Secure Key Design Approaches using Entropy Harvesting in Wireless Sensor Network: A Survey

Amrita Ghosal[1], Subir Halder[1] and Stefano Chessa[2]

[1]Department of CSE, Dr. B. C. Roy Engineering College, Durgapur, India

[2]Department of Computer Science, University of Pisa, Pisa, Italy

ghosal_amrita@yahoo.com, subir_ece@rediffmail.com, stefano.chessa@unipi.it

Abstract: Physical layer based security design in wireless sensor networks have gained much importance since the past decade. The various constraints associated with such networks coupled with other factors such as their deployment mainly in remote areas, nature of communication etc. are responsible for development of research works where the focus is secured key generation, extraction, and sharing. Keeping the importance of such works in mind, this survey is undertaken that provides a vivid description of the different mechanisms adopted for securely generating the key as well its randomness extraction and also sharing. This survey work not only concentrates on the more common methods, like received signal strength based but also goes on to describe other uncommon strategies such as accelerometer based. We first discuss the three fundamental steps viz. randomness extraction, key generation and sharing and their importance in physical layer based security design. We then review existing secure key generation, extraction, and sharing mechanisms and also discuss their pros and cons. In addition, we present a comprehensive comparative study of the recent advancements in secure key generation, sharing, and randomness extraction approaches on the basis of adversary, secret bit generation rate, energy efficiency etc. Finally, the survey wraps up with some promising future research directions in this area.

Keywords: Channel impulse response, Information entropy, Randomness extraction, Received signal strength, Wireless sensor network.

1. Introduction

Due to the impetuous advancement of technologies in the last years, wireless sensor networks (WSNs) have become a reliable and mature technology, widely used in several applications ranging from industry to military and home. In a typical deployment, the sensors are battery-powered microsystems that embed a variable number of transducers to monitor their surroundings. The sensors also embed a wireless radio and form a wireless network autonomously, through which they communicate their sensed data. One or more sensor(s) in WSN are also connected to the internet or to other external networks, and act as gateways for forwarding the sensed data to remote users. In some applications, WSNs need to work unattended for long periods of time, either to reduce the costs of maintenance, or because they are deployed in hardly

Corresponding author addresses: S. Halder, Department of Computer Science and Engineering Department, Dr. B. C. Roy Engineering College, Durgapur, India. E-mail: subir_ece@rediffmail.com; Phone No: +919433438861, Fax: +91 343 2504059/+91 343 2503424.

accessible (or even hostile) places. Furthermore, some of the sensors may be deployed on mobile objects (either robots, animals, vehicles etc.) and are thus mobile.

Despite their versatility and usefulness, WSNs are vulnerable to attacks. In particular, the broadcast nature of wireless communications used by the sensors make them highly prone to attacks by adversaries, for example, confidentiality or availability of sensed data may be breached. Therefore, providing security to WSNs has become an inevitable requirement of their design. On the other hand, this requirement is difficult to achieve due to the constrained resources of sensors in most applications leading to conventional security schemes being hardly applicable. As a matter of example, the use of asymmetric cryptography and authentication is a challenging task for very low power sensors.

A prime issue in security design of WSNs is generation of secret keys and their sharing because of the restrictions posed by the sensor nodes as mentioned earlier. On the contrary, as shown by the recent developments, the generation of secret keys may take advantage of the intrinsic randomness of the physical layer or environment in which the sensors operate. One of the most notable example is given by the received signal strength (RSS), which is an indicator commonly used in sensors' radios. In this case, the combination of a strong decorrelation of the wireless channel in time and space and the variability of the environment itself (for example due to the presence of moving people or objects) makes the RSS readings vary in an unpredictable way. This fact, combined with the reciprocity properties of the wireless channel makes a pair of RSS readings collected at the same time by two communicating sensors highly related as well as opens the way for a number of methods that extract randomness from the RSS readings to generate secret keys [1-4]. These methods leverage on the reciprocity of the wireless channel to facilitate the key's sharing, and they rely on the unpredictability of the RSS fluctuations to make the keys hardly identifiable by other sensors. The measurements of RSS are however not the only potential source of randomness from which a sensor can leverage to create keys. For example, the sensors can exploit the on board transducers to extract randomness from the measurements of the surrounding environment [5-8]. Also, with these methods however, the issue is how to deal with the predictability of the measurements and how to share the keys that are generated.

In the existing literatures, a number of issues relating to channel reciprocity based key establishment technique are reviewed. In [9], Shehadeh, and Hogrefe reviewed existing physical layer based secret key generation techniques. In particular, they reviewed mainly two types of secret key generation techniques, namely: (i) RSS based key generation, and (ii) channel impulse response (CIR) based key generation. In addition, they reviewed few latest key generation mechanisms such as random channel hopping based mechanism. Similar to [9], Wang et al. [10] reviewed existing physical layer based key establishment techniques for wireless networks. However, unlike [9], the authors reviewed the existing works under three categories, namely: (i) quantization methods used to form secret key from wireless channel reciprocity, (ii) reconciliation and privacy amplification methods used to handle communication errors, and (iii) the feasibility and security issues related to

channel reciprocity based key establishment techniques. In contrast to [9, 10], our work differs from the previous efforts in terms of emphasis and comprehensiveness. In particular, the taxonomy of physical layer based security design approaches described in this survey is depicted using Figure 1. We summarize our main contributions as follows:

- Initially, unlike [9, 10], we classified the existing physical layer based security design issue into three categories, namely, secret key generation, sharing, and extraction. We then briefly discuss about the three fundamental steps i.e., generation, sharing, and extraction and their importance in the physical layer based security design.
- Unlike [9, 10], we present the latest achievements on secure key generation, sharing, and randomness extraction approaches particularly in WSNs. Most importantly, unlike [9, 10], we focus especially on the methods based on RSS, frequency selectivity, and CIR not only because these methods are more mature, but also present other methods that exploit the measurements obtained by the on-board transducers. We also discuss the pros and cons of the existing secure key design approaches.
- We present a comprehensive comparative study of the recent advancements in secure key generation, sharing, and randomness extraction approaches on the basis of number of parameters like type of nodes, adversary, secret bit generation rate, secret bit mismatch rate, energy efficiency etc.
- Finally, we identify the future research trends for the benefit of both general and expert readers.

This survey work is organized as follows. In section 2, we briefly explain each of the three fundamental steps viz. randomness extraction, key generation and sharing and their importance in designing of physical layer based security mechanisms in WSNs. In section 3, existing physical layer based security design methods are discussed; these include RSS measurement, frequency selectivity, and CIR measurements etc. Section 4, provides a broad picture of future research directions. Finally, the survey is concluded in Section 5.

2. Overview of Physical Layer Based Security Design

The design of physical layer based security mechanisms for WSN involves three primary steps, i.e., key generation, randomness extraction, and sharing. Key generation refers to the different mechanisms that are implemented for efficient on-line generation of secret keys in WSN. Traditional approaches for key generation are not suitable for WSNs due to the severe resource constrained nature of such networks. Several concepts are being used for key generation in WSNs by exploiting the physical characteristics of wireless channels [11]. Such physical properties are in the form of multipath fading, reciprocity of the wireless channel, path loss etc.These physical properties are sources of randomness [1, 4, 9]. Such random sources form correlated random processes, which are shared between two parties and decorrelate rapidly if the physical parameter is changed. In this way, the output of the random process is unknown to anyone at different physical positions, and can

therefore be used as a shared secret. Strong decorrelation of channel behaviour in both time and frequency domains is exploited for achieving the purpose of secret key generation. Very fast decorrelation is found to occur in the measured RSS and using this property the attacker is evaded, as it is unaware of RSS estimations of legitimate nodes [1]. The channel response measured at the receiver is considered a frequency and position-dependent random variable that carries some information entropy and can be utilized as a source of randomness [5, 7].

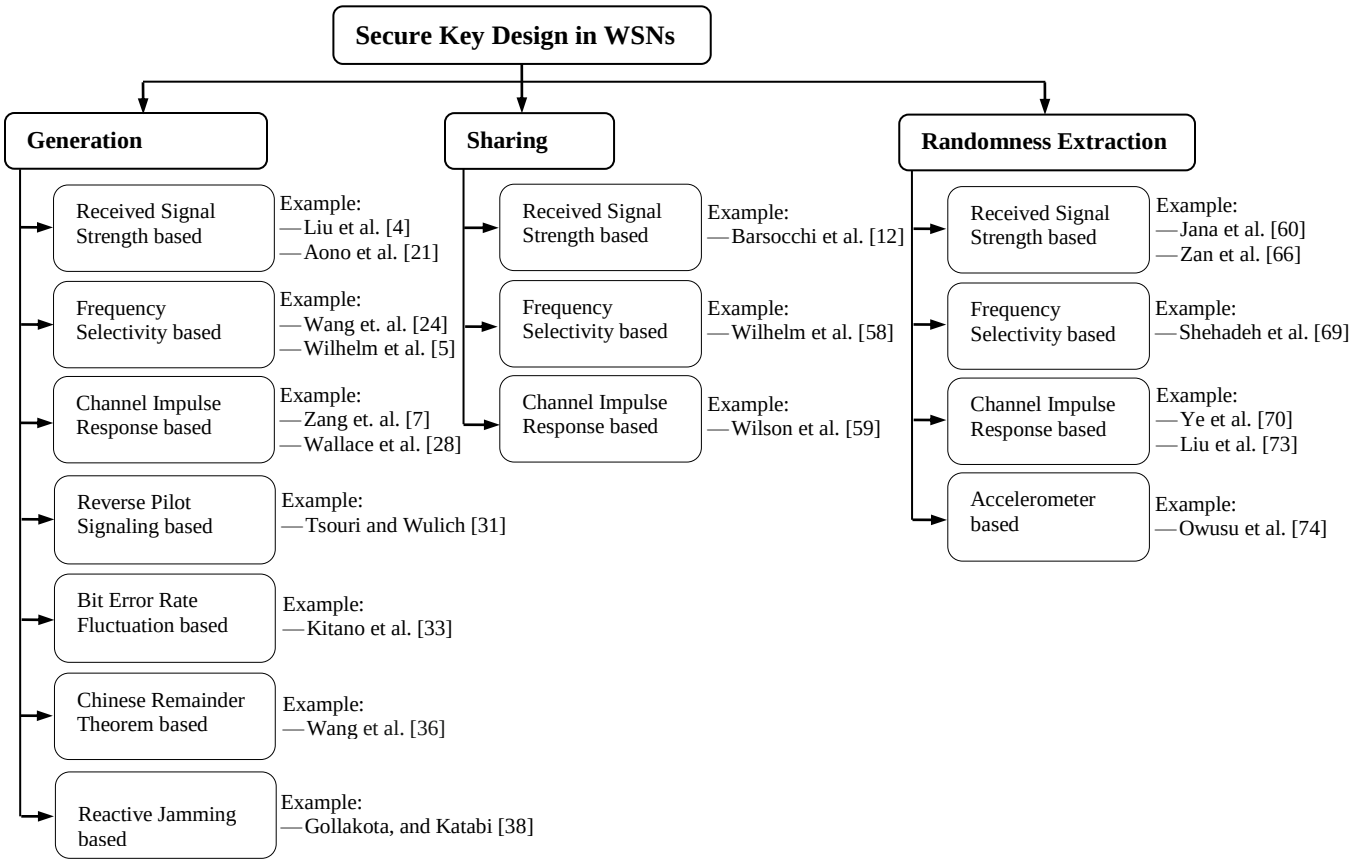

Figure 1: Taxonomy of physical layer based security design approaches in WSNs

In WSNs, efficient and secure key distribution [12] is required for allowing key establishment in a simple manner. Existing works in this field have concentrated on using conventional security measures that include installation of secrets by the user manually, their imprint during the production process or by use of public key cryptography. It has been found that adversaries in most of the cases take the advantage of disproportions arising out of performance related issues coupled with the broadcast nature of wireless channel for launching attacks (e.g., flooding that directly consumes resources). Another approach utilizes the properties of wireless channels as useful security primitives. Depending on the mobility pattern and the transmission frequency, if the channel response between the two transmitters is sampled over a short time interval, it is observed that both the transmitters generate highly correlated estimates. Wireless channel reciprocity results in correlated

measurements of the channel statistics at both transmitters. Also, the channel response is affected in an unpredictable manner by the physical environment and multipath fading. Therefore, two transmitters are able to generate shared secrets from their inherent physical behaviour irrespective of computational capabilities of adversaries. The messages exchanged between the two legitimate transmitters do not contain any content; rather they are used to provide channel statistics. This approach provides an alternate mechanism for generation of symmetric secret keys without depending on asymmetric cryptography. All the mechanisms described above demand for arbitrary movements of sensors for generation of secret keys. Nevertheless, in WSNs, as sensors are generally static in nature mainly due to application specific requirements, the advantage of physical environment is taken into account in such scenarios. Different events such as human movements make an impact on the signal propagation in an unpredictable yet correlated manner. This makes it possible for legitimate transmitters to take the benefit of such an advantage as a source of randomness for obtaining new shared secrets. Randomness extraction refers to the different mechanisms that are used to obtain random numbers from the environment for generating the keys. Extraction of randomness from the wireless channel needs bi-directional measurements [11]. Most of the works involving key extraction have made use of a single transmitter and a single receiver. Randomness extracted from channel measurements were first suggested in [13]. Some of the channel characteristics that are used for randomness extraction are measurement of phase, channel impulse response, amplitude gain etc. Challenges involved in randomness extraction include time correlated nature of channel measurements that reduce the cryptographic strength of the key (unless this is accounted for in the algorithm design) and the non-reciprocities which occur due to the half-duplex nature of the channel measurements. For the second challenge, for ensuring complete agreement between the two generated secret keys, information reconciliation [14] is generally used to correct a small number of discrepancies without giving away the entire secret key.

The main features [15] that enable the extraction of randomness from radio communications are the following:

- *Reciprocity of the wireless radio channel*: The different multipath properties of the radio channel, e.g. gains, phase-shifts, and delays are identical in both directions of the link at any point of time and on any given frequency channel.
- *Temporal variations in the radio channel*: With progress in time, the multipath channel changes that occur because of movement at either end of the link, and also due to motion of people and objects in the environment near the link.
- *Spatial variations*: The properties of the radio channel are unique to the locations of the two endpoints of the link.

3. Source of Randomness/Entropy

According to information theory, entropy is a measure of the uncertainty associated with a random variable. The average amount of information that is obtained on observation of the outcome of the random variable is quantified by entropy. A typical measure of entropy of a random variable *X*, over the set of *n* symbols $x_1, x_2, \ldots, x_n$ is given by [1, 3, 12],

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

where $p(x_i)$ is the probability of occurrence of i^{th} symbol x_i. For binary symbols, a value close to 1 indicates high entropy [3]. For easy reference, we summarize the notations in Table 1.

Table 1: Summary of the used notation

Notation	Description
X	Discrete random variable
$H(X)$	Entropy of X
$p(x_i)$	Probability of occurrence of i^{th} symbol x_i
C_j	CIR measurement at jth pair of location

The wireless channel is a source of randomness with non-uniform distributions of outcomes due to the unpredictable multipath propagation and the resulting fading behaviour of wireless channel as well as randomness of the RSS. Entropy measurements provide a measure of the randomness of the channel that is used for secret generation, randomness extraction and/or sharing of keys.

Many works have been reported so far that deal with the issue of secret generation, randomness extraction, and sharing. All these works have been conducted through different approaches based on different channel characteristics [9, 16, 17]. Some of these characteristics are RSS, multiple phases or frequencies, amplitudes or gains of signals. Out of these, RSS is most commonly available because of low device cost and it can easily be measured on a per-packet basis with off-the-shelf hardware. Nevertheless, as RSS is extracted from a single frequency, thus, it can only provide coarse-grained information of the radio channel, resulting in low bit generation rates. On the contrary, multiple phases and gains of signal based approaches have considered leveraging the whole information provided by the multipath channel. In this case, the whole channel response is represented by either gains or phases of the different channel responses. Hence, a higher number of secret bits are expected to be extracted by leveraging the whole channel response. In this survey, we have categorized the existing works mainly by three approaches (based on their commonality in approaches) viz. RSS, multiple phases or frequencies, multiple amplitudes or gains of signal(s). In addition to these three approaches, several other approaches were proposed to generate, extract and share secret keys based on some properties of the physical layer of wireless communication. A number of state-of-the-art works belonging to each of the above mentioned approaches are reviewed in the next and subsequent sub-sections.

3.1 Secure Key Generation Strategies

In general, secure key generation strategies in the literature can be broadly classified into three main classes: (i) RSS based strategies [1-4, 18-22], (ii) frequency selectivity based strategies [5, 6, 23, 24], (iii) channel impulse response based strategies

[7, 8, 25-30]. Further, in recent years, different innovative approaches were proposed by authors for secret key generation such as reverse pilot signaling [31, 32], bit error rate fluctuation [33, 34], chinese remainder theorem [35-37], reactive jamming [38, 39]. In this section, we have elaborated each of these categories of classes. At present, it became a common practice to use the nomenclature Alice, Bob, and Eve to refer to the legitimate transmitter, intended receiver, and unauthorized eavesdropper, respectively. In our survey, we also consider the same nomenclature in describing the existing mechanisms.

3.1.1 RSS

RSS is by far the most commonly measured channel characteristic because RSS measurement capability is built into sensor nodes. In this section, we illustrate the state-of-the-art secure key generation mechanisms based on the philosophy of RSS variation.

A cyber-physical approach for secret key generation is proposed in [1]. This approach utilizes the properties of the physical world and includes these properties while designing lightweight security protocols. It utilizes the signal strength fluctuations resulting from dynamic physical environments, e.g. environments experiencing human movements. This work addresses the following- (a) secret key extraction by designing a robust key generation protocol for static WSNs that takes into account events occurring in the environment, (b) protocol implementation by using sensor devices and evaluating the same in a real environment, (c) analysis of data collected with respect to primary factors that influence the rate of successful key exchange, and (d) evaluation of an adversarial strategy for combating the RSS based attack. Real life experimental evaluation is done by analyzing the effect of various moving patterns on legitimate devices and an eavesdropper. The scenario considered is crowded in nature where randomness is extracted from the movement of persons for sharing new secrets between the sensors. The received power is considered as shared information between the transmitter and the receiver under the hypothesis of signal propagation on a symmetric channel [18, 19]. This work leverages RSS variation resulting out of disturbing events that cross the line of sight for generating shared secrets between pairs of sensors. Movement characteristics such as speed and direction of the disturbing event dynamically changes and cannot be understood beforehand by adversaries. Both environmental changes and channel reciprocity are considered in this work for allowing sensors to share secrets among themselves. The experimental scenario chosen for this work is shown in Figure 2. The line of sight between Alice and Bob is shown using a dotted line while three positions of Eve are considered, all equidistant from Bob. The vulnerability of the proposed scheme is analyzed by defining a new RSS attack, where the adversary desires access to the secret key establishment using a RSS sniffing process. The results of this work show that the fresh secret keys can be generated even in static WSNs using the human movements in the environment. Hence, the proposed mechanism can be

applied to a wide range of scenarios where the sensor networks are deployed as a part of ambient intelligence applications, such as assisted living and building monitoring applications, i.e., where the physical environment is affected by frequent human movements.

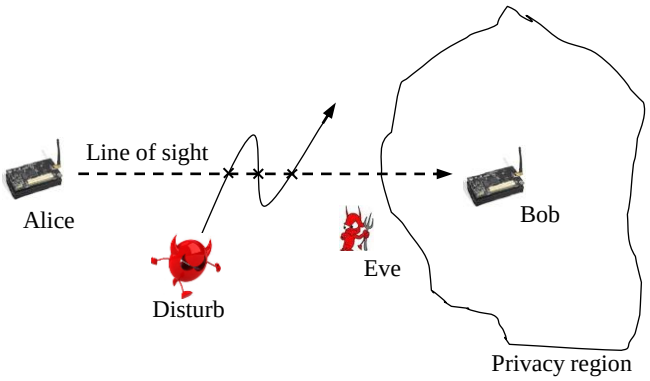

Figure 2: Generating secrets from frequent line of sight disturbances.

In [2], the authors proposed an algorithm for generating the key using RSS. The scenario which is best suited for the use of this algorithm is where the peers have very different computational resources. The adversary considered here is a global eavesdropper that has the ability of estimating the RSS values of the packets transmitted between two legitimate sensors. Also, the adversary is aware of the key establishment protocol and the parameters used by it. Initially, the authors perform a preliminary computation on raw RSS values and translate them into symbols. The translation is done with the help of two consecutive phases, namely averaging and quantization. Averaging is done by taking the equal-length batches of RSS measurements, and later the average computed from them is used as the batch representative. Quantization is involved with the translation of each batch representative into symbol. The final key is computed on the sequence of symbols. Authors show that the batch length and the number of symbols required to determine a key can be set arbitrarily. Also, they show that the batch length has an effect on the performance of the protocol. It is worth noting that the averaging and quantization operations reduce the difference of data collected at the two endpoints to a large extent. In this work, a single-round reconciliation is done where only one hash is transmitted between the two parties. An algorithm is used for sampling the input space of the hash function that produces statistical knowledge of the channel. The algorithm is evaluated using theoretical analysis and is validated through real world measurements. In the real world measurements, the authors considered two communicating components, viz. a non-constrained device (A) such as laptop and another device that has limited memory as well as computational abilities such as sensor node (B). The experimental scenario is illustrated in Figure 3 where device A is placed at the center while device B has six different locations $(B_1,\ldots,B_6)$. The position of the adversary is always shown as changing such that it can listen to all the communications between A and B. Based on the experiments,

the authors show that the proposed protocol generates high entropy bit at remarkable rates with minimal computational complexity requirements.

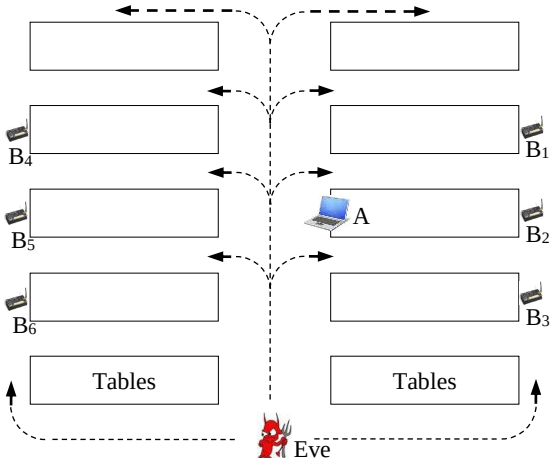

Figure 3: Experimental scenario: a non-constrained device A at the center, six different positions $(B_1,\ldots,B_6)$ considered for sensor node B and trajectory of Eve.

More recently, S. T. Ali et al. [3] proposed a secret key generation scheme based on RSS measurement. In the proposed scheme, the keys are shared using near-perfect agreement to avoid reconciliation cost. The threat model for this work assumes the presence of one or more adversaries in the environment whose channel sampling time is same as that of legitimate sensors and they also have knowledge about the key extraction algorithm along with its parameters. Channel measurement asymmetries due to non-simultaneous probing of the channel by the two end points are analyzed. A practical filtering scheme is proposed to minimize the asymmetries of channel measurements. The filtering scheme is found to improve the signal correlation between the communicating pair of sensors without reducing entropy. This work demonstrates that the channel mismatch between the communicating pair is due to the time delay between the measurements at the two ends. For restricting bit generation to the periods of high motion-related fluctuation, a mechanism is used by the authors, where further reduction in disagreement in channel estimation is done, thereby virtually eliminating key-bit mismatch. Authors show that adjustment of activity threshold yields near-perfect key agreement by trading-off against key generation rate. In the proposed mechanism, the channel sampling is done in the course of routine transmission. Low complexity filtering controls the actual source of bit differences and channel entropy is created based on the human movement. Channel entropy is needed here for key generation. Experimental results exhibit that the scheme is of low cost and does not require dedicated channel sampling or information reconciliation. It is also able to generate high entropy key bits at a rate that is very much suitable for key renewal.

In order to satisfy users' requirement for key generation rate and to use the wireless channel in an efficient way, Wei et al. introduced an adaptive channel probing system as shown in Figure 4 based on Lempel-Ziv complexity and PID (Proportional-Integral-Derivative) controller [20]. The authors used the concept of Lempel-Ziv complexity to obtain accurate estimates of the entropy rate. The PID controller is used to dynamically alter the probing rate to stabilize the key generation rate according to the user's requirement.

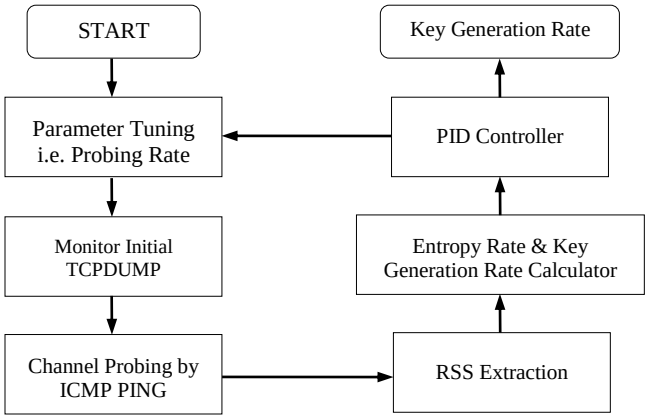

Figure 4: Workflow of adaptive channel probing system.

Further, the authors build a mathematical model for channel probing and derived that the key generation rate is proportional to probing rate. Furthermore, they proposed a utility function and showed that the probing rate is inversely related to utility. Nevertheless, if a sensor wants to generate a key within a given time, high probing rate is required. A series of experiments are conducted by the authors to test the performance using different speeds, different mobile types, different sites and different key generation rates. Experimental results show that the proposed channel probing system can adaptively change its probing rate due to noise, interference, other channel impediments, human movement and environment dynamics. It not only satisfies key generation rate requirement, but also makes the probing process as efficient as possible. However, from the experiments, it is observed that the overshoot of key generation rate is a bit high.

Key generation among a group of wireless devices leveraging RSS is proposed in [4, 40]. The RSS characteristics resulting from shadow fading is robust against some specific outside attacks and this feature is exploited in [4]. Authors consider a passive adversary whose task is to follow the trajectory of one of the communicating node's and eavesdrop on the communication between a pair of sensors. The attacker is able to measure the radio channels used by the communicating pair of sensors. Also, it is able to obtain the key extraction algorithm together with its parameter values. Communication between mobile nodes which are not within each other's communication ranges are achieved by employing relay nodes. The authors

defined a metric called DOSS which represents the difference of RSS measured at a node via different radio channels. These DOSS values are passed to other devices for facilitating key extraction without involving passing of RSS measurements directly. In this work, two protocols are proposed for enabling secret group communication. The protocols are namely star-based and chain-based. They are developed by making use of RSS from multiple devices for performing group key generation collectively. In particular, the star-based collaborative key extraction is designed for scenarios where multiple nodes are within each other's communication range. On the other hand, chain-based approach deals with scenarios where not all the nodes under consideration are within each other's communication range, though they are interconnected through a mobile relay node. Authors developed two building blocks for their framework- fading trend based secret key extraction and relay node assisted collaborative key extraction. The normal RSS measurement technique is combined with threshold RSS measurements for obtaining secret keys. As the fading trend is similar or exact in RSS measurements between pair of nodes, this trend helps in better capturing the similarity, resulting due to channel reciprocity as against RSS measured values. Mobile relay node for key extraction is used by the authors when communicating pair of nodes cannot communicate directly. The mobile relay node is responsible for communicating with the pair of nodes and transmits DOSS values to them. The communicating pair of nodes uses the received DOSS values and the measured RSS readings for secret key generation. Experimental results show that the proposed method achieves lower bit mismatch compared to existing works.

In contrast to earlier schemes, a novel secret key generation scheme is proposed in [21] based on fluctuation of RSS by using electronically steerable parasitic array radiator antenna. Here, fluctuation of RSS is controlled by the reactance values of the antenna. Further, the authors have improved their scheme in [22] by including a received signal strength indicator (RSSI) based interleaving scheme, which enables to acquire more randomized and stronger secret keys. Unlike the works [1-4, 20], a few works [41-43] have considered multiple antenna enabled nodes to generate secret key. The purpose of using multiple antennas is to collect enough mutual information from the channel and subsequently use multi-level quantization technique on the collected information to enhance secret key generation rate. To confirm the enhancement of secret key generation rate, authors [42] have performed testbed experiments and results show that the secret key generation rate increases by four times in multiple antenna enabled nodes compared to single-antenna enabled nodes.

3.1.2 Frequency Selectivity

The phase differences and/or frequency at the receiver depend on the length of the multipaths, environment, and frequency of the signal. Thus, constructive interference on one given frequency can turn into complete destruction of the signal simply by using a different frequency. By measuring the channel response over several different channels, the specific multipaths increase or decrease the resulting signal phase and/or frequency at the receiver unpredictably. By frequency selectivity based

strategies, henceforth, we mean the strategies that are based on measuring the phase differences and/or frequency at the two communicating peers. In this section, we provide description on potential secure key generation methods based on frequency selectivity.

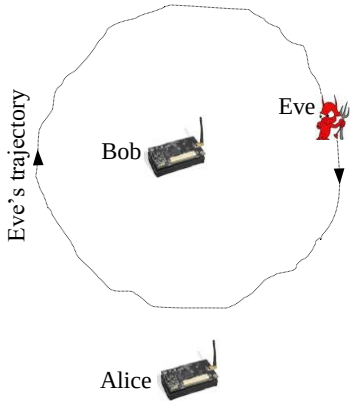

Figure 5: Experimental scenario: Alice and Bob are placed at some distant positions and Eve's moves in close proximity (10 cm) around Bob.

In [5], the authors proposed a key generation protocol based on the frequency-selectivity of channel fading for indoor WSNs. The proposed protocol considers conventional off-the-shelf static sensors without additional equipments e.g., electronically steerable antenna, ultra wideband (UWB) radios. Channel selectivity is considered with respect to position and carrier frequencies. The practical advantage of this approach is that node movement is not required. The authors initially studied the amount of uncertainty the adversary faces. The average amount of information of a discrete random variable is obtained by using the idea of entropy. A stochastic model of the system is designed to get the secrecy of it based on RSS distributions of the measurements. A random vector is considered whose measurements are conducted on different frequencies. If on evaluation, the elements of the random vector are independent, the amount of uncertainty is directly obtained from the entropy values that are derived from individual frequencies. The resultant entropy values provide an upper bound on the joint entropy. To see the magnitude of the effects of these uncertainties, the authors conducted experiments where the position of Eve continuously changes while Alice and Bob try to communicate with each other (Figure 5). The scheme is designed keeping in mind the limited hardware capabilities of sensors. The authors also try to increase the error tolerance of their key generation scheme by using the mean of the collected RSS values. The mean value is designated as a random variable that is distributed depending on the features of wireless propagation. Multi-level quantization is also used for making nearby measurements equal. The key generation protocol works in three phases viz. sampling phase, key generation phase, and key verification phase. The channel state is obtained and correlated measurements are collected by the

authenticated nodes in the sampling phase. The deviations that occur in the sampling phase are corrected in the key generation phase and a secret bit string is formed. The key verification phase is responsible for ensuring correct key agreement. The error correction property of the proposed protocol is able to defend the effects resulting due to measurement errors and temporal activities. The protocol is implemented on MICAz motes and experimental results prove its robustness.

In [6], Wilhelm et al. proposed a protocol based on the frequency selectivity of channel fading for key generation. Similar to [5], here also the authors considered WSN consisting of conventional off-the-shelf static sensors without additional equipments. A random vector is considered that is measured on various frequencies for increasing the volume of information between a pair of sensors. The amount of reciprocity is directly obtained using the entropy values from independent channels. This value is used to represent the upper bound of joint entropy and decrease the overall uncertainty of the adversary. It is known that wireless channels face correlated fading if the distance between the center frequencies is smaller than the coherence bandwidth. So, the authors have analyzed the dependency structure for determining the amount of uncertainty. In other words, the secret behind generation of keys by the protocol is analyzed. Authors have conducted measurements by sampling RSS values of different frequencies. Certain numbers of samples are also collected from the RSS values. The proposed approach does not depend on node movement as the basis of randomness. The protocol also has error correction property that is able to defend the effects of measurement errors and temporal effects. The error tolerance is enhanced by calculating the mean value of the RSS samples. The calculated mean is designated as the random variable that is distributed following Rayleigh or Ricean distributions. The protocol has three phases- sampling phase, key generation phase and key verification phase. In the sampling phase, the communicating pair of sensors exchanges sampling messages on the set of available wireless channels. Samples are collected in an interleaved manner to remove the noise. The key generation phase is responsible for using the information gathered from multilevel quantization that is used for producing an equal bit string on both sides. The key verification phase is used by both parties for verifying that the secret keys were generated successfully.

It has been seen that to construct a good key generation scheme, accurate channel measurement is utmost necessary. To collect precise channel measurements, a dedicated set of hardware and antenna are essential, that alone can record accurate measurements. Therefore, there is a tradeoff between the use of specialized hardware and complexity of the system. In this circumstance, Ambekar et al. [23] proposed a secret key generation method based on the variation of wireless channel without involving any specialized hardware. While proposing the scheme, the authors have assumed that the network consists of conventional sensors and passive adversaries. Here, the passive adversaries are considered as resourceful as sensors and can eavesdrop on all the communication between legitimates sensors, Alice and Bob. In the proposed method, Alice and Bob record the variations in the wireless channel. Based on the measured channel variation, both Alice and Bob construct the channel profile. The collected channel profiles are then enhanced by using a l_1-norm minimization technique [44]. The

enhanced channel profiles are quantized into streams of bits to obtain the preliminary keys. In quantization, the threshold is determined based on the mean of all the values of the enhanced profile. Values above the threshold are quantized as 1 and below are quantized as 0. Finally, the preliminary keys are synchronized using a localized reconciliation technique and their privacy is amplified by generating secure hashes [45].

Wang et al. [24] proposed a secret key generation protocol based on the phase information of channel responses for both static and mobile environments. It is assumed that sensors cannot transmit and receive signals at the same frequency simultaneously. Also, each sensor possesses a single isotropic antenna and employs a maximum likelihood estimator for frequency and phase estimations. On the contrary, in this work, similar to [23], adversaries are assumed as passive. The proposed protocol supports both pair-wise and group key generations. The basic philosophy of key generation protocol is that channel response between two transceivers is unique and location-specific, and the transmitted signals from each other will experience almost the same fading in the phase. The pair-wise key generation protocol comprises of two timeslots for each key generation round. In each timeslot, each node transmits a unit-amplitude sinusoidal primary beacon. After receiving a beacon, a node estimates the channel phase information and converts the estimated channel phase information into bit vectors. Here, the estimated channel phase information is converted into bit vectors according to a pre-defined quantization method. Such bit vector generation operation continues for a pre-defined number of rounds, generating a key of pre-defined size that is finally shared between the nodes.

On the contrary, group key generation protocol comprises of multiple rounds of pair-wise key generation protocol between a group head node and the other group nodes. At the end of each round, every group node possesses a pair-wise key and it continues until the rounds equal the number of nodes in a group. Finally, each node combines the pair-wise computed key to generate a group key of pre-defined size. One of the limitations of this group key generation protocol is that as the number of node increases in the group, the number of interactions between the nodes linearly increases. To alleviate the limitation, the authors proposed a slotted round-trip scheme for group key generation. In this scheme one node that is chosen as an initiator starts the key generation process and transmits the beacons from both clockwise and anticlockwise directions. As the sum of phase estimates obtained from clockwise and counterclockwise transmissions are nearly identical at each node, a common key is effectively generated. In order to enhance the robustness of the proposed scheme, the authors used cryptographic information reconciliation and privacy amplification tools [46, 47] to reconcile bit discrepancies and improve the randomness of the generated keys. The simulation shows that both the proposed pair-wise and group key generation protocols improve the analytical key bit generation rate by a couple of orders of magnitude.

A novel secret key generation scheme is proposed using the channel reciprocity and the time-variant frequency characteristics in [48]. However, the proposed scheme is suitable for OFDM (Orthogonal Frequency Division Multiplexing)

system. Forman and Young [49] examined the secret key generation rate enhancement problem by exploiting frequency characteristics in a higher bandwidth channel. Thereafter, to enhance the secret key generation rate, they divided the wideband channel into number of different and independent sub-channels. Now, normalized phase of these sub-channels are quantized to obtain the secret key with enhanced generation rate. Similar to [24], Sayeed and Perrig [50], Shehadeh et al. [51], Wang et al. [52], Premnath et al. [53], and Zhanget et al. [54] also proposed a secret key generating method based on the phase information of channel response. However, the method proposed in [50] is particularly suitable for wideband channel, whereas the method proposed in [52] is specifically suitable for narrowband channel.

3.1.3 CIR

Unlike RSS, wireless link signature or CIR provides information about the amplitude or gain of different multipath channel components [55]. As such, many more bits can be extracted from each measurement. In this section, we describe state-of-the-art secure key generation works based on CIR measurement.

Zhang et al. [7] proposed a secret key generation technique based on CIR measurements. In the proposed technique, the authors considered that both Alice and Bob are mobile and measured the wireless link signatures at different unpredictable locations and combined these measurements to produce strong secret keys. Here, the adversary, Eve is considered to be able to overhear conversation between pair of nodes. Also, the adversary may be present in locations where the transmitting or receiving node has been in the past or will be there in future. In this work, the CIR magnitude measurement is used as wireless link signature measurement which is actually a vector of 25 channel impulse responses measured over time.

Both devices, Alice and Bob, are mobile and measure the CIR magnitude at j different pair of locations, where j=1,2,…,J and measured CIR magnitudes are stored in themselves. Let C_j be the CIR measurement of the wireless link between Alice and Bob when they are at any jth pair of locations. Therefore, Alice and Bob use a previously agreed upon and publicly known function of these measurements, $f(C_1,C_2,...,C_J)$ to compute the shared key. As the mobility of Alice and Bob is not fully retraceable by Eve, therefore Eve will not be able to compute the secret key. The authors examined the proposed scheme by considering the three mobility models viz. random walk, Brownian motion and Levy walk.

Further, the authors proposed a new Jigsaw encoding method to encode CIR magnitudes and reconcile the differences in the bits extracted between Alice and Bob. To reconcile the bits, Reed-Solomon forward error correction scheme is adopted in the work. Through quantitative analysis it is shown that when movement step size is longer than one foot, the measured wireless link signatures are mostly uncorrelated. Finally, the authors show that the proposed scheme efficiently generates very high entropy secret bits and that too at a high bit rate.

In [8], Hamida et al. proposed a secret key generation method exploiting the reciprocity of UWB channel. Initially, through experiment, authors have validated the reality that secret key generation based on physical layer in a free-space environment will not work. It is due to the fact of insufficient channel variation in free-space environment. It is assumed that the attacker listens to all communications between legitimate nodes and is capable of measuring between itself and each of the communicating nodes. Thereafter, they proposed an adaptive quantization scheme for generating secret key from CIR measurement. In another work [25], Ye et al. proposed a secret key generation method exploiting the International Telecommunication Union (ITU) channels. Unlike the scheme illustrated above, in [26-28, 56, 57], the authors presented an interesting approach for secret key generation from CIR measurement in a multi-antenna, Multiple-Input Multiple-Output (MIMO) system. More interestingly, in [26], the authors have observed through simulation that the length of the established key grows as antennas are added. On the contrary, in [27], the authors have observed that channels with higher order of diversity (higher number of paths) are more suitable for secret key generation. Considering this observation, they proposed two secret key generation schemes. First one is based on channel quantization [50] and another is based on an intelligent Channel Quantization mechanism with Guardbands (CQG). It is mainly based on mitigating errors by the separation of the decision areas by guard bands. Further, CQG mechanism is examined by a group of authors in [29, 30]. In one such work [29], the authors investigated the performance of the CQG mechanism and found expressions for the key generation efficiency and the bit error rate, whereas in [30], the authors derived the optimal quantization and guard band parameters for the CQG mechanism.

3.1.4 Reverse Pilot Signal

In [31], Tsouri and Wulich proposed a reverse pilot signaling technique for generating secret key over single input single output wireless system. Initially, in the proposed technique, both the transmitter and receiver are synchronized. Thereafter, the receiver transmits a pilot signal towards the transmitter so that the latter can estimate the channel from itself to receiver. Based on the results of channel estimation, the transmitter sends a burst of M-PSK data symbols over the same frequency as the pilot signal. The receiver senses the received signal and generates secret key based on a priory known signal constellation. In order to compensate small changes during channel estimation, the receiver uses a decision feedback mechanism. Further, they investigate this key generation mechanism and derive the relation between the efficiency of the source, the coherence bandwidth, and the Doppler bandwidth. Through simulation, the authors have shown that the proposed technique achieves high key generation rate without any overheads on key distribution, enciphering and deciphering.

Further, authors have extended their work in [32] by elaborating the scheme to support a plurality of transmitters in a superposition modulation setting with joint decoding at the receiver. They have shown that the elaborated protocol can be

practically used to obtain information theoretic security with low implementation complexity, no memory requirements and no overhead on throughput and energy.

3.1.5 Bit Error Rate Fluctuation

A new secret key generation scheme based on the fluctuation of Bit Error Rate (BER) considering an OFDM signal transmission is proposed by Kitano et al. [33]. Initially, in the proposed scheme, communicating peers exchange information of channel characteristics among themselves. By interpolating in time at one of the peers, effect of the measurement in time difference is eliminated. Subsequently, the measurement is performed repeatedly at specific time interval to obtain multiple independent channel characteristics, and binary digitized values are generated according to the obtained channel characteristics. While transmitting the binary digitized values, authors have deliberately distorted the signal to introduce bit error, resulting in subsequent increase in bit error rate. They introduced distortion in signal by phase compensation at QPSK demodulation of all sub-carriers. The phase compensation at QPSK demodulation of all subcarriers is done by the detected phase rotation at the center frequency of the OFDM spectrum. Simulation results show that the proposed scheme successfully achieves the key agreement at SN ratio of 15dB in multipath fading environments and the fading frequency is less than 40 Hz. In [34], similar to [33], the authors introduced phase distortion in signals for producing bit error.

3.1.6 Chinese Remainder Theorem

An interesting observation has been made by a group of researchers in their state-of-the-art works [35, 36] related to the Frequency Division Duplex (FDD) systems. They observed that in case of the FDD systems, the complex channel coefficients for transmitting and receiving signals are different. However, if the frequency separation is not too large, the transmitting and receiving signals exhibit the same directional dependence and the multipath angles are reciprocal in FDD systems. Considering this principle, Wang et al. [34] proposed a secret key generation method based on Chinese Remainder Theorem (CRT). They have utilized the reciprocity of the multipath angle and delay in FDD systems for the proposed method. Initially, the communicating peers collect the angles and delays of different multipath signals of each other. In the next step, both measured angles and delays of different multipath signals are quantized. Errors that occur during quantization process are now grouped and shared by communicating peers via public channels. Thereafter, a CRT based error correction method is used to generate the secret key from grouped quantization error. Authors have argued that as the secret key is generated from quantization instead of quantization result, thus the key will not be revealed to eavesdroppers. Through simulation, authors have shown that the proposed method improves the key agreement ratio of legitimate communicating peers even in presence of eavesdropper. In contrast to the earlier works [35, 36], Wang et al. [37] used the reciprocity of the

wireless channel in Time Division Duplex (TDD) mode for their proposed scheme. Also, unlike [35, 36], a CRT based error correction method is used to generate secret key from the channel estimation error.

3.1.7 Reactive Jamming

Aiming at effective and faster generation of secret key, a channel independent method based on reactive jamming by the receiver is proposed by Gollakota, and Katabi [38] and Zheng et al. [39]. The basic philosophy of the proposed method [38] is that the sender transmits two OFDM symbols back-to-back. For each sample in these repeated transmissions, the receiver randomly jams either the sample in the original transmission, or the corresponding sample in the repetition. Since the eavesdropper does not know which signal sample is jammed and which one is clean, it cannot correctly decode the data. Nevertheless, the receiver knows which samples it jammed. Therefore, the receiver picks the correct samples from the signal and its repetition and rearranges them to get a clean signal, which it can decode using standard methods. The authors have examined different modulations such as BPSK, 4QAM, 16QAM, 64QAM and enhanced the efficacy of the proposed method by making it eavesdroppers' location independent. Finally, through real implementation in indoor environment, authors have demonstrated that the proposed method achieves secret key generation rate 3~18 Kb/s with a 0% bit disagreement.

In contrast to the earlier scheme, Zheng et al. [39] proposed a secret key generation scheme where the destination node simultaneously acts as a receiver as well as a jammer. In particular, while receiving data, the receiver transmits jamming noise to degrade the eavesdropper channel. In the proposed work, the authors have considered that the source has single antenna whereas both the receiver and eavesdropper has multiple antennas. Also, it is assumed that the receiver operates at full duplex mode.

3.2 Key Sharing Strategies

In this section, existing secret key sharing strategies are discussed.

3.2.1 RSS

Barsocchi et al. [12] have introduced a security scheme that exploits the unpredictable and erratic behaviour of wireless communication for key generation and sharing. This work considers Ambient Assisted Living (AAL) scenarios. Key generation and sharing for both static and mobile sensors are considered. Static sensors form a portion of the infrastructure of the AAL system while mobile sensors are applied on the body of a person. In this context, static sensors implement complex key generation/distribution protocols and are subjected to constant monitoring as well as maintenance. Mobile sensors are allowed to dynamically enter/exit the AAL space as there is a possibility of their deployment on an elder or impaired person. Therefore, mobile sensors are much more prone to attacks and so providing security to these sensors is very crucial. The

randomness that is introduced by the mobility of the user's body greatly helps in the process of entropy harvesting for generation of keys. The scenario considered in this work consists of three main entities, namely user, adversary and smart space. Secure communication is requested by the user with smart space so that no adversaries can breach the user's privacy. The smart space is essentially an intelligent environment envisioned to provide service to the users and is connected to the internet. It is characterized by Secure Network Infrastructure (SNI) that is composed of sensor nodes that can communicate securely among themselves. The user contains a sensor which communicates with the smart space via the SNI. On-board RSSI estimation capability is provided to the sensor's radio for estimating the received signal strength of every received packet. The SNI authenticates the sensor of the user using the pre-loaded secret key. The adversary is assumed to be global eavesdropper and is responsible only for gathering as much information as possible avoiding code injection strategies for attacking. So, in this scenario security can be provided by introducing a fresh randomness i.e. a data unknown to the adversary. This scheme is implemented in a real-world scenario. It is effective against the adversary behaviour in four different cases: brute force on the on-fly packet, sensor compromise, RSSI guessing attack, and finally, symbols statistical analysis. Analysis shows how different factors affect the amount of randomness collected from the environment and also shows that guessing attacks from an eavesdropper are negligible.

3.2.2 Frequency Selectivity

The work in [58] uses the reciprocity of the wireless channel response between two transceivers as a correlated random variable. A random vector is formed from several frequencies and the shared secret key is derived from that random vector. Error correction techniques are applied to control the trade-off between the extent of secrecy and the strength of the protocol. The protocol is applicable in both static and dynamic networks. The probe phase of the protocol is responsible for collecting samples of the channel responses obtained from the available channels. The mean of every sample is also calculated. A set of samples is gathered for reducing the cause of temporal effects on the measurements. The maximum amount of entropy is extorted in the key generation phase using a suitable code having a specific tolerance. Depending on the error that can be possible in the measurements, a different parameter may be used for every channel. To ensure successful creation of the secret key, a challenge-response scheme is used in the acceptance phase. The protocol provides guarantee in finding a shared secret if the deviations between the sender and receiver are restricted. Here, sender and receiver are considered as static conventional sensors equipped with CC2420 radio transceiver chips using omnidirectional antennas. The performance and robustness of the protocol are proved by considering different distances with both line of sight and without line of sight connections. Experimental results show that the protocol is applicable on resource-constrained nodes and the use of channel response is stable as well as unpredictable for generating information on shared key.

3.2.3 CIR

Wilson *et al.* [59] were one of the first to propose a key sharing method called channel identification on the philosophy of theory of reciprocity for antennas and electromagnetic propagation. The authors have considered indoor environment and UWB CIR as a source of common randomness between sender and receiver pair. Initially, they revealed that, under some common UWB channel model, the secret key sharing rate is upper bounded by the mutual information between the observations of each receiver. Based on this fact, the authors derived expressions of mutual information between the channel observations, which form an upper bound on the average secret key rate under single and multiple propagation paths. Further, they examined the variation of average secret key rate as a function of the signal bandwidth. Interestingly, they found that the maximum secret key rate does not increase monotonically with signal bandwidth. Accordingly, they derived the optimal signaling bandwidths to maximize the sharing rate of secret key as a function of SNR for some typical channel excess delays. Finally, the proposed channel identification scheme is validated considering various public communication methods such as Reed-Muller, Trellis Codes and simulation results reveal that such channel identification scheme is feasible. Although, the secret key sharing method is validated in various public communication methods, however, the secret key extraction process is prone to errors and requires strong signals to work reliably.

3.3 Randomness Extraction Strategies

Due to the reciprocity property of electromagnetic propagation, the same key is expected to be derived by the communicating pairs. However, randomness extraction of secret key bits from noisy radio channel measurements at communicating pairs is a major statistical signal processing problem. Under this scenario, the communicating pairs obtained varied channel estimations, which may lead to some discrepancies in the derived keys. To overcome this problem, the researchers devised number of strategies based on RSS, CIR etc. In this section, we reviewed the recent approaches in this area.

3.3.1 RSS

The effectiveness of randomness extraction using RSS variations on the wireless channel between pair of sensors is evaluated by the authors in [60-62]. Particularly, in [60, 62], the authors have used real life measurements of RSS in different environmental settings considering passive adversaries. From their results the authors found that in some environments the extracted bits have very low entropy due to lack of variations in the wireless channel. They found that the bits obtained from low entropy were not suitable for secret key generation. Also, they found that prediction of randomness in static environments becomes easier for adversaries whereas in dynamic environments high entropy bits are obtained quite fast. The authors developed an environment adaptive randomness secret key extraction scheme that uses an adaptive lossy quantizer

along with Cascade-based information reconciliation [63] and amplification [64]. The proposed randomness extraction scheme consists of three components viz. quantization, information reconciliation and privacy amplification. The scheme is implemented in two nodes. Specially crafted 802.11 management frames are used for communication in place of standard frames. The authors have designed their own acknowledgement receipt mechanism. Beacon frames are used between the sender and the receiver. The sequence number field of the beacon packet is used as the proposed protocol's sequence number for handling packet loss and retransmissions. The communicating parties exchange twenty beacon frames per second. Finally, the authors show that the secret key generation rate is increased when multiple sensors are involved in the randomness extraction process.

In [15], randomness extraction of secret key bits from noisy radio channel measurements between pair of nodes is addressed. The authors consider the problems of non-simultaneous directional measurements, correlated bit streams, and low bit rate of secret key generation. Here a framework named as High Rate Uncorrelated Bit Extraction (HRUBE) is proposed for interpolating, transforming for de-correlation, and encoding channel measurements using a multi-bit adaptive quantization scheme. This quantization scheme allows multiple bits per component. Three signal processing methods, namely Fractional interpolation, De-correlation transformation and Multi-bit Adaptive Quantization (MAQ) are used for bit extraction. Fractional interpolation induces various amounts of delay at every node for substantiating the fact that two directional measurements are not done simultaneously. De-correlation transformation is responsible for generating a measurement vector having uncorrelated components using Karhunen-Lo'eve transformation of the original channel measurement vector. MAQ performs the task of converting real valued channel measurements into bits based on the measured value. This is done using communication to facilitate agreeing of the two nodes on the quantization scheme. Here, all these processes are used for transforming correlated, real valued radio channel signal measurements into uncorrelated binary data at the two nodes. The combination of the methods is referred as HRUBE. The objective of quantization in this work is to obtain long length secret key and error minimization by lowering the probability of the secret key to such an extent that it does not match at the two nodes. Zero covariance between elements of secret key is also maintained here. Experimental data is used for proving the efficiency of this scheme. Similar to [60, 62], this scheme also works against passive adversaries.

In another work [65], a group of researchers proposed a more robust bit extraction method, called adaptive ranking-based uncorrelated bit extraction, on the basis of HRUBE framework. Compared to [15], the proposed scheme reduces the non-reciprocities caused due to different hardware characteristics by including a ranking step after the interpolation filtering. In a recent work, Zan et al. [66] examined the robustness of randomness extraction process by RSS measurement against active attacks. Unlike the existing works, authors have proposed a differential technique to derive secret key. Further, the same group of authors extended their work in [67] by introducing two agreement algorithms. The first algorithm allows two

legitimate nodes to derive a common secret key through an information-theoretic manner. The second algorithm uses the channel diversity property to generate secret key between a central server and a node. Considering the secret key generation scheme proposed in [22], Yasukawa et al. [68] proposed a scheme to increase the randomness extraction rate. They have applied a multilevel quantization technique to achieve the same.

3.3.2 Frequency Selectivity

In [69], Shehadeh et al. proposed a randomness extraction mechanism based on quantizing the phase information of channel responses. To start with, they explored the effects of delay between the channel estimates at two nodes and node mobility on the performance of the key generation procedure. It is revealed that, in mobile scenario, the channel estimation needs to be performed in a very short period. Thereafter, authors studied the correlation between mobility and the randomness extraction of secret bits, and investigated the overall key generation rate as a function of the Doppler spread. They found that from a single channel observation as a function of the Doppler spread, leads to a lower average number of secret bits generation. Finally, through simulation, they confirmed that that mobility is in fact an advantage due to the faster decorrelation of the channel permitting a faster re-keying. The results demonstrated that the overall secret bit extraction rate increases as a function of mobility despite the lower average number of secret bits generated per single channel realization.

3.3.3 CIR

Ye et al. [70] developed two different techniques for randomness extraction of secrets from the channel state between a pair of nodes in a richly scattered wireless environment. In the first technique, a simple algorithm entitled as level crossing algorithm is proposed. The level crossing algorithm is based on the observation of correlated excursions in the measurements between a pair of nodes. The authors have incorporated a self-authenticating mechanism in the algorithm to prevent adversarial manipulation of message exchanges during the algorithm. The proposed level crossing algorithm is well-suited for environments that can be characterized as Rayleigh or Rician fading models associated with a richly scattered environment. Since, in the first technique, the time-varying nature of the channel acts as the source of randomness, it limits the number of random bits that can be extracted from the channel for the purpose of a cryptographic key. To overcome the limitation of the first technique, the authors proposed the second algorithm. This second algorithm is motivated by observations from quantizing jointly Gaussian processes, but exploits empirical measurements to set quantization boundaries and a heuristic log likelihood ratio estimate to achieve an improved secret key generation rate. The proposed second algorithm is applicable to more general distributions for the shared channel information between a pair of nodes, and is able to achieve improved secret key extraction rates at the tradeoff of increased complexity. The adversary considered for this

work mainly deals with passive attacks. Finally, the authors validated both proposed algorithms through experimentations using a customized 802.11a platform, and showed that the reliable secret key establishment can be accomplished at the rate of 10 bits/second.

Similar to [26-28], Chen and Jensen [71] have also considered the MIMO system and proposed an interesting randomness extraction scheme from CIR measurement. The paper further discusses several error reduction techniques such as gray coding, least-square estimation, channel averaging, and LDPC codes that can efficiently enhance key agreement between multiple-antenna nodes. A different attempt has been made by Ye et al. [72]. They proposed a randomness extraction scheme by measuring CIR from jointly Gaussian random variables. They derived the secret key capacity as a function of the received Signal-to-Noise Ratio (SNR). More recently, Liu et al [73] proposed a randomness extraction technique by quantizing the amplitude of OFDM subcarriers. Experimental results reveal that the proposed technique is able to achieve higher key extraction rate compared to RSS based technique. Finally, the authors show that the proposed technique is resilient to predictable channel attack [60], and stalking attack [4].

3.3.4 Accelerometer

In [74], Owusu et al. have shown that accelerometer readings are a powerful side channel that can be used to extract secret key between a pair of nodes. This possesses two difficulties: privacy invasion through unauthorized access and the fact that the accelerometer does not require special privileges for accessing operating systems. They have devised a predictive model that is trained for only acceleration measurements of password entry. Inference accuracy is evaluated as a function of number of parameters like sampling frequency of the accelerometer etc. The proposed application is compliant with the Android developer in terms of use. This application has two collection modes: area and character. The area mode interface consists of a 10×6 array of buttons. The size of the buttons is similar to the size of the buttons found on standard Android keyboards. The area mode data collection screen is developed mainly for two reasons: (i) for evaluating the inference accuracy at different levels of granularity for obtaining information about the noisy accelerometer data streams, and (ii) for quantifying the fact that certain regions of the screen reveal more information about keystrokes given a specific typing style. The character mode interface is made up of a QWERTY keyboard arranged similarly to the Android soft keyboard screen. The character mode is considered the testbed for the keystroke reconstruction attack. Here, data analysis consists of three main phases, namely preprocessing, feature subset selection, and classification. Data collection was done from four participants using the HTC ADR6300 node. Participants were all regular smart phone users between the ages of 18 and 30. For the area mode inference experiment, data was collected for about 1300 key presses, where each one of the 60 screen areas received approximately 20 positive samples. Participants were instructed to press keys in any order until all of the keys received at

least one press prior to each data collection run. K-fold cross-validation was used for testing. For the character mode inference experiment, training data was collected for about 2700 key presses. For getting uniform sampling intervals throughout, the dataset linear interpolation is used. Interpolation provides smoothing of data that defends baseline signal noise in the data. Preprocessing the raw acceleration measurements produces a modified dataset. Feature selection is done by obtaining the set of 46 features for every preprocessed acceleration stream. The first eleven features summarize the acceleration stream information for each dimension separately. For ensuring selection of an optimal set of features for the classification task, the Wrapper feature subset selector is used [75]. The Wrapper algorithm is combined with a classification algorithm and is responsible for performing exhaustive searches through the feature space for the set of features that maximizes a pre-specified "evaluation measure". Here authors have considered evaluation measure as the cumulative classification accuracy of their model. Classification operation is involved with selecting acceleration streams that correspond to particular touch events. A feature vector is taken as input where the output is a prediction label. In the area mode analysis keystrokes are identified as a hierarchical classification problem. Each area of the screen is divided into two portions recursively. Individual keys are then classified within each new sub-area. Key accuracy of every subdivision is calculated by taking the cumulative product of the accuracies for each subdivision. Authors show that accelerometer measurements can be used to extract 6-character passwords using a few trials.

3.4 Summary of Performance

In earlier sections, existing works on entropy harvesting and key generation and sharing under various categories were discussed. It is worthy noting from the above discussions that the RSS based security design mechanisms are dominating than other categories as they are easily obtained from wireless device drivers [1-4]. Since no additional hardware is required in RSS based scheme, the RSS based security design mechanisms are cost saving. Further, it is seen that the RSS based security design is equally effective in both static and mobile scenarios [1, 18]. Although, the RSS based security design mechanisms are applicable only for pair-wise key generation, however it is capable of generating secret key at fair rate. On the contrary, the CIR based security design mechanisms are most suitable in static scenario compared to mobile scenario [7, 8]. Even though, the CIR based security design mechanisms are capable of providing high key bit generation rate, but such mechanisms require advance channel estimation technique and time synchronization. Similar to RSS based methods, frequency selectivity based security design techniques are equally effective in both static and mobile scenarios [24, 52]. In addition, these mechanisms are capable of securing both the pair-wise and group communications. However, frequency selectivity based security design technique can only provide coarse-grained information of the radio channel and thus key bit

generation rate is very low. To provide an overall comparison, we summarize the pros and cons of these three physical layer based secure key design mechanisms in Table 2.

Table 2: Pros and Cons of different secure key design approaches

Category	**Advantage(s)**	**Shortcoming(s)**
RSS based	• RSS readings are readily available in the existing wireless infrastructure and thus, it makes key generation using off-the-shelf devices feasible without significant hardware modifications. • RSS-based schemes are more robust to synchronization issues.	• RSS based methods either use only the deep fades or RSS measurement above or below the threshold, the other samples are all discarded. • RSS based methods that are only applicable for pair-wise key generation. • The key bit generation rate supported by RSS-based methods is low.
Frequency selectivity based	• Frequency selectivity based approaches work in both static and mobile environments. • Support both pair-wise key and group key generation.	• Single frequency can only provide coarse-grained information of the radio channel and do not provide sufficient entropy in practical environments.
CIR based	• CIR based methods do not require device movement during key establishment. • The key bit generation rate supported by these approaches is high.	• CIR based methods require advanced channel estimation techniques and time synchronization.

Since different experimental methods like testbeds, simulations are used by the authors to evaluate the performance of the proposed mechanisms, thus posing a difficulty for finding a common ground to evaluate them. It is worth noting that a quantitative comparison of these algorithms is infeasible on account of a lack of information given by the authors. Hence, for a better understanding, we compared the performance of the discussed schemes on the basis of the following parameters: design approach, types of nodes, adversary, secret bit generation rate, secret bit mismatch rate, energy efficiency, communication overhead, and processing overhead. The comparison of existing physical layer based secure key generation, sharing, and extraction techniques are presented in Tables 3, 4, and 5, respectively. The not available (N/A) entry in Tables 3, 4, and 5 indicates that a particular scheme does not measure the metric while evaluating the performance of the proposed technique. Note that this section is not meant to be an exhaustive evaluation comparison of the state-of-the-art mechanisms. This is left as a future work.

- *Design approach*: The design approach metric indicates the key philosophy of the proposed physical layer based secure key design schemes such as RSS, CIR, frequency selectivity etc.
- *Type of nodes*: It indicates whether static and/or mobile nodes are used by the authors during devising the schemes. An adversary can set up different types of attack on the network such as node capture attack, denial-of-service attacks and each of such attack focuses on different goals depending on their knowledge on the resource-limitation of the sensor nodes. The attacks can be classified in different ways but generally they are passive or active [76]. Passive attacks aim to

obtain transmitted information by eavesdropping without disrupting the protocol operations. On the contrary, active attacks are involved in the alteration process by the adversary or creation of false messages.

- *Secret bit generation rate (BGR)*: BGR represents the number of secret bits extracted/generated per measurement.
- *Secret bit mismatch rate (BMR)*: For key extraction between a pair of communicating nodes, BMR is defined as the number of bits that do not match between two nodes divided by the number of bits extracted from quantization process [73]. For group key extraction, it is defined as the averaged bit mismatch rate from all pairs of nodes in the group [73].
- *Energy efficiency (EE)*: Energy is a critical resource of WSN since it is one of the main elements that define the survivability of the network. Deciding if a security technique is suitable for a specific application highly depends on the energy efficiency i.e. how efficiently energy consumption is taking place during the protocol's functionality.
- *Communication overhead (CO)*: Each physical layer based security design mechanism follows its own approach based on the application's objectives and requirements. These procedures create communication overhead with the messages that need to be exchanged between nodes during the setup, data forwarding and maintenance phases of each procedure. Therefore, the algorithms that evaluate how many messages are transmitted are considered under this criterion. This may be a concern for security related packets, e.g. key setup, control and data packets.
- *Processing overhead (PO)*: The security design approach taken by each mechanism creates a computation overhead related to the processing of signals and quantization. These are aspects that are calculated by protocols that assess the processing overhead of their approach.

Table 3 shows the comparison of physical layer based secure key generation protocols on the basis of parameters mentioned in earlier paragraph. It is worth noting from the table that the RSS, frequency selectivity, and CIR based security mechanisms are more mature than other techniques. Although the RSS, frequency selectivity, and CIR based security mechanisms have been extensively evaluated in the literatures, proposed solutions both theoretical and practical ones have several limitations. In fact, many approaches rely on strong assumptions which generally do not hold in practice, such as the densely crowded environment considered in several papers. Further, in nearly all cases, it is assumed that the legitimate nodes, Alice and Bob have collected a sufficiently large number of channel estimates which also does not hold in practice. As shown in Table 3, nearly all the RSS – with the relevant exceptions of [4, 24], and reverse pilot signaling based security mechanisms are more energy efficient than the other categories. It is due to the fact that the mechanisms in these categories have low communication overhead and moderate processing overhead. Also, it is noticed that CIR based mechanisms have least BMR and high processing overhead- except [5]. Furthermore, the frequency selectivity based mechanisms exhibit a high BMR, and at the same time, achieves a moderate performance in terms of its energy efficiency, and communication

overhead. Finally, it is shown that the recently developed security mechanisms such as fluctuation of BER, CRT, reactive jamming are most suitable in static scenario compared to mobile scenario, and at the same time achieves a moderate performance in terms of its energy efficiency except [36].

Table 3: Comparison of secure key generation protocols

Schemes	Design Approach(s)	Type of Nodes	Adversary	BGR	BMR	EE	CO	PO
Barsocchi et al. [1]	RSS	Static and mobile	Passive	N/A	0.1	High	Low	Low
Barsocchi et al. [2]		Static	Passive	0.278	NA	Moderate	Low	Moderate
Ali et al. [3]		Mobile	Passive	0.083	1~8	Moderate	Low	Moderate
Liu et al. [4]		Mobile	Passive	2	0.029~0.073	Low	High	High
Mathur et al. [18]		Static and mobile	Active and passive	10^{-7}	< 1	High	Low	Low
Aono et al. [21]		Mobile	N/S	0.333	2	Moderate	High	Moderate
Zeng et al. [42]		Mobile	Passive	0.3~0.8	0.1	Moderate	Moderate	High
Wilhelm et al. [5]	Frequency selectivity	Static	N/A	20~40	0.03	Moderate	High	Moderate
Wilhelm et al. [6]		Static	N/A	N/A	N/A	Moderate	Moderate	High
Wang et al. [24]		Static and mobile	Passive	> 100	0.15 <	Low	High	High
Forman and Young [49]		Static	N/A	640	N/A	Moderate	Moderate	High
Shehadeh et al. [51]		Static	Passive	90	0~0.9	Moderate	Moderate	High
Wang et al. [52]		Static and mobile	Passive	150~650	2~5	Moderate	Moderate	High
Zhang et al. [7]	CIR	Mobile	Passive	2.59~5	0.0032~0.038	Moderate	Moderate	High
Hamida et al. [8]		Mobile	Passive	1	N/A	Moderate	Low	High
Wallace [27]		Static	Passive	0~0.1	0~0.01	Moderate	Moderate	High
Wallace et al. [28]		Static	Passive	7.3~16.9	0~0.001	Moderate	Moderate	High
Wallace et al. [57]		Static	Passive	0~0.1	0~0.1	Moderate	Moderate	High
Tsouri and Wulich [31]	Reverse pilot signaling	Mobile	N/A	20~40	N/A	Moderate	Low	Moderate
Tsouri and Wulich [32]		Mobile	N/A	20~40	N/A	High	Low	Low
Kitano et al. [33]	Fluctuation of BER	Static	N/A	11	0~5	Moderate	Moderate	High
Kitano et al. [34]		Static	N/A	80	N/A	Moderate	Moderate	High
Wang et al. [36]	CRT	Static	Passive	40	0~0.01	Moderate	Moderate	Low
Wang et al. [37]		Static	Passive	1~10	0~0.1	Moderate	Moderate	Moderate
Gollakota, and Katabi [38]	Reactive jamming	Static	Active	3000~18000	0.01~0.0001	Moderate	Moderate	Moderate
Zheng et al. [39]		Static	Passive	6	N/A	Moderate	High	Moderate

Table 4 shows the comparison of physical layer based secure key sharing mechanisms on the basis of parameters mentioned earlier. It is worth noting from the table that only a handful number of works has been proposed so far. To summarize, CIR based strategy shows high BGR and low BMR compared to the other two strategies. It is expected as CIR based security mechanism utilizes advance channel estimation strategy to share secret bits. Further, it is noticed that CIR based security mechanism exhibits high energy efficiency, and at the same time, provides low communication and processing overheads. Similar to CIR based mechanism, RSS based mechanism also exhibits high energy efficiency, and at the same time, provides low communication and processing overheads. Nevertheless, the BGR is significantly less in RSS based mechanism compared to CIR based mechanism. Further, it is noticed that the BMR is fairly high in RSS based mechanism while it is significantly less in frequency selectivity based mechanism. Finally, it is shown that frequency selectivity based mechanism achieves a moderate performance in terms of its energy efficiency, communication overhead, and processing overhead.

Table 4: Comparison of secure key sharing protocols

Schemes	Design Approach(s)	Type of Nodes	Adversary	BGR	BMR	EE	CO	PO
Barsocchi et al. [12]	RSS based	Static and mobile	Passive	0.9~1	1	High	Low	Low
Wilhelm et al. [58]	Frequency selectivity based	Static	Passive	N/A	0.05	Moderate	Moderate	Moderate
Wilson et al. [59]	CIR based	Mobile	Passive	95~150	0.5~0.06	High	Low	Low

The comparison of physical layer based secure key extraction techniques is shown in Table 5. Similar to the earlier two tables, same parameters are considered in Table 5. It is worth noting that except RSS and CIR based mechanisms, none of the other techniques are extensively studied by the researchers. Even though the RSS, and CIR based security mechanisms have been rigorously evaluated in the literatures, proposed solutions have several limitations. In fact, most of the approaches rely on strong assumptions which generally do not hold in practice, such as Eve cannot be very close to either Alice or Bob while Alice or Bob are extracting their secret key. Further, in nearly all cases, it is assumed that Eve cannot jam the communication channel between Alice and Bob which actually does not holds in practice. To summarize, except RSS based strategies, nearly all the strategies except [62] show fairly high BGR and less BMR. It is expected since in RSS based security mechanism, RSS measurement above or below a threshold is discarded, resulting in low secret bit extraction rate. Finally, it is noticed that nearly all RSS except [15], CIR except [73], and accelerometer based security mechanisms exhibit moderate energy efficiency, and at the same time, provides high communication and processing overheads. In contrast, frequency selectivity

based mechanism exhibits high energy efficiency, and at the same time, provides low communication and processing overheads.

Table 5: Comparison of secure key extraction protocols

Schemes	Design Approach(s)	Type of Nodes	Adversary	BGR	BMR	EE	CO	PO
Patwari et al. [15]	RSS based	Static	Passive	22	0.482	Low	High	High
Jana et al. [60]		Static and mobile	Passive	0.533	0~0.55	Moderate	Moderate	Low
Premnath et al. [62]		Static and mobile	Active	0.055~0.4	0.02~0.24	Moderate	Moderate	Low
Croft et al. [65]		Static	Passive	0.38~1	0.01~0.07	Moderate	Moderate	High
Zan et al. [66]		Mobile	Active	100~150	0.005~0.02	Low	High	High
Shehadeh et al. [69]	Frequency selectivity based	Mobile	Passive	45~67	0.5~0.001	High	Low	Low
Ye et al. [70]	CIR based	Static and mobile	Passive	9~13	0~0.16	Moderate	Moderate	High
Chen and Jensen [71]		Mobile	Passive	5~20	0.01~0.001	Moderate	High	Moderate
Liu et al. [73]		Static and mobile	Passive	60~90	3~5	Low	High	High
Owusu et al. [74]	Accelerometer	Mobile	Passive	29~60	N/A	Moderate	High	Moderate

4. Future Research Directions

This section summarizes the different areas for secret key generation, randomness extraction and sharing that can be explored in future.

- Cyber physical systems are emerging as a promising area for secret key generations that are drawing the attention of researchers. Many areas such as entropy and probability of key agreement relationship, analysis on how radio source interferences can affect secret key agreement etc. can be taken up by researchers.
- Wireless networks are very much prone to different kinds of attacks. In this perspective more work can be done considering several attacks that have not been addressed till now as very few works have undertaken specific attacks that can be launched by adversaries in the context of key generation, randomness extraction or sharing.
- Exploiting multiple antenna diversity for studying opportunistic channel probing in wireless networks along with application of other amplification techniques for efficient key combination can be interesting topics for future research.
- Secure key generation in the physical layer is a topic that has not been deeply explored so far. Also the possibility of real implementations of CIR-based key generation needs to be validated.
- Security issues in the physical layer for multiuser systems have been dealt with by very few works. For example, improvising the robustness of key extraction mechanism in the physical layer by introducing mobility is an interesting

area of research that can be carried out in future. Also the application of the existing physical layer techniques in commercially deployed wireless systems needs to be tested.

- Another field of research that has not been explored to a large extent is the cross-layer issues while handling secure key generation, randomness extraction or sharing.
- For body area networks the study of multi-party key agreement between communicating devices and countermeasures against active attackers are areas that demand the attention for future research.
- Another important area that has been largely unexplored is what role active attacks such as jamming may play while information bits are exchanged during the key setup phase. This is because the active adversaries can very much eavesdrop on the communication as well as disrupt message transfers. So, mechanisms need to be devised to overcome such adversaries so that crucial communication leading to key generation, randomness extraction or sharing is not affected.

5. Conclusion

WSNs have become an important area of research since the last decade and many new areas are being explored that will facilitate the use of such networks in real life implementations. These networks are susceptible to various forms of attacks mainly because of their broadcast nature of communication and deployment in areas inaccessible to human beings. As such different physical layer based security techniques have been devised in the past that ensure secure generation, sharing and extraction of keys used for communication in WSNs. This survey work deals with the objective of providing a vivid description to readers on works that deal with secure key generation, randomness extraction and sharing of keys involving different mechanisms. It mainly draws the attention of works that involve the mechanism of variations in the received signal strength followed by other methods such as frequency selectivity and other innovative techniques such as accelerometer based. Finally, the survey winds up giving possible directions of future work in this area.

References

[1] P. Barsocchi, S. Chessa, I. Martinovic, G. Oligeri, A Cyber-Physical Approach to Secret Key Generation in Smart Environments, *Journal of Ambient Intelligence and Humanized Computing*, vol. 4, no. 1, pp. 1-16, 2013.

[2] P. Barsocchi, G. Oligeri, C. Soriente, SHAKE: Single HAsh Key Establishment for Resource Constrained Devices, *Ad Hoc Networks*, vol. 11, no. 1, pp. 288-297, 2013.

[3] S. T. Ali, V. Sivaraman, D. Ostry, Zero Reconciliation Secret Key Generation for Body-Worn Health Monitoring Devices, *Proc. of 5th ACM Int'l Conf. on Security and Privacy in Wireless and Mobile Networks*, pp. 39-50, 2012.

[4] H. Liu, J. Yang, Y. Wang, Y. Chen, Collaborative Secret Key Extraction Leveraging Received Signal Strength in Mobile Wireless Networks, *Proc. of 31st IEEE INFOCOM,* pp. 927-935, 2012.

[5] M. Wilhelm, I. Martinovic, J. B. Schmitt, Secure Key Generation in Sensor Networks Based on Frequency-Selective Channels, *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779-1790, 2013.

[6] M. Wilhelm, I. Martinovic, J. B. Schmitt, Secret Keys from Entangled Sensor Motes: Implementation and Analysis, *Proc. of 3rd ACM Int'l Conf. on Wireless Network Security*, pp. 139-144, 2010.

[7] J. Zhang, S. K. Kasera, N. Patwari, Mobility Assisted Secret Key Generation using Wireless link Signatures, *Proc. of 29th IEEE INFOCOM*, pp. 1-5, 2010.

[8] S. T. B. Hamida, J. B. Pierrot, C. Castelluccia, An Adaptive Quantization Algorithm for Secret Key Generation using Radio Channel Measurements, *Proc. of 3rd Int'l Conf. on New Technologies, Mobility and Security, (NTMS)*, pp. 59–63, 2009.

[9] Y. E. H. Shehadeh, D. Hogrefe, A Survey on Secret Key Generation Mechanisms on the Physical Layer in Wireless Networks, *Security and Communication Networks*, vol. 8, no. 2, pp. 332-341, 2015.

[10] T. Wang, Y. Liu, A. V. Vasilakos, Survey on Channel Reciprocity based Key Establishment Techniques for Wireless Systems, *Wireless Networks*, vol. 21, no. 6, pp 1835-1846, 2015.

[11] M. Wilhelm, *Implementation and Analysis of a Key Generation Protocol for Wireless Sensor Networks*, PhD Thesis, 2009.

[12] P. Barsocchi, S. Chessa, I. Martinovic, G. Oligeri, AmbiSec: Securing Smart Spaces using Entropy Harvesting, *Proc. of 1st Int'l Joint Conf. on Ambient Intelligence*, LNCS, vol. 6439, pp. 73-85, 2010.

[13] A. Lempel, J. Ziv, On the Complexity of Finite Sequences, *IEEE Trans. on Information Theory*, vol. 22, no. 1, pp. 75–81, 1976.

[14] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, R. Renner, Unifying classical and quantum key distillation, *Proc. of 4th Theory of Cryptography Conference*, LNCS, vol. 4392, pp. 456-478, 2007.

[15] N. Patwari, J. Croft, S. Jana, S. K. Kasera, High Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements, *IEEE Trans. on Mobile Computing*, vol. 9, no. 1, pp. 17-30, 2010.

[16] K. Ren, H. Su, Q. Wang, Secret Key Generation Exploiting Channel Characteristics in Wireless Communications, *IEEE Wireless Communications*, vol. 18, no.4, pp. 6–12, 2011.

[17] A. Mukherjee, S. A. A. Fakoorian, J. Huang, A. L. Swindlehurst, Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey, *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

[18] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel, *Proc. of 14th ACM Int'l Conf. on Mobile Computing and Networking*, pp. 128–139, 2008.

[19] J. Zhang, M. H. Firooz, N. Patwari, S. K. Kasera, Advancing Wireless Link Signatures for Location Distinction, *Proc. of 14th ACM Int'l Conf. on Mobile Computing and Networking*, pp. 26–37, 2008.

[20] Y. Wei, K. Zeng, P. Mohapatra, Adaptive Wireless Channel Probing for Shared Key Generation, *Proc. of 30th IEEE INFOCOM*, pp. 2165-2173, 2011.

[21] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, H. Sasaoka, Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels, *IEEE Trans. on Antennas and Propagation*, vol. 53, no.11, pp. 3776–3784, 2005.

[22] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, H. Sasaoka, Wireless Secret Key Generation Exploiting the Reactance-Domain Scalar Response of Multipath Fading Channels: RSSI Interleaving Scheme, *Proc. of European Conf. on Wireless Technology*, pp. 173–176, 2005.

[23] A. Ambekar, N. Kuruvatti, H. D. Schotten, Improved Method of Secret key Generation based on Variations in Wireless Channel, *Proc. of 19th Int'l Conf. on Systems, Signals and Image Processing*, pp. 60-63, 2012.

[24] Q. Wang, H. Su, K. Ren, K. Kim, Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks, *Proc. of 30th IEEE INFOCOM*, pp. 1422-1430, 2011.

[25] C. Ye, A. Reznik, G. Sternberg, Y. Shah, On the Secrecy Capabilities of ITU Channels, *Proc. of 66th IEEE Vehicular Technology Conference (VTC-Fall)*, pp. 2030–2034, 2007.

[26] C. Chen, M. A. Jensen, Random Number Generation from Multipath Propagation: MIMO-Based Encryption Key Establishment, *Proc. of IEEE Int'l Symposium on Antennas and Propagation Society*, pp. 1–4, 2009.

[27] J. Wallace, Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits, *Proc. of IEEE Int'l Conf. on Communications (ICC)*, pp. 943–947, 2009.

[28] J. Wallace, R. K. Sharma, Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis, *IEEE Trans. on Information Forensics and* Security, vol. 5, no.3, pp. 381–392, 2010.

[29] X. Sun, W. Xu, M. Jiang, C. Zhao, Improved Generation Efficiency for Key Extracting from Wireless Channels, *Proc. of IEEE Int'l Conf. on Communications (ICC)*, pp. 1–6, 2011.

[30] Y. Shehadeh, D. Hogrefe, An Optimal Guard-Intervals Based Mechanism for Key Generation from Multipath Wireless Channels, *Proc. of 4th IEEE Int'l Conf. on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, 2011.

[31] G. R. Tsouri, D. Wulich, Reverse Piloting Protocol for Securing Time Varying Wireless Channels, *Proc. of 7th IEEE Wireless Telecommunications Symposium (WTS)*, pp. 125–131, 2008.

[32] G. R.Tsouri, and D. Wulich, Securing OFDM Over Wireless Time-Varying Channels using Subcarrier Overloading with Joint Signal Constellations, *EURASIP Journal on Wireless Communications and Networking*, vol. Mar 2009, pp. 1-18, 2009.

[33] T. Kitano, A. Kitaura, H. Iwai, H. Sasaoka, A Private Key Agreement Scheme based on Fluctuations of BER in Wireless Communications, *Proc. of 9th Int'l Conf. on Advanced Communication Technology*, vol. 3, pp. 1495–1499, 2007.

[34] T. Kitano, H.Iwai, H. Sasaoka, Secret Key Agreement Scheme Based on BER Fluctuation in Radio Communication System, *Science and Engineering Review of Doshisha University*, vol. 50, no. 3, pp. 35-42, 2009.

[35] A. Czylwik, Downlink Beamforming for Mobile Radio Systems with Frequency Division Duplex, *Proc. of IEEE Int'l Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 72–76, 2000.

[36] W. Wang, H. Jiang, X. Xia, P. Mu, Q. Yin, A Wireless Secret Key Generation Method Based on Chinese Remainder Theorem in FDD Systems, *SCIENCE CHINA Information Sciences*, vol.55, pp. 1605–1616, 2012.

[37] W. Wang, C. Wang, X. G. Xia, A robust quantization method using a robust Chinese remainder theorem for secret key generation, *Proc of IEEE Int'l Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1904-1907, 2011.

[38] S. Gollakota, D. Katabi, Physical Layer Wireless Security Made Fast and Channel Independent, *Proc. of 30th IEEE INFOCOM*, pp. 1125–1133, 2011.

[39] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, B. Ottersten, Improving physical layer secrecy using full-duplex jamming receivers, *IEEE Trans. on Signal Processing*, vol. 61, no. 20, pp. 4962-4974, 2013.

[40] H. Liu, J. Yang, Y. Wang, Y. Chen, C. E. Koksal, Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation, *IEEE Trans. on Mobile Computing*, vol. 13, no. 12, pp. 2820-2835, 2014.

[41] A. Kitaura, H. Iwai, H. Sasaoka, A Scheme of Secret Key Agreement Based on Received Signal Strength Variation by Antenna Switching in Land Mobile Radio, *Proc. of 9th Int'l Conf. on Advanced Communication Technology,* vol. 3, pp. 1763–1767, 2007.

[42] K. Zeng, D. Wu, A. Chan, P. Mohapatra, Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks, *Proc. of 29th INFOCOM*, pp. 1837–1845, 2010.

[43] S. Im, H. Jeon, J. Choi, J. Ha, Secret Key Agreement with Large Antenna Arrays under the Pilot Contamination Attack, *IEEE Trans. on Wireless Communications*, DOI: 10.1109/TWC.2015.2456894, 2015.

[44] E. Candes, J. Romberg, *l1-magic: Recovery of Sparse Signals via Convex Programming*, October 2005.

[45] *NIST, Secure Hash Standard*, Federal Information Processing Standards, 2002.

[46] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data, *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

[47] B. Kanukurthi, L. Reyzin, Key Agreement from Close Secrets over Unsecured Channels, *Proc. of Advances in Cryptology-EUROCRYPT*, LNCS, vol. 5479, pp. 206-223, 2009.

[48] A. Kitaura, H. Sasaoka, A Scheme of Private Key Agreement Based on the Channel Characteristics in OFDM Land Mobile Radio, *Electronics and Communications in Japan, Part 3 (Fundamental Electronic Science)*, vol. 88, No 9, p 1-10, 2005.

[49] M. A. Forman, D. Young, A Generalized Scheme for the Creation of Shared Secret Keys Through Uncorrelated Reciprocal Channels in Multiple Domains, *Proc. of 18th Int'l Conf. on Computer Communications and Networks, (ICCCN)*, pp. 1–8, 2009.

[50] A. Sayeed, A. Perrig, Secure Wireless Communications: Secret Keys Through Multipath, *Proc. of IEEE Int'l Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3013-3016, 2008.

[51] Y. E. H. Shehadeh, O. Alfandi, K. Tout, D. Hogrefe, Intelligent Mechanisms for Key Generation from Multipath Wireless Channels, *Proc. of 10th IEEE Wireless Telecommunications Symposium (WTS)*, pp. 1–6, 2011.

[52] Q. Wang, K. Xu, K. Ren, Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels, *IEEE Journal on Selected Areas in Communications*, vol.30, no. 9, pp. 1666-1674, 2012.

[53] S. N. Premnath, J. Croft, N. Patwari, S. K. Kasera, Efficient High-Rate Secret Key Extraction in Wireless Sensor Networks using Collaboration, *ACM Trans. on Sensor Networks*, vol. 11, no. 1, article no. 2, 2014.

[54] Y. Zhang, Y. Xiang, X. Huang, L. Xu, A Cross-Layer Key Establishment Scheme in Wireless Mesh Networks, *Proc. of 19th European Symposium on Research in Computer Security(ESORICS)*, LNCS, vol. 8712, pp. 526-541, 2014.

[55] T. H. Chou, V. Y. F. Tan, S. C. Draper, The Sender-Excited Secret Key Agreement Model: Capacity, Reliability, and Secrecy Exponents, *IEEE Trans. on Information Theory*, vol. 61, no. 1, pp. 609-627, 2015.

[56] B. T. Quist, M. Jensen, Bound on the Key Establishment Rate for Multi-Antenna Reciprocal Electromagnetic Channels, *IEEE Trans. on Antennas and Propagation*, vol. 62, no. 3, pp. 1378-1385, 2014.

[57] J. Wallace, C. Chen, M. A. Jensen, Key Generation Exploiting MIMO Channel Evolution: Algorithms and Theoretical Limits, *Proc. of 3rd European Conf. on Antennas and Propagation (EUCAP)*, pp. 1499–1503, 2009.

[58] M. Wilhelm, I. Martinovic, J. B. Schmitt, On Key Agreement in Wireless Sensor Networks based on Radio Transmission Properties, *Proc. of 5th IEEE Workshop on Secure Network Protocols*, pp. 37-42, 2009.

[59] R. Wilson, D. Tse, R. A. Scholtz, Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels, *IEEE Trans. on Information Forensics and Security*, vol. 2, no. 3, pp. 364-375, 2007.

[60] S. Jana S, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments, *Proc. of 15th Annual Int'l Conf. on Mobile Computing and Networking (MobiCom)*, pp. 321–332, 2009.

[61] S. N. Premnath, S. K. Kasera, N. Patwari, Secret Key Extraction in MIMO-Like Sensor Networks using Wireless Signal Strength, *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 1, pp. 7-9, 2010.

[62] S. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. Kasera, N. Patwari, S. Krishnamurthy, Secret Key Extraction from Wireless Signal Strength in Real Environments, *IEEE Trans. on Mobile Computing*, vol. 12, issue 5, pp. 917-930, 2013.

[63] G. Brassard, L. Salvail, Secret Key Reconciliation by Public Discussion, *Proc. of Advances in Cryptology-EUROCRYPT*, LNCS, vol. 765, pp. 410-423, 1994.

[64] R. Impagliazzo, L. A. Levin, M. Luby, Pseudo-Random Generation from One-way Functions, *Proc. of 21st Annual ACM Symposium on Theory of computing*, pp. 12-24, 1989.

[65] J. Croft, N. Patwari, S. K. Kasera, Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors, *Proc. of 9th ACM/IEEE Int'l Conf. on Information Processing in Sensor Networks (IPSN)*, pp. 70–81, 2010.

[66] B. Zan, M. Gruteser, F. Hu, Improving Robustness of Key Extraction from Wireless Channels with Differential Techniques, *Proc. of Int'l Conf. on Computing, Networking and Communications (ICNC)*, pp. 980–984, 2012.

[67] B. Zan, M. Gruteser, F. Hu, Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems, *IEEE Trans. on Vehicular Technology*, vol. 62, no. 8, pp. 4020-4027, 2013.

[68] S. Yasukawa, H. Iwai, H. Sasaoka, A Secret Key Agreement Scheme with Multi-level Quantization and Parity Check using Fluctuation of Radio Channel Property, *Proc. of IEEE Int'l Symposium on Information Theory (ISIT)*, pp. 732–736, 2008.

[69] Y. E. H. Shehadeh, O. Alfandi, D. Hogrefe, Shehadeh, On Improving the Robustness of Physical-layer Key Extraction Mechanisms Against Delay and Mobility, *Proc of 8thInt'l Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1028–1033, 2012.

[70] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N. B. Mandayam, Information-theoretically Secret Key Generation for Fading Wireless Channels, *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 2, pp. 240-254, 2010.

[71] C. Chen, M. A. Jensen, Secrecy Extraction from Increased Randomness in a Time-Variant MIMO Channel, *Proc. of IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, 2009.

[72] C. Ye, A. Reznik, Y. Shah, Extracting Secrecy from Jointly Gaussian Random Variables, *Proc. of IEEE Int'l Symposium on Information Theory*, pp. 2593–2597, 2006.

[73] H. Liu, Y. Wang, J. Yang, Y. Chen, Fast and Practical Secret Key Extraction by Exploiting Channel Response, *Proc. of 32rd IEEE INFOCOM*, pp. 3048-3056, 2013.

[74] E. Owusu, J. Han, S. Das, A. Perrig, J. Zhang, Accessory: Password Inference using Accelerometers on Smartphones, *Proc. of 12th Workshop on Mobile Computing Systems & Applications*, article no. 9, 2012.

[75] R. Kohavi, and George H. John, Wrappers for feature subset selection, *Artificial intelligence*, vol. 97, no. 1, pp. 273-324, 1997.

[76] A. Ghosal, S. Halder, Security in Mobile Wireless Sensor Networks: Attacks and Defenses, *Cooperative Robots and Sensor Networks*, pp. 185-205, 2015.