Lietzen, Jari; Tirkkonen, Olav

Secret Key Generation Between Ambient Backscatter Devices

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2023.3243063

Published: 07/02/2023

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 December 2022, accepted 29 January 2023, date of publication 7 February 2023, date of current version 13 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3243063

RESEARCH ARTICLE

Secret Key Generation Between Ambient Backscatter Devices

JARI LIETZÉN AND OLAV TIRKKONEN, (Fellow, IEEE)
Department of Communications and Networking, Aalto University, 02150 Espoo, Finland
Corresponding author: Jari Lietzén (jari.lietzen@aalto.fi)

This work was supported in part by the Academy of Finland under Grant 334539.

ABSTRACT We analyze secret key generation between ambient backscatter devices where the channel between an ambient transmitter and the backscatter devices is used as a source of randomness. The devices do not need to estimate or measure the channel between themselves, which greatly simplifies the gathering of raw key material. We analyze the eavesdropper's mutual information based on fundamental principles and apply privacy amplification to remove any information that the eavesdropper overheard during the error correction phase. We show how the legitimate users can estimate the eavesdropper's knowledge and trade off between achievable key rate and the eavesdropper's knowledge of the final key. When modeling the channel between the ambient transmitter and the backscatter devices using state-of-the-art 3GPP channel models we show that even in non-line-of-sight channels the distance from legitimate users to an eavesdropper being larger than a few wavelengths is not alone a sufficient security guarantee. This is in contrast with previous secret key generation methods where distance is assumed to prevent the eavesdropper from having any information about the key prior to error correction. Our simulations show that a distance based approach is too optimistic and there is a possibility that the eavesdropper still knows a substantial part of the final key.

INDEX TERMS Secret key generation, physical layer security, ambient backscatter communication.

I. INTRODUCTION

In recent years the interest in the wireless Internet of Things (IoT) and Ambient Intelligence has increased significantly. While IoT has made it possible for things and people to interact with each other anytime and any place, the security of IoT devices has become a concern [1], [2]. Ambient Intelligence is based on collecting and using data from distributed sensing devices [3]. As the devices are communicating with each other or to some coordinator, it is important that the devices can trust to each other. There should be sufficient protection against confusing with other users' devices or active eavesdropping. As the computational and electrical power of the devices is often rather limited, a reasonably secure and efficient method to produce an authentication key is needed.

The use of cryptographic methods to enforce security to the connected devices is the usual course of action. The issue here is key management, the secret keys need to be delivered to the devices [4]. One solution is to use pre-shared keys, e.g., installed at the time of manufacturing the devices.

Traditional security schemes are based on public key cryptography or public key infrastructure (PKI) to support confidentiality, data integrity and authentication [5], [6], [7]. Public key cryptographic methods are asymmetric as they use a public key to encrypt messages and a private key to decrypt them [8]. Asymmetric cryptography has high energy and implementation costs, as these methods rely on computational hardness to provide security [6], [9].

A symmetric encryption method uses the same key for encryption and decryption, but this raises the question of key distribution, as both parties must have the same key [10]. It is not practical to preconfigure the keys, and dynamic updating and pairing devices and keys requires a trusted third party to operate the key distribution [9].

Preconfiguring the secret keys does not scale well; adding and removing devices may require updating the existing keys. Another solution is to use a configuration system to deliver the keys to the devices, but this approach is vulnerable to eavesdropping during the configuration phase [4]. This is

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

especially problematic for wireless IoT devices, due to the broadcast nature of wireless channels. An alternative is to distill keys from the environment, e.g., extracting keys from wireless channel properties [11], [12]. Instead of using a fixed infrastructure for key distribution, it would be more practical to generate the keys automatically when needed [5], [9]. In *Camouflage Learning* [3], data privacy is achieved using non-reversible aggregation of feature values, as no party has at time complete information on the underlying machine learning model.

A. RELATED WORK

Physical layer properties are a viable source of randomness for secret key generation [5], [6], [7], [9], [10], [11], [13], [14], [15], [16]. A comprehensive survey of physical layer classifications and applications for security techniques and confidentiality is presented in [17]. An informative taxonomy of wireless key establishment techniques is shown in [18, Fig. 2]. Research on the more general topic of acquiring a shared secret key from correlated random variables using public discussion was started by Maurer [19], [20], [21] and Ahlswede and Csiszár [22].

The wireless environment with multipath propagation is typical in wireless scenarios and is characterized by a fading channel response. As wireless channels change in time, exploiting the randomness of the fading channel provides information theoretic security [6], [13], [16]. Relative movement between the user equipment and the environment leads to random amplitude and phase fluctuations of the received signal [6], [23]. The radio channel acts as a time and space-varying filter. The filter's response at any point in time is the same from location A to location B, and vice versa [7], [14]. Therefore the short term fading process is hard to predict and is best modeled stochastically [23].

The raw key material from which the final secret key is obtained, is based on measuring the channel response between the users and then extracting secret bits from the raw material. The information for creating secret keys is extracted from random spatial and temporal variations of the reciprocal wireless channel [7]. The most common method is to use the amplitude or channel gain as a source for key generation, as amplitude or received power is relatively easy to measure [14]. On the other hand, the randomness of the radio channel also limits the information that an eavesdropper can get at the bit level, even if the eavesdropper has unlimited computational power [10]. In addition to using the wireless channel to be the source of the secret key, the problem of key distribution is also solved. The legitimate users already have the keys and the keys can be also renewed as needed [15].

The security of using physical layer as a source of random bits relies on the reciprocity principle. The channel is unique between communicating parties as the multipath propagations are highly correlated, symmetric and sufficiently random in their nature [5], [9], [16], [24]. The legitimate users can obtain strongly correlated channel measurements, and since the channel fluctuations are spatially specific in multipath radio environments, an eavesdropper cannot get similar channel responses [16], [24], [25], [26]. In multipath-rich environment, channel responses are rapidly decorrelating both in time and space [13].

In contrast, [27] distills the secret key from the signal originating from an ambient transmitter, such as a local TV broadcast. Now there is no channel reciprocity between the devices, but if the devices are close to each other, the channels from the ambient transmitter to the devices are correlated and the measurements can be used as a source of randomness. Given ambient signal carrier wavelength λ, [27] assumes the devices to be located within 0.1λ distance from each other, and the eavesdropper needs to be at least 0.4λ away from either one of the legitimate devices in order to reliably derive a secret key.

When generating key bits from channel measurements, the most common bit extraction method is based on measuring the amplitude or channel gain, the received signal strength indicator (RSSI) [6], [7]. For example, a legitimate user Alice sends a probe to another user Bob and Bob sends immediately an acknowledgement back to Alice. In general, probes and acknowledgements are just packets that the users are sending to each other and are measuring the RSSI values of those packets [7], [11]. In [11] the authors used RSSI values to extract a secret key between two moving cars. The devices are continuously sampling the wireless link between the cars by actively sending and receiving packets to each other and using the RSSI fluctuations to produce the secret key.

After the users have made a series of RSSI measurements, they need a method to convert the measured values to bits that can be turned into a secret key. A simple *level-crossing method* may be used to convert the RSSI values to bits by comparing the measured values to predefined thresholds and deciding bit values accordingly [11], [23].

The bits collected from RSSI measurements cannot be directly used as a secret key. There may be differences in the bit strings collected by Alice and Bob and there is a possibility that an eavesdropper Eve has some information about the bits. Therefore after measuring the RSSI values and quantizing the values, a key agreement phase is used to prepare the secret key [24]. The key agreement phase comes in two parts. The first part is the *information reconciliation* or error correction procedure, and the second part is the *privacy amplification* procedure. The information reconciliation procedure makes sure that the key strings agree upon the same key and the privacy amplification procedure removes any information that the eavesdropper has managed to acquire [5], [7], [26], [28].

A notable example of symmetric key distribution to produce and distribute secret keys is quantum key distribution (QKD) setting [7], [14], [23], [29]. In QKD the non-orthogonal states of a quantum system provide correlated observations of randomness for end users [23]. The wireless

fading channel provides another comparable source of secrecy that can be used to provide information theoretically secure keys [23], [25].

In backscatter communication wireless nodes do not have any active RF components [30]. Instead the received RF transmission is modulated and reflected back to the receiver [31], [32]. In ambient backscatter communications (AmBC) the wireless nodes are embedding their messages on top of the ambient transmitter's signal [33], [34]. Due to the broadcast nature of AmBC, it is easy for an eavesdropper to obtain information about the messages. Therefore an important design issue is to make backscatter communication secure [16], [34]. In a backscatter scenario there is no direct channel between the users. The channel between two users is always constructed from two sections, one section from the ambient transmitter to the first user and second section from the first user to the second user.

Our work is preceded by Wang et al. who proposed a method to indirectly measure the channel between two backscatter devices and use that information as a source of a shared secret [16]. This approach needs the channel estimate between the devices, thus requiring communication and processing resources. Also Mathur et al. used ambient signals as a source of randomness in their proximity-based device pairing system [27], but their solution relies on a very close proximity of the devices and instead of AmBC the devices use conventional transceivers for communication.

B. CONTRIBUTION

In this paper we show that it is possible to use the radio channel from an ambient transmitter to backscatter devices as a source of randomness to secure AmBC. To the best of our knowledge our work is the first to utilize the direct channels from the ambient transmitter to the sensors as the source of a shared secret in an AmBC setting. In our system the users do not need to estimate or measure the channel between themselves, which greatly simplifies the gathering of raw key material. The key generation is based on correlations between received signals, rather than relying on channel reciprocity between the users.

In contrast to [27] we analyze Eve's mutual information based on fundamental principles, we are not making security assumptions based on Eve's distance from Alice or Bob. We analyze Eve's knowledge on the secret key at different locations compared to Alice or Bob, and show that Eve's knowledge of that key can be made very small.

Our approach is an application of the satellite model for secret key agreement, where a satellite is sending random bits and the legitimate users try to agree on a secret key while an eavesdropper receives the same bits, possibly through a better channel than the legitimate users [19]. We are proposing the use of Two-way Protocol with Parity bit Reconciliation (TPPR) [35], first introduced in QKD setting in [29], for key generation.

The rest of the paper is organized as follows. Section II discusses the system model, the backscatter communication system, the users and their sensors, and the properties of a fading wireless channel and channel measurements. The quantization process, key agreement, and how to distill a shared secret from ambient signal is discussed in Section III. The simulation setup that is used to analyze our system and the corresponding performance evaluation is presented in Section IV. Section V concludes this paper with discussion on achieved results.

II. SYSTEM MODEL

The system consists of a number of users and sensors associated with each user. The sensors belonging to a user are communicating to each other, and possibly with a coordinator. The users are moving in an environment where a signal from an ambient transmitter is present all the time. In order to save energy, the sensors do not have dedicated RF transmitters; they utilize the signal from the ambient transmitter and use backscattering to embed their messages on top of the ambient signal.

The sensors associated with one user should be reasonably confident that they are communicating with each other, and not with some other users' sensors. This is accomplished by using a shared secret between the sensors of a user. The shared secret is distilled from the noisy signals received from an ambient source in their environment. This setup is an example of a secret key distribution protocol applied in a satellite setting [20], [36].

The key generation schemes discussed in Section I-A rely on two communicating parties sending probing signals to each other and measuring channel responses. In AmBC, and backscatter systems in general, the backscatter devices cannot directly estimate the channel between devices. The channel between two backscatter devices consists of two sections. The first section is from the ambient transmitter to the device and the second section is from one device to another. Therefore it is challenging to use existing physical layer security methods in AmBC systems, especially in case of direct backscatter device-to-device (D2D) communications [16], [34]. The channels from ambient transmitter to backscatter devices are not identical, and thus the channel between two backscatter devices cannot be used as a shared randomness source [16]. As a solution, Wang et al. proposed a method to estimate the channel between two backscatter devices based on the observation that the channel between devices is one side of a triangle formed by the ambient transmitter and two backscatter devices [16]. The proposed method constructs a multiplication of three channels as a source of shared randomness.

A. BACKSCATTER COMMUNICATION

In backscatter communication wireless nodes are communicating without any active RF components [30]. The received RF transmission by a wireless device is modulated and reflected back to the receiver instead of generating the RF

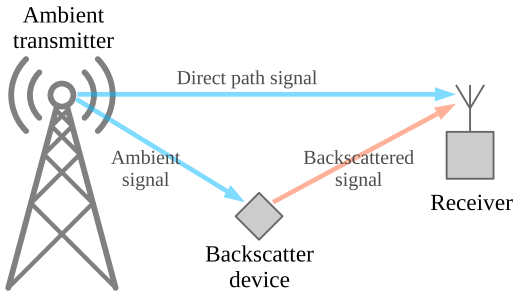

FIGURE 1. The ambient backscatter communication system.

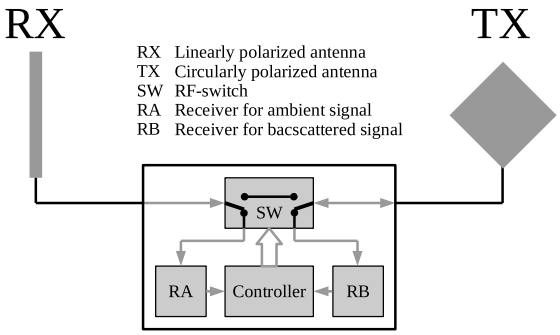

FIGURE 2. Block diagram of the backscatter device.

signal at the device itself. Harry Stockman first introduced this concept in 1948 [37].

AmBC systems utilize signals from surrounding ambient RF sources, e.g. terrestrial TV, FM radio, cellular mobile stations, or wireless access points. A backscatter device modulates the ambient signal and reflects it as shown in Fig. 1. Therefore the backscatter device does not need a dedicated RF signal source. The receiver sees the message on top of the ambient signal. However, as the backscattered signal is superimposed to the ambient signal, it is important that the backscattered signal is not causing interference for the users of the ambient system [38].

A drawback is that the backscattered signal is usually several orders of magnitude weaker than the direct path ambient signal. The ambient signal appears as direct-link interference (DLI) at the AmBC receiver, as illustrated in Fig. 1. In cooperative AmBC the receiver is able to acquire information about the ambient signal before signal detection, and therefore the receiver can cancel the ambient signal prior detecting the backscattered symbols [39]. In non-cooperative model the AmBC receiver has very limited amount of information about the ambient signal, or none at all [39].

We use a non-coherent receiver for detecting the received symbols. Non-coherent detection only needs a filter matched to the RF pulse, an envelope detector, a sampler and a comparator for making the detection decision [40]. The idea behind the first AmBC receiver was that if the information rate of the backscatter device is lower than that of the ambient signal, the receiver can use averaging to extract the backscattered information [33].

We proposed a method based on polarization conversion in [41] to significantly reduce the ambient signal level at the receiver, thus making it easier for the receiver to recover the backscattered signal. Under ideal circumstances the proposed method completely removes the ambient signal, and a 25 dB attenuation at 2.4 GHz was confirmed by measurements. The proposed method converts a linear polarized ambient signal to a circular polarized backscatter signal and the receiver uses circular polarized antennas. The use of circular polarization also helps the alignment of the sensors, as the rotational angle between the backscatter device and the receiver is no longer an issue. An additional advantage is that the reflections originating from the ambient transmitter are also suppressed by the same attenuation as the direct path signal [41].

B. BACKSCATTER DEVICE

The backscatter device needs to measure the ambient transmitter's signal level and therefore needs a corresponding receiver. This is a distinctive feature of the proposed backscatter device as devices doing only backscatter modulation do not need a receiver.

The operating principle of the proposed backscatter device is illustrated in Fig. 2. The modulator SW in the figure is an RF switch and the controller is e.g. a microcontroller that generates the modulating waveform. The modulation is realized by either connecting the two antennas together or isolating them from each other. The receiver connected to the linear polarized antenna receives the ambient signal and is responsible for making the channel measurements. The backscatter receiver connected to the circular polarized antenna listens other sensors. We assume a polarization conversion method as in [41] to better mitigate the suppression of the ambient signal at the receiver.

An actual realization of the backscatter device could use a commercially available power sensor IC to measure the incoming RF power. The output voltage of the power sensor IC is proportional to the input power. The ambient receiver could either use an RF demodulator in front of the power sensor to enable tuning the receiver to a certain ambient RF signal, or a simple band-pass filter could be used instead, if the frequency of the ambient signal is fixed. The output of the power sensor IC is sampled to obtain the raw power measurements.

The backscatter receiver could use a non-coherent receiver, as discussed in Section II-A, to detect the received symbols. A general purpose microcontroller is used to make measurements, process the information originating from another sensor, and controlling the backscatter modulator as needed.

A software defined radio (SDR) platform could be used to implement the required functionalities as well. This approach could be used during prototyping phase, when developing the implementation.

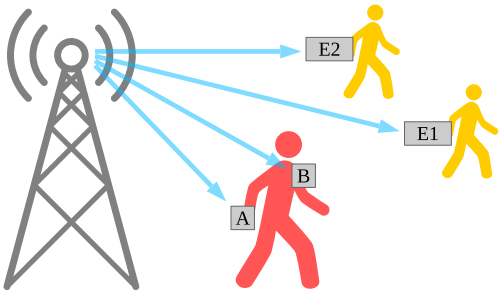

FIGURE 3. System model showing the ambient transmitter on the left, users and their sensors, and the signal paths to the users. The legitimate user has sensors A and B.

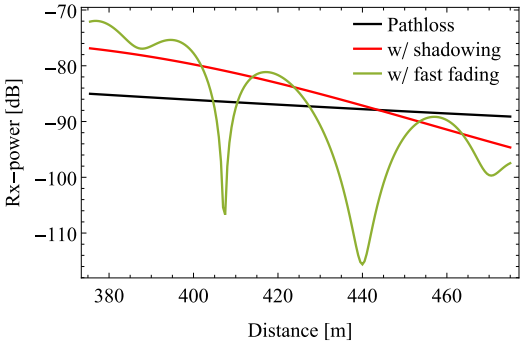

FIGURE 4. An example of wireless channel fading response.

C. USERS AND SENSORS

The users are carrying two or more sensors with them and each users' sensors are only talking to each other. To ensure that, shared secrets are used to distinguish users from each other. Three users with their sensors are illustrated in Fig. 3. The first user is carrying sensors A and B and the two other users are carrying sensors E1 and E2, correspondingly. The information source for the shared secret among the sensors of a user is obtained from the properties of an RF signal path. Each sensor has its own signal path from the ambient transmitter, as shown in Fig. 3. All users share a common environment, but the signal paths are different. The signal paths to the sensors of one user are more similar than the paths to different users.

In a bistatic backscatter system such as AmBC, the backscattered signal is strongest if the backscatter device is either near the transmitter or the receiver [42]. It is therefore beneficial that in our use case the sensors are near each other compared to the ambient transmitter.

D. FADING WIRELESS CHANNEL

The relative movement between the user equipment and the environment leads to random amplitude and phase fluctuations of the received signal [6], [23]. The fading channel response arises in wireless environments with multipath propagation, the radio channel is a time and space-varying filter. The filter's response at any point in time is the same from location A to location B, and vice versa [7], [14].

An example of a wireless channel response as a function of distance is presented in Fig. 4. The figure shows the three main components affecting the channel's response: pathloss, shadowing, and fast fading [43]. The nature of fast fading is clearly visible in the figure. The received signal level changes rapidly and there can be very large changes in the received signal power, as much as 30 to 40 dB [43].

As the amplitude or power level of the received signal is relatively easy to measure, these are the most common sources for key generation.

III. DISTILLING A SHARED SECRET FROM AMBIENT SIGNAL

The sensors need to have a shared secret in order to ensure that only sensors belonging to the same user are communicating to each other. We generate key material from the ambient transmitter's signal levels at the sensors, as the users are moving with regard to the ambient transmitter. The sensors are receiving the ambient signal and measuring the received signal power. This is shown in Fig. 5 as step (a). The measurements are done in a coordinated way to increase correlation between the measurements, which leads to higher key rates. One of the sensors can act as a coordinator and send a command to the other sensor to start the power measurement procedure. Alternatively, a certain signal pattern from the ambient transmitter can trigger the measurements. Either way, the sensors are making the measurements simultaneously, thus avoiding the time delay problem described in Section I-A.

Let the measured values be $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ where X corresponds readings from sensor A and Y corresponds readings from sensor B. The sensors use X and Y as raw key material, and independently extract random bits from them using a quantizer, as shown as step (b) in Fig. 5.

The bits extracted during step (b) are not the same for both sensors. Therefore, in step (c), an information reconciliation protocol is used to produce a key that both sensors A and B agree on. In this paper, we consider two-way communication in this step. Finally, in step (d) a privacy amplification protocol is applied to the key to make it secure. This is based on one-way communication. The sensors A and B use backscatter communication to exchange messages between them in steps (a), (c) and (d).

A. CHANNEL MEASUREMENTS

The most common bit extraction method from Section II-D uses RSSI values for generating a secret key. The basic steps taken when using RSSI values are [6]:

- probing the channel, i.e. measure RSSI,
- quantize RSSI values and convert them to bits, and
- use error correction to obtain a shared key.

As the wireless environment is changing continuously, there exists a *channel coherence time* during which the channel does not change significantly. As an example, in Fig. 4 the channel stays relatively stable in the time scale of

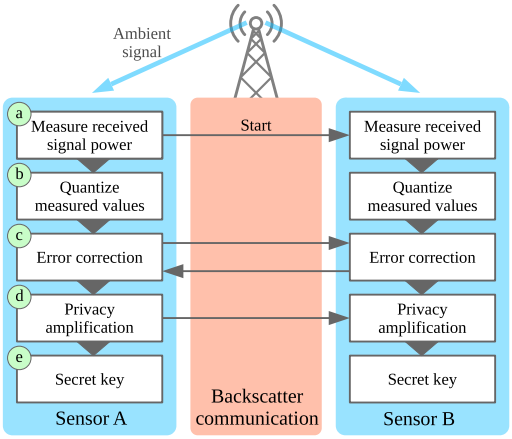

FIGURE 5. Device operation and communication for key generation from ambient signal.

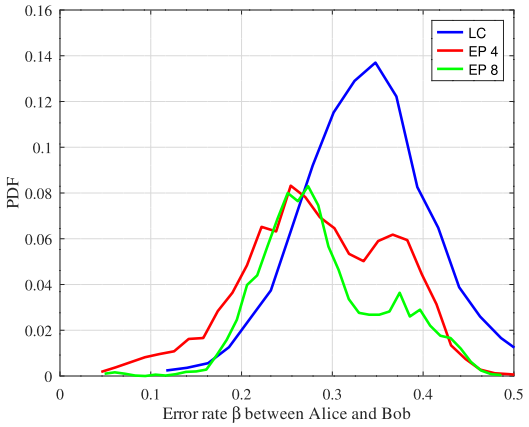

FIGURE 6. Estimated error rate distributions with different quantizers.

moving a few meters, between large changes in the received signal power caused by the fast fading phenomenon. The coherence time window makes it possible to obtain correlated measurements. The coherence time T_c

$$T_c \sim \frac{1}{f_m}, \tag{1}$$

where $f_m = \frac{v \cdot f_c}{c}$, c is the speed of light, v is the speed of the user, and f_c is the carrier frequency [43]. The extracted bits need to be separated in time by at least a coherence time interval (1) to ensure that successive bits are almost independent [5].

The mean RSSI value needs to be filtered out of the measured RSSI values, as the mean is closely related to the distance between users, corresponding the pathloss component shown in Fig. 4. Otherwise an eavesdropper could use the knowledge of the distance between users to predict parts of the secret key [7].

B. QUANTIZATION

A quantizer is used to convert the measured RSSI values to bits, which are further processed to obtain the secret key. The RSSI measurements for Alice and Bob, corresponding sensors A and B in Fig. 3, are $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$. X and Y are called raw data or raw readings. Each reading of X is mapped to a temporary bit using quantizer Q [23]

$$Q(x) = \begin{cases} 1, & \text{if } x > q_+ \\ 0, & \text{if } x < q_- \\ e, & \text{otherwise.} \end{cases} \tag{2}$$

The thresholds q_+ and q_- are adaptive

$$\begin{aligned} q_+ &= \text{mean}(X^n) + \alpha\, \sigma(X^n) \\ q_- &= \text{mean}(X^n) - \alpha\, \sigma(X^n), \end{aligned} \tag{3}$$

where $\alpha \geq 0.2$ and estimates between q_+ and q_- are dropped [7], [23]. The quantizer is applied to blocks, their size n being an adjustable parameter. Alice and Bob can use the readings they both quantized to bits, discarding positions where either one of them got an e. Alice and Bob can also identify excursions in temporary bits, e.g. find the locations of three bits that are the same. Then the positions of excursions are shared between Alice and Bob and each common excursion is coded to a bit [11]. The level-crossing method does not necessarily produce a random bit string [11].

However, the simple level crossing method produces only one bit per raw data reading. More bits per reading are produced with multilevel quantization. An equiprobable quantizer is introduced in [25] where all outputs from the quantizer are equally probable. The quantizer takes a unit-variance Gaussian distribution and divides it to intervals $(-\infty, \bar{q}_1], (\bar{q}_1, \bar{q}_2], \ldots, (\bar{q}_{i-1}, \infty)$, where $\bar{q}_i$ is determined as [25]

$$\int_{-\infty}^{\bar{q}_i} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx = \frac{i}{v}, \tag{4}$$

where i is the interval and v is the total number of intervals. For variance σ and mean μ the general quantizer function reads

$$Q(x) = \int_{-\infty}^{\bar{q}_i} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} dx = \frac{1}{2} \text{erf}\left(\frac{x-\mu}{\sigma\sqrt{2}}\right) \tag{5}$$

A more elaborate quantization method, multibit adaptive quantization (MAQ) [14], takes real valued channel measurements and converts them to bits. This quantization scheme needs to be agreed between the users, necessitating communication before the measured values can be converted to bits.

A comparison of the resulting error rate distributions between Alice and Bob is shown in Fig. 6. A level crossing quantizer is compared to 4- and 8-level equiprobable quantizers. The dataset used to produce the comparison is the same set of channel measurements that is later used as an input to the key agreement protocols. The error probabilities for each quantizer are calculated using the channel measurements from 5000 simulation cases.

The bit strings Alice and Bob collect from RSSI values are not necessarily the same and it is also possible that

an eavesdropper has some information about the bits. As discussed in Section I-A information reconciliation and privacy amplification procedures are needed before the bits can be used as a secret key.

C. KEY GENERATION FROM CORRELATED SIGNALS

The satellite setting [20] is an example of the *source model* secret key agreement method [44], where a source is broadcasting a signal in the form of a sequence of uniformly distributed random bits U. All sensors receive these bits through independent binary symmetric channels (BSCs) with individual error probabilities. This is a method of secret key agreement using two-way communication over a public channel, starting from some correlated information [19], [20]. As the aim is to agree on a secret key, Alice's and Bob's sensors A and B exchange messages publicly and these messages are overheard by Eve's sensors as well.

In a *one-way* protocol Alice sends Bob enough redundant information that he can correct his keyword, or vice versa. If Eve has a better channel than either Alice or Bob, a one-way protocol cannot produce any key.

Even if Eve's channels are originally better than Alice's or Bob's, they can use a two-way protocol based on *advantage distillation* to concentrate only to those bits that sensors A and B received reliably and throwing away the rest. The parity-check protocol (PCP) by Maurer [20], [36] is a prototypical advantage distillation protocol. We demonstrated in [35] that TPPR, first introduced in QKD setting in [29], is able to outperform the information theoretic bound limiting the performance of all one-way protocols. In TPPR, parity checking is used for advantage distillation as in PCP, but instead of discarding parity bits after each advantage distillation round, key bits are collected from error corrected parity bits.

We now replace the satellite with an ambient transmitter. As the ambient source is transmitting its own signal, and not purely random bits, the sensors need a method to get raw key bits from the ambient signal. As discussed in Section I-A, the most common bit extraction method is to measure amplitude or channel gain. Conventional physical layer security methods take advantage of the reciprocal nature of a fading radio channel between two users. Our scenario uses the channel characteristics between the ambient transmitter and the users, as shown in Fig. 3.

In the original satellite setting [20] the satellite is broadcasting a signal in the form of a sequence of uniformly distributed random bits U. Alice, Bob and Eve receive these bits through three independent BSCs C_A, C_B and C_E, with corresponding error probabilities ϵ_A, ϵ_B, and ϵ_E. Following [20], after N consecutive uses of the channel Alice has a length N i.i.d binary sequence with equal probabilities for 1's and 0's and Bob's sequence Y is X received through a BSC with crossover probability

$$\beta = \epsilon_A(1-\epsilon_B) + (1-\epsilon_A)\epsilon_B \,. \tag{6}$$

As in AmBC setting there is no satellite, there are no error probabilities corresponding to ϵ_A, ϵ_B, and ϵ_E either. Instead Alice and Bob can directly measure the crossover probability β. The error rate γ between Alice and Eve and the error rate η between Bob and Eve can be estimated. We define Bob's and Eve's error sequences as

$$\mathrm{B} = \mathrm{Y} \oplus \mathrm{X}\,, \quad \mathrm{E} = \mathrm{Z} \oplus \mathrm{X}. \tag{7}$$

These are correlated with the joint distribution given as $\mathrm{P}_{\mathrm{E_i},\mathrm{B_i}}(\mathrm{e},\mathrm{b}) = \alpha_{\mathrm{be}}$ with

$$\begin{aligned}
\alpha_{00} &= 1 - \frac{1}{2}(\beta+\eta+\gamma)\\
\alpha_{01} &= \frac{1}{2}(\eta+\gamma-\beta)\\
\alpha_{10} &= \frac{1}{2}(\beta+\eta-\gamma)\\
\alpha_{11} &= \frac{1}{2}(\beta-\eta+\gamma).
\end{aligned}$$

These will be used later when calculating the secret key rates for PCP and TPPR. The key rate for a one-way protocol is defined as

$$\mathrm{R_{OW}} = \begin{cases} \mathrm{h}(\gamma) - \mathrm{h}(\beta), & \text{if Alice's bits are corrected} \\ \mathrm{h}(\eta) - \mathrm{h}(\beta), & \text{if Bob's bits are corrected} \end{cases} \tag{8}$$

where $\mathrm{h(p)} = -\mathrm{p}\log_2\mathrm{p} - (1-\mathrm{p})\log_2(1-\mathrm{p})$ is the binary entropy function.

In PCP [20], [36], Alice and Bob construct parity bits from their raw key material, and exchange these publicly with each other. One bit from each block where Alice and Bob agreed about the parity bit, is kept for the next round. After M rounds of parity bit construction, the distilled key is corrected by exchanging redundancy information. In a *privacy amplification* phase, the information that Eve has acquired about the key during the key distillation process, is removed by hashing.

The key rate for PCP is calculated using [36, Theorem 2], rephrased from [45], as:

$$\mathrm{R_{PCP}} \geq 2^{-\mathrm{M}}\Phi\left(2^{\mathrm{M}},\beta,\gamma,\eta\right)\prod_{\mathrm{i}=0}^{\mathrm{M}-1}\left(\beta_{2^{\mathrm{i}}}^2 + (1-\beta_{2^{\mathrm{i}}})^2\right)\,, \tag{9}$$

where

$$\begin{aligned}
\Phi(\mathrm{L},\beta,\gamma,\eta) &= \sum_{\mathrm{w}=0}^{\mathrm{L}} \mathrm{F}(\mathrm{L},\mathrm{w},\beta)\,\mathrm{h}\left(\mathrm{G}(\mathrm{L},\mathrm{w})\right) - \mathrm{h}(\beta_{\mathrm{L}}),\\
\mathrm{F(L,w},\beta) &= \binom{\mathrm{L}}{\mathrm{w}}\frac{\mathrm{p_{L,w}}}{\beta^{\mathrm{L}}+(1-\beta)^{\mathrm{L}}}\,,\\
\mathrm{G(L,w)} &= \frac{\mathrm{p_{L,w}}}{\mathrm{p_{L,w}}+(1-\mathrm{p_{L,L-w}})}\,,\\
\mathrm{p_{L,w}} &= \alpha_{00}^{\mathrm{L-w}}\alpha_{01}^{\mathrm{w}} + \alpha_{10}^{\mathrm{L-w}}\alpha_{11}^{\mathrm{w}}\,,\\
\beta_{\mathrm{L}} &= \frac{\beta^{\mathrm{L}}}{\beta^{\mathrm{L}}+(1-\beta)^{\mathrm{L}}}\,.
\end{aligned}$$

TPPR [35] differs from PCP in that the parity bits used for advantage distillation are error corrected in secrecy, and

key is gathered from them. After M rounds of parity bit construction, the remaining bits are error corrected, as in PCP, considered as a round M + 1 in the protocol. In privacy amplification, Eve's information about the collected key is removed. The key rate for TPPR is a sum over rounds [35]

$$\mathrm{R_{TPPR}} \geq \sum_{\mathrm{m}=1}^{\mathrm{M}+1} \mathrm{p_m}\, \mathrm{R_m}\, \mathrm{H}(\mathrm{q_m}|\mathrm{C_m}) \;-\; \mathrm{h}\left(\mathrm{p_m}\right)\,, \tag{10}$$

where

$$\begin{aligned}
\mathrm{p_m} &= 2\beta_\mathrm{m}(1-\beta_\mathrm{m})\,,\\
\beta_\mathrm{m} &= \frac{\beta_{\mathrm{m}-1}^2}{\beta_{\mathrm{m}-1}^2 + (1-\beta_{\mathrm{m}-1})^2}\,,\\
\mathrm{R_m} &= \frac{1}{2^\mathrm{m}} \prod_{i=0}^{\mathrm{m}-1} \left(1-\mathrm{p_i}\right),
\end{aligned}$$

and the entropy of Eve's error codeword arising from the corrected parity bits in rounds m = 1, ... M is

$$\mathrm{H}(\mathrm{Q_m}|\mathrm{C_m}) = -\sum_{(\mathrm{w_0},\mathrm{w_1})\in\mathcal{W}} \mu(\mathrm{w_0},\mathrm{w_1})\, \Psi(\mathrm{w_0},\mathrm{w_1})\, \log_2 \Psi(\mathrm{w_0},\mathrm{w_1}).$$

Here

$$\begin{aligned}
\mu(\mathrm{w_0},\mathrm{w_1}) &= \binom{\frac{1}{2}L}{\mathrm{w_0}}\binom{\frac{1}{2}L}{\mathrm{w_1}}\nu(\mathrm{w_0},\mathrm{w_1})\\
\nu(\mathrm{w_0},\mathrm{w_1}) &= \frac{1+(1-\delta_{\mathrm{w_0},\mathrm{w_1}})(1-\delta_{\mathrm{w_0},\mathrm{L}/2-\mathrm{w_1}})}{1+\delta_{\mathrm{w_0},\mathrm{L}/4}\,\delta_{\mathrm{w_0},\mathrm{L}/4}},\\
\Psi(\mathrm{w_0},\mathrm{w_1}) &= \Phi(\mathrm{w_0},\mathrm{w_1}) + \Phi\left(\frac{\mathrm{L}}{2}-\mathrm{w_0},\frac{\mathrm{L}}{2}-\mathrm{w_1}\right)\\
&\quad + \Phi(\mathrm{w_1},\mathrm{w_0}) + \Phi\left(\frac{\mathrm{L}}{2}-\mathrm{w_1},\frac{\mathrm{L}}{2}-\mathrm{w_0}\right),\\
\Phi(\mathrm{w_0},\mathrm{w_1}) &= \frac{1}{2}\frac{\alpha_{00}^{\mathrm{L}/2-\mathrm{w_0}}\,\alpha_{01}^{\mathrm{w_0}}\,\alpha_{10}^{\mathrm{L}/2-\mathrm{w_1}}\,\alpha_{11}^{\mathrm{w_1}}}{(\alpha_{00}+\alpha_{01})^{\mathrm{L}/2}\,(\alpha_{10}+\alpha_{11})^{\mathrm{L}/2}}.
\end{aligned}$$

The entropy of Eve's error codeword arising from the final bits in round M + 1 is

$$\mathrm{H}(\mathrm{Q_{M+1}}|\mathrm{C_{M+1}}) = \;-\sum_{\mathrm{w}=0}^{\mathrm{L}} \binom{\mathrm{L}}{\mathrm{w}}\, \Upsilon(\mathrm{w})\, \log_2\, \Upsilon(\mathrm{w}),$$

where

$$\begin{aligned}
\Upsilon(\mathrm{w}) &= \mathrm{P_B}(0)\; \Xi(\mathrm{w}|0) + \mathrm{P_B}(1)\; \Xi(\mathrm{w}|1),\\
\Xi(\mathrm{w}|\mathrm{b}) &= \frac{\alpha_{\mathrm{b},0}^{\mathrm{L}-\mathrm{w}}\alpha_{\mathrm{b},1}^{\mathrm{w}}}{\left(\alpha_{\mathrm{b},0}+\alpha_{\mathrm{b},1}\right)^{\mathrm{L}}}.
\end{aligned}$$

As the sensors A and B can only measure the error rate β between themselves, they can only guess the error rates γ and η between an eavesdropper and themselves. In [36], the knowledge of A and B about the channel between the satellite and E was estimated in terms of a maximum size of the antenna array of E. Here, we take a similar approach. We model Alice's and Bob's estimates of γ and η in terms of a multiplicative factor k; Alice and Bob run privacy amplification assuming that

$$\gamma = \eta = \min(\mathrm{k}\beta, 0.5). \tag{11}$$

TABLE 1. Number bit operations per input bit for three rounds of the protocol.

β	0.05	0.10	0.20	0.30
Parity bit error correction	170	260	380	440
Error correction of last bits	0.01	0.15	1.9	7.3
Total	170	260	380	450

In a given operational situation, these estimates may be more conservative than the realized error rates, or they may be too optimistic. In the latter case, Eve retains information of the key after privacy amplification. This approach allows us to calculate the achievable key rates in Section IV-B and estimate Eve's average knowledge of the resulting secret key as a function of k in Section IV-C.

D. COMPUTATION AND COMMUNICATION COMPLEXITY

The sensors need to perform a series of computations in order to end up having a common shared secret. For example, if we start TPPR with 1000 input bits, Alice and Bob at first calculate 500 parity bits and Alice sends Bob enough redundancy bits so that Bob can correct his parity bits. Bob then sends Alice the positions where the parities disagreed, and then they both discard the corresponding two-bit blocks. From each remaining block they jointly select one bit and the protocol enters a new round. The bits remaining after the last round are error corrected and added to the shared secret.

In Table 1 we report the estimated number of operations per input bit during three protocol rounds, for a selection of input bit error rates. The number of bit operations in error correction depends on the bit error rate. Correcting parity bits is the heaviest task; when considering the errors remaining after the last round, less computations are needed, as the advantage distillation process is very effective in decreasing the error rate. We assume that bit errors are corrected using 50 iterations of a low density parity-check code (LDPC) which has an average check node degree of 7.

The computational load in operations per second depends on the rate at which input bits are created. We may consider a situation corresponding to the scenario simulated in Section IV in this paper. If we assume a user walking at a 5 km/h pace, a carrier frequency of 590 MHz, taking samples at $\mathrm{T_c}$ intervals calculated from (1), and using an equiprobable quantizer from (5) with 4 levels, this results in 5.5 input bits per second. With the worst error rate considered in Table 1, this requires 2500 operations per second. If we have a low performance microcontroller running at e.g. 4 MHz clock rate and assume that one instruction takes four clock cycles to execute, the microcontroller may execute one million instructions per second. The computations related to key generation in this scenario take only a small fraction of the microcontroller capacity.

Another implementation aspect worth considering is the required amount of communication between Alice and Bob. Alice has to send the redundancy bits to Bob and in return Bob sends Alice the positions of erroneous parity bits. These

TABLE 2. Communication cost in terms of communicated bits per input bit.

β	0.05	0.10	0.20	0.30
Number of redundancy bits	0.24	0.37	0.55	0.64
Parity bit positions	0.84	0.81	0.75	0.70
Total	1.1	1.2	1.3	1.3

bits represent the communication cost between the sensors. The communication cost per input bit during three protocol rounds is presented in Table 2. The achievable transmission rates in AmBC systems start from kbits/s, giving ample room for coding and protocol overhead as the sensors need to communicate less than 8 bits/s in the considered scenario where 5.5 input bits are created per second.

Since the number of input bits per second is relatively low, neither the computational nor the communication capacity of the backscatter device will be a bottleneck.

The number of instructions that is needed to run the key agreement protocol can be reduced by using precalculated lookup tables (LUT) to assist the protocol execution. For example, the parity check matrices for the LDPC code and the amount of needed privacy amplification can be precalculated for a selection of error rates, and the corresponding shortening algorithm could also be stored to a precalculated table. The parity bit calculation at the heart of the TPPR protocol is a simple exclusive-OR instruction, available at hardware level in a microcontroller.

The LUTs take up memory, and the more detailed the tables are, the more memory is needed. However, as the contents of the tables are static, they can be stored in non-volatile memory, thus helping to decrease the energy consumption of the backscatter device.

IV. PERFORMANCE EVALUATION

We simulate secret key generation from channel data using state-of-the-art wireless channel models from 3GPP [46] and show that the distance between an eavesdropper and the legitimate users is not alone a sufficient security guarantee.

A. SIMULATION SETUP

The signal paths shown in Fig. 3 are illustrating only the line of sight (LOS) components from the ambient transmitter to the users. However, there are usually numerous multipath components, and there may not even be a LOS signal path at all. The radio channels from the ambient transmitter to the sensors are modeled using Quasi Deterministic Radio channel Generator (QuaDRiGa) [47]. QuaDRiGa has several built in radio propagation models. We used the 3GPP TR38.901 urban and rural macro models to simulate the radio signal propagation between the transmitter and the receiver [46]. For each of these environments the non-LOS variant was used in the simulations.

The receivers are placed in three different configurations as shown in Fig. 7. The sensors A and B belong to the legitimate user, and sensors E1 and E2 belong to the eavesdropper. The

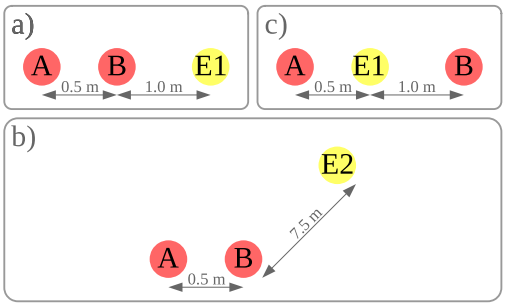

FIGURE 7. The receiver positions, a) baseline situation, b) Eve is further away, and c) Eve is between sensors A and B.

TABLE 3. Distances between sensors and half wavelengths at simulation frequencies.

Sensor pairs	Distance	100 MHz $\lambda/2 = 1.5$ m	590 MHz $\lambda/2 = 0.25$ m
A - B	0.5 m	$\lambda/6$	λ
B - E1	1.0 m	$\lambda/3$	2λ
B - E2	7.5 m	$5\lambda/4$	14.8λ

sensors for each user are at the same height, 1.5 m from the ground level. The configuration a) is the baseline situation, where the eavesdropper is near sensor B. In configuration b) the eavesdropper is further away from sensors A and B, and in configuration c) the eavesdropper is positioned between sensors A and B.

The distances between sensors are listed in Table 3, both in meters and in units of wavelengths corresponding the carrier frequencies used in the simulations. At 100 MHz the sensors A and B are within the $\lambda/2$ limit, therefore the spatial channel responses should be alike. However, sensor E1 is also within the same limit to B, while sensor E2 is outside the $\lambda/2$ limit. At 590 MHz all sensors are farther away from each other than $\lambda/2$.

For each simulation case the users are randomly dropped inside a 7.5 km square. The users are walking a 250 m long route at a 5 km/h pace keeping the distances they got at the beginning. The starting positions and random walking directions for a sample of 300 simulation cases are shown in Fig. 8. The ambient transmitter is located at coordinates X $=$ 0 and Y $=$ 0, marked with a red cross in Fig. 8. It is located 100 m above the ground level. The transmitter antenna is a half-wave dipole and the receiver antennas are omnidirectional. Therefore the orientation of the receiver antennas does not matter, making them suitable for modeling wearable sensors.

The ambient transmitter is either a terrestrial TV station or an FM radio station. The center frequencies are 590 MHz and 100 MHz, correspondingly.

B. ACHIEVED KEY RATES

The simulations were at first run with known error rates. Both β between Alice and Bob as well as γ and η between Eve and the legitimate users is assumed to be known. The error rates for each simulated walking route were calculated for each receiver configuration shown in Fig. 7 from the quantized

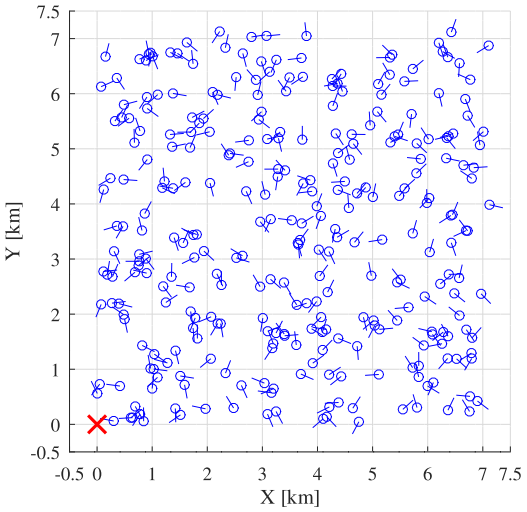

FIGURE 8. Random starting positions and walking directions for 300 simulation cases.

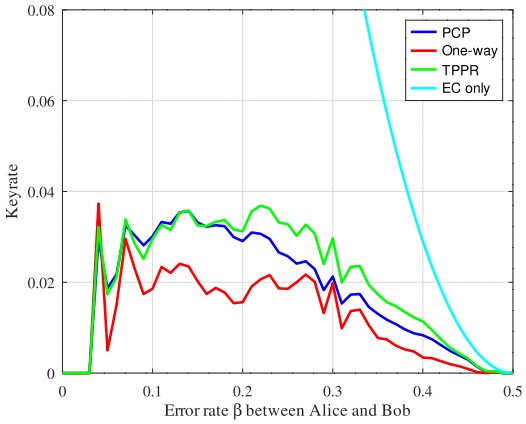

FIGURE 9. Average key rates for PCP and TPPR protocols compared to one way protocol key rate in baseline situation.

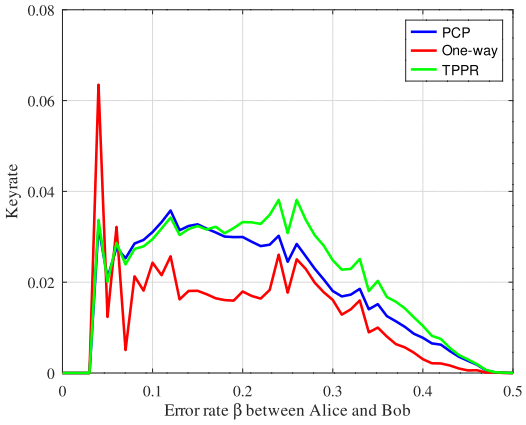

FIGURE 10. Average key rates for PCP and TPPR protocols compared to one way protocol key rate when Eve is between Alice and Bob.

power levels. Each sensor measures power levels at T_c second intervals, calculated from (1). For this work the equiprobable quantization method from Section III-B was selected because it produces more bits per measurement than the level crossing method. The number of quantization intervals was set to four, which provides a wide range of error probabilities, as seen on Fig. 6. The error rates were used as input to one-way, PCP and TPPR protocols from Section III-C using (8), (9), and (10), correspondingly. 5000 simulation cases were used to produce the input to the key-generation protocols. Both PCP and TPPR were run three rounds and the best key rate was taken for each of the 5000 cases. The radio channels were modeled using the 3GPP urban macro scenario at 590 MHz center frequency.

The averaged key rates over all simulation cases are presented in Fig. 9 for the baseline configuration. On the average both PCP and TPPR are able to generate secret key even in the presence of an eavesdropper over a wide range of error rates and in most cases producing more secret key than one-way protocols.

If the distance between Eve and the legitimate users were the only security guarantee, the key rate would have been substantially higher. In this case only the cost of error correction is taken into account when calculating the key rate, as Eve is supposed to have no prior knowledge of the key. For a comparison the resulting key rate is shown in Fig. 9 with the *EC only* label. The proximity based device pairing system in [27] would reach this key rate for the baseline configuration.

Even if Eve is located between Alice and Bob as in receiver configuration c), it is possible to generate a secret key. The averaged key rates for configuration c) are shown in Fig. 10. In this configuration, the method of [27] would not produce any key, as Eve is too close to Alice.

Because the protocols of interest are capable of producing key with a wide range of error rates β, the choice of the quantizer does not play a significant role. However, there may be other reasons to favor a specific quantizer, e.g. the ease of implementation.

It is possible to distill secret key from a random source only if there is some correlation between the raw key material, in this case in the measured power levels. The correlation of the power measurements as a function of distance was simulated for both urban and rural environments at 100 MHz and 590 MHz frequencies. The averaged correlations as a function of distance expressed in wavelengths are presented in Fig. 11. The positions of sensors B, E1 and E2 relative to sensor A are marked to the figures as the sensor A is located at $X = 0$.

It can be seen from the figures that although the correlation decreases rapidly when the distance is in the range of $\lambda/2$, the level of correlation stays relatively high even for distances of several wavelengths. The reason for this is that even though the channels are non-LOS, they are locally dominated by a few multipath components. As Fig. 11 shows, the level of correlation is similar at both frequencies and therefore the resulting key rates would be similar too. The correlation stays even higher in rural environments as there are fewer obstacles causing multipath propagation. It should be noted

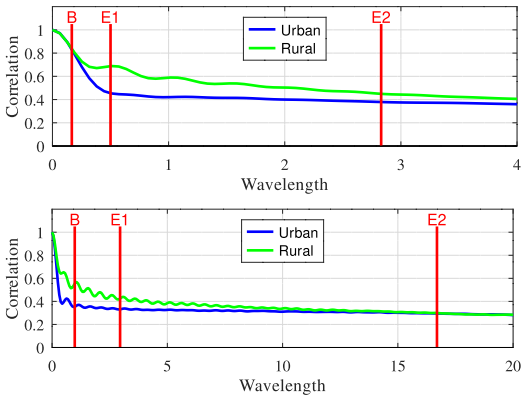

FIGURE 11. The mean correlation between power measurements as a function of distance in urban and rural environments for center frequencies 100 MHz above and 590 MHz below.

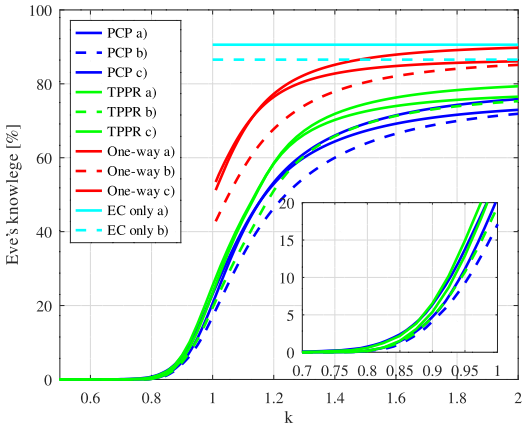

FIGURE 12. Eve's average residual knowledge of the final key when Eve's error probability is assumed k times Alice's and Bob's.

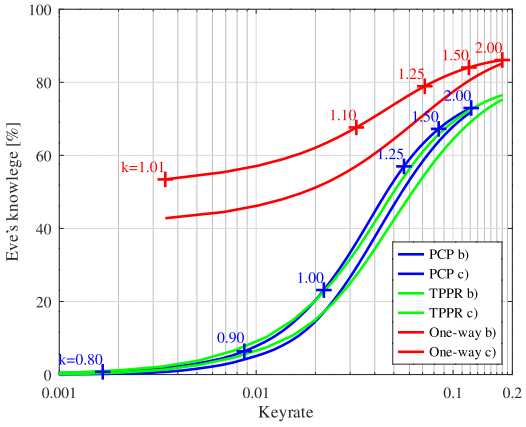

FIGURE 13. Tradeoff between Eve's average knowledge of the key vs. achieved key rate.

that in order to extract the same number of secret bits at 100 MHz would take more time, or longer walking route, as the coherence time is longer compared to that at 590 MHz.

C. ESTIMATING EVE's KNOWLEDGE

Were these sensors operated in a real world situation, Alice and Bob could only measure the error rate β between themselves. They do not know the error probability between themselves and a nearby eavesdropper. The amount of key material that has to be discarded during privacy amplification phase depends on the mutual information that the eavesdropper has of the secret key and that in turn is related to the error rate between Eve and the legitimate users. Therefore Alice and Bob need to estimate the error rate γ between Alice and Eve, and the error rate η between Bob and Eve. If the estimation were too optimistic, the key rate would be higher but Eve would possess residual information about the secret key even after privacy amplification.

We model Alice's and Bob's estimates of γ and η in terms of a factor k as in (11), with k in the range from 0.5 to 2. With S the key rate with estimated error rates and R the actual key rate with realized error rates, Eve's residual knowledge of the secret key is

$$\mathrm{K} = \begin{cases} \dfrac{\mathrm{S}-\mathrm{R}}{\mathrm{S}} & \text{if } \mathrm{S}-\mathrm{R} > 0 \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Eve's average residual knowledge of the secret key over all 5000 simulation cases are presented in Fig. 12 for PCP and TPPR as well as for the one-way protocol. The figure shows results for receiver configurations a), b) and c) from Fig. 7. When $\mathrm{k} < 1$ a one-way protocol can not produce any key. When $\mathrm{k} > 1$ Eve's knowledge of the secret key increases rapidly. A zoomed out region when $0.7 < \mathrm{k} < 1$ is shown in the same figure for PCP and TPPR.

If again the distance between Eve and Alice or Eve and Bob were the only security guarantee, Eve's average knowledge of the key would be approximately 90% as shown in Fig. 12 with the *EC only a)* label in case a), and approximately 85% in case b) as shown with the *EC only b)* label. Note that in the simulated scenario, sensors A and B are at one wavelength distance from each other, while Eve is two wavelengths from B in case a) and almost 15 wavelengths in case b).

In the studied realistic channel model, the distance based security guarantee is too optimistic as Eve still knows a substantial part of the secret key. The factor k does not affect Eve's knowledge in this case as Eve's distance is not taken into account, and therefore error rates γ and η are not used at all.

By choosing a suitable value for factor k it is possible to balance between the reduction of achieved key rate and Eve's knowledge of the final key. Fig. 13 shows the tradeoff between Eve's knowledge of the final key vs. the achieved key rate. The results are shown for configurations b) and c). The curves start from $\mathrm{k} = 0.78$, for which Eve's knowledge is practically zero. Six values of k are marked to the PCP c) curve and five values are marked to the one-way c) curve. E.g. if $\mathrm{k} = 1$ Eve knows on the average $\sim 23\%$ of the final key produced using either PCP or TPPR. With a smaller k, Eve's knowledge is reduced. This assumes that Eve has an advantage compared to Alice and Bob as the assumption is

that $\gamma = \eta < \beta$ meaning that no one-way protocol is able to produce a key anymore.

V. CONCLUSION

In this paper, we proposed a method where the sensors carried by one user can securely communicate with each other using backscatter communication, even if there are other users with similar sensors nearby. Our setting uses the fading radio channel from the ambient transmitter to the sensors as a source of randomness for secret key generation. Existing secret key generation methods use the reciprocal radio channel between users as a source of randomness.

We showed that secret key generation is possible in this setting and that the distance from legitimate users to an eavesdropper does not guarantee a sufficient level of secrecy. In a realistic ambient backscatter channel relying on the distance to the eavesdropper as a safeguard is insufficient. Our simulations show that such an approach leads to too optimistic assumptions on Eve's knowledge, and there is a possibility that the eavesdropper knows a substantial part of the final key. Furthermore, one-way protocols are insufficient for key generation, they lead either to no key, or Eve knowning most of the key.

A working solution is based on a two-way key distillation protocol, and assuming that Eve's error rates are k times that of Alice's and Bob's, with $k < 1$. On the average this approach decreases significantly Eve's knowledge of the final key, at the expense of achievable key rate. This method gives Alice and Bob the freedom to trade off between achievable key rate and Eve's knowledge of the final key.

REFERENCES

[1] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 1–27, Feb. 2018.

[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[3] L. Ngu Nguyen, S. Sigg, J. Lietzen, R. Dieter Findling, and K. Ruttik, "Camouflage learning: Feature value obscuring ambient intelligence for constrained devices," *IEEE Trans. Mobile Comput.*, vol. 22, no. 2, pp. 781–796, Feb. 2021.

[4] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Information*, vol. 7, no. 3, p. 49, 2016.

[5] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.* New York, NY, USA: Association for Computing Machinery, Sep. 2008, pp. 128–139.

[6] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[7] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[8] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice*, 6th ed. London, U.K.: Pearson, 2014.

[9] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2nd Quart., 2014.

[11] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2283–2291.

[12] H. Hentila, V. Koivunen, H. Vincent Poor, and R. S. Blum, "Secure key generation for distributed inference in IoT invited presentation," in *Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2019, pp. 1–6.

[13] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, Oct. 2010.

[14] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[15] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[16] P. Wang, L. Jiao, K. Zeng, and Z. Yan, "Physical layer key generation between backscatter devices over ambient RF signals," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, May 2021, pp. 1–10.

[17] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[18] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Mar. 2015.

[19] U. M. Maurer, "Protocols for secret key agreement by public discussion based on common information," in *Advances in Cryptology—CRYPTO*, vol. 92, E. F. Brickell, Ed. Berlin, Cham, Switzerland: Springer, 1993, pp. 461–470.

[20] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[21] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[22] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[23] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[24] S. Tmar Ben Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *Proc. 3rd Int. Conf. New Technol., Mobility Secur.*, Dec. 2009, pp. 1–5.

[25] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.

[26] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[27] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst., Appl., Services*. New York, NY, USA: Association for Computing Machinery, 2011, pp. 211–224, doi: 10.1145/1999995.2000016.

[28] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur.* New York, NY, USA: Association for Computing Machinery, 2007, pp. 401–410, doi: 10.1145/1315245.1315295.

[29] J. Lietzén, R. Vehkalahti, and O. Tirkkonen, "A two-way QKD protocol outperforming one-way protocols at low QBER," in *Proc. IEEE Int. Symp. Inform. Theory*, Jun. 2020, pp. 1106–1111.

[30] C. Boyer and S. Roy, "Backscatter communication and RFID: Coding, energy, and MIMO analysis," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 770–785, Mar. 2014.

[31] A. Bletsas, S. Siachalou, and J. N. Sahalos, "Anti-collision backscatter sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5018–5029, Oct. 2009.
[32] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Bistatic backscatter radio for power-limited sensor networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 353–358.
[33] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM*, vol. 43, no. 4, pp. 39–50, Aug. 2013.
[34] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014.
[35] J. Lietzen, O. Tirkkonen, and R. Vehkalahti, "Secret keys from parity bits in the satellite setting," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2022, pp. 1–6.
[36] D. Jost, U. Maurer, and J. L. Ribeiro, "Information-theoretic secret-key agreement: The asymptotically tight relation between the secret-key rate and the channel quality ratio," in *Theory of Cryptography*, A. Beimel and S. Dziembowski, Eds. Cham, Switzerland: Springer, 2018, pp. 345–369.
[37] H. Stockman, "Communication by means of reflected power," *Proc. IRE*, vol. 36, no. 10, pp. 1196–1204, Oct. 1948.
[38] N. Van Huynh, D. Thai Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2889–2922, 4th Quart., 2018.
[39] Q. Zhang, H. Guo, Y.-C. Liang, and X. Yuan, "Constellation learning-based signal detection for ambient backscatter communication systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 452–463, Feb. 2019.
[40] B. P. Lathi and Z. Ding, *Modern Digital and Analog Communication Systems*, 4th ed. New York, NY, USA: Oxford Univ. Press, 2010.
[41] J. Lietzén, A. Liljemark, R. Duan, R. Jäntti, and V. Viikari, "Polarization conversion-based ambient backscatter system," *IEEE Access*, vol. 8, pp. 216793–216804, 2020.
[42] B. Badihi, A. Liljemark, M. U. Sheikh, J. Lietzén, and R. Jäntti, "Link budget validation for backscatter-radio system in sub-1 GHz," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.
[43] T. S. Rappaport, *Wireless Communications, Principles and Practices*. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.
[44] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.
[45] M. J. Gander and U. M. Maurer, "On the secret-key rate of binary random variables," in *Proc. IEEE Int. Symp. Inform. Theory*, Jun. 1994, p. 351.
[46] *Technical Specification Group Radio Access Network; Study on Channel Model for Frequencies From 0.5 to 100 GHz*, document TR 38.901 V16.1.0, 3GPP, 2019.
[47] S. Jaeckel, K. Raschkowski, K. Börner, and L. Thiele, "QuaDRiGa—Quasi deterministic radio channel generator, user manual and documentation," Fraunhofer Heinrich Hertz Inst., Berlin, Germany, Tech. Rep. v.2.6.1, 2021.

JARI LIETZÉN received the M.Sc. degree (Hons.) in communications engineering from Aalto University, Finland, in 2016, where he is currently pursuing the doctoral degree. His research interests include error correction and key growing protocols in quantum key distribution and backscatter communications.

OLAV TIRKKONEN (Fellow, IEEE) received the M.Sc. and Ph.D. degrees in theoretical physics from the Helsinki University of Technology, in 1990 and 1994, respectively. He held the postdoctoral positions at UBC, Vancouver, Canada, and NORDITA, Copenhagen, Denmark. He was at the Nokia Research Center (NRC), Helsinki, Finland, from 1999 to 2010. Since 2006, he has been a Faculty Member at Aalto University, Finland, where he is currently an Associate Professor of communication theory. From 2016 to 2017, he was a Visiting Associate Professor at Cornell University, Ithaca, NY, USA. He has published some 300 papers and is the inventor of some 85 families of patents and patent applications which include 1% of all patents declared essential for the first standardized version of 4G LTE. His current research interests include coding for random access and quantization, quantum computation, and machine learning for cellular networks. He is an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.