Physical Layer Protection Against Relay/Replay Attacks for Short-Range 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*—In response to the rise of crime in short-range communication systems, a novel method for authenticating co-located devices is presented. Our method, Channel Randomness Yields Secure Proximity (ChRYSP) exploits the fundamental properties of the wireless RF channel to protect against relay attacks and replay attacks - the two most common impersonation attacks in short-range communication systems. ChRYSP is based on the fact that two devices in close proximity - typically a couple of wavelengths - experience correlated fading on a received RF signal. ChRYSP is facilitated by the employment of a helper node and can be implemented by low-cost, narrowband transceivers. Numerical results demonstrate high accuracy in detecting both relay attacks and replay attacks.**

***Index Terms*—Authentication, multipath fading, physical layer security, relay attack, replay attack, short-range communications, spatial channel correlation.**

I. Introduction

Short-range communications systems such as Bluetooth and RFID 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 [1]. A common assumption of such systems is that the physical constraints of the communication channel implicitly proves the proximity of a device. However, this assumption is far from true and two types of impersonation attacks, namely, relay attacks and replay attacks are a real threat.

A. Relay/replay attacks

Relay and replay attacks are two types of impersonation attacks that target the authentication phase of a communication system between two devices. The verifying device is referred to as the verifier, whereas the prover is the device that needs to prove its legitimacy. For example, in a door-access control system, the prover is a key-fob and the verifier is a device placed by the door. The verifier challenges the prover to send authentication credentials such as an encrypted identification number. When the verifier receives valid credentials, it assumes that a genuine device is in close proximity and grants access.

Formally known as a Mafia-Fraud attack, a relay attack is a type of distance fraud whereby the verifier is deceived in believing that a legitimate prover is closer than it is in reality; The adversary captures, amplifies and re-transmits the signals sent from the verifier to the prover and vice versa. A relay attack is often launched by two attack nodes as shown in Fig. 1 in order to increase the distance over which the attack can be successful.

A popular variant of Mafia Fraud is a replay attack. Mafia Fraud and replay attacks account for the vast majority of car crime [2] and the two attacks are often perceived to have the same meaning in articles that address the public [3], [4]. Whereas, both attacks involve the retransmission of the signal, a replay attack is not a real-time attack, i.e., it is not launched during the data extraction. In a replay attack, the adversary retransmits the response that was captured during a previous authentication process between the verifier and the legitimate receiver [5].

B. Existed methods

Whereas replay attacks can be dealt with in the upper layers of the protocol stack with cryptographic primitives, protection against relay attacks typically requires the exploitation of the physical medium. Well-established techniques against bound the distance between the verifier and the prover by performing RSS, phase, or time-of-flight measurements. RF fingerprints and ambient-conditions based techniques are potential countermeasures against relay attacks as well as replay attacks.

1) Physical Layer Identification: Physical Layer Identification (PLI) is based on the unique RF characteristics of a device introduced by the imperfections in its analogue circuitry, [6]. Although PLI is a promising solution for authentication purposes, installation of related hardware is costly [7]. More research on the feasibility and system design is needed to prove that such an investment is worthwhile [8].

2) Ambient conditions: Authentication based on ambient conditions uses sensing technology to check the prox-

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

imity between the verifier and the prover. When the prover is close to the verifier, the environment around them will be similar. e.g., in terms of temperature, humidity, and sound [9]. Ambient-based methods have some potential in devices equipped with multiple (>6) sensors [10], [11]. Whether ambient-based methods can result in resilient and practical authentication is yet to be investigated [10], [12].

3) RSS and phase-based ranging: Given that there is a direct link between two communicating parties, the receiver can estimate the distance of the transmitter by RSS/RSSI or phase [13] measurements. These measurements are often used as distance-bounding technique against relay attacks [13], [14] due to their low cost and low power requirements. It is a widely held view [13]–[15] that techniques are vulnerable against distance fraud and should be avoided.

4) Time-of-flight distance bounding: To the author's belief, the most promising solution against relay attacks relies on the Distance Bounding (DB) technique that measures the time-of-flight of an incoming signal. However, due to their requirement of time accuracy, DB protocols require specialised hardware and an Ultra-Wide Bandwidth (UWB) channel [16], [17] in order to be effective.

C. Our solution

Channel Randomness Yields Secure Proximity (ChRYSP) is an authentication method that exploits the fundamental properties of the multipath radio frequency (RF) channel. ChRYSP is realised with the help of an external node which is referred to as the helper. The helper transmits a signal which is used as a reference signal for channel measurements at the verifier and the prover. When the authentication process begins, the verifier and the prover observe and quantise the channel fluctuations on the reference signal to obtain a *channel sequence*. The prover sends its channel sequence to the verifier along with a cryptographic signature to the verifier. If the channel sequence is correlated with the verifier's sequence, proximity is verified. The spatial correlation properties of the RF channel protect against relay attacks, whereas the temporal decorrelation properties protect against replay attacks.

Compared to DB techniques, ChRYSP does not require additional cryptographic methods in order to protect against replay attacks. The channel measurements can be thought of as a one-time session key with an expiration time equal to the coherence time of the channel. Moreover, the suggested method does not require an ultra-wideband channel or specialised hardware. Channel measurements such as those based on channel state information or received signal strength can be performed with low-cost devices. The latter statement is also the advantage of ChRYSP over RF fingerprints and ambient-based methods.

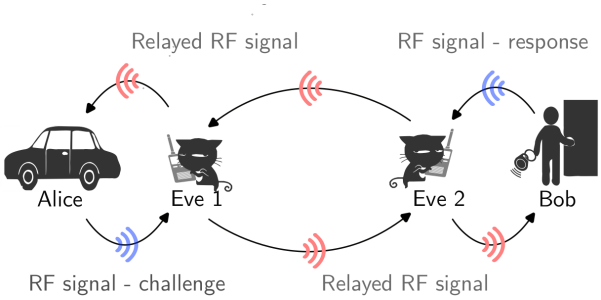

Fig. 1. A relay attack may be launched by two adversary nodes (Eve 1 & Eve 2) when the physical separation between the verifier (Alice) and the prover (Bob) is large.

D. Contributions and Organisation

To the author's best knowledge, it is the first time that the spatial/temporal properties of the RF channel are considered as a potential solution against relay or replay attacks. This paper communicates the idea behind ChRYSP and tests its performance based on a theoretical model.

The following section establishes the essential background and system model. The methodology is presented in Section III. After defining the performance metrics in Section IV, Section V demonstrated numerical examples. Lastly, Section VI concludes the paper and discusses future directions.

II. ChRYSP

A. Channel correlation

In a short-range communication system, Alice and Bob play the role of the verifier and the legitimate prover, respectively. Eve is the attacker who tries to impersonate Bob by launching a replay attack, or a relay attack. If a relay attack is launched by two attackers, Eve is the adversary closer to Alice. A helper node, Randy is employed to facilitate the authentication scheme. A dynamic flat fading multipath channel is assumed in between Randy and the receivers. Let $h_a, h_b, h_e \in \mathbb{C}$ denote the complex fading channels between Randy and Alice, Bob, and Eve, respectively. When the identity of the prover is not known, notation h_p is used to refer to the prover's channel, i.e., $p \in \{b, p\}$.

Channels h_a and h_p are assumed to be wide stationary which means that the first and second order statistics do not change. The mean value and variance of $h_u, u \in \{a, b, p\}$ are denoted by μ_u and σ_u^2), respectively. Shall the prover is in close proximity to Alice, channels h_a and h_p will be correlated. We choose the correlation metric to be the complex Pearson correlation coefficient given by

$$R(h_a, h_p) = \frac{E[(h_a - \mu_a)(\overline{h_p - \mu_p})]}{\sigma_a \sigma_p}. \tag{1}$$

Remark 1. When h_a and h_p are drawn from the Rayleigh distribution, the correlation given by (1) is a real valued number.

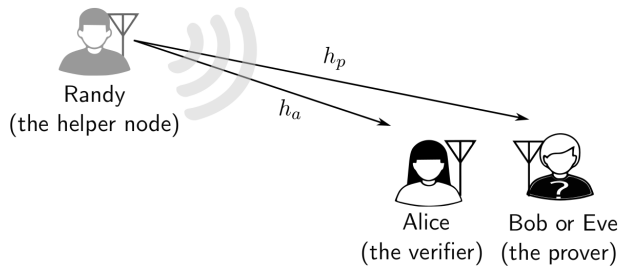

Fig. 2. Channel model

To facilitate analysis, it is assumed that, when there is no attack, Bob approaches Alice in close proximity such that

$$|R(h_a, h_b)| \geq R_o > 0 \quad \text{(no attack)} \tag{2}$$

That is, the fading correlation of their channels is at least R_o. On the other hand, if a relay attack takes place, Bob is distanced and the channels are decorrelated:

$$R(h_a, h_b) = 0 \quad \text{(relay attack)} \tag{3}$$

Due to the dynamic nature of the multipath channel, channels h_a and h_b have zero correlation if they are separated in time with the time separation being much bigger than the channel's coherence time. As such, equation $R(h_a, h_p) = 0$ implies separation either in the time domain or the spatial domain.

Note, that the channel correlation $R(h_a, h_p)$ can be expressed in terms of distance if the geometry of the environment is known. Many statistical models are known such as the one ring model, and Rappaport's model [18]. Aiming to provide a generic solution that is not specific to a singular type of environment, we choose not to express the channel correlation in terms of the distance between the two receivers. As such, we provide results that are not dependent on the geometry of the environment.

To give an insight on the relationship between distance and channel correlation, the channel correlation in a typical indoors office environment is higher than 0.5 when the two receivers are positioned in less than a couple of wavelengths apart (e.g., 10-20cm apart when the operating frequency is 2.4GHz) [19]. In outdoors environments, the channels tend to correlate over longer distances [18], [20].

B. Channel measurements

As it will be seen in Section III, ChRYSP begins with channel measurements that are made upon Randy's signal transmission. We assume that both Alice and the prover can track their channel over a period of time in a synchronised manner*.

For simplicity, we assume block fading and we partition Randy's transmitting signal into a sequence of blocks: $\mathbf{s} = \mathbf{s}_1, \ldots, \mathbf{s}_n$; The fading channel remains static during the transmission of each block and changes randomly from one block to the other. Let $h_u[i]$ be the channel realisation during the transmitting block $\mathbf{s}_i$ at receiver $u \in \{a, b, e\}$. The received block of symbols at Alice/prover is

$$\mathbf{y}_u[i] = h_u[i]\mathbf{s}_i + \mathbf{n}_u, \quad u \in \{a, b, e\}, \tag{4}$$

where $\mathbf{n}_u$ is additive noise. To evaluate $h_u[i]$, the simplest technique is maximum likelihood estimator whereby the receivers multiplies $\mathbf{y}_u[i]$ with $\mathbf{s}_i^H$, where $(\cdot)^H$ is the transpose conjugate operator. The larger the block sequence, the more accurate the estimation of h_i is. To communicate the key components of ChRYSP, the channel estimation error is not taken into account and perfect channel estimation is assumed at each receiver. By repeating the process over different blocks each receiver attains a sequence of N independent and identically distributed (i.i.d.) samples. Alice obtains

$$\{h_a[i]\} = (h_a[1], \ldots h_a[N]), \quad h_a[i] : \text{ i.i.d..} \tag{5}$$

The channel sequence at the prover is

$$\{h_p[i]\} = (h_p[1], \ldots h_p[N]), \quad h_p[i] : \text{ i.i.d.} \tag{6}$$

Note that the independence refers to the samples within the receiver's channel sequence. Sequence $\{h_a[i]\}$ can be correlated to $\{h_p[i]\}$. The sample correlation based on the observed channel sequences $\{h_a[i]\}$ and $\{h_p[i]\}$ is given by:

$$\hat{R}(h_a, h_p) = \frac{\sum_{i=1}^{N} (h_a[i] - \hat{\mu}_a)\,\overline{(h_p[i] - \hat{\mu}_p)}}{N\hat{\sigma}_a\hat{\sigma}_p}, \tag{7}$$

where $\hat{\mu_u}$ and $\hat{\sigma_u^2}$ are the sampled mean and sampled variance:

$$\hat{\mu_u} = \frac{1}{N}\sum_{i=1}^{N} h_u[i] \tag{8}$$

$$\hat{\sigma_u^2} = \frac{1}{N}\sum (h_u[i] - \mu_u)\overline{(h_u[i] - \mu_u)}. \tag{9}$$

C. Valid tags

It is assumed that Alice and Bob share a secret key, k, i.e., a random sequence that is known to them only. To pass the legitimacy test, a prover needs to demonstrate knowledge of the key by computing a valid keyed cryptographic hash function such as a message authentication code, or a keyed SHA-2 [21].

Definition 1. Let $tag_k(\mathbf{s})$ be a (keyed) cryptographic hash function with inputs the secret key, k, and sequence $\mathbf{s}$. The pair $(\mathbf{t}, \mathbf{s})$ is said to be valid if and only if $\mathbf{t} = tag_k(\mathbf{s})$. For a valid pair $(\mathbf{t}, \mathbf{s})$, we say that tag $\mathbf{t}$ is valid for sequence $\mathbf{s}$.

Remark 2. Commonly used keyed hash functions require binary inputs. If the sequence $\mathbf{s}$ is not binary, we need to take its binary representation, say $f(\mathbf{s})$, to a certain level of precision and calculate the hash function of $tag_k(f(\mathbf{s}))$.

*Perfect synchronisation is not required as long as the time-offset between the measurements is less than coherence time of the channel.

We simplify the notation by merging the notation of the composite function $tag_k \cdot f$ to tag_k.

We assume that only the holder of the pre-shared key, k, can produce valid pairs. However, Eve may eavesdrop the communications between Alice and Bob and attain valid tags for some strings.

III. Methodology

ChRYSP blends together two tests, namely the proximity test and the and legitimacy test. The proximity is based on the channel correlation, whereas the legitimacy test requires the computation of a valid tag for the prover's channel sequence. Overall, the method comprises four stages.

Stage 1:*Channel measurements.* Randy transmits a sequence of known symbols. Alice and the prover record N independent realisations of h_a and h_p. Alice's channel sequence is $\{h_a[i]\}$, and the prover's channel sequence is $\{h_p[i]\}$ as per Eq. (5) and (6).

Stage 2: *Signing the channel sequence.* The prover computes tag, $\mathbf{t}$, for their channel sequence $\{h_p[i]\}$. The prover sends $\mathbf{t}$ followed by $\{h_p[i]\}$ to Alice.

Stage 3: *Legitimacy test.* Upon reception of $(\mathbf{t}, \{h_p[i]\})$, Alice computes $tag_k(\{h_p[i]\})$ and checks whether it is equal to $\mathbf{t}$. If it is, the received tag is valid, the prover passes the legitimacy test, and Alice proceeds to the last stage. If the tag is not valid, Alice rejects the prover and the authentication process terminates.

Stage 4: *Proximity test.* Alice estimates the channel correlation $R(h_a, h_p)$ as per Eq. (7). For a given threshold τ, if $|\hat{R}| \geq \tau$, the prover passes the proximity test and authentication has been successful. If $|\hat{R}| \geq \tau$, the prover fails the test and Alice rejects the prover.

$$\text{If } |\hat{R}| \geq \tau, \text{ accept the prover;}$$
$$\text{Otherwise, reject the prover.}$$

IV. Performance metrics

Due to the finite sample of (h_a, h_p), the estimated correlation $\hat{R}$ may differ from the true channel correlation R. As such, there might be scenarios whereby Alice falsely accepts or falsely rejects the prover.

A. Detecting a relay/replay attack

A relay attack will pass the legitimacy test but will fail the proximity test. Indeed, when Bob is deceived in believing that he communicates with Alice, he computes and sends a valid pair $(\mathbf{t}, \{h_b[i]\})$. Since the tag is valid only for Bob's channel observations, Eve cannot relay the tag but change the channel sequence. Eve relays $(\mathbf{t}, \{h_b[i]\})$ and successfully passes the legitimacy test. The detection of the relay attack depends on Stage 4. Due to the spatial separation between Alice and Bob, channels h_a and h_b are decorrelated. A missed detection may occur due to the estimation error of the true channel correlation. The probability of a missed detection of a relay attack is equal to $P(\hat{R} > \tau | R = 0)$, where $R = R(\{h_a[i]\}, \{h_b[i]\})$.

In a replay attack, Eve possesses a valid pair $(\mathbf{t}, \{h_b[i]\})$ by having eavesdropped on previous message exchanges between Alice and Bob. When Eve replays $(\mathbf{t}, \{h_b[i]\})$, she will successfully pass the legitimacy test. Detecting Eve relies again on Stage 4. Thanks to the temporal decorrelation of dynamic channels, Bob's old channel is decorrelated to Alice's channel at the time of the replay attack, i.e., $R(h_a, h_b) = 0$. Hence, the probability of missed detection of a relay attack is equal to the probability of a missed replay attack.

The importance of Stage 3 is to ensure that Bob is involved in the authentication process. Without, Stage 3, any node in close proximity to Alice would be successfully authenticated. As such, Stage 3 is vital. Observe that Eve stands a chance of success when she does not send her own channel h_e; Eve either relays Bob's channel sequence, or replays Bob's old channel sequence. There are three possible events for a prover that has made it to Stage 4:

1) No attack: Bob is in close proximity. In this case $R := R(h_a, h_b) \geq R_o$.
2) Relay attack: Bob is distanced. In this case $R = 0$.
3) Replay attack: Bob's channel sequence belongs to a different time frame. In this case: $R = 0$.

Hence, Alice's binary decision between accepting the prover and rejecting the prover relies on choosing between '$R \geq R_o$' (no attack) versus '$R = 0$' (attack).

Definition 2. By the term False Negative Rate (FNR), we refer to the probability of missed detection of a relay attack or a replay attack. It can be thought as the probability of falsely accepting Eve.

$$\text{FNR} := P(|\hat{R}| \geq \tau | R = 0). \tag{10}$$

The complement of FNR, i.e., the probability of detecting the attack is referred to as the the True Positive Rate (TPR).

$$\text{TPR} := 1 - \text{FNR} = P(|\hat{R}| < \tau | R = 0). \tag{11}$$

Definition 3. By the term False Positive Rate (FPR), we refer to the probability of falsely assuming an attack, i.e., rejecting Bob although there is no attack.

$$\text{FPR} := P(|\hat{R}| < \tau || R| \geq R_o). \tag{12}$$

The complement of FPR, is referred to the True Negative Rate and can be thought as the probability of correctly accepting Bob.

$$\text{TNR} := P(|\hat{R}| \geq \tau | R \geq R_o). \tag{13}$$

Remark 3. As channel correlation increases, e.g. due to Bob approaching Alice closer, the performance of the scheme in terms of FPR increases. FPR is upper bounded by

$$\text{FPR} \leq P(|\hat{R}| < \tau || R| = R_o). \tag{14}$$

Choosing a pessimistic approach, the graphs of Section V only consider the maximum value of FPR which is denoted by $\text{FPR}_{\max}$.

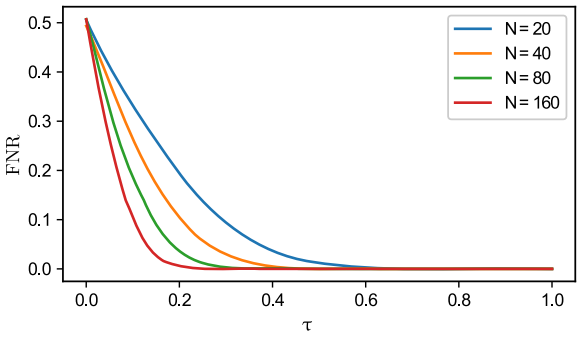

Fig. 3. False-negative rate against the decision threshold

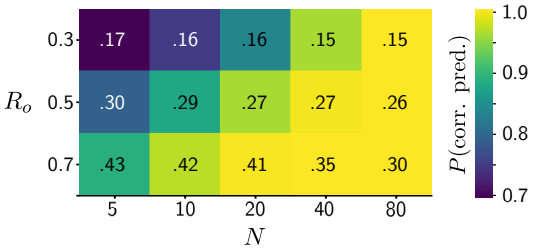

Fig. 4. Optimal thresholds for increasing the probability of correct predictions

V. Numerical Examples

The choice of the decision threshold, τ, and the sample size, N, is a problem that needs to be studied case by case depending on the system's requirements and restrictions. Let us consider the restriction where the time of channel probing is at most T_p. Then N can be at most $\lfloor T_p/T_c \rfloor$, where T_c is the channel's coherence time. Asymptotically, as $N \to \infty$, the sample correlation converges to the true correlation, and Alice's predictions will be 100% correct for any decision threshold $0 < \tau \leq R_o$. For a fixed N, the choice of the decision threshold will determine the values of FNR and FPR.

To give numerical examples, we run simulations whereby the events of 'attack' and 'no attack' occur in the same frequency. I.e. $P(\text{'attack'}) = P(\text{'no attack'}) = 0.5$. Standard complex channels are considered: h_a, $h_b \sim \mathbf{CN}(0, 1)$. In the case of an attack, Bob's re(p)layed channel is decorrelated from Alice's channel such that $R(h_a, h_b) = 0$, otherwise, $R(h_a, h_b) = R_o$.

Fig. 3 suggests that for $N = 160$, any threshold $\tau \geq 0.17$ meets the requirement, whereas, for $N = 20$, the decision threshold needs to be at least 0.5. Observe from (10) and (12) that there is a trade-off between the values of FPR_{max} and FNR. As such, for minimising FPR whist meeting the requirement of the form $\text{FNR} < \epsilon$, the smallest possible decision threshold needs to be considered.

To find the threshold that maximises the probability of correct predictions, $P(\text{corr. pred.})$, observe that this is equal to the summation of:

$$P(\text{corr. pred.}) = \tag{15}$$
$$P(|\hat{R}| \geq \tau, R \geq R_o) + P(|\hat{R}| < \tau, R = 0) = \tag{16}$$
$$\frac{1}{2}P(|\hat{R}| \geq \tau | R \geq R_o) + \frac{1}{2}P(|\hat{R}| < \tau | R = 0) = \tag{17}$$
$$\frac{1}{2}(\text{TPR} + \text{TNR}). \tag{18}$$

Figure 4 demonstrates that the threshold that maximises $P(\text{corr. pred.})$, denoted by τ_o, is roughly half the size of the correlation coefficient R_0 when $N = 40$. The optimal threshold slowly decreases with N; Halving the size of channels samples (N) results in less than 1% change in τ_o. A sample size of $N = 80$ guarantees 99.95% of correct predictions even when the channel correlation is as low as $R_o = 0.3$.

To examine the overall performance of a binary classification problem ('fraud' or 'no fraud'?) without fixing the decision threshold, Receiver Operator Characteristic (ROC) graphs are commonly used. A ROC graph is plotted by considering TPR and FPR as functions of τ and plotting $\text{TPR}(\tau)$ against $\text{FPR}(\tau)$ for all $0 \leq \tau \leq 1$. Typically, a binary classifier is considered to be 'accurate' when the Area Under the Curve (AUC) is 0.9 or higher. In the ideal case where AUC = 1, the system, i.e. Alice, makes 100& correct predictions. Graphs in Fig. 5 plot the ROC curves for the cases of $R_o = 0.3, 0.5$ and 0.7 respectively. The level of accuracy for the values of AUC is three decimal places. For $N \geq 40$, the binary classifier is accurate as long as $R_0 \geq 0.3$. When $R_0 < 0.3$, a fast varying dynamic channel is needed to ensure a sufficiently large sample size, N.

VI. Conclusion and Future Directions

ChRYSP (Channel Randomness Yields Secure Proximity) is a novel authentication method that exploits the spatial channel correlation and temporal channel decorrelation to protect against relay attacks and replay attacks. The case of narrowband communications has been studied which is typical in short-range communication systems. Under perfect channel estimation, simulations suggest that ChRYSP is a promising solution against relay/replay attacks in non-static environments. A channel rich in entropy allows the required minimum channel correlation to be a small value thereby enabling authentication over longer distances.

Despite the (almost) stationary nature of short-communication systems, ChRYSP can be applied in a variety of systems whereby the prover -the device subject to authentication- is in close proximity to the verifying device. We suggest the following research directions:

- Re-configurable intelligent surfaces are employed for creating a dynamic multipath environment between the helper node and the verifier/prover.

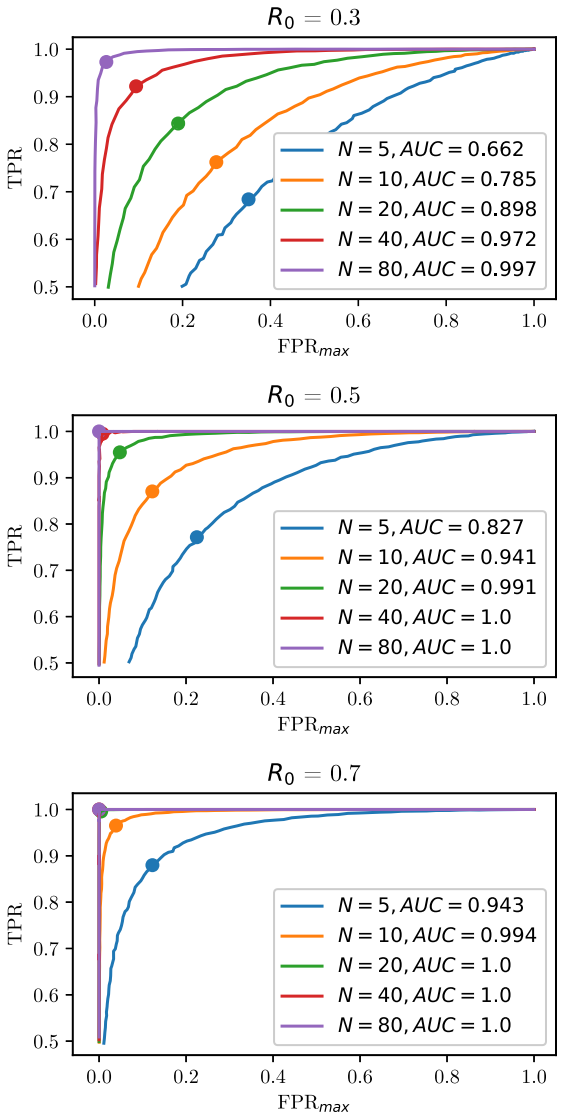

Fig. 5. ROC graphs for $R_0 = 0.3, 0.5, 0.7$. The marked coordinates correspond to the optimal performance of the binary classifier in terms of increasing the probability of correct predictions.

- The channel measurements at the verifier and the prover are facilitated through the training sequences transmitted by mutliple WiFi routers;
- The helper node is equipped with multiple antennas or a distributed antenna system and changes the angle of departure by transmitting from a random selection of antennas.

References

[1] C. Paschou, O. Johnson, Z. Zhu, and A. Doufexi, "A lightweight protocol for validating proximity in UHF RFID systems," in *2021 IEEE94th Vehicular Technology Conference (VTC2021-Fall)*, pp. 1–7, IEEE, 2021.

[2] Y. E. Post, "How to prevent your car being stolen without keys, as thefts continue to rise."

[3] T. car expert, "To key or not to key?."

[4] I. news, "Insurance crime bureau warns of rise in car thefts through relay attacks."

[5] S. Akter, S. Chellappan, T. Chakraborty, T. A. Khan, A. Rahman, and A. A. Al Islam, "Man-in-the-middle attack on contactless payment over nfc communications: design, implementation, experiments and detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 3012–3023, 2020.

[6] E. Uzundurukan, Y. Dalveren, and A. Kara, "A database for the radio frequency fingerprinting of bluetooth devices," *Data*, vol. 5, no. 2, p. 55, 2020.

[7] L. Cui, Z. Zhang, N. Gao, Z. Meng, and Z. Li, "Radio frequency identification and sensing techniques and their applications—a review of the state-of-the-art," *Sensors*, vol. 19, no. 18, p. 4012, 2019.

[8] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the third ACM conference on Wireless network security*, pp. 89–98, 2010.

[9] W. Choi, M. Seo, and D. H. Lee, "Sound-proximity: 2-factor authentication against relay attack on passive keyless entry and start system," *Journal of Advanced Transportation*, vol. 2018, 2018.

[10] G. Haken, K. Markantonakis, I. Gurulian, C. Shepherd, and R. N. Akram, "Evaluation of apple idevice sensors as a potential relay attack countermeasure for apple pay," in *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, pp. 21–32, 2017.

[11] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication," in *2014 IEEEInternational Conference on Pervasive Computing and Communications (PerCom)*, pp. 163–171, IEEE, 2014.

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

[13] H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the security of carrier phase-based ranging," in *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 490–509, Springer, 2017.

[14] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[15] P. De Cauwer, T. Van Overtveldt, J. Doggen, F. Van der Schueren, M. Weyn, and J. Bracke, "Study of rss-based localisation methods in wireless sensor networks," in *European Conference on the Use of Modern Information and Communication Technologies (ECUMIT), Ghent*, 2010.

[16] D. H. Yum, J. S. Kim, S. J. Hong, and P. J. Lee, "Distance bounding protocol for mutual authentication," *IEEETransactions on Wireless Communications*, vol. 10, no. 2, pp. 592–601, 2010.

[17] 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*, pp. 879–898, 2020.

[18] R. B. Ertel, P. Cardieri, K. W. Sowerby, T. S. Rappaport, and J. H. Reed, "Overview of spatial channel models for antenna array communication systems," *IEEEpersonal communications*, vol. 5, no. 1, pp. 10–22, 1998.

[19] 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*, vol. 2013, no. 1, pp. 1–11, 2013.

[20] 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)*, vol. 138, no. 2, pp. 81–86, 1991.

[21] N. Sklavos and O. Koufopavlou, "On the hardware implementations of the sha-2 (256, 384, 512) hash functions," in *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03.*, vol. 5, pp. V–V, IEEE, 2003.