method can be applied to key establishment, satellite signal authentication, etc. On the other hand, tamper-evident pairing is an in-band device pairing protocol for 802.11 devices, which uses a tamper-evident announcement that protects the message integrity by embedding cryptographic authentication information (e.g., a hash) into the physical signals, such that any tampering with it will be caught by the receiver.

Though the concept of the above is appealing, there are two limitations. First, security of I-code and tamper-evident pairing is based on the infeasibility of energy cancellation. But these methods only achieve a weak security guarantee, since recently Popper et al. [64] proposed a stronger yet practical correlated signal cancellation attack using a pair of directional antennas. Second, it is difficult to apply these methods to securely initialize multiple constrained devices such as medical sensors due to the scalability issue. I-code and tamper-evident-announcement are both one-to-one message authentication primitives suitable for pairwise communication. If implemented on a sensor platform with 250 kbps transmission rate, an I-coded message requires 0.5 s to transmit 50 bits on a ZigBee sensor platform, given a slot length of 5 ms [57]. In tamper-evident-announcement each synchronization packet must be at least 19 ms long [63]. In addition, the number of "ON_OFF" slots is large (roughly equals a hash length). This yields a total of more than 750 ms for each tamper-evident-announcement. Thus, direct usage or simple extension of I-code or tamper-evident pairing is not scalable to a large group of constrained devices, whereas the delay is critical in many real-world BAN applications.

3.4.2 *"Chorus": Authenticated Message Comparison over Wireless Channel*

We aim at making ad hoc trust initialization work strictly in-band and scalable to a group of devices, by introducing a novel physical-layer primitive called "Chorus," which achieves authenticated message comparison over the insecure wireless channel, and use it to construct secure group authenticated key agreement protocols. The Chorus is partially inspired from I-code and tamper-evident pairing in that it exploits the infeasibility of signal cancellation and unidirectional error detection codes. However, it also combines an idea similar to I-code with the concept of empirical OOB channels used in message authentication protocols to achieve key authentication and confirmation. In most of the group message authentication protocols, the role of OOB channels is to achieve secure comparison: an authentication string (AS) is typically derived by each device from the protocol transcript (messages to be authenticated); when all nodes' ASs are equal to each other all devices should accept the received messages, and whenever any nodes' ASs are not equal all devices should reject the received messages.

The key idea of Chorus is to let N devices compare the equality of their fixed-length strings by simultaneously emitting specially encoded signals, such that any differences among the strings will be detected by all the devices. Chorus only outputs 1 bit of information (accept-all strings are equal, or reject-some strings are different). Due to the unidirectional property of the wireless channel (attacker can only flip a "0" to "1" but not vice versa), changing the comparison result from reject to accept is impossible except negligible probability. This makes Chorus an ideal replacement for traditional OOB channels. The detailed steps are as follows:

1. Chorus starts with a synchronization packet sent by one node (called coordinator), which contains random content and is longer than a usual packet. All other nodes detect the existence of this packet via threshold energy detection.
2. After a short period when the sync packet ends, the coordinator broadcasts a short CTS_TO_SELF packet of length T_{cts}, which reserves the channel for the time period until Chorus concludes, by suppressing unwanted interference from other co-existing devices.
3. Comparison phase: Each node i encodes its bit string s_i (of length l) using Manchester coding to obtain a $2l$ bit string ($0 \rightarrow 01$ and $1 \rightarrow 10$), and map each encoded bit (1/0) into an ON/OFF slot, respectively (of the same duration T_s). During each time slot $1 \leq j \leq 2l$, if it is an ON slot for a node, a short packet with random content is transmitted, simultaneously with everyone else ("chorus"); but if j is an OFF slot for a node, it remains silent and listens to the channel. If $\forall 1 \leq j \leq 2l$, a node i does not detect energy in any of its own OFF slots, it accepts the received messages, otherwise it rejects the received messages.

A sample timing diagram of a Chorus run is depicted in Figure 2, where node N's string is " $1110\cdots$ " which differs from others' strings ("$1100\cdots$") by one bit. The encoded strings are " $10101001\cdots$ " and " $10100101\cdots$," respectively. This can be detected by all nodes (including N itself), because N will detect the aggregated signal of all other nodes during its 6th (OFF) slot, while all other nodes detect energy during their 5th (OFF) slot.

Different from I-code, in Chorus when each node sends its own signal, it cannot receive others' signals (we do not assume full-duplex transceivers). It seems that half of the information is lost. Thus the question is whether non-spoofing property can still be achieved. We can show that it is indeed the case as long as an adversary can only flip a "0" to a "1" bit but not vice versa (i.e., if signal cancellation is infeasible) [65]. In addition, when we consider an attacker that can only inject a signal generated by itself, it can be shown that the realization of basic Chorus is secure against such type of attacks [65].

We also need to defend against correlated signal cancellation attacks where the attacker does not generate its own signal. A practical attack was proposed by Popper et al. [64]. It is based on signal relaying, i.e., the attacker is located at a distance away from both the sender and receiver, and utilizes a pair of directional antennas to relay the sender's signal to the receiver. If the attacker creates a phase delay for the carrier signal on the relay channel that is a multiple of π and with the same signal amplitude, the received signal strength can be completely attenuated. This attack doesn't depend on the packet content and modulation, while it mainly works under stable and predictable channel environments (e.g., static indoor scenarios).

In [65], we proposed to make novel use of uncoordinated frequency hopping (UFH) [66] to protect Chorus from the above type of attack. The basic idea is to make the probability of cancellation arbitrarily small by randomly hopping over multiple frequencies (minislots) within each slot. This is due to the observation that the key factor for an attacker to succeed is to create a phase difference of $\Delta\phi = (2k-1)\pi, k = 1, 2, \ldots,$ which can be defeated by changing the frequency. We assume the processing delay at the attacker is negligible. For each node, in each OFF slot, as long as it detects energy during at least one of the minislots, this node will reject the received messages. Otherwise, if it does not detect energy in any OFF slot, it outputs accept.

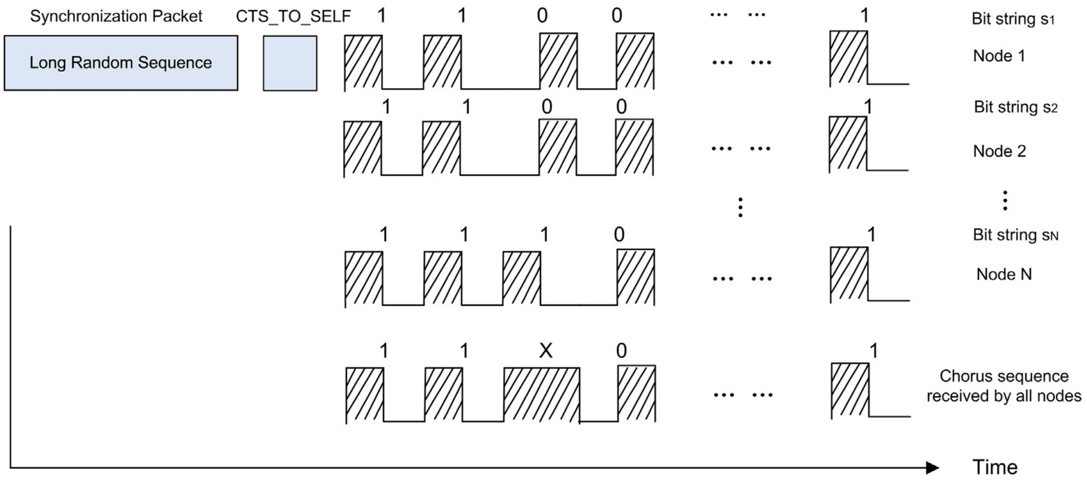

FIGURE 2 An example execution of basic Chorus using Manchester coding.

Based on Chorus, secure in-band trust initialization protocols were designed [65], where all the messages to be authenticated are exchanged using the normal high-bandwidth wireless transmission, with only one run of Chorus in the end of the protocols. Such protocols can achieve greater scalability than previous solutions and are suitable for constrained devices. Specifically, in the setting of BANs, as long as the user has a correct device count for the designated devices, she can input it into the controller and start the trust initialization protocol. Since the use of Chorus makes it resistant to man-in-the-middle attacks, even if an attacker passes BANA's proximity verification it cannot successfully impersonate a legitimate device (any attempts to block or tamper with the messages from a legitimate device can be detected).

4. SUMMARY

In this chapter, we focused on the important problem of initial trust establishment in WBANs. It is the prerequisite for security and privacy protection in WBANs, without which patients' safety can be at risk. It is also challenging due to the simultaneous requirements of high security, efficiency, and usability. We surveyed state-of-the-art solutions to trust establishment and analyzed their strengths and weaknesses in the context of WBANs. We then identified the need for establishing trust based on only wireless channels, without using any secure out-of-band channels. This is necessary to free the user from active participation and achieve "plug-and-play," while eliminating the need for additional hardware interfaces. We presented two of our initial solutions in this direction, namely ASK-BAN and Chorus. The former authenticates BAN devices and generates secret keys among them based on their co-location/proximity with regard to the human body, exploiting channel characteristics. The latter authenticates an arbitrary group of devices designated by the human user through creating an authenticated string comparison based on recent advances in anti-signal-cancellation in the wireless channel. Both solutions involve little or no user effort, and are lightweight. Their security is analyzed via analysis and experiments.

Regarding practical implementation of security mechanisms in WBANs, the selection of proper methodologies depends on various factors. There is no single method that suits all scenarios. One needs to jointly consider the application level functionalities, system security requirements, hardware/software/power/physical constraints, usability requirements, and the tradeoffs among them. For example, traditional encryption may not be a feasible choice in some legacy medical devices such as implanted ones, as software updates require the device be taken out. The channel-based trust establishment approaches proposed in this chapter may be more suited for resource-constrained wearable sensor devices that do not have common sensing capabilities for biometrics, while enjoying a similar level of usability.

In the future, work can focus on relaxing the assumption of trusted devices on the body as the sensor devices can be compromised. For example, compromise detection mechanisms and trust establishment protocols that are resilient to compromised devices.

References

[1] Implantable Medical Devices: Hacking Humans, <https://www.blackhat.com/us-13/briefings.html>, (Last Accessed: 01.07.14).

[2] Scientists work to keep hackers out of implanted medical devices, <http://www.cnn.com/2010/TECH/04/16/medical.device.security/index.html>, (Last Accessed: 01.07.14).

[3] Medical Device Hacking Prompts Concern, <http://www.cyberprivacynews.com/2011/08/medical-device-hacking-prompts-concern/>, (Last Accessed: 01.07.14).

[4] Black Hat: Insulin pumps can be hacked, <http://www.scmagazine.com/black-hat-insulin-pumps-can-be-hacked/printarticle/209106/>, (Last Accessed: 01.07.14).

[5] How hackers can kill you, <http://situationroom.blogs.cnn.com/2013/06/15/how-hackers-can-kill-you/>, (Last Accessed: 01.07.14).

[6] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, Proc. 9th ACM conference on Computer and communications security, ACM, New York, NY, USA, 2002, pp. 41−47.

[7] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks," in Security and Privacy, 2003, Proc. 2003 Symp (2003) 197−213.

[8] W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur. 8 (2) (2005) 228−258.

[9] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, Proc. 10th ACM conference on Computer and Communications Security, ACM, New York, NY, USA, 2003, pp. 52−61.

[10] D. Liu, P. Ning, W. Du, Group-based key predistribution for wireless sensor networks, ACM Trans. Sen. Netw. 4 (2) (2008) 11:1−11:30.

[11] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, Spins: security protocols for sensor networks, Wirel. Netw. 8 (5) (2002) 521−534.

[12] A.K. Jain, K. Nandakumar, Biometric Authentication: System Security and User Privacy, Computer 45 (11) (2012) 87−92.

[13] K. Malasri, L. Wang, Addressing security in medical sensor networks, Proc. 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, ACM, New York, NY, USA, 2007, pp. 7−12.

[14] S.A. Devi, R.V. Babu, B.S. Rao, A new approach for evolution of end to end in wireless sensor network, Int. J. Comput. Sci. Eng. 3 (6) (2011) 2531−2543.

[15] M. Mana, M. Feham, B.A. Bensaber, A light weight protocol to provide location privacy in wireless body area networks, Int. J. Netw. Secur. Appl. 3 (2) (2011) 1−11.

[16] O. Delgado-Mohatar, A. Fuster-Sabater, J.M. Sierra, A light- weight authentication scheme for wireless sensor networks, Ad Hoc Netw. 9 (5) (2011) 727−735.

[17] T. Zia, A. Zomaya, A lightweight security framework for wireless sensor networks, J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl. 2 (2011) 53−73.

[18] M. Li, W. Lou, K. Ren, Data security and privacy in wireless body area networks, Wireless Commun. IEEE 17 (1) (2010) 51−58.

[19] M. Li, S. Yu, W. Lou, K. Ren, Group device pairing based secure sensor association and key management for body area networks, INFOCOM 2010 Proc. IEEE (2010) 1−9.

[20] M. Li, S. Yu, J.D. Guttman, W. Lou, K. Ren, Secure ad-hoc trust initialization and key management in wireless body area networks, ACM Trans. Sens. Netw. (TOSN) (2012).

[21] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, et al., Exploiting prediction to enable secure and reliable routing in wireless body area networks, INFOCOM 2012 Proc. IEEE (2012) 388−396.

[22] <http://en.wikipedia.org/wiki/Attribute-based_encryption>, (Last Accessed: 01.07.14).

[23] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-Policy Attribute-Based Encryption, Proc. IEEE Symp. Secur. Priv. (2007).

[24] C. Hu, F. Zhang, X. Cheng, X. Liao, D. Chen, Securing communications between external users and wireless body area networks, Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec '13), ACM, New York, NY, USA, 2013, pp. 31−36.

[25] J. Akinyele, M. Pagano, M. Green, C. Lehmann, Z. Peterson, A. Rubin, Securing electronic medical records using attribute-based encryption on mobile devices, pages 75−86. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, ACM, 2011

[26] C. Hu, N. Zhang, H. Li, X. Cheng, X. Liao, Body area network security: A fuzzy attribute-based signcryption scheme. to appear in IEEE Journal on Selected Areas in Communications (JSAC), Spec. Issue Emerg. Technol. Commun. (2012).

[27] C.C. Tan, H. Wang, S. Zhong, Q. Li, Body sensor network security: an identity-based cryptography approach, Proceedings of the First ACM Conference on Wireless Network Security (WiSec '08), ACM, New York, NY, USA, 2008, pp. 148−153.

[28] C.C. Tan, H. Wang, S. Zhong, Q. Li, IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks, Info. Technol. Biomed. IEEE Trans. 13 (6) (2009) 926−932.

[29] C. Rong, H. Cheng, Authenticated health monitoring scheme for wireless body sensor networks, Proceedings of the 7th International Conference on Body Area Networks (BodyNets '12), ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 2012, pp. 31−35.

[30] X. Hei, X. Du, Biometric-based two-level secure access control for implantable medical devices during emergencies, 30th IEEE Int. Conf. Comput. Commun. (INFOCOM 2011) (2011) 346−350, Shanghai, P. R. China.

[31] Z. Zhang, H. Wang, A.V. Vasilakos, H. Fang, ECG-Cryptography and Authentication in Body Area Networks, Info. Technol. Biomed. IEEE Trans. 16 (6) (2012) 1070−1078.

[32] R. Mayrhofer, H. Gellersen, Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices, Mobile Comput. IEEE Trans. 8 (6) (2009) 792−806.

[33] A. Varshavsky, A. Scannell, A. LaMarca, E. De Lara, Amigo: proximity-based authentication of mobile devices, Proc. 9th Inter- National Conference on Ubiquitous Computing, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 253−270.

[34] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, A. LaMarca, Ensemble: cooperative proximity-based authentication, Applications, and Services. Proc. 8th International Conference on Mobile Systems, ACM, New York, NY, USA, 2010, pp. 331−344.

[35] L. Cai, K. Zeng, H. Chen, P. Mohapatra, Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas, Netw. Distributed Syst. Secur. Symp. (2011).

[36] K. Zeng, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks], IEEE Wireless Commun. 17 (2010) 56−62.

[37] N. Patwari, S.K. Kasera, Robust location distinction using temporal link signatures, Proc. 13th Annual ACM International Conference on Mobile Computing and Networking, ACM, New York, NY, USA, 2007, pp. 111−122.

[38] A. Varshavsky, A. Scannell, A. LaMarca, E.D.e. Lara, Amigo: proximity-based authentication of mobile devices, Proc. 9th Inter-National Conference on Ubiquitous Computing, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 253−270.

[39] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, N. Mandayam, Proximate: proximity-based secure pairing using ambient wireless signals, applications, and services. Proc. 9th International Conference on Mobile Systems, ACM, New York, NY, USA, 2011, pp. 211−224.

[40] S. Brands, D. Chaum, Distance-bounding protocols, Workshop on the Theory and Application of Cryptographic Techniques on Advances In Cryptology, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1994, pp. 344−359.

[41] K.B. Rasmussen, C. Castelluccia, T.S. Heydt-Benjamin, S. Capkun, Proximity-based access control for implantable medical devices, Proc. 16th ACM Conference on Computer and Communications Security, ACM, New York, NY, USA, 2009, pp. 410−419.

[42] K.B. Rasmussen, S.C. apkun, Realization of rf distance bounding, Proc. 19th USENIX Conference on Security, USENIX Association, Berkeley, CA, USA, 2010, pp. 25−25.

[43] L. Shi, M. Li, S. Yu, J. Yuan, BANA: body area network authentication exploiting channel characteristics, Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC '12), ACM, New York, NY, USA, 2012, pp. 27−38.

[44] L. Shi, M. Li, S. Yu, J. Yuan, BANA: Body Area Network Authentication Exploiting Channel Characteristics, Selected Areas, Commun. IEEE J. 31 (9) (2013) 1803−1816.

[45] K. Singh, V. Muthukkumarasamy, Authenticated key establishment protocols for a home health care system. In Intelligent Sensors, Sensor Networks and Information, 2007, ISSNIP 2007. 3rd Int. Conf. (2007) 353−358.

[46] K. Venkatasubramanian, A. Banerjee, S. Gupta, Pska:Usable and secure key agreement scheme for body area networks, Info. Technol. Biomed. IEEE Trans. 14 (1) (2010) 60−68.

[47] K.K. Venkatasubramanian, S.K.S. Gupta, Physiological value-based efficient usable security solutions for body sensor networks, ACM Trans. Sen. Netw. 6 (4) (2010) 31:1−31:36.

[48] F. Xu, Z. Qin, C. Tan, B. Wang, Q. Li., Imdguard: Securing implantable medical devices with the external wearable guardian. In INFOCOM, 2011 Proc. IEEE (2011) 1862−1870.

[49] C. Poon, Y. Zhang, S. Bao., A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, IEEE Commun. Mag. 44 (4) (2006) 73−81.

[50] S. Bao, C. Poon, Y. Zhang, L. Shen, Using the timing information of heartbeats as an entity identiffer to secure body sensor network, IEEE Trans. Inf. Technol. Biomed. 12 (6) (2008) 772−779.

[51] S. Cherukuri, K. Venkatasubramanian, S. Gupta., Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, Parallel Process. Workshops 2003 Proc. 2003 Int. Conf. (2003) 432−439.

[52] D. Bichler, G. Stromberg, M. Huemer, M. Low, Key generation based on acceleration data of shaking processes, Proceedings of the 9th International Conference on Ubiquitous Computing, UbiComp'07, Springer-Verlag, Berlin, Heidelberg, 2007.

[53] R. Mayrohofer, H. Gellersen, Shake well before use: authentication based on accelerometer data, Proceedings of the 5th International Conference on Pervasive Computing, Pervasive'07, Springer-Verlag, Berlin, Heidelberg, 2007.

[54] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik., Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, pages 128−139. Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, MobiCom '08, ACM, New York, NY, USA, 2008

[55] S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, S. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, pages 321−332. Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, Mobicom'09, ACM, 2009

[56] L. Lai, Y. Liang, and W. Du. Phy-based cooperative key generation in wireless networks. In Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on.

[57] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, M. Srivastava, Integrity codes: Message integrity protection and authentication over insecure channels, IEEE Trans. Dependable Secure Comput. 5 (4) (2008) 208−223.

[58] M. Li, W. Lou, K. Ren, in: H. Tilborg, S. Jajodia (Eds.), "Secure Device Pairing," in Encyclopedia of Cryptography and Security, Second ed., Springer, 2011.

[59] F. Stajano, R.J. Anderson., The resurrecting duckling: Security issues for ad-hoc wireless networks, IWSP '00 (2000) 172−194.

[60] D. Balfanz, D.K. Smetters, P. Stewart, H.C. Wong, Talking to strangers: authentication in ad-hoc wireless networks, NDSS '02 (2002).

[61] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J.M. McCune, A. Studer, et al., Gangs: gather, authenticate 'n group securely, MobiCom '08 (2008) 92−103.

[62] C. Kuo, M. Luk, R. Negi, A. Perrig., Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes, SenSys '07 (2007) 233−246.

[63] S. Gollakota, N. Ahmed, N. Zeldovich, D. Katabi, Secure in-band wireless pairing, pages 16−16. USENIX, SEC'11, USENIX Association, Berkeley, CA, USA, 2011

[64] C.P. opper, N.O. Tippenhauer, B. Danev, S. Capkun, Investigation of signal and message manipulations on the wireless channel, ESORICS'11 (2011) 40−59.

[65] Y. Hou, M. Li, J.D. Guttman, Chorus: Scalable In-band Trust Initialization for Multiple Constrained Devices over the Insecure Wireless Channel, The sixth ACM Conf Secur Priv Wireless Mobile Netw. (ACM WiSec 2013) (2013) 17−19, Budapest, Hungary.

[66] M. Strasser, S. Capkun, C. Popper, M. Cagalj, Jamming-resistant key establishment using uncoordinated frequency hopping, IEEE S & P (2008) 64−78, IEEE.