A Lightweight Protocol for Validating Proximity in UHF RFID Systems

Chrysanthi Paschou*, Oliver Johnson†, Ziming Zhu‡, Angela Doufexi*.
*Department of Electrical & Electronic Engineering, University of Bristol, UK— † School of Mathematics, University of Bristol, UK
‡Bristol Research and Innovation Laboratory, Toshiba Research Europe Ltd, Bristol, U.K.
e-mail: chrysanthi.paschou@bristol.ac.uk

***Abstract*—We present a novel scheme for testing the proximity of an Ultra-high frequency (UHF) Radio Frequency Identification (RFID) transponder, based on the fact that two co-located devices experience correlated channel fluctuations on a reference signal. When the interrogator requests data from the transponder, the latter performs backscattering modulation on the carrier-wave provided by a helper node. The interrogator applies signal processing techniques on the backscattered signal to extract the channel characteristics of the channel between itself and the helper, and the channel between the transponder and the helper. If the two channels are correlated, then the proximity of the transponder is validated by the fundamental properties of spatial channel correlation. The proposed scheme can be employed seamlessly in RFID systems from the transponder's point of view and is resilient to distance-fraud attack.**

***Index Terms*—Backscattering modulation, channel propagation, distance bounding, physical layer security, RFID systems, distance fraud, spatial channel correlation.**

I. Introduction

A. Motivation

Over the last few years, short-range communications systems have become an essential part of everyday life. Contactless payments, for example, have replaced cash payments for many individuals, and the same is expected to happen with key-fobs or access cards replacing physical keys. Smartphones are paired with a touch for data transfer and e-passports speed up long queues in airports. There are countless new applications of short-range communications and there are many more to come.

It is often assumed that the physical constraints of the communication channel implicitly prove the proximity of a device but such an assumption is far from true; Many proximity attacks have been recorded the most common of which are (solo) distance fraud [1], Mafia fraud [21], and Terrorist fraud attacks [5]. Our proposed scheme tackles the problem of distance fraud whereby a dishonest device with valid credentials attempts to deceive the verifying device (the interrogator) that it is in a closer distance than it is in reality.

A naïve method to tackle the problem of distance fraud would use the received signal strength to indicate the distance of the transmitting device. However, a device can 'shorten' its distance by transmitting with a higher power which makes such a method ineffective. The most well-established technique to counter distance fraud is based on a Distance Bounding (DB) method that measures the Round-Trip-Time (RTT) on an Ultra-Wide-Band (UWB) signal as first introduced by Brands *et al*. in their paper [3]. Relying on the fact that information cannot travel faster than the speed of light, measuring the RTT allows the verifier to give an upper bound of the distance (hence the name 'distance-bounding') between itself and the transmitting device [2], [10], [20]. The effectiveness of these protocols relies heavily on estimation accuracy. For example, a time offset of just 1μs translates to a 30-meter estimation error of the distance. Our proposed scheme does not require specialised hardware for time accuracy and it can be implemented in both UWB and narrowband channels. Since a lightweight protocol for distance bounding in narrowband systems is missing from the literature, we examine the case of narrowband systems.

B. Relevant work

Our work differs from the aforementioned distance-bounding protocols because no time measurements are required. The most closely related work is perhaps [12] whereby Marthur et al. suggest channel measurements for key generation between two co-located devices. Similar to ours, their work is based on the fact that two co-located devices experience similar channel fluctuations on a reference signal. In their scheme, the channel fluctuations are quantised by both devices (the verifier and the verifying device) in order to attain two symmetrical keys. We focus on systems that use backscattering modulation, and we show how the verifier can extract information for the ambient environment captured in the backscattered signal. In contrast to [12], no channel measurements are made by the verifying device (transponder) and no keys are generated. Key generation requires multiple rounds of information exchange between the legitimate pair for key reconciliation and secrecy amplification [12]. Without the need of keys, our scheme does not require extra rounds of communication. The intelligence is kept entirely at the verifier's side which makes our scheme lightweight, and therefore, suitable for RFID transponders.

This work was supported by the Engineering and Physical Sciences Research Council grant number EP/I028153/1 and Toshiba Research Europe Limited.

C. Organisation

Our scheme requires some basic knowledge on RFID systems and spatial correlation which is provided in the next section. In Section III, the channel models are defined and the reception of the tag's backscattered signal is formulated. Section IV explains how the reader uses the backscattered signal to evaluate the spatial correlation between itself and the tag. A decision of accepting or rejecting the tag is made based on a threshold, the choice of which is critical for the performance of the scheme, as Section V demonstrates. Finally, Section VI summarises the paper and suggests future directions.

II. Background and Overview

A. RFID basics

There are many different technologies that can be classified as short-range communications such as Body Area Networks (BAN), Personal Area Networks (PAN), RFID systems, and their sub-field of Near Field Communication (NFC). Our scheme relies on radiative coupling as currently employed by RFID systems that operate in the UHF spectrum [7]. UHF RFID systems are often found in secure access control, file tracking, supply chain management, and smart labeling. Although our scheme can be applied to any systems that use radiative backscattering modulation, we make UHF RFID systems our case study.

An RFID system mainly comprises a transponder (or tag), an interrogator (or reader), and a host computer or back-end database. A tag is a small, cheap, and simple device that is used for identification purposes [7]. Tags have memory constraints due to their low cost and they may (semi-passive case) or may not (passive case) have local power. Once excited by the reader, the tag responds by sending data through backscattering modulation. Upon reception, the reader forwards the data from the tag to the host computer for further processing. The computing power can, therefore, be thought to be concentrated at the reader.

B. Backscattering modulation and encoding

A tag-antenna is not a typical radio transmitter, in the sense that it does not transmit its own electromagnetic (EM) wave. To send the data requested by the reader, a tag performs EM backscattering modulation. In this type of modulation, the EM wave that carries the tag's baseband message is provided by the reader who transmits a continuous sinusoidal wave. The tag reflects back the carrier wave after modulating the signal, usually by means of Amplitude Shift Keying (ASK) or Phase Shift Keying (PSK) modulation. Our scheme uses 100% ASK which means that the digital data is represented as the presence or absence of the backscattered carrier wave. Such a modulation is commonly found in protocols compliant with the *Electronic Product Code (EPC) Gen2 UHF specification*: the de facto specification for UHF RFID tags [4].

Most EPC Gen2 UHF RFID protocols use the FM0 code or Miller code as encoding schemes. With FM0, a binary 0 is represented by a high or low voltage occupying the entire bit window whereas a binary 1 is represented by a transition in the middle of the bit window. Miller coding guarantees a transition in every other bit [9] which results in larger pulse width, hence less bandwidth to be transmitted.

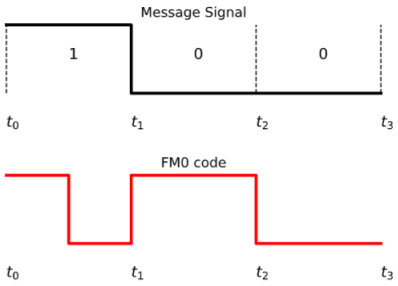

Fig. 1. Example of FM0 encoding at the transponder.

Example 1. To send binary string 100, the baseband message with FM0 coding is

$$m(t) = \begin{cases} 1 & \text{for } t \in [t_0, t_0/2) \\ 0 & \text{for } t \in [t_0/2, t_1) \\ 1 & \text{for } t \in [t_1, t_2) \\ 0 & \text{for } t \in [t_2, t_3) \end{cases} \tag{1}$$

where $(t_{i+1} - t_i)$ is the bit duration, primarily defined by the reader. The bit duration usually takes a value in the range between 6μs and 25μs. Fig. 1 gives a visual representation of the encoded message.

To modulate a binary one/zero of the encoded message with 100% ASK, the tag closes/opens its circuit for the duration of the binary bit. As such, we can associate the values of $m(t) = 1$ and $m(t) = 0$, as reflection and non-reflection, or simply as 'on' and 'off', respectively.

UHF tags operate in the region around 915MHz or 433MHz with corresponding wavelengths of 33cm and 69cm. The tag-antenna in these frequencies comes in many shapes such as dipoles, folded dipoles, printed dipoles or patch antennas [9], [19]. Our scheme requires undirected gain patterns which can be provided by dipoles or folded dipoles. The communication range in these frequencies can reach up to 100m if the tag is power-assisted or up to 10 m if no local power is available (passive case).

C. Spatial correlation and multipath fading

In a multipath environment, a transmitting signal follows many paths before it reaches the receiver(s). Each multipath component is associated with a complex number $A_i \in \mathbb{C}$, that we shall refer to as *complex path gain* with phase $\angle A_i$ and amplitude $|A_i|$. When two receivers with a uniform gain pattern are sufficiently close to one another, they observe similar complex path gains. Let $A_1(u)$ and $A_2(u)$ be the complex gains at two receivers that correspond to the multipath component arriving from direction $u \in S$, where S is the unit

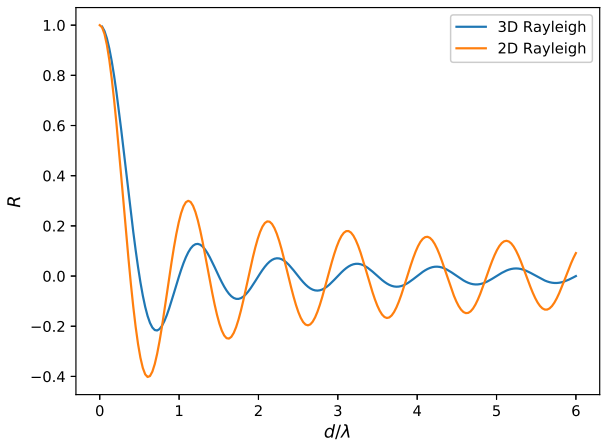

Fig. 2. Spatial correlation against the distance between the reader and the tag normalised to the wavelength.

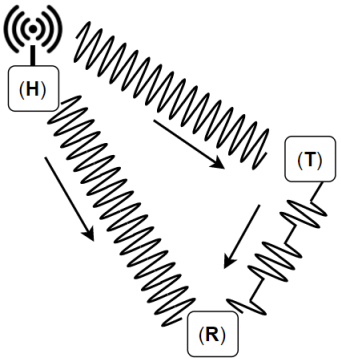

Fig. 3. The reader receives the superposition of two transmitting signals. At times when the tag does not reflect the reader evaluates the channel h_1, whereas h_2 is measured during reflection ($m(t) = 1$).

sphere. The path correlation between the two receivers is given as [6]

$$\rho(u) = \frac{A_1(u)A_2^*(u)}{|A_1(u)||A_2(u)|}, \tag{2}$$

where $(\cdot)^*$ is the complex conjugate, and operator $|\cdot|$ is the amplitude of the enclosed complex number. Averaging over all complex path gains, we attain the spatial channel correlation between two receivers. In practical scenarios where the exact geometry of the environment is not known, statistical models are used instead, in which case the spatial channel correlation is the statistical expectation of the path correlation

$$R := \mathbb{E}(\rho(u)), \tag{3}$$

which has been studied for several statistical models [15]–[18].

The spatial correlation is often referred to as Angle-of-Arrival (AoA)-statistics since it depends on the distribution of the unit vector $u \in S$. Vector u is often expressed in spherical coordinates $(1, \alpha, \beta)$, where α is the polar angle and β is the azimuthal angle. The term AoA refers to the pair (α, β).

Although our scheme can be applied to any multipath channel model, for reasons of exposition we focus on Rayleigh channels, for which the spatial correlation takes a closed form. We remind the reader that a Rayleigh (fading) channel is a rich-scattering channel for which:

- the phases $\angle A(u)$ are uniformly distributed across $[0, 2\pi]$ and are independent for different $u \in S$;
- the amplitudes $|A(u)|$ are identically and independently distributed for different $u \in S$.

The summation of all complex path gains as observed at the receiver results in a Rayleigh channel coefficient (or Rayleigh channel for brevity), h, the phase of which is also uniformly distributed, whereas its amplitude is a Rayleigh distributed random variable [19].

Let d be the distance between the tag and the reader, and let λ be the wavelength of the carrier frequency. If the unit sphere, S, lives in the three-dimensional (3D) space, the spatial correlation can be expressed as a function of the distance [13]:

$$R = \text{sinc}\left(\frac{2\pi d}{\lambda}\right) \qquad \text{(3D Rayleigh)}, \tag{4}$$

where $\text{sinc}(x) = \sin(x)/x$, when $x \neq 0$, and $\text{sinc}(0) = 1$. Such a model can be a good fit for indoor environments for which the ceiling and the floor act as good reflectors creating a 3D diffuse field. Eq. (4) is the basis of the rule-of-thumb stating that the channel decorrelates in half a wavelength.

The second most common geometry model restricts the AoA in one plane and the sphere S lives in the two-dimensional (2D) space. It is usually applied for rural environments, or when the antennas are vertically orientated and receive in the azimuthal plane. In this case, the spatial correlation can be expressed as [6]:

$$R = J_0\left(\frac{2\pi d}{\lambda}\right) \qquad \text{(2D Rayleigh)}, \tag{5}$$

where J_0 is the zeroth-order Bessel function of the first kind [6]. This formula (5) is popular because it gives a good approximation for 3D diffuse fields as long as one of the spherical angles (e.g. the polar angle) takes values from a limited range [15]. Fig. 2 plots the spatial correlation against the distance for the two channel models. It can be seen that the first zero correlation for the 2D case occurs at 0.38 wavelengths, which translates to approximately 12 cm when the carrier frequency is 915 MHz. Observe that the spatial correlation is an oscillating function of distance.

III. The Communication Channel

A. Channel model

There are three entities in our scheme, the tag (T), the reader (R), and the helper (H). The tag and the reader are equipped with single antennas, whereas the helper may have an arbitrary number of antennas. Different to typical RFID systems, when the reader requests data transfer from the tag, the EM energy is provided by the helper instead of the reader itself. The tag

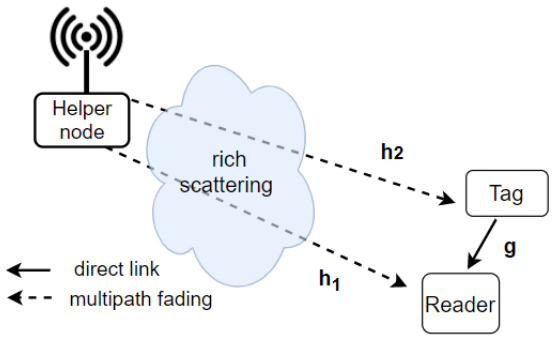

Fig. 4. Channel model: For authentication purposes, the tag needs to be displayed close to the reader, in which case both h_1 and h_2 are Rayleigh channels, whereas $g \in \mathbb{C}$ is a fixed LoS channel.

and the reader are considered to be stationary. To prove its proximity, the tag needs to be displayed close to the reader, in which case the channel between (T) and (R), denoted by $g(t)$ is deterministic due to a strong Line-of-Sight (LoS) component between the entities, that is:

$$g(t) = g \in \mathbb{C}, \tag{6}$$

for all t during the period of transmission.

As illustrated in Fig. 4, the helper is distanced to the reader, and the channel (H→R), denoted by h_1, is assumed to be a Rayleigh channel and dynamic in nature, i.e. it does not remain static but changes over time. The channel between the helper and the tag is denoted by h_2 and is also a Rayleigh channel. When the tag is distanced to the reader (at a distance much bigger to the wavelength), h_2 is independent of h_1.

The helper transmits a continuous wave sinusoid of constant phase and amplitude. For simplicity, the amplitude is normalised to one and the phase is set to zero. That is, at time t the helper node transmits:

$$c(t) = e^{j2\pi f_c t}, \tag{7}$$

where f_c is the carrier frequency. The corresponding wavelength is denoted by λ. The signal $c(t)$ reaches the reader and the tag as $r_1(t)$ and $r_2(t)$, respectively:

$$r_1(t) = h_1(t)c(t) + n_1(t) \tag{8}$$
$$r_2(t) = h_2(t)c(t) + n_2(t) \tag{9}$$

Components $n_1(t)$ and $n_2(t)$ are Additive White Gaussian Noise (AWGN) of zero mean and variance σ_i that vary independently from one another and for different samples.

$$n_i(t) \sim \mathcal{CN}(0, \sigma_i), \quad i = 1, 2. \tag{10}$$

B. Backscattered signal

The tag modulates the baseband signal, $m(t)$, on the received carrier frequency resulting the passband signal of $m(t)[h_2(t)c(t)) + n_2(t)]$. Let γ be the antenna reflection of the tag. This is a complex number fixed at the time of tag manufacture. The backscattered signal reaches the reader as

$$b(t) = \gamma g \underbrace{[h_2(t)m(t)c(t) + n_2(t)]}_{passband} + n_3(t), \tag{11}$$

for some AWGN noise $n_3(t) \sim \mathcal{CN}(0, \sigma_3)$, independent to $n_2(t)$. The tag employs 100% ASK modulation and FM0 (or Miller) coding scheme. As such, the baseband signal fluctuates between two values.

With the helper node transmitting continuously during the data transfer, the reader observes the superposition of two signals $r_1(t)$ (from the helper) and the backscattered signal $b(t)$ (from the tag), as seen in Fig. 3. The reader receives:

$$\begin{aligned} y(t) &= \underbrace{h_1(t)c(t) + n_1(t)}_{r_1(t)} + \underbrace{\gamma g[h_2(t)m(t)c(t) + n_2(t)] + n_3(t)}_{b(t)} \\ &= \begin{cases} h_1(t)c(t) + n(t), & \text{when } m(t) = 0 \\ [h_1(t) + \gamma g h_2(t)]c(t) + n(t), & \text{when } m(t) = 1 \end{cases}, \end{aligned} \tag{12}$$

where $n(t)$ captures all noise components. Observe the amplitude of the received signal is higher when $m(t) = 1$ than when $m(t) = 0$. As such, the reader is able to demodulate by 'observing' the envelope of the received signal.

IV. Evaluating the Spatial Correlation

A. Approximation

As seen in (3), the spatial channel correlation is the average of the correlation of all complex paths gains as observed at the two receivers. However, knowledge of the complex path gains is impractical in narrowband communications and a different approach for estimating R is needed.

Authors in [18] showed that given a rich scattering environment, the spatial correlation can be evaluated by the expectation of $h_1 h_2^*$ along with the variance of the individual channels:

$$R = \frac{\mathbb{E}(h_1 h_2^*)}{[\mathbb{E}(|h_1|^2)\mathbb{E}(|h_2|^2)]^{1/2}} \tag{13}$$

The estimation of the spatial correlation requires the estimation of multiple channel coefficients. The reader finds the sample mean of $\tilde{h_1} h_2{}^*$ and $|\tilde{h_i}|^2$, where $\tilde{h_i}$ is the estimation of the channel coefficient h_i. The spatial channel correlation for our statistical models (5), (4) is a real number as seen in (5) and (4). If the estimation of the spatial correlation, denoted by $\hat{R}$, gives rise to a complex number, the imaginary part shall be discarded. Thus, the estimation of the spatial correlation[1] equal to:

$$\hat{R} = \text{Re}\left(\frac{\hat{\mathbb{E}}(\tilde{h}_1 \tilde{h}_2^*)}{\left[\hat{\mathbb{E}}(|\tilde{h}_1|^2)\hat{\mathbb{E}}(|\tilde{h}_2|^2)\right]^{1/2}} \right), \tag{14}$$

[1]For cases when the reader can only measure the amplitude of the channel coefficient, the square of the spatial channel correlation, R^2, can be approximated by the envelope cross-correlation [8], [11] defined as $R_{\text{env}} := \frac{\mathbb{E}(|h_1||h_2|) - \mathbb{E}(|h_1|)\mathbb{E}(|h_2|)}{[\mathbb{E}(|h_1|^2 - \mathbb{E}(|h_1|)^2)\mathbb{E}(|h_2|^2 - \mathbb{E}(|h_2|)^2)]^{1/2}}$

where Re(·) is the real part of a complex number. $\hat{\mathbb{E}}(\cdot)$ denotes the sample mean, for example $\hat{\mathbb{E}}(\tilde{h}_1\tilde{h}_2^*)) = \sum_{i=0}^{M-1}(\tilde{h}_1(\tau_i)\tilde{h}_2^*(\tau_i))/M$, where M is the sample size.

B. Tracking the channels

The reader tracks the channel between itself and the helper (H→R) at times when the tag does not reflect, i.e., when $m(t) = 0$, whereas, during reflection, the reader is able to track the channel between the helper and tag (H→T) since this information is apparent on the backscattered signal. We show how by focusing first at one coherence block: a time interval, T_c, at which the channel h_1 remains static. If the tag is co-located with the reader, channels h_1 and h_2 will remain static for the same period of time: $h_1(t) = h_1(\tau_0)$ and $h_2(t) = h_2(\tau_0)$, for all $t \in T_c$ and some $\tau_0 \in T_c$.

Given the nature of FMO (or Miller) coding, there are no long runs of zeros or ones. Furthermore, the channel(s) typically change in a much slower rate than the bit rate. We can therefore say that within the coherence time, there exist two sub-intervals, $T_1 \subset T_c$ and $T_2 \subset T_c$ for which $m(t)$ takes the value zero when $t \in T_1$, whereas, when $t \in T_2$, $m(t) = 1$. The channel $h_1(\tau_0)$ and $h_2(\tau_0)$ are estimated at times $t \in T_1$ and $t \in T_2$, respectively.

1) Estimating h_1: Referring (8), when $m(t) = 0$ the received signal at the reader is $y(t) = h_1(t)c(t) + n_1(t)$. A sample for the channel coefficient h_1 is taken at time t_i by multiplying the received signal with the conjugate of the carrier:

$$\widehat{h_1}(t_i) = y(t_i)c^*(t_i) = h_1(\tau_0) + n(t_i)c^*(t_i) \tag{15}$$

Having collected a number of samples within the time interval T_1, the estimation of $h_1(\tau_0)$ is attained by taking the sample mean of $\hat{h_1}(t_i)$, i.e., $\tilde{h}_1(\tau_0) = \widehat{\mathbb{E}}(\hat{h_1}(t_i))$.

Lemma 1. *As the number of samples of $h_1(\tau_0)$ increases, the sample mean $\widehat{\mathbb{E}}(\hat{h_1})$ converges to the true channel coefficient $h_1(\tau_0)$.*

Given the low data rate of RFID systems (e.g. $m(t)$ remains zero for at least 5μs), we assume that a sufficient number of samples are taken resulting in an accurate evaluation of $h_1(\tau_0)$.

2) Estimating h_2: Within the coherence block of duration T_c, there will be times where $m(t) = 1$, $t \in T_2 \subset T_c$. From (9) the reader receives $y(t) = [h_1(t) + \gamma g h_2(t)]c(t) + n(t)$. Channel coefficient $h_1(t) = h_1(\tau_0)$ has been already evaluated. The coefficients γ and g are assumed to be known at the reader; Such a knowledge can be achieved by a priori direct communication with the tag. The reader applies simple operations on the received signal to attain a sample of $h_2(\tau_0)$:

$$\widehat{h_2}(t_i) = \frac{(\gamma g)^*}{|\gamma g|^2}(y(t)c^*(t) - h_1) = h_2 + \frac{\gamma^* g^*}{|\gamma g|^2}n'(t). \tag{16}$$

Similarly to Lemma1, it can be shown that for a sufficiently large sample size taken within the time interval T_2, an accurate estimation of $h_2(\tau_0)$ can be attained by taking the sample mean $\widehat{\mathbb{E}}(\widehat{h_2}(t_i))$. Similarly to h_1, we assume that a sufficient number of samples are collected and an accurate evaluation of $h_2(\tau_0)$ is attained. Such an assumption simplifies the theoretical analysis presented in Section V.

3) Repeating the process M times: The process presented for attaining $h_1(\tau_0)$ and $h_2(\tau_0)$ is repeated for different coherence blocks resulting in two sequences of size M:

$$\mathscr{H}_1 := [\tilde{h}_1(\tau_0), \ldots, \tilde{h}_1(\tau_{M-1})] \tag{17}$$

$$\mathscr{H}_2 := [\tilde{h}_2(\tau_0), \ldots, \tilde{h}_2(\tau_{M-1})] \tag{18}$$

The elements within each $\mathscr{H}_i$ are independent of one another, but the two sequences will be correlated shall the tag is in close proximity to the reader. Based on $\mathscr{H}_1$ and $\mathscr{H}_2$, the reader finds the sample mean of $\tilde{h_1}\tilde{h_2}^*$, and $|\tilde{h_i}|^2$ and applies Eq.(14) to attain an estimation of the spatial correlation between itself and the tag. M can be thought as the number of independent channel realisations and the sample-size for estimating the spatial correlation. After estimating the spatial correlation, the reader will:

- validate the tag's proximity if $\hat{R} \geq \epsilon$;
- reject the tag if $\hat{R} < \epsilon$,

for some decision threshold $\epsilon \in \mathbb{R}$.

V. On the values of M and ϵ

A. User's experience

1) Practicality: Observe that the spatial correlation as seen in Fig. 2 is not a monotonic function of distance. As such, there might be a case whereby the tag passes the proximity check ($\hat{R} \geq \epsilon$) for a given decision threshold and distance, but if it moves slightly closer to the reader, the check fails ($\hat{R} < \epsilon$). To avoid such a scenario, we introduce the definition of the *practical threshold* and we show that its value lives in a region (subset of the image of R) where the spatial correlation is injective and monotonic.

Definition 1. A threshold ϵ is *practical* if for every distance d_0 for which $R(d_0) \geq \epsilon$, it is implied that $R(d) \geq \epsilon$ for all $d < d_0$.

Lemma 2. *A decision threshold, ϵ, is practical if*

$$\epsilon \geq \max_{d>0}\{R(d) \text{ such that: } R^{'}(d) = 0\} \tag{19}$$

where $R^{'}$ is the derivative with respect to the distance, d.

The larger the threshold is, the closer the tag needs to be towards the reader in order to be accepted. E.g., for the $3D$ case, a threshold of $\epsilon = 0.9$ would bind the tag at a distance of 0.1λ, e.g. at 3.3 cm when $f_c = 900MHz$. Depending on the application scenario, this range may be too restrictive and the lowest possible decision threshold may be preferred. Fig. 5 shows the trade-off between minimum practical threshold and maximum distance for validation.

Corollary 1. *The minimum practical decision threshold for the 3D Rayleigh model is 0.128 which allows a tag to be validated from a maximum distance of 0.44λ. For the 2D Rayleigh case the minimum practical decision threshold is 0.3 and corresponds to the maximum validation distance of 0.29λ.*

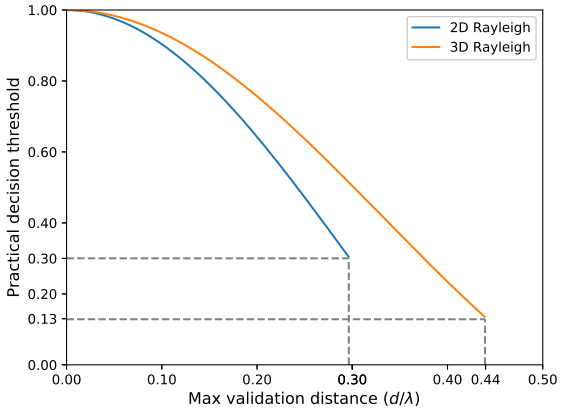

Fig. 5. The decision threshold against the maximum distance for proximity validation for two case models.

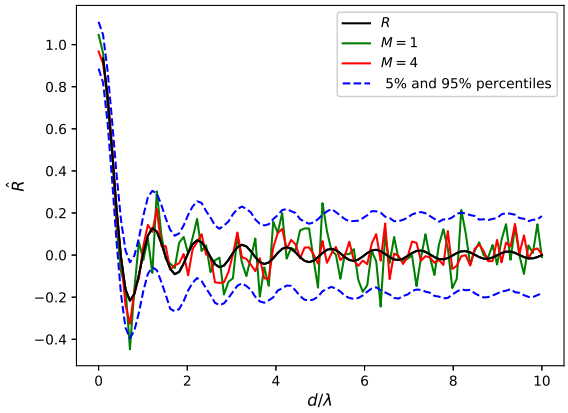

Fig. 6. The estimated spatial channel correlation for the $3D$ Rayleigh channel model for the cases when $M = 1$, $M = 4$, and $M \to \infty$ (R). When $M = 1$, 90% of the $\hat{R}$ values lie between the dashed lines.

2) Reliability: A false-alarm event occurs when the reader falsely rejects the tag due to an inaccurate estimation of the spatial channel correlation, R. I.e., the reader decides 'reject' due to $\hat{R} > \epsilon$, when in fact $R \leq \epsilon$. For a reliable system, we are interested in a low false-alarm probability:

$$P\left(\text{false alarm}\right) := P\left(\hat{R} < \epsilon | R \geq \epsilon\right) \tag{20}$$

Asymptotically, as $M \to \infty$ then $\hat{R} \to R$ and the probability of false alarm probability converges to zero. However, a large M can be impractical if the channel does not change fast enough during the transmission of the tag's message. Besides, typical RFID messages from the tag to the reader are short in length and they may not span multiple channel realisations. We are interested in examining the false-alarm probability for small values of M.

Providing an analytical expression for the false-alarm probability is a hard-problem and an empirical approach is used instead. For our simulations, the two receivers were surrounded by fifty far-field scatterers, but similar results attained for a 'less rich' scattering environment since the variance of $\hat{R}$ only decreases linearly with the number of paths N [14]. Our finding suggest that as long as the tag is positioned close to the reader at distance less than half a wavelength, even one channel realisation can provide a good estimation of the true spatial channel correlation as demonstrated in Fig.6.

Remark 1. The requirement of a short validation distance ($d < \lambda/2$) has two advantages. First, it corresponds to a practical decision threshold, and second, it guarantees an accurate estimation of the spatial channel correlation resulting in a low false-alarm probability.

B. Security

For our scheme to be effective, the proximity test of the tag shall fail if the tag is distanced to the reader ($d \gg \lambda$). When the tag is multiple wavelengths apart, the geometry of its environment will be different to that of the reader, and as such, it will experience uncorrelated multipath fading to the reader. The true value of the spatial correlation will be zero: $R = 0$, but when the sample size, M, is small, the estimated spatial correlation may diverge from the true value and the reader may falsely accept the distanced tag. When this happens, we say that a missed detection has occurred. We are interested in attaining a low probability of missed detection:

$$P\left(\text{missed detection}\right) := P\left(\hat{R} \geq \epsilon | R = 0\right) \tag{21}$$

Theorem 1. *For a given decision threshold ϵ and a number of independent channel realisations M, the probability of missed detection is equal to:*

$$P\left(\textit{missed detection}\right) = 1 - \frac{1}{M!} \sum_{k=0}^{\lfloor M(2\epsilon-1) \rfloor} (-1)^k \binom{M}{k} (M(2\epsilon - 1) - k)^M \tag{22}$$

Fig. 7 plots the probability of missed detection against the plane $M \times \epsilon$, whereas Fig.8 fixes ϵ for a 2D representation.

Observe that for a fixed decision threshold ϵ, an arbitrarily low probability of missed detection can be achieved with an appropriate choice of M. For example, when $\epsilon = 0.3$, a requirement of $P\left(\text{missed detection}\right) \leq 0.01$ can be achieved for $M = 5$.

Similarly, for a fixed M, an appropriate choice of decision threshold ϵ can result in an arbitrarily low probability of low detection. E.g., when $M = 3$, a choice of $\epsilon = 0.77$ satisfies $P\left(\text{missed detection}\right) \leq 0.01$.

Example 2. A decision threshold equal to $\epsilon = 0.5$ is practical for both channel models and guarantees an accurate estimation of the spatial correlation (6) resulting in low false alarm probability. Fig.5 suggests that a tag can be validated from a distance of at least 0.24λ, i.e., form a distance of 8cm assuming a carrier frequency of $f_c = 914MHz$. When $P(\text{missed detection}) \leq 0.05$ is acceptable, four independent channel realisations ($M = 4$) are sufficient, whereas when

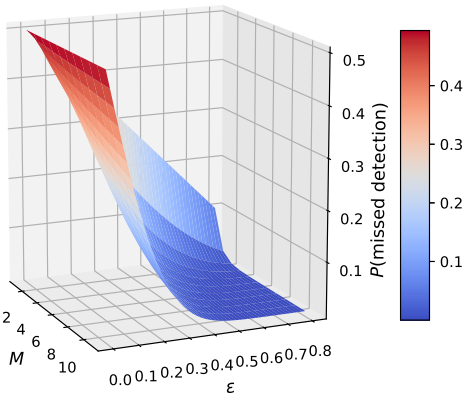

Fig. 7. Probability of missed detection against decision threshold (ϵ) and number of independent channel realisations measured by the reader (M)

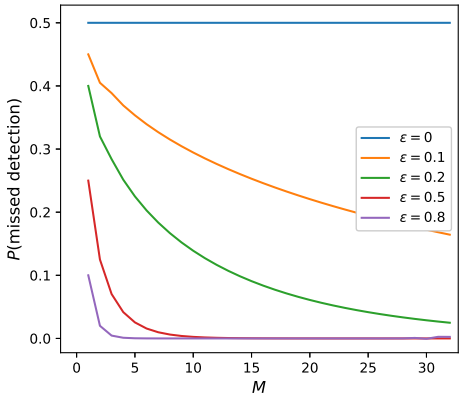

Fig. 8. Cuts parallel to the plane (P, M) of the plot of Fig.7.

$M = 10$ the probability decreases to less than 0.001 as seen in Fig.8.

VI. Conclusion

A novel scheme for checking the proximity between two devices has been presented. An overview on the topics of spatial correlation and backscattering modulation has been provided in Section II. Using Rayleigh fading as our study case (Section III), the combination of these two topics was made possible by employing a helper node, as shown in Section IV. The signal transmitted by the helper has two uses; First, it provides the electromagnetic energy required for backscattering, and second, it is used as reference signal to capture the ambient environment between two co-located devices: the interrogator and the transponder. In Section V we demonstrated how to choose an appropriate decision threshold given the number of independent channel realisations and vice versa. We saw that a high decision threshold is beneficial both for reliability and security but it requires a short distance for validation. The choice of a relatively low decision threshold can be compensated by increasing the number of channel realisations measured by the reader. As for future directions, the scheme can be extended to encounter Rician channels and other directive channels which are expected to enable proximity validation over longer distances ($d > \lambda$).

References

[1] G. Avoine, M. A. Bingöl, I. Boureanu, S. Čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla, et al. Security of distance-bounding: A survey. *ACM Computing Surveys (CSUR)*, 51(5):1–33, 2018.

[2] I. Boureanu, T. Chothia, A. Debant, and S. Delaune. Security analysis and implementation of relay-resistant contactless payments. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 879–898, 2020.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[4] M. Burmester and B. De Medeiros. The security of EPC Gen2 compliant IEEE protocols. In *International Conference on Applied Cryptography and Network Security*, pages 490–506. Springer, 2008.

[5] T. Chothia, J. De Ruiter, and B. Smyth. Modelling and analysis of a hierarchy of distance bounding attacks. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1563–1580, 2018.

[6] R. H. Clarke. A statistical theory of mobile-radio reception. *Bell system technical journal*, 47(6):957–1000, 1968.

[7] D. M. Dobkin. *The RFin IEEE: UHF IEEE in practice*. Newnes, 2012.

[8] M. Feeney and J. Parsons. Cross-correlation between 900 MHz signals received on vertically separated antennas in small-cell mobile radio systems. *IEE Proceedings I (Communications, Speech and Vision)*, 138(2):81–86, 1991.

[9] N. C. Karmakar. *Handbook of smart antennas for IEEE systems*. John Wiley & Sons, 2011.

[10] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira. The swiss-knife IEEE distance bounding protocol. In *International Conference on Information Security and Cryptology*, pages 98–115. Springer, 2008.

[11] P. Kyritsi, D. C. Cox, R. A. Valenzuela, and P. W. Wolniansky. Correlation analysis based on MIMO channel measurements in an indoor environment. *IEEE Journal on Selected areas in communications*, 21(5):713–720, 2003.

[12] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th international conference on Mobile systems, applications, and services*, pages 211–224, 2011.

[13] M. K. Ozdemir, E. Arvas, and H. Arslan. Dynamics of spatial correlation and implications on MIMO systems. *IEEE Communications Magazine*, 42(6):S14–S19, 2004.

[14] C. S. Patel, G. L. Stuber, and T. G. Pratt. Simulation of Rayleigh-faded mobile-to-mobile communication channels. *IEEE Transactions on Communications*, 53(11):1876–1884, 2005.

[15] J. Salz and J. H. Winters. Effect of fading correlation on adaptive arrays in digital mobile radio. *IEEE transactions on Vehicular Technology*, 43(4):1049–1057, 1994.

[16] U. Schilcher, J. F. Schmidt, M. K. Atiq, and C. Bettstetter. Autocorrelation and coherence time of interference in poisson networks. *IEEE Transactions on Mobile Computing*, 19(7):1506–1518, 2019.

[17] P. D. Teal, T. D. Abhayapala, and R. A. Kennedy. Spatial correlation for general distributions of scatterers. *IEEE signal processing letters*, 9(10):305–308, 2002.

[18] L. Tian, X. Yin, X. Zhou, and Q. Zuo. Spatial cross-correlation modeling for propagation channels in indoor distributed antenna systems. *EURASIP Journal on Wireless Communications and Networking*, 2013(1):1–11, 2013.

[19] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[20] Y.-J. Tu and S. Piramuthu. IEEE distance bounding protocols. In *First International EURASIP Workshop on IEEE Technology*, pages 67–68. Citeseer, 2007.

[21] Y.-J. Tu and S. Piramuthu. On addressing IEEE/NFC-based relay attacks: An overview. *Decision Support Systems*, 129:113194, 2020.