This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Physical Layer, Zero-round-trip-time, Multi-factor Authentication Protocol

MIROSLAV MITEV[1], MAHDI SHAKIBA-HERFEH[2], *(Member, IEEE)*, **ARSENIA CHORTI[2],** *(Senior Member, IEEE)*, **MARTIN REED[3],** *(Member, IEEE)*, **and SAJJAD BAGHAEE[4],** *(Student Member, IEEE)*

[1]Barkhausen Institut, Dresden, Germany (e-mail: miroslav.mitev@barkhauseninstitut.org)
[2]ETIS UMR8051, CY Cergy Paris University, ENSEA, CNRS, F-95000, Cergy, France (e-mails: {mahdi.shakiba-herfeh, arsenia.chorti}@ensea.fr)
[3]CSEE, University of Essex, Colchester, UK (mjreed@essex.ac.uk)
[4]Department of Electrical and Electronics Engineering, METU, 06800, Ankara, Turkey (e-mail: sajjad@baghaee.com)

Corresponding author: Miroslav Mitev (e-mail: miroslav.mitev@barkhauseninstitut.org).

While conducting this study M. Mitev and A. Chorti were supported by the DIM RFSI project SAFEST; M. Shakiba-Herfeh and A. Chorti were supported by the ELIOT ANR-18-CE40-0030 - FAPESP 2018/12579-7 and the INEX Projects eNiGMA and PHEBE; M. Reed was supported by the H2020 project SerIoT with project agreement no 780139 funded by the EU.

ABSTRACT Lightweight physical layer security schemes that have recently attracted a lot of attention include physical unclonable functions (PUFs), RF fingerprinting / proximity based authentication and secret key generation (SKG) from wireless fading coefficients. In this paper, we propose a fast, privacy-preserving, zero-round-trip-time (0-RTT), multi-factor authentication protocol, that for the first time brings all these elements together, i.e., PUFs, proximity estimation and SKG. We use Kalman filters to extract proximity estimates from real measurements of received signal strength (RSS) in an indoor environment to provide soft fingerprints for node authentication. By leveraging node mobility, a multitude of such fingerprints are extracted to provide resistance to impersonation type of attacks e.g., a false base station. Upon removal of the proximity fingerprints, the residual measurements are then used as an entropy source for the distillation of symmetric keys and subsequently used as resumption secrets in a 0-RTT fast authentication protocol. Both schemes are incorporated in a challenge-response PUF-based mutual authentication protocol, shown to be secure through formal proofs using Burrows, Abadi, and Needham (BAN) and Mao and Boyd (MB) logic, as well as the Tamarin-prover. Our protocol showcases that in future networks purely physical layer security solutions are tangible and can provide an alternative to public key infrastructure in specific scenarios.

INDEX TERMS Physical layer security, multi-factor authentication, PUF, Kalman filter, SKG, 0-RTT.

I. INTRODUCTION

AUTHENTICATION is central in building secure networks; confirming the identity of devices and their role in a network's hierarchy eliminates the possibility of numerous attacks [1]–[3]. However, stringent latency and computational power constraints are present in many emerging verticals, typically involving Internet of things (IoT) infrastructure [4], [5], rendering the design of respective authentication mechanisms a challenging task. As an example, a recent 3GPP report on the security of ultra reliable low latency communication (URLLC) systems notes that authentication for URLLC is still an open problem [6]. Current solutions rely on modulo arithmetic in large fields and typically incur considerable latency, as an example, it has been reported that verifying digital signatures in a vehicular networking scenario, utilizing a typical 400 MHz processor, takes around 20 ms [7]. Moreover, a full authentication procedure with EAP-TLS (used for the narrow-band IoT standard [8], [9]) on a 1.73 GHz processor tablet takes on average 165.5 ms in static conditions and 336.7 ms for high mobility conditions [10]; the value decreases to approximately 55 ms for the re-authentication process in static environments [10], [11]. Additionally, with the advance of quantum computing, traditional asymmetric key cryptographic schemes will become semantically insecure while, at the same time, current proposals for post-quantum alternatives use keys of substantial lengths [12] and might not be compatible with constrained devices. Therefore, the proposal of new lightweight security primitives and protocols for device authentication is timely.

Notably, many critical IoT networks require fast authentication, e.g., in V2X applications, telemedicine and haptics. In this framework, physical layer security (PLS) emerges as

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

TABLE 1: Paper Contributions

	Technology	Novelty	Overall contributions
Initial authentication	Proximity estimation	As an initial factor of authentication we propose a novel proximity detection mechanism leveraging user mobility to authenticate a static server.	The combination of all the technologies in a single solution gives a novel and secure authentication protocol. To support the employment of PHY layer SKG in short blocklength communication protocols, we provide the complete chain of the SKG process. We validate the performance of the proposed mobility-based proximity detection and the SKG process through real-life experiments. The security properties of the protocol are formally proven using MB logic and the Tamarin-prover. We introduce a novel, physical layer, forward secure 0-RTT resumption authentication mechanism.
	PUFs	Standard PUF mechanisms are used as a main factor of authentication in our two-party protocol. Combining PUFs and mobility-based proximity estimation can prevent impersonation attacks in the presence of a malicious server.	
	SKG	The proposed system utilize the randomness in the wireless fading coefficients to generate maximum entropy session keys.	
0-RTT resumption	SKG	In a subsequent communication between the nodes the generated keys are incorporated in a novel PHY-based 0-RTT protocol to provide forward secrecy and protection against replay attacks.	

a lightweight alternative to computational complexity based schemes [13], [14]. The increasing interest in PLS has been stimulated by many practical needs, as it comes with negligible overheads. Moreover, it relies upon information-theoretic security concepts and could provide quantum resistant solutions that are scalable to large IoT networks.

PLS schemes exploit physical layer entropy sources in both the hardware and in the communication medium [15]–[17]. With respect to the former, physical unclonable functions (PUFs) are hardware entities harnessing entropy from physically unclonable variations that occur during the production process of a silicon device [18], [19]. Due to their unclonability, PUFs can be used in challenge – response authentication protocols, where a challenge can refer to measuring the jitter of a ring oscillator, power-on state, etc., [20]–[23]. Published experimental results show that PUF based authentication is indeed faster (around 5.6 ms in a ring oscillator PUF [24]) compared to standard asymmetric key based alternatives, mentioned previously.

Furthermore, localization is widely accepted nowadays as a second authentication factor. Some of the employed localization methods, including time-of-flight, multilateration and multiangulation can achieve high precision, but typically require complex operations and measurements from multiple reference points. Alternatively, proximity estimation has a very low computational complexity and can easily be implemented in constrained IoT devices (e.g., using Bluetooth Low Energy ports) [25] to estimate the distance from a single reference point to a transmitting beacon [26]. Importantly, such techniques could be useful to address impersonation attacks in the radio access, which fall under the general umbrella of false base stations [27].

Apart from authentication, the wireless channel can also be treated as a source of entropy. More concretely, small scale fading components in channel state information (CSI), e.g., due to the unpredictable movement of entities that cause scattering, can be used for secret key generation (SKG). With respect to the robustness of SKG under unpredictability requirements [28], a key point introduced in [29] and [30] concerns the removal of predictable components from the observed CSI as a necessary pre-processing step before performing SKG. Furthermore, with respect to reconciliation, in [31] various short Slepian Wolf decoders have been compared in the short blocklength.

Bringing together the above elements, in this paper we introduce a fast, multi-factor authentication protocol that uniquely combines the above PLS techniques, namely: PUF authentication; proximity estimation from received signal strength (RSS); pre-processing of RSS for SKG; and, reconciliation at the short blocklength. The symmetric SKG keys are used as resumption secrets in a 0-RTT authentication protocol. Furthermore, as devices might store sensitive information, a one-time alias scheme is incorporated to provide anonymity with respect to the identity of the nodes during authentication.

The contributions of this work are summarized in Table 1. We propose a two-phase authentication protocol between two legitimate nodes, comprising an initial enrollment phase and an authentication phase. The authentication protocol uniquely combines a number of PLS schemes and showcases for the first time, to the best of our knowledge, that a purely physical layer security handshake protocol is tangible. In detail, the following elements are brought together to build an all physical layer handshake protocol:

1) *A novel, mobility-enhanced proximity estimation using Kalman filters is proposed for soft authentication.* A novel aspect of our proposal is that it provides robustness against impersonation attacks by leveraging node mobility. In more detail, by allowing a mobile node to choose freely the distances at which proximity estimation to a base station (access point) is performed, false base stations would not be able to adapt their transmission power and as a result will fail to launch impersonation attacks;
2) *SKG from small scale fading.* We propose to isolate entropy rich, small scale, fading in the observed RSS by treating the output of the Kalman filter as a predictable component [29], [30] that has to be removed before SKG. The novelty of this contribution is that the Kalman filter low pass filtering properties are used to isolate persistent, location dependent trends in the RSS. We note that in [29] and [30] the isolation of small scale

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

fading was performed by using power domain separation techniques (e.g., principal component analysis and autoencoders), while in our work an alternative method is presented for the separation of large scale fading from small scale fading in the time domain (i.e., through low pass filtering).

3) *Proof of concept through experimental results.* In detail, we will showcase proximity estimation and reconciliation performed on the quantized residual measurements with real RSS measurements in an indoor setting using WiFi technology.
4) *A 0-RTT protocol using PUFs, in which, resumption keys are generated using SKG.* The combination of PUFs, SKG and mobility based-proximity detection ensures security properties such as untraceability, anonymity, protection against cyber impersonation attacks and many more.
5) *The security properties of the proposed protocol are verified through formal methods.* We first verify the proposed protocol using the well-known Burrows, Abadi, Needham (BAN) [32] logic. However, BAN logic typically does not account for active attacks, hence, it can only ensure secrecy based on a set of assumptions. To overcome that, we perform a further security analysis using Tamarin-prover [33]. Tamarin provides unbounded, symbolic analysis for security protocols and has been widely employed to provide security proofs for protocols such as TLS 1.3 [34], 5G AKA [35], and more [36]. To the best of our knowledge, this is the first time formal methods are used to demonstrate the veracity of PLS protocols.

The rest of the paper is organized as follows: related work is discussed in Section II, the mobility-based proximity estimation and reconciliation of the extrapolated small scale fading residuals and proof of concept are discussed in Section III. In Section IV the proposed authentication protocol is presented while its security properties are verified in Section V using formal proofs and the Tamarin-prover. Finally, Section VI concludes this paper.

II. STATE OF THE ART AND BEYOND

Numerous PUF based authentication protocols have been proposed, both for unilateral authentication and mutual authentication [37]. Some of the protocols assume the use of PUFs as the only factor of authentication [23], [38]. However, relying on PUFs as a single security factor can expose the system to a variety of threats, especially in an IoT scenario [39]. Therefore, combining two or more independent credentials can be used to build a secure multi-factor authentication protocol [20]–[22]. For example, [20] proposes a privacy-preserving authentication protocol between an IoT device and a server both connected through a third party wireless gateway. The authors propose to use: PUFs for device authentication; and, RSS measurements, taken between the IoT device and the gateway, to achieve data provenance. However, the process of gateway authentication is not clarified, which makes the scheme open to relay attacks (in the presence of a malicious gateway). In addition the authors propose a challenge-response pair (CRP) update process which must be performed after each communication, hence, introducing extra overhead. Moreover, the encryption of the CRP update process is performed using the same key used during authentication, opening the protocol to vulnerabilities related to key reuse.

Another multi-factor privacy preserving authentication protocol was proposed in [21]. The proposed scheme achieves mutual authentication by combining PUFs with location information. The location estimation process uses raw RSS measurements and its validity is confirmed through a comparison to a pre-stored threshold. However, as shown later in this paper (Fig. 3), raw RSS measurements typically vary by tens of dBms and could lead to incorrect location estimation. Furthermore, the authors in [21] assumed that session keys are generated using pseudo random number generators (PRNGs) modules, that typically generate low-entropy keys, thus making the protocol vulnerable to many possible attacks [40].

A different PUF-based privacy preserving scheme was proposed in [22]. As a second factor of authentication the authors propose the usage of pre-shared secret keys. Unlike the above studies, this scheme takes into account the noise present in PUF structures and uses fuzzy extractors for reconciliation. However, as noted in [21], this scheme is open to physical attacks.

To overcome the issues identified above, we propose a multi-factor authentication protocol based on several PLS techniques. While PUFs are used as a main authentication factor we propose to use a simple proximity estimator as a complementary second factor. Proximity-based methods rely on measuring the RSS. The RSS is mainly determined by the transmit power and the distance, i.e., large scale fading phenomena (typically modelled by an inverse-square law) and can thus be used to estimate the distance between two nodes. As received signals are corrupted by noise and small scale fading, filtering is necessary to improve accuracy. A drawback of these methods is that, they are usually used to simply estimate distance and do not provide direction or positioning information. However, a clear advantage of proximity-based methods is that they do not require any additional hardware and can be easily deployed without extra costs, which makes them well suited for constrained IoT devices [41].

Due to the ease of implementation, proximity estimation has recently received great interest, especially in the healthcare vertical [42]. Several works have demonstrated its applicability as a lightweight authentication mechanism. For example, the authors of [43] propose an unilateral authentication approach where static users rotate their smartphones to create predictable variation in the RSS values. However, the proposed authentication approach can succeed only if close proximity between devices is present, e.g., 20 cm. Another approach is presented in [44] where users authenticate using

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

third party signals (e.g., FM or TV broadcasting). The goal of the study was to demonstrate that users in close proximity would experience similar channel characteristics, hence, this could be used as an advantage over eavesdroppers for authentication. While this is an interesting approach, its success relies on the assumption of very close proximity between users. Further, it is not commented on how users build trust to the third party signals. A different approach was presented in [45], where the authors focus on attendance monitoring, i.e., users are authenticated only if they are inside a premise. However, as those systems rely on a single authentication factor, i.e., RSS measurements, it has been shown that they might be susceptible to a number of attacks [46]. Other works focus on a more precise localization [47]–[53]. To improve the performance most of these works rely on complex operations [50]–[53], (e.g. machine learning techniques), making them unsuitable for constrained IoT devices, while others propose solutions that rely on the use of multiple nodes and measurements of the RSS at multiple locations [49].

In this work, we propose a simple, impersonation attack resistant proximity estimator, as a second factor of authentication. To extract the location-dependent trend from the received signals we use a standard Kalman filter [54]. The complexity of the filter is negligible [55] making it suitable for real-time IoT applications [56]–[58]. The novelty of our solution is that instead of deploying multiple nodes (which would need to be mutually authenticated), we propose to leverage the mobility of a single node, allowing it to capture RSS values from multiple locations. More details, including experimental results, are given in Section III-A. It is important to note that, in this work, proximity estimation is used as a second factor of authentication to complement the primary authentication procedure carried out using PUFs. While, second factors of authentication are typically weaker than primary, they provide an additional security layer and increase the cost and complexity of possible attacks.

Finally, the third PLS solution used in our protocol is SKG from wireless fading coefficients. Fading is a complex physical process process, including both large scale fading (path loss and shadowing) and small scale fading components. With respect to their role in security applications, in [29] and [30] it has been noted that large scale fading is primarily useful for node authentication (e.g., through high precision localization), while small scale fading is a valuable source of entropy for SKG [59]. The separation of the two types of processes can in principle be performed in the time or in the power domain. Note that large scale fading is expected to dominate in power [30], providing a basis for separation using principal component analysis or other unsupervised learning methods.

In fact, it has recently been established that without any pre-processing of the source of shared randomness (i.e., the channel coefficients), the generated keys are susceptible to prediction attacks [60]. In this work, we propose a novel RSS-based SKG approach where entropy-rich, small scale fading components are isolated and subsequently used for key generation. The idea is to subtract the filtered RSS time series (used here for proximity estimation) from the original RSS measurements, hence, suppress the dominant component in the power measurements and use the residual at the input of the SKG. We have evaluated the SKG rates of our proposed solution in an experimental setup using CRC-aided Polar codes that operate in the short block length (Section III-B). We note that, finding an error correcting code that operates in the short block lengths and that is suitable for resource constrained IoT devices is still an open issue [61]. Hence, our experimental work can be considered as a contribution, towards future performance analyses.

To summarise, we propose a multi-factor and privacy-preserving authentication protocol entirely based on PLS techniques. With respect to privacy preservation, similarly to earlier works, we use a one-time alias ID scheme[1]. First, primary authentication is performed using PUFs. Next, to enhance the security levels, apart from PUFs, we propose to additionally use two independent PLS credentials: proximity estimation and SKG. While existing studies are typically focused on a single PLS credential, here, we propose a unique combination that is shown to withstand numerous attacks. Some high level key differences between the proposed multi-factor protocol and existing solutions, based on a single PLS credential, are summarized below:

- PUFs are seen as a lightweight alternative to currently used, complex, authentication solutions. Unfortunately, relying on PUF alone might expose the system to malicious attacks, hence, introducing the challenge of finding further, IoT-friendly, solutions that can complement PUFs and contribute to overall system security. In the current work, we identify two possible candidates and propose a unique combination that is well suited for resource constrained devices and could be implemented without introducing additional costs.
- Proximity estimation is a simple technique that could provide valuable information towards the authentication process. Similarly to PUFs, it is not recommended to use it as a single security factor. Therefore, in this work, estimated distances are used only for soft authentication, that provides initial level of trust before applying the PUF. The novelty of the proposed mechanism is that we leverage the natural movement of users to prevent impersonation attacks, which has not been considered before.
- The literature on SKG solutions is vast. While numerous studies show that key extraction is possible at acceptable rates it is not clear how those keys are i) authenticated; ii) used. Here we show that when SKG is used in combination with PUFs and proximity estimation, the authenticity of the generated keys can be successfully confirmed. Next, we identify a specific application

[1] In such a scheme, the IoT device does not use its real ID during the authentication process, instead it uses a one-time alias ID which is updated in every session.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

where PHY generated keys can be utilized, e.g., 0-RTT resumption protocols. It is important to mention that by combining currently used resumption techniques with PHY generated keys we overcome the threat of replay attacks.

In the following section, we describe the proposed proximity estimation and SKG methods in greater detail and demonstrate their potential through a set of real-life experiments. The relationship between all three PLS credentials used to build our authentication protocol is also discussed.

III. PROXIMITY ESTIMATION AND SKG USING RSS

In this section, we evaluate the performance of the proposed RSS-based proximity estimation and SKG techniques. First, we separate the location fingerprints (in the RSS measurements) from the small scale fading components by using a fast Kalman filter. After separation, the location dependent trend is used towards proximity estimation while the fast varying and unpredictable components are used as an input for SKG. Finally, as a proof of concept, we present experimental results for the proposed methods using WiFi chipsets in an indoor office environment.

A. MOBILITY-ENHANCED PROXIMITY ESTIMATION

Introducing a "smart movement" environment brings a number of advantages to IoT systems, including energy savings, control over the node mobility and increased overall quality-of-experience (QoE) [62]. In this direction, we propose in this section a proximity estimation approach, leveraging mobility. The novelty in our strategy relies upon the fact that if Alice (a mobile IoT node) moves in a manner unpredictable for adversaries, she can take successive measurements of the RSS transmitted by a static entity, Bob, (e.g., a static access point) and use them for proximity estimation, as shown in Fig. 1. In fact, this lightweight proximity estimation approach allows Alice to detect impersonation attacks[2] when used in combination with the authentication protocol presented in the next section. We will present a straightforward algorithm for proximity estimation using Kalman filters.

Due to the ease of implementation and signal availability, RSS-based localization is usually a favoured technique. Focusing on large scale fading, according to the inverse-square law, the RSS at Alice can be used to estimate the distance between her and Bob. Based on the fact that the large scale fading coefficients typically follow a log-normal power distribution, we assume a standard path loss model to map RSS values to distances between two nodes [63], i.e., we assume the following model:

$$\hat{d} = d_0 10^{\frac{P_0 - P}{10n}} e^{-\frac{1}{2}\left(\frac{\sigma_{X_\sigma} \ln(10)}{10n}\right)^2}, \qquad (1)$$

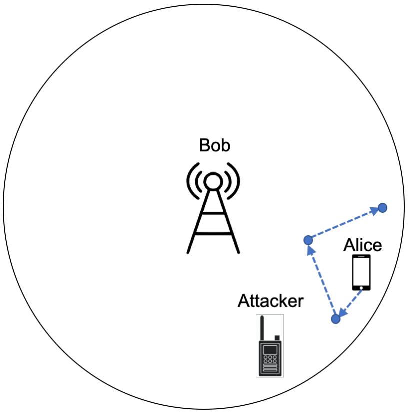

FIGURE 1: Proposed proximity estimation.

where $\hat{d}$ is the estimated distance to the transmitter, P is the strength of the received signal in dB, P_0 represents the average RSS at some reference distance d_0 in dB, n is an attenuation factor that describes the relation between distance and received power in a given environment, and $X_\sigma \sim \mathcal{N}(0, \sigma^2_{X_\sigma})$ is a zero mean Gaussian random variable modelling shadowing [64].

To extrapolate the components that follow (1) from the measured RSS, we propose the use of a Kalman filter. Kalman filters have been widely used in literature to improve the reliability of RSS-based localization [65]. The filter's parameters are usually in the form of matrices resulting in a computational complexity higher than $\mathcal{O}(N^2)$ [66]. However, as the target in the scenario assumed here is static, all of the parameters reduce to scalar values. This allows us to apply a lightweight version of the filter, the *fast Kalman filter*, without penalty in performance [67], [68]. The computational complexity of the fast Kalman filter is only $\mathcal{O}(N)$ [55], [68], making the algorithm suitable for real-time applications on resource constrained devices, e.g., a low-end IoT nodes [56]–[58]. The smoothing process at Alice works under the assumption that the current state $Y_{A,i}$ is related to the previous state $Y_{A,i-1}$ as follows:

$$Y_{A,i} = Y_{A,i-1} + K_{A,i}(X_{A,i} - Y_{A,i-1}), \qquad (2)$$

where $X_{A,i}$ and $Y_{A,i}$, with $i = 1, \dots, N$, are elements within the vectors X_A and Y_A that contain raw and filtered RSS measurements, respectively, and $K_{A,i}$ is a parameter that determines the convergence of the filter, called Kalman gain (the filtering process at Bob is defined identically). Note that, the initial values K_1 and Y_0 must be pre-defined (for the purpose of this work we assume the initial values to be equal for Alice and Bob). For more details on the filtering algorithm the readers are referred to [67], [68].

To validate the proposed proximity estimation technique we have performed a set of experiments in an indoor environment. The experiments were performed using two nodes, each equipped with an ESP32 low-power system on a microcontroller chip with integrated WiFi. The measurement setup

[2] An impersonation attack when proximity estimation is used as an authentication factor can be mounted by altering the transmission power level, e.g., as in some false base station types of attack. By taking successive measurements of the RSS in unpredictable locations, this attack can be overcome.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

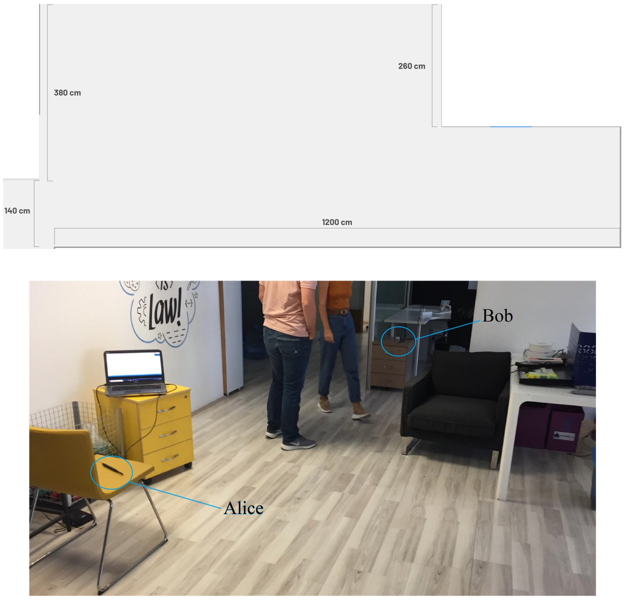

FIGURE 2: Room dimensions and measurement setup.

TABLE 2: Experimental setup and parameters

Scenario	Office space
Transmit power	19.5 dBm
Carrier frequency	2.4 GHz
Measurement period	500 ms
Estimated interference level	≈ -80 dBm
Measured distances	$d \in \{1, 3, 6, 9\}$
Presence of line of sight	80%

is illustrated in Fig. 2 and setup parameters are summarized in Table 2.

First, in Fig. 3, a set of raw RSS measurements X_A and X_B, taken at a distance of 9 m, are depicted along with outputs of the Kalman filters for Alice, Y_A, and Bob, Y_B. The initialization parameters for the filter were chosen as $K_1 = 0.5$ and $Y_0 = -32$. It is observed that both the RSS measurements and the filter outputs at the two nodes are highly reciprocal. Note that, the filter output quickly stabilizes smoothing out the fast variations in the raw data (e.g., due to small scale fading). In fact, it converges in less than 20 samples and afterwards its output varies only by a few dBms. Based on this observation, we allow for a small margin in terms of convergence time, and assume that the 30-th output of the Kalman filter, $Y_{A,30}$ in (2), is the "decision" output which is used by Alice to determine her distance to Bob.

Next, the path loss model for the considered scenario was determined. A set of 50 independent measurement sessions were performed at each of the distances $d \in \{1, 3, 6, 9\}$. From each set the "decision" output of the Kalman filter, $Y_{A,30}$, as well as the corresponding RSS measurement, $X_{A,30}$, were extracted. The values were used to estimate the unknown variables in (1). This is illustrated in Fig. 4 where the standard deviation of the raw measurements and the filter

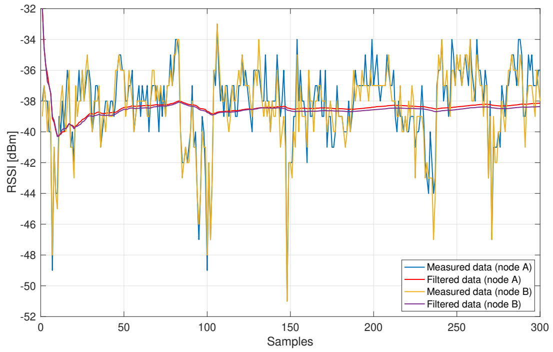

FIGURE 3: Measured RSS data and filtered data using Kalman filter at distance of 9 meters. The filter is initialized using $K_1 = 0.5$ and $Y_0 = -32$ dBm.

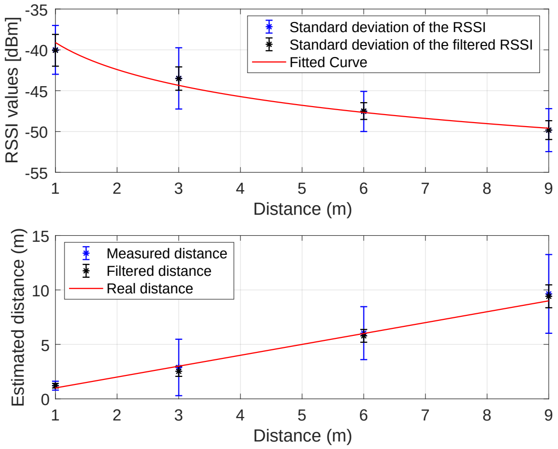

FIGURE 4: Curve fitting of the path loss model (TOP) and distance estimation (BOTTOM).

outputs are plotted against a fitted curve based on (1). The estimated parameters used for curve fitting are $P_0 = -47.56$ dBm, $d_0 = 6$ m, $n = 1.1$ and $\sigma_{X_\sigma} = 3.24$. It is clear that the impact of small scale fading, due to movement as well as noise effects, is efficiently removed, leaving a stable source for our proximity estimation.

Based on the performed experiments, distances are classified in four categories: immediate ($d \leq 1$m), near (d between 1 and 3m), medium (d between 3 and 6m) and far ($d \geq 9$m). To validate the approach a new, independent set of measurements was taken at each distance. Table 3 presents the classification probabilities, when the estimated distance is evaluated as follows:

$$\hat{d} = \underset{d_i \in \{1,3,6,9\}}{\arg\min} |Y_{A,30} - Y_M(d_i)|, \tag{3}$$

where Y_M are the values corresponding to the fitted curve in Fig. 4. It is observed that correct classification is achieved with a probability higher than 0.82 in all cases, while mis-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

TABLE 3: Classification probability of proximity estimation

	Immediate	Near	Medium	Far
$d = 1$	0.82	0.18	0	0
$d = 3$	0.06	0.88	0.06	0
$d = 6$	0	0.10	0.84	0.06
$d = 9$	0	0	0.16	0.84

classification occurs primarily between neighbouring ranges of distances.

This straightforward proximity estimation technique is used by Alice as an independent factor in the multi-factor authentication protocol presented in Section IV. As noted earlier, upon removal of the proximity fingerprints, the residual measurements are used as an entropy source for SKG, i.e., the input for the SKG is evaluated as: $X_A - Y_A$ for Alice and $X_B - Y_B$ for Bob. The performance of this SKG approach is evaluated in the next section.

B. SKG BASED ON RSS

The steps in the SKG scheme can be summarized as follows: i) Alice and Bob pass their SKG inputs through a quantizer, obtaining binary sequences $Y_{K,A}$ and $Y_{K,B}$, respectively; as is standard in literature, in this work we use an equal probability quantizer. To reconcile mismatches at the generated binary sequences, one of the legitimate parties, e.g. Alice, sends syndrome information S_A to Bob. Finally, to create maximal entropy secret keys, both users employ privacy amplification over the reconciled information [69].

To evaluate the SKG scheme, we gathered 38,000 RSS measurements at a user distance of 3 m. We experimented with equal probability quantizers using $1, 2$ and 3 bits, respectively, and employed gray coding to minimize the bit mismatch probability. For information reconciliation we implemented CRC-aided polar codes with list size 128 and blocklength of 1024 bits [31]. The CRC bits aid the decoders in selecting the correct decoding route from a list of options. The decoder can drop a frame if none of the options in the list verifies the CRC conditions. The reconciliation rate is measured as the ratio of output (reconciled) bits over the number of input (quantized) bits. The experimental results are depicted in Table 4. As expected, it is observed that the mismatch probability increases with the number of quantization bits. This is due to the fact that each increase in the number of the quantization bits leads to a decrease in the range represented by a single quantization region. Next, we have chosen the reconciliation rates shown in Table 4 as the highest rates for which the users can correct all mismatched bits, while dropping the frames that they are unable to correct. The information reconciliation rate naturally decreases with increasing the mismatch probability. Finally, the overall number of generated key bits (from the 38,000 RSS measurements) are also depicted in Table 4, after performing privacy amplification (conforming to the reconciliation rate). We observe that the 1-bit quantizer generates the highest number of key bits thanks to its low bit mismatch probability and drop frame probability. Note that the 3-bit quantizer outperforms the 2-bit quantizer in terms of number of generated key bits due to the fact that longer bit sequences are fed to the reconciliation decoder. As an overall conclusion, depending on the RSS quality, the quantizer and reconciliation decoder should be jointly chosen to optimize the overall key generation rate.

TABLE 4: SKG using different quantizers (distance 3m) over 38,000 RSS measurements. Each measurement was quantized to $m \in \{1, 2, 3\}$ bits, resulting in different reconciliation rates [b/s/Hz] to achieve error free reconciliation.

Quantization order	1-bit	2-bit	3-bit
Mismatch probability	0.138	0.199	0.266
Reconciliation rate	0.25	0.09	0.06
Number of frames dropped	1	8	3
Number of generated key bits	9472	6256	6771

To conclude this section, Fig. 5 visualizes the overall structure of the proposed protocol. It is clear that the authentication relies on both the interplay between the employed PLS credentials as well as their independent performance. The full process, including the message flow, is explained in the next section.

IV. PROPOSED MULTI-FACTOR AUTHENTICATION PROTOCOL

This section presents a lightweight multi-factor authentication scheme, leveraging PUFs, proximity estimation and SKG. It provides a mutual authentication between Alice (a mobile node) and Bob (static access point) and consists of: an enrollment phase, an authentication phase and uses SKG as a quick resumption mechanism. We note that during the channel estimation (through pilot exchange in both directions) the parties can take measurements of the RSS and / or of the full channel state information (CSI) if needed. Using the RSS measurements, Alice performs the mobility-based proximity introduced in Section III-A. She positions herself in diverse (unpredictable) locations and takes multiple measurements in order to estimate Bob's location. Next, both Alice and Bob perform SKG as discussed previously, in Section III-B. Before providing the overall security analysis, we first present all individual primitives. The notation used throughout this section is defined as follows:

- A SKG scheme generates as outputs binary vectors K and S_A of sizes $k = |K|$ and $|S_A|$, respectively, with $K \in \mathcal{K}$ denoting the key obtained after privacy amplification and $S_A \in \mathcal{S}$ denoting Alice's syndrome. An important advantage of the SKG scheme, as compared to currently used solutions (e.g., EAP-TLS), is that its performance improves with the mobility of the user [70], [71].
- Alice's PUF denoted by P_A that generates a response $R \in \mathcal{R}$ to a challenge $Ch \in \mathcal{C}h$, i.e., $R = P_A(Ch)$. Although different PUF constructions exist, both in literature and in practice [37], [72], in this study we do not

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

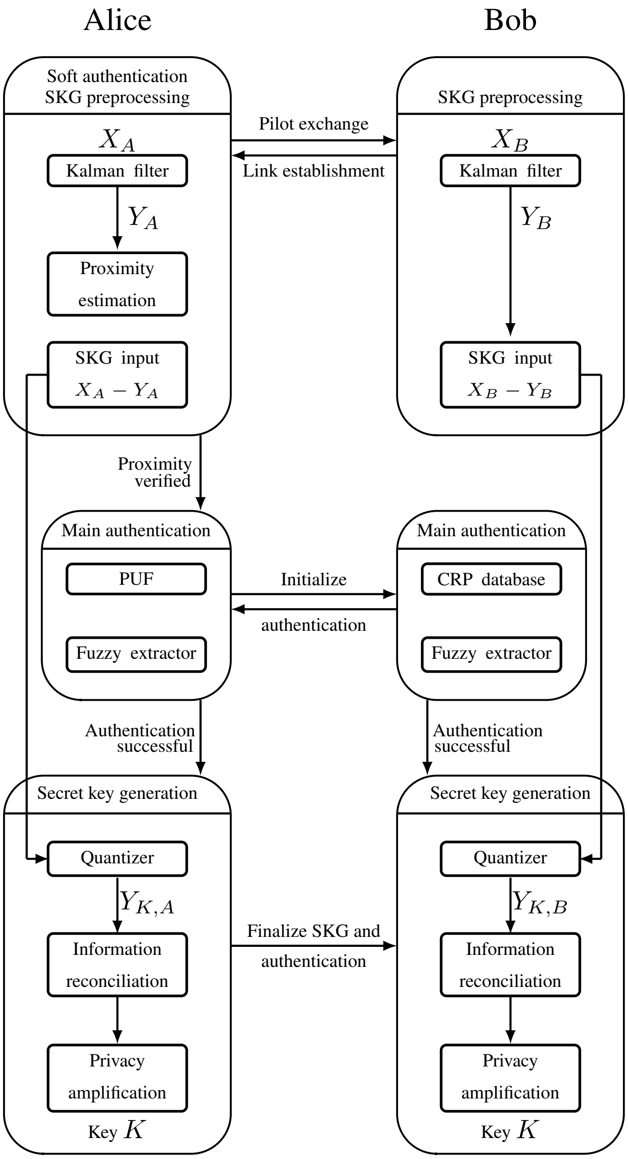

FIGURE 5: Outline of the proposed authentication protocol. Unlike typical authentication protocols the key generation process and authentication procedure are both finalized in a single message.

limit ourselves by choosing a specific construction. In fact, depending on the application different PUFs are expected to have different performance. It was shown that some constructions could be susceptible to voltage variations while others to temperature variations, causing a bias in their response (i.e., probability of 1 or 0 higher than 0.5) or introducing a high number of errors upon response reproduction [72]–[74]. Therefore, to achieve optimal performance the choice of the PUF construction must be application specific. In terms of delay requirements, several PUF constructions have been tested over IoT systems showing response generation time in the range of $1 - 6$ ms [75]–[78].

- A pair of fuzzy extractor algorithms, denoted by $\texttt{Gen} : \mathcal{R} \to \mathcal{K}_R \times \mathcal{H}_R$, accepting as input the PUF response and generating as outputs the identification (fuzzy) key and helper data, with corresponding reproduce algorithm $\texttt{Rep} : \mathcal{R} \times \mathcal{H}_R \to \mathcal{K}_R$, such that:

$$\texttt{Gen}(R) = (H_R, K_R), \tag{4}$$
$$\texttt{Rep}(R', H_R) = K_R, \tag{5}$$

where $R, R' \in \mathcal{R}, K_R \in \mathcal{K}_\mathcal{R}$ and $H_R \in \mathcal{H}_R$. Similarly, to the SKG process, a fuzzy extractor requires the implementation of an error correcting code and a hash function. The helper data H_R is obtained using error correction code, e.g., if a linear (n, k, t) BCH code[3] is used, H_R represents a syndrome with size $n - k$. In our protocol, H_R is considered to be public, hence, an entropy of $n - k$ about R is leaked [73], [74], [79]. Therefore, to obtain the key K_R, a one-way compression mechanism is applied, e.g., a cryptographic or universal hash function. This reduces the size of the sequence to $k < n$ bits, but increases the entropy per bit. Next, within the $\texttt{Rep}$ algorithm, a decoder is used to reproduce the original response, R, which is then hashed to the key K_R. A hash function has a typical complexity of $\mathcal{O}(nk)$ [80], [81] which, when performed on an IoT device, requires less than 0.3 ms [75], [82], [83]. Regarding the error correction, the computation required for a standard BCH encoding mechanisms is trivial compared to the hashing and requires less computational overhead [24], [84]. However, the decoding has greater computational overhead than the encoding [73], hence, in the proposed scheme we perform the more complex operation, i.e., $\texttt{Rep}$ on the resourceful device rather than on a constrained IoT node.
- A symmetric encryption algorithm, e.g., AES-256 in Galois field counter mode (GCM)[4], denoted by $\texttt{Es} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}_\mathcal{T}$ where $\mathcal{C}_\mathcal{T}$ denotes the ciphertext space with corresponding decryption $\texttt{Ds} : \mathcal{K} \times \mathcal{C}_\mathcal{T} \to \mathcal{M}$, i.e.,

$$\texttt{Es}(K, M) = C,$$
$$\texttt{Ds}(K, C) = M,$$

for $M \in \mathcal{M}$, $C \in \mathcal{C}_\mathcal{T}$. The average run-time of AES for constrained IoT systems is approximately 1 ms [82]. For further detail the readers are referred to [85] where benchmarking results are presented for 12 lightweight block ciphers.
- A pair of message authentication code (MAC) algorithms, denoted by $\texttt{Sign} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$, with a

[3] In a (n, k, t) BCH code, n denotes the size of the codeword, k the number of information bits and t the error correcting capability of the code.

[4] We note that using a block cipher such as AES-256 in a GCM operation allows to the use of the same key K to encrypt typically Gigabytes of data.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

corresponding verification algorithm $\mathtt{Ver} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \rightarrow \{yes, no\}$:

$$\mathtt{Sign}(K, M) = T,$$

$$\mathtt{Ver}(K, M, T) = \begin{cases} yes, & \text{if integrity verified} \\ no, & \text{if integrity not verified} \end{cases}$$

Similarly to the above mechanisms, the security community has been working on realizing lightweight MAC algorithms suitable for constrained IoT devices; for examples see [83], [86]–[88].

- A cryptographic (irreversible) one-way hash function

$$\mathtt{Hash} : \{0, 1\}^q \rightarrow \{0, 1\}^k,$$

that is used to compress the size of an input binary vector of length q to a binary vector of length $k = |K|$. As mentioned above, hash functions are well suited for IoT devices. For a complete study and performance evaluation with respect to lightweight implementations please see [89].

In all of the previously defined functions, the insertion of an index $i - 1$ denotes the value of a variable or quantity one instance earlier than its corresponding value at instance i, e.g., Ch_1 denotes the PUF challenge at instance 1 while Ch_2 denotes the PUF challenge at instance 2. Furthermore, following from the definition of PUFs, every challenge produces a unique response, corresponding helper data and authentication keys, i.e., $P_A(Ch_1) \neq P_A(Ch_2)$ and $\mathtt{Gen}(P_A(Ch_1)) \neq \mathtt{Gen}(P_A(Ch_2))$. Finally, concatenation of two binary vectors X and Y is denoted by $(X||Y)$.

A. DEVICE ENROLLMENT

The enrollment is a one-time operation carried out off-line over a secure channel between Alice (referred to in the following as node A) and Bob (referred to in the following as node B). The steps taken during enrollment are summarized in Fig. 6 and are performed as follows:

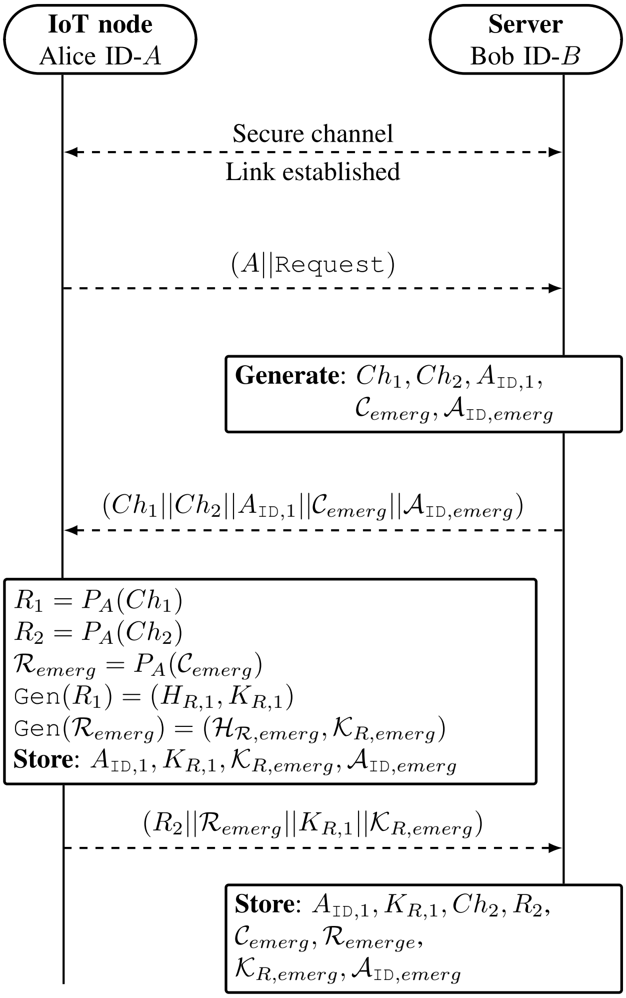
IoT node
Alice ID-A
Server
Bob ID-B
Secure channel
Link established
$(A||\mathtt{Request})$
Generate: $Ch_1, Ch_2, A_{\mathtt{ID},1}, \mathcal{C}_{emerg}, \mathcal{A}_{\mathtt{ID},emerg}$
$(Ch_1||Ch_2||A_{\mathtt{ID},1}||\mathcal{C}_{emerg}||\mathcal{A}_{\mathtt{ID},emerg})$
$R_1 = P_A(Ch_1)$
$R_2 = P_A(Ch_2)$
$\mathcal{R}_{emerg} = P_A(\mathcal{C}_{emerg})$
$\mathtt{Gen}(R_1) = (H_{R,1}, K_{R,1})$
$\mathtt{Gen}(\mathcal{R}_{emerg}) = (\mathcal{H}_{\mathcal{R},emerg}, \mathcal{K}_{R,emerg})$
Store: $A_{\mathtt{ID},1}, K_{R,1}, \mathcal{K}_{R,emerg}, \mathcal{A}_{\mathtt{ID},emerg}$
$(R_2||\mathcal{R}_{emerg}||K_{R,1}||\mathcal{K}_{R,emerg})$
Store: $A_{\mathtt{ID},1}, K_{R,1}, Ch_2, R_2, \mathcal{C}_{emerg}, \mathcal{R}_{emerge}, \mathcal{K}_{R,emerg}, \mathcal{A}_{\mathtt{ID},emerg}$

FIGURE 6: Enrollment phase

1) In order to establish the link between them, both devices need to exchange pilot signals. During this exchange A measures the RSS. Furthermore A downloads (or creates) a map of the premises which contains the location of B to enable proximity based authentication.
2) After establishing the connection, Alice sends her ID, A, with a request for registration $\mathtt{Request}$.
3) Upon receiving the request, B first checks if the received ID has already been registered. If B finds the ID within his database the request is rejected. If A has not been registered B generates two initial PUF challenges Ch_1, Ch_2 and an initial one-time alias ID $A_{\mathtt{ID},1}$. These challenges will be used during subsequent authentication and will be updated with each run of the protocol. Next, B generates *sets* of emergency challenges and one-time alias IDs $\mathcal{C}_{emerg}$ and $\mathcal{A}_{\mathtt{ID},emerg}$, respectively, such that $|\mathcal{C}_{emerg}| = |\mathcal{A}_{\mathtt{ID},emerg}|$. The emergency sets are used only in a case of de-synchronization between the devices and have multiple entries to allow for multiple recoveries. Finally, Bob sends the message $(Ch_1||Ch_2||A_{\mathtt{ID},1}||\mathcal{C}_{emerg}||\mathcal{A}_{\mathtt{ID},emerg})$ to Alice. Note that the two emergency sets are linked such that each element has a corresponding one in the other set.
4) After receiving the message, Alice excites her PUF P_A with Ch_1, Ch_2 and all challenges from the set $\mathcal{C}_{emerg}$, producing responses R_1, R_2 and $\mathcal{R}_{emerg}$, respectively. Next, she uses R_1 and $\mathcal{R}_{emerg}$ as inputs to her fuzzy extractor to generate the pair $(H_{R,1}, K_{R,1})$ and the sets of pairs $(\mathcal{H}_{R,emerg}, \mathcal{K}_{R,emerg})$. Afterwards, Alice stores $A_{\mathtt{ID},1}, K_{R,1}, \mathcal{K}_{R,emerg}, \mathcal{A}_{\mathtt{ID},emerg}$ and sends the following message to Bob $(R_2||\mathcal{R}_{emerg}||K_{R,1}||\mathcal{K}_{R,emerg})$.
5) To finalize the registration process, B stores the following elements that correspond to ID A in his database: initial authentication parameters $A_{\mathtt{ID},1}, K_{R,1}, Ch_2, R_2$ and emergency authentication parameters in case of de-synchronization $\mathcal{C}_{emerg}, \mathcal{R}_{emerge}, \mathcal{K}_{R,emerg}, \mathcal{A}_{\mathtt{ID},emerg}$.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

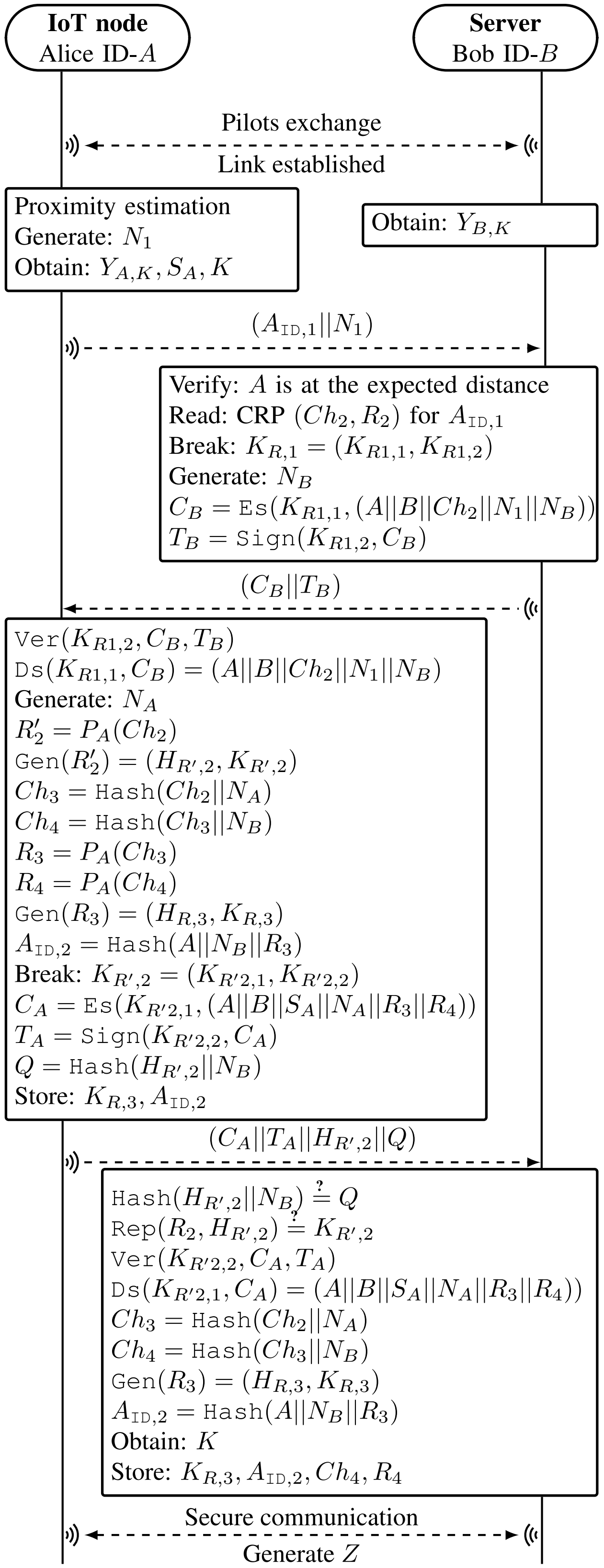
IoT node
Alice ID-A
Server
Bob ID-B
Pilots exchange
Link established
Proximity estimation
Generate: N_1
Obtain: $Y_{A,K}, S_A, K$
Obtain: $Y_{B,K}$
$(A_{\mathtt{ID},1}||N_1)$
Verify: A is at the expected distance
Read: CRP (Ch_2, R_2) for $A_{\mathtt{ID},1}$
Break: $K_{R,1} = (K_{R1,1}, K_{R1,2})$
Generate: N_B
$C_B = \mathtt{Es}(K_{R1,1}, (A||B||Ch_2||N_1||N_B))$
$T_B = \mathtt{Sign}(K_{R1,2}, C_B)$
$(C_B||T_B)$
$\mathtt{Ver}(K_{R1,2}, C_B, T_B)$
$\mathtt{Ds}(K_{R1,1}, C_B) = (A||B||Ch_2||N_1||N_B)$
Generate: N_A
$R_2' = P_A(Ch_2)$
$\mathtt{Gen}(R_2') = (H_{R',2}, K_{R',2})$
$Ch_3 = \mathtt{Hash}(Ch_2||N_A)$
$Ch_4 = \mathtt{Hash}(Ch_3||N_B)$
$R_3 = P_A(Ch_3)$
$R_4 = P_A(Ch_4)$
$\mathtt{Gen}(R_3) = (H_{R,3}, K_{R,3})$
$A_{\mathtt{ID},2} = \mathtt{Hash}(A||N_B||R_3)$
Break: $K_{R',2} = (K_{R'2,1}, K_{R'2,2})$
$C_A = \mathtt{Es}(K_{R'2,1}, (A||B||S_A||N_A||R_3||R_4))$
$T_A = \mathtt{Sign}(K_{R'2,2}, C_A)$
$Q = \mathtt{Hash}(H_{R',2}||N_B)$
Store: $K_{R,3}, A_{\mathtt{ID},2}$
$(C_A||T_A||H_{R',2}||Q)$
$\mathtt{Hash}(H_{R',2}||N_B) \overset{?}{=} Q$
$\mathtt{Rep}(R_2, H_{R',2}) \overset{?}{=} K_{R',2}$
$\mathtt{Ver}(K_{R'2,2}, C_A, T_A)$
$\mathtt{Ds}(K_{R'2,1}, C_A) = (A||B||S_A||N_A||R_3||R_4))$
$Ch_3 = \mathtt{Hash}(Ch_2||N_A)$
$Ch_4 = \mathtt{Hash}(Ch_3||N_B)$
$\mathtt{Gen}(R_3) = (H_{R,3}, K_{R,3})$
$A_{\mathtt{ID},2} = \mathtt{Hash}(A||N_B||R_3)$
Obtain: K
Store: $K_{R,3}, A_{\mathtt{ID},2}, Ch_4, R_4$
Secure communication
Generate Z

FIGURE 7: Authentication protocol

B. AUTHENTICATION

Once the enrollment is finished, both devices can use the established parameters for future authentication over an insecure channel. The steps taken during authentication are summarized in Fig. 7 and are performed as follows:

1) First, the devices exchange pilot signals and measure the RSS. Next, to confirm the location of B, A filters the RSS observations and performs the proximity verification, discussed in Section III-A. If the verification fails, she stops the authentication process. If it succeeds, she subtracts the Kalman filter's output from the raw RSS measurements and completes the steps of the SKG process, described in Sec. III-B, calculating her syndrome S_A and key K. The key will be used later as a session key if the authentication is successful. Then, A sends her request for authentication which contains a one-time alias ID $A_{\mathtt{ID},i}$ and a fresh random nonce N_1.
2) Upon reception, B accesses the database and loads the parameters that corresponds to the ID, i.e., CRP (Ch_2, R_2) and key $K_{R,1}$. Then he generates a fresh random nonce N_B and breaks $K_{R,1}$ into two parts as follows: $K_{R,1} = (K_{R1,1}, K_{R1,2})$. He uses the first part to encrypt $C_B = \mathtt{Es}(K_{R1,1}, (A||B||Ch_2||N_1||N_B))$, and uses the second part to sign C_B as: $T_B = \mathtt{Sign}(K_{R1,2}, C_B)$. Finally, he sends the ciphertext C_B and the signature T_B to A.
3) By using her stored key $K_{R,1}$, A verifies the authenticity of B and the integrity of C_B. If one of the verification checks fails, A rejects the message's claim to authenticity. If the verification succeeds, she accepts and excites her PUF with the received challenge Ch_2. By running it on her PUF she obtains a new measurement $R_2' = P_A(Ch_2)$ and $\mathtt{Gen}(R_2') = (H_{R',2}, K_{R',2})$. Afterwards, she generates a new fresh random nonce N_A and calculates the next two challenges as follows: $Ch_3 = \mathtt{Hash}(Ch_2||N_A)$ and $Ch_4 = \mathtt{Hash}(Ch_3||N_B)$. Next, she excites her PUF to produce R_3 and R_4. In order to generate the key that will be used in a future execution of the authentication protocol, A executes $\mathtt{Gen}(R_3) = (H_{R,3}, K_{R,3})$. Next, she calculates the one-time alias ID for future execution of the protocol as $A_{\mathtt{ID},2} = \mathtt{Hash}(A||N_B||R_3)$ which due to the randomness of N_B and R_3, cannot be linked to $A_{\mathtt{ID},1}$. Updating the parameter allows Alice to use a fresh ID during subsequent authentications and, therefore, preserves her privacy from eavesdroppers. The pairs (Ch_4, R_4) and $(K_{R3}, A_{\mathtt{ID},2})$ will be used in a subsequent connection with B. Next, A breaks her key $K_{R',2}$ into two parts $K_{R',2} = (K_{R'2,1}, K_{R'2,2})$. Similarly, to the previous step she uses half of the key to encrypt the message $C_A = \mathtt{Es}(K_{R'2,1}, (A||B||S_A||N_A||R_3||R_4))$. Then, A uses the second half of the key to sign the ciphertext $T_A = \mathtt{Sign}(K_{R'2,2}, C_A)$. A sends C_A, T_A, $H_{R',2}$ and $Q = \mathtt{Hash}(H_{R',2}||N_B)$ to B. Sending a hash value, Q, allows Bob to detect helper data manipulation attacks

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

as the one introduced in [74]. Finally, A stores the pair $K_{R,3}, A_{\mathtt{ID},2}$.

4) Upon receiving the preceding message, B verifies the conditions $\mathtt{Hash}(H_{R',2}||N_B) \overset{?}{=} Q$ and $\mathtt{Rep}(R_2, H_{R',2}) \overset{?}{=} K_{R',2}$ by using the stored R_2 (from the enrollment phase) and the received helper data $H_{R',2}$. If a verification fails, B rejects the claim to authenticity. If the claim is accepted, he verifies the integrity of C_A using the signed ciphertext T_A. Next, using R_3 and the principles of the fuzzy extractor, B performs $\mathtt{Gen}(R_3) = (H_{R,3}, K_{R,3})$. He calculates $A_{\mathtt{ID},2} = \mathtt{Hash}(A||N_B||R_3)$. Following that, he stores the pairs $(K_{R,3}, A_{\mathtt{ID},2}), (Ch_4, R_4)$ which will be used during the next round of the protocol. Finally, using the received syndrome S_A, B corrects the discrepancies in his observation $Y_{B,K}$ to obtain $Y_{A,K}$ and calculates the session key $K = \mathtt{Hash}(Y_{A,K})$.
5) After the authentication process finishes, A and B enter the secure communication stage using the session key K. During this stage, they generate a resumption secret Z. Instead of performing full authentication in subsequent sessions, the secret can be used as a parameter to quickly “resume" sessions in a 0-RTT, as is described next.

C. RESUMPTION PROTOCOL

This section presents a novel physical layer resumption protocol that allows A to send encrypted data in a 0-RTT. During the secure communication stage of the authentication protocol in Fig. 7, B sends to A a look-up identifier. Then, both derive a resumption secret Z that is a function of the look-up identifier and the session parameters. The use of a resumption secret for authentication helps to avoid man-in-the-middle attacks in the scenario assumed here. Given the above, the resumption protocol follows the steps:

1) As before, to establish the link, both devices perform pilot exchange. A and B obtain channel observations and generate sequences $Y_{A,K}$ and $Y_{B,K}$, respectively. Note that, Z and $Y_{A,K}, Y_{B,K}$ have the same length.
2) Next A, generates a fresh random nonce N_1 and reads the resumption secret Z to generate $Y^* = Z \oplus Y_{A,K}$. Then, using her Slepian Wolf decoder she calculates the new syndrome S^*, that corresponds to Y^*, and generates the session key as $K^* = \mathtt{Hash}(Y^*)$. She also calculates the one-time alias ID that will be used for a subsequent session as: $A_{\mathtt{ID},i+1} = \mathtt{Hash}(A||Y_{A,K})$. A breaks her key into two parts $K^* = (K_1^*, K_2^*)$ and uses the first part to encrypt the early 0-RTT data M as $\mathtt{Es}(K_1^*, M) = C$. The second part she uses to sign the cipher text $\mathtt{Sign}(K_2^*, C) = T$. Finally, she sends $(S^*||A_{\mathtt{ID},i}||N_1||C||T)$. Note that the key K^* can only be obtained if both the physical layer generated key and the resumption key are valid; this method can be shown to be forward secure [90].
3) Upon receiving the output from the last step, B reads the resumption secret Z and obtains $Y^{*'} = Z \oplus Y_{B,K}$. Using that and the received syndrome S^*, B first corrects the discrepancies in $Y^{*'}$ to obtain Y^* and then performs $K^{*'} = \mathtt{Hash}(Y^*)$. He uses the condition $K^{*'} \overset{?}{=} K^*$ to verify the authenticity of A and the integrity of the message. If the above succeeds he calculates $Y_{A,K} = Y^* \oplus Z$ and stores $A_{\mathtt{ID},i+1} = \mathtt{Hash}(A||Y_{A,K})$. Using the obtained key, B can now decrypt the message M.
4) After the resumption process finishes, the two devices enter the secure communication stage using K^* as a session key. During this stage, they use the channel and session properties to generate new shared resumption secrets that can be used in subsequent resumptions.

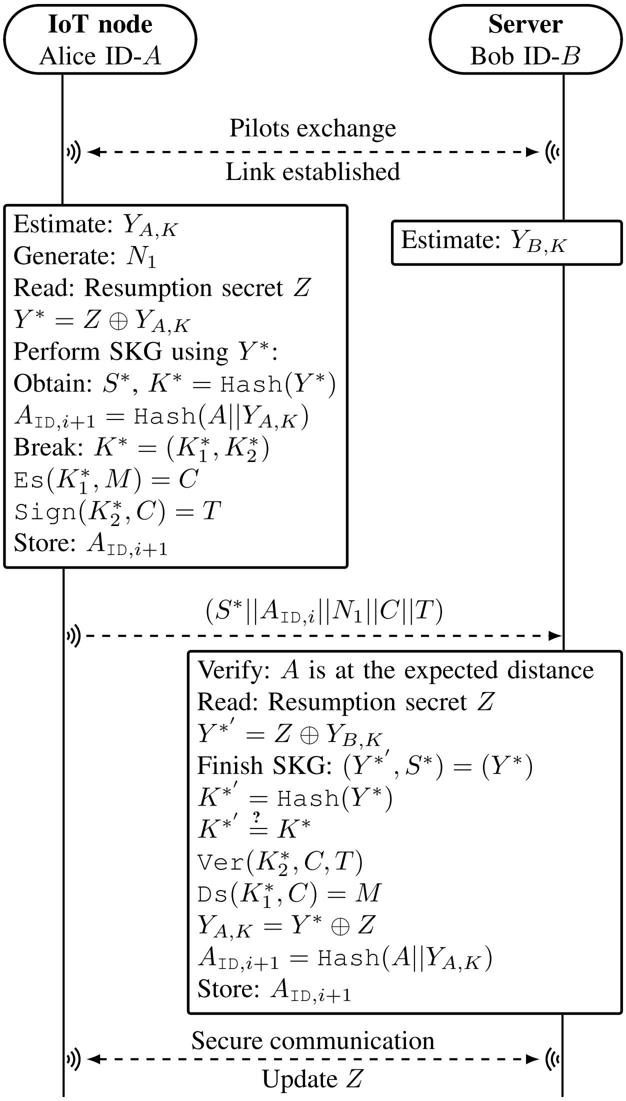
IoT node
Alice ID-A
Server
Bob ID-B
Pilots exchange
Link established
Estimate: $Y_{A,K}$
Generate: N_1
Read: Resumption secret Z
$Y^* = Z \oplus Y_{A,K}$
Perform SKG using Y^*:
Obtain: S^*, $K^* = \mathtt{Hash}(Y^*)$
$A_{\mathtt{ID},i+1} = \mathtt{Hash}(A||Y_{A,K})$
Break: $K^* = (K_1^*, K_2^*)$
$\mathtt{Es}(K_1^*, M) = C$
$\mathtt{Sign}(K_2^*, C) = T$
Store: $A_{\mathtt{ID},i+1}$
Estimate: $Y_{B,K}$
$(S^*||A_{\mathtt{ID},i}||N_1||C||T)$
Verify: A is at the expected distance
Read: Resumption secret Z
$Y^{*'} = Z \oplus Y_{B,K}$
Finish SKG: $(Y^{*'}, S^*) = (Y^*)$
$K^{*'} = \mathtt{Hash}(Y^*)$
$K^{*'} \overset{?}{=} K^*$
$\mathtt{Ver}(K_2^*, C, T)$
$\mathtt{Ds}(K_1^*, C) = M$
$Y_{A,K} = Y^* \oplus Z$
$A_{\mathtt{ID},i+1} = \mathtt{Hash}(A||Y_{A,K})$
Store: $A_{\mathtt{ID},i+1}$
Secure communication
Update Z

FIGURE 8: Resumption protocol

V. SECURITY ANALYSIS

In this section, we analyze the security of the proposed multi-factor authentication protocol illustrated in Fig. 7. For the purpose of our security proofs we consider a Dolev-Yao

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

[91] type of adversary, who has control over the wireless channel between A and B. Furthermore: 1) the adversary can send any type of messages and queries using its knowledge gained through observation; 2) all functions and operations performed by the legitimate users during the execution of the protocol are public except $P_A(\cdot)$ and the entire enrollment phase; and, 3) the adversary can launch denial of service (DoS) attacks and block parts of the protocol in order to de-synchronize the connection between A and B. In terms of the SKG, for simplicity, in this work we assume a rich Rayleigh multipath environment where the adversary is more than a few wavelengths away from each of the legitimate parties and the SKG rates are given as in Section III-B.

A. MUTUAL AUTHENTICATION

The proposed protocol uses a set of factors to achieve mutual authentication. It uses a mobility-based proximity estimation as a first factor of authentication. This verifies whether the server is at the expected distance. Next, A authenticates B by verifying whether the correct key is used for creating C_B and T_B. On the other hand, B authenticates A by first confirming the validity of the received one-time alias ID $A_{\mathtt{ID},i}$ and second by verifying whether she produced a valid response to Ch_i. The second condition is confirmed only if A uses the correct key to generate the pair C_A, T_A.

B. UNTRACEABILITY AND ANONYMITY

During the execution of the authentication protocol, A must posses a valid one-time alias ID $A_{\mathtt{ID}}$ for each session. The one-time alias identity cannot be used twice and there is no direct relationship between subsequent IDs. Thus, no one except B would know the origin of the message. Furthermore, in case of de-synchronization the device can use the set of emergency IDs $\mathcal{A}_{\mathtt{ID},emerg}$. After using an emergency ID it has to be deleted from A's and B's memory. This approach provides privacy against eavesdroppers and ensures the user's anonymity and identity untraceability properties.

C. PERFECT FORWARD SECRECY

Assuming an attacker compromises A and obtains all stored secrets, i.e., $(K_R, A_{\mathtt{ID}})$, they cannot obtain previous keys or one-time alias IDs. First, each K_R is generated using a CRP and CRPs are randomly generated and independent. Hence, by obtaining $K_{R,i}$ an adversary cannot learn $K_{R,i-1}$. Next, one-time alias IDs are generated using a one-way hash function of unique parameters for each session; if an adversary obtains $A_{\mathtt{ID},i}$, they can not inverse the hash function. Furthermore, using the randomness of the wireless channel ensures that session keys are unique and independent for each session. Therefore, the proposed authentication protocol ensures the perfect forward secrecy property.

D. PROTECTION AGAINST REPLAY ATTACK

If an adversary intercepts previous communication between A and B, they can replay the same messages and try to pass the authentication process. In the protocol presented in Fig. 7 none of the parameters in the initial request are allowed to be sent twice, hence, if an attacker resends the same message to B the attack will be detected and the request will be rejected. Next, if the adversary tries to re-send C_B to A, they will be detected, since the key used to encrypt C_B is changed during every session. Similarly, if the adversary tries to re-send C_A, they will be detected and the request will be rejected because the key used to encrypt C_A is changed every session. The above shows that the proposed protocol provides resistance against replay attacks.

E. PROTECTION AGAINST IMPERSONATION ATTACK

A successful impersonation attack will allow the adversary to be authenticated as a legitimate user. Following from above, an adversary cannot perform a replay attack, which limits their options to perform an impersonation attack. Following from that, in order to impersonate A they must generate 1) a valid one-time alias ID, and, 2) a valid ciphertext C_A. However, due to the unclonability properties of the PUF and the fact that the connection between a device and its PUF is secure, (i.e., system on chip) the adversary cannot generate a valid ciphertext C_A, hence cannot impersonate A. Next, in order to impersonate B, the adversary must posses a valid key $K_{R,1}$ and generate a valid ciphertext C_B. However, even if an adversary obtains $K_{R,1}$, (an example of such a scheme vulnerable to this attack can be found in [22]) the attack could still be detected using the proposed proximity detection approach if the adversary is not in close proximity to the legitimate device. Overall, a false base station attack would succeed if and only if the attacker possesses a valid authentication key and is located in proximity to B (more precisely, in the same proximity interval as B).

F. PROTECTION AGAINST HELPER DATA MANIPULATION ATTACKS

Recently, several helper data manipulation attacks have been introduced [74], [92]. The authors of [74] proposed an attack in which a malicious user sends a series of modified helper data queries to the device that implements the reproduce algorithm, `Rep`. The malicious device observes whether the attack results in a decoding failure, hence, learns sensitive information regarding the PUF response. As a simple countermeasure to this attack, we add a hash value Q that allows B to check the integrity of the helper data before performing the decoding step. A different type of helper data manipulation attack was proposed in [92]. The goal of this attack is to send a valid pair H_R'' and Q'' to B that trigger the generation of the authentication key, $K_R'' \neq K_R$. The success of the attack depends on both: the error correcting capabilities at B, and the number of errors when B uses H_R'' as helper data. Interestingly, it was demonstrated that not all error correcting codes are susceptible to this attack; in fact, [92], showed that linear BCH codes with syndrome decoding (also discussed in Section IV) are immune to this attack. While we do not bound our protocol to a specific error correcting implementation,

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

we note that it is of great importance to examine the chosen constructions prior to deployment.

G. RESISTANCE TO DOS ATTACK

To ensure security against DoS and de-syncronization attacks, the authentication protocol uses unlinkable one-time alias IDs and pairs of sets with emergency parameters $(\mathcal{C}_{emerg}, \mathcal{R}_{emerge})$ and $(\mathcal{K}_{R,emerg}, \mathcal{A}_{\mathtt{ID},emerg})$. If an adversary manages to block a message from a legitimate party, such that it does not reach its intended receiver, the authentication process will stop and the used $A_{\mathtt{ID},i}$ will not be updated. To overcome that, A can use one of her emergency IDs from the set $\mathcal{A}_{\mathtt{ID},emerg}$. B will then read the corresponding $K_{R,emerg}$ from the set $\mathcal{K}_{R,emerg}$ and use it to encrypt a message containing an emergency challenge C_{emerg} from the set $\mathcal{C}_{emerg}$. Next, both parties can continue the authentication process as usual and setup a new one-time alias ID. In order to prevent replay attacks all used emergency parameters must be deleted from the corresponding set. It is important to mention that an attack could aim to introduce an error state at A, and exhaust all emergency IDs. To detect and redirect this type of malicious traffic different machine learning techniques can be used [93]. The investigation on which anomaly detection scheme would best fit our protocol is left as a future work.

H. PROTECTION AGAINST CLONING ATTACKS

A successful cloning attack allows the adversary to use a captured device in order to obtain secrets stored on another device. In the proposed protocol each device posses a unique pair $(K_R, A_{\mathtt{ID}})$. Furthermore, all devices have unique PUFs and will produce a unique response to a challenge. Hence, the adversary cannot use secrets derived from one device in order to clone another.

I. PROTECTION AGAINST PHYSICAL ATTACKS

Successful physical attacks could be performed by physical tampering of the IoT device in order to change its behavior. However, by changing its behavior, the PUF will not produce the desired response, hence, B will detect the attack. Therefore, the proposed protocol is resistant against physical attacks.

J. SECRECY PROOFS USING BAN AND MB LOGIC

The secrecy evaluation of security protocols ensures that an adversary cannot obtain or alter secret parameters. In this regards, the BAN logic [32] is a widely used secrecy verification tool. However, some weaknesses were identified by the authors of [94]. They extended and improved the BAN logic to a more reliable version, namely MB logic, which is used in this paper. Formal proofs are deduced using a set of initial beliefs and rules which are based upon the message exchange within the protocol. The initial steps of MB logic are idealization of the protocol and identification of the initial beliefs. The protocol message idealization is used to interpret the implicit context-dependent information into an explicit protocol specification. Based on the set of rules defined in [94], the protocol in Fig. 7 is idealized as:

1) $A \rightarrow B : A_{\mathtt{ID},1}, N_1$
2) $B \rightarrow A : \{N_B \mathfrak{R} N_1\}_{K_{R,1}}$
3) $A \rightarrow B : \{R_3 | R_4 \mathfrak{R} N_A \mathfrak{R} N_B\}_{K_{R,2}}$

where $\mathfrak{R}$ gives the relation of the parameters, as defined in [94]. Next, denoting principals as A, B, messages and keys as M, K, respectively and formulas as X, the main properties of MB logic are: $A \models X$ denotes A believes X is true; $A \overset{K}{\triangleleft} M$ denotes A sees M using key K; $A \overset{K}{\mid\!\sim} M$ denotes A encrypts M using key K; $\#(M)$ denotes M is of type fresh; $A \overset{K}{\leftrightarrow} B$ denotes K is a good shared key between A and B; $A \triangleleft \Vert M$ denotes M is not available to A; $\sup(B)$ denotes B is a super-principal. Following that, the inference rules defined in [94], as used in this paper, are given in Table 5 (Note, $\{\cdot\}^C$ denotes complement). Given the fact that the enrollment phase is performed on a secure channel the initial beliefs can be defined as follows:

A1 $A \models A \overset{K_{R,1}}{\leftrightarrow} B$ and $B \models A \overset{K_{R,1}}{\leftrightarrow} B$
A2 $A \models A \overset{K'_{R,2}}{\leftrightarrow} B$ and $B \models A \overset{K'_{R,2}}{\leftrightarrow} B$
A3 $B \models A \models A^C \triangleleft \Vert R_3 | R_4 \mathfrak{R} N_A \mathfrak{R} N_B$
A4 $B \models \sup(A)$
A5 $B \overset{K'_{R,2}}{\triangleleft} R_3 | R_4 \mathfrak{R} N_A \mathfrak{R} N_B$
A6 $A \models B^C \triangleleft \Vert R_3 | R_4 \mathfrak{R} N_A \mathfrak{R} N_B$
A7 $A \overset{K'_{R,2}}{\mid\!\sim} R_3 | R_4 \mathfrak{R} N_A \mathfrak{R} N_B$
A8 $A \models \#(N_1)$, $A \models \#(N_A)$, $A \models \#(R_3)$, $A \models \#(R_4)$
A9 $A \overset{K_{R,1}}{\triangleleft} N_B \mathfrak{R} N_1$
A10 $A \models B \models B^C \triangleleft \Vert N_B$ and $B \models \#(N_B)$
A11 $A \models \sup(B)$
A12 $B \models A^C \triangleleft \Vert N_B \mathfrak{R} N_1$
A13 $B \overset{K_{R,1}}{\mid\!\sim} N_B \mathfrak{R} N_1$

Given the initial beliefs, the authentication property of the current run of the protocol can be directly verified using the authentication rule (R1) as shown in Table 5. In fact, the authentication of B to A (A to B) can be proven by simply using assumptions A1 and A9 (A2 and A5) in the numerator of the rule.

TABLE 5: Inference rules adopted from MB logic

Notation	**Description**
$\dfrac{A \models A \overset{K}{\leftrightarrow} B \wedge A \overset{K}{\triangleleft} M}{A \models B \overset{K}{\mid\!\sim} M}$	Authentication rule (R1)
$\dfrac{A \models B \overset{K}{\mid\!\sim} M \wedge A \models B \models A \overset{K}{\leftrightarrow} B \wedge A \models B \models B^C \triangleleft \Vert M}{A \models B \models \{A \cup B\}^C \triangleleft \Vert M}$	Confidentiality rule (R2)
$\dfrac{A \models \#(M) \wedge A \triangleleft N \mathfrak{R} M}{A \models \#(N)}$	Fresh rule (R3)
$\dfrac{A \models \{A,B\}^C \triangleleft \Vert K \wedge A \models \#(K)}{A \models A \overset{K}{\leftrightarrow} B}$	Good-key rule (R4)
$\dfrac{A \models \#(N) \wedge A \models B \overset{K}{\mid\!\sim} N}{A \models B \models A \overset{K}{\leftrightarrow} B}$	Nonce verification rule (R5)
$\dfrac{A \models B \models X \wedge A \models \sup(B)}{A \models X}$	Super-principal rule (R6)

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

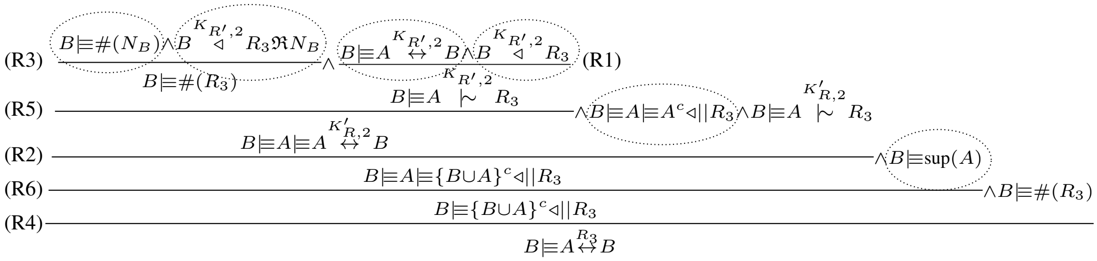
(R3)
$B|\equiv\#(N_B)\wedge B \overset{K_{R',2}}{\triangleleft} R_3 \Re N_B$
$B|\equiv\#(R_3)$
$\wedge$
$B|\equiv A \overset{K_{R',2}}{\leftrightarrow} B \wedge B \overset{K_{R',2}}{\triangleleft} R_3$
(R1)
$B|\equiv A \overset{K_{R',2}}{|\!\sim} R_3$
(R5)
$\wedge B|\equiv A|\equiv A^c \triangleleft || R_3 \wedge B|\equiv A \overset{K'_{R,2}}{|\!\sim} R_3$
$B|\equiv A|\equiv A \overset{K'_{R,2}}{\leftrightarrow} B$
(R2)
$\wedge B|\equiv \mathrm{sup}(A)$
$B|\equiv A|\equiv \{B\cup A\}^c \triangleleft || R_3$
(R6)
$\wedge B|\equiv\#(R_3)$
$B|\equiv \{B\cup A\}^c \triangleleft || R_3$
(R4)
$B|\equiv A \overset{R_3}{\leftrightarrow} B$

FIGURE 9: Secrecy proof in tableau format demonstrating B believes R_3 is a good shared secret between A and B. Initial beliefs, due to communication events are denoted with ellipses. The rules used to deduce the final goal are denoted when implied.

Next, we prove the secrecy of parameters R_3 (the proofs for secrecy of N_A and R_4 are identical) which could be used as initial belief for the next run of the protocol. The proof for $B \mid\equiv A \overset{R_3}{\leftrightarrow} B$ is given in Fig. 9. Similarly, one can prove that $A \mid\equiv A \overset{R_3}{\leftrightarrow} B$ and therefore, both parties A and B agree that R_3 is a good shared secret. However, the proof for A is not presented here due to the space limitation, instead we provide a formal verification of all the security properties using the Tamarin-prover [95]. Given the above, and using the fuzzy extractor properties [96], it can be concluded that $K_{R,3}$ and $K_{R,4}$ are good shared keys between A and B.

K. SESSION KEY AGREEMENT

It is a common practice in literature to use nonces as part of the session key generation process [21]–[23]. However, note that even if N_A and N_B are good shared secrets between A and B the low entropy of pseudo-random number generator (PRNG) modules may provoke a set of attacks [40], and lead to information leakage. Furthermore, it has been shown that true-random number generators (TRNGs) can greatly increase the time complexity in a resource limited systems making the generation time infeasible [97]. Therefore, we limit the role of the nonces in the proposed scheme to only a source of freshness. On the other hand, the randomness already present in the wireless channel allows for a secure and lightweight key generation process through the SKG procedure, as illustrated in Section III. Finally, we note that if the session key gets compromised, the authentication process remains secure as the adversary cannot obtain the PUF response using the session key.

L. SECURITY VERIFICATION USING THE TAMARIN-PROVER

There are many tools that can be used for automated security verification of authentication protocols. Nevertheless, only few of those support security analysis for an unbounded number of sessions, i.e., allowing the adversary to observe the legitimate communication for an unbounded number of sessions before launching an attack. The most widely used tools that can provide this feature are: Scyther [98], ProVerif [99] and Tamarin-prover [33]. However, different studies have reported that the former two options have several weaknesses as compared to Tamarin-prover [33], [100], [101]. For example, Scyther does not support user-specified equational theories and relies only on a set of fixed cryptographic primitives [33], [100], [102], [103]. ProVerif does not have this problem, however, it experiences difficulties when dealing with precise states within the protocol description [100], [102], [103]. This makes the tool susceptible to false attacks [101]. Based on these findings, we use Tamarin-prover [33] as a formal verification tool for the authentication protocol proposed in Section IV. Tamarin is a computer simulation tool that allows for user-specified security properties and cryptographic primitives, it supports equational theories, and can successfully maintain state information. Tamarin has an automated proof search which returns either a security proof (assuming an unbounded number of sessions) or a counterexample (attack). In this work Tamarin was used to prove: secrecy, aliveness, weak agreement, non-injective agreement, injective agreement, untraceablity and anonymity. The code used for our Tamarin simulation and all security proofs are publicly accessible and can be found at [95]. More detail regarding Tamarin-prover and a step by step guide on how to reproduce our results, can be found in Section III and Appendix A of [104].

VI. CONCLUSIONS

In this work we introduced a fast, privacy preserving, multi-factor mutual authentication protocol for IoT systems, leveraging SKG from fading coefficients, proximity estimation leveraging mobility and PUFs. Next, we conducted a set of experiments to demonstrate the applicability of our proposed proximity detection and SKG process, with an ESP32 low-power system. Finally, we validated the properties of the proposed authentication protocol through a detailed security analysis, using BAN and MB logic as well as the Tamarin-prover. Our analysis demonstrates the potential of the proposed protocol as a lightweight, multi-factor alternative to the currently used computationally intensive authentication schemes, with a particular interest in IoT networks of constrained devices and wireless sensor networks. As a future work the authors intend to further enhance the proposed authentication protocol and provide more security guarantees, e.g., through in-depth camera estimation and anomaly

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

detection techniques.

REFERENCES

[1] I. Stellios *et al.*, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 2018.

[2] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: authentication, integrity and confidentiality," *arXiv:2001.07153*, 2020.

[3] J. Hu, M. Reed, N. Thomos, M. F. AI-Naday, and K. Yang, "Securing SDN-controlled IoT networks through edge blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2102–2115, 2021.

[4] D. Karatzas, A. Chorti, N. M. White, and C. J. Harris, "Teaching old sensors new tricks: Archetypes of intelligence," *IEEE Sensors J.*, vol. 7, no. 5, pp. 868–881, May 2007.

[5] M. Mitev, M. M. Butt, P. Sehier, A. Chorti, L. Rose, and A. Lehti, "Smart link adaptation and scheduling for IIoT," *IEEE Networking Letters*, vol. 4, no. 1, pp. 6–10, 2022.

[6] "3GPP TR 33.825 V0.3.0, Study on the Security for 5G URLLC (Release 16)," 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects.

[7] A. Teniou and B. A. Bensaber, "Efficient and dynamic elliptic curve qu-vanstone implicit certificates distribution scheme for vehicular cloud networks," *Security and Privacy*, Jan. 2018.

[8] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, and A. F. Skarmeta, "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/3/882

[9] C. Lundqvist, A. Keränen, B. Smeets, J. Fornehed, C. Azevedo, and P. von Wrycza, "Key technology choices for optimal massive iot devices," pp. 48–59, 2019.

[10] P. Bachan and B. Singh, "Performance evaluation of authentication protocols for ieee 802.11 standard," in *2010 International Conference on Computer and Communication Technology (ICCCT)*, 2010, pp. 792–799.

[11] A. Chiornită, L. Gheorghe, and D. Rosner, "A practical analysis of eap authentication methods," in *9th RoEduNet IEEE International Conference*, 2010, pp. 31–35.

[12] D. Moody, "The ship has sailed: the nist post-quantum cryptography "competition"," in ., 2017, invited talk.

[13] A. Chorti and H. V. Poor, "Achievable secrecy rates in physical layer secure systems with a helping interferer," in *2012 Int. Conf. Computing, Netw. Commun. (ICNC)*, Jan 2012, pp. 18–22.

[14] A. Chorti, C. Hollanti, J. Belfiore, and H. V. Poor, "Physical layer security: A paradigm shift in data confidentiality," *Lecture Notes Electr. Eng.*, vol. 358, Jan 2016.

[15] M. Mitev, A. Chorti, M. Reed, L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *EURASIP JWCN*, no. 122, June 2020.

[16] M. Mitev, A. Chorti, and M. Reed, "Subcarrier scheduling for joint data transfer and key generation schemes in multicarrier systems," in *IEEE Global Commun. Conf. (GLOBECOM)*, Dec 2019, pp. 1–6.

[17] M. Mitev, A. Chorti, E. V. Belmega, and M. Reed, "Man-in-the-middle and denial of service attacks in wireless secret key generation," in *IEEE Global Commun. Conf. (GLOBECOM)*, Dec 2019, pp. 1–6.

[18] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.

[19] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, 2014.

[20] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for iot with light weight authentication and privacy preservation," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 441–10 457, 2019.

[21] ——, "Two-factor authentication for IoT with location information," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3335–3351, April 2019.

[22] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, 2019.

[23] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, 2019.

[24] R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *Cryptographic Hardware and Embedded Systems – CHES*. Springer Berlin Heidelberg, 2012, pp. 302–319.

[25] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[26] C. Shao, Y. Kim, and W. Lee, "Zero-effort proximity detection with zigbee," *IEEE Communications Letters*, pp. 1–1, 2020.

[27] G. TR33.809, "Study on 5g security enhancements against false base stations (rel 16)," 2018.

[28] A. Rock, "Phd thesis, pseudorandom number generators for cryptographic applications," 2005.

[29] M. Srinivisan, S. Skaperas, and A. Chorti, "On the use of CSI for the generation of RF fingerprints and secret keys," in *Proc. ITG International Workshop on Smart Antennas (WSA)*, 2021.

[30] M. Srinivisan, S. Skaperas, M. Shakiba-Herfeh, and A. Chorti, "Joint localization-based node authentication and secret key generation," in *Proc. IEEE Int. Conf. Communications (ICC)*, 2022.

[31] M. Shakiba-Herfeh and A. Chorti, "Comparison of short blocklength slepian-wolf coding for key reconciliation," in *2021 IEEE Statistical Signal Processing Workshop (SSP)*, 2021, pp. 111–115.

[32] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[33] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The tamarin prover for the symbolic analysis of security protocols," in *Proc. of the 25th Int. Conf. on Comp. Aided Ver.*, vol. 8044, 2013, pp. 696–701.

[34] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, "A comprehensive symbolic analysis of tls 1.3," in *ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 1773–1788. [Online]. Available: https://doi.org/10.1145/3133956.3134063

[35] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1383–1396. [Online]. Available: https://doi.org/10.1145/3243734.3243846

[36] D. Basin, C. Cremers, J. Dreier, and R. Sasse, "Tamarin: Verification of large-scale, real world, cryptographic protocols," in *IEEE Security and Privacy Magazine*. IEEE, 2022.

[37] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs," *ACM Comput. Surv.*, vol. 48, no. 2, 2015.

[38] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[39] A. Babaei and G. Schiele, "Physical unclonable functions in the internet of things: State of the art and open challenges," in *Sensors*, 2019.

[40] T. Miki *et al.*, "A random interrupt dithering SAR technique for secure ADC against reference-charge side-channel attack," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 67, no. 1, pp. 14–18, 2020.

[41] S. Sadowski and P. Spachos, "Rssi-based indoor localization with the internet of things," *IEEE Access*, vol. 6, pp. 30 149–30 161, 2018.

[42] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of covid-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134 577–134 601, 2020.

[43] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based iot device authentication," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017, pp. 1–9.

[44] 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*, ser. MobiSys '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 211–224. [Online]. Available: https://doi.org/10.1145/1999995.2000016

[45] S. Griffiths, M. S. Wong, C. Y. T. Kwok, R. Kam, S. C. Lam, L. Yang, T. L. Yip, J. Heo, B. S. B. Chan, G. Xiong, and K. Lu, "Exploring bluetooth beacon use cases in teaching and learning: Increasing the sustainability of physical learning spaces," *Sustainability*, vol. 11, no. 15, 2019. [Online]. Available: https://www.mdpi.com/2071-1050/11/15/4005

[46] M. Kim, J. Lee, and J. Paek, "Neutralizing ble beacon-based electronic attendance system using signal imitation attack," *IEEE Access*, vol. 6, pp. 77 921–77 930, 2018.

[47] P. Roy and C. Chowdhury, "A survey on ubiquitous WiFi-based indoor localization system for smartphone users from implementation perspec-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

tives," *CCF Transactions on Pervasive Computing and Interaction*, 01 2022.

[48] C. H. Lam, P. C. Ng, and J. She, "Improved distance estimation with ble beacon using kalman filter and svm," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.

[49] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: Cooperative proximity-based authentication," in *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 331–344. [Online]. Available: https://doi.org/10.1145/1814433.1814466

[50] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1506–1521, 2021.

[51] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-free physical layer authentication based on machine learning for industrial wireless cps," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6481–6491, 2019.

[52] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, 2019.

[53] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2089–2100, 2013.

[54] G. Welch and G. Bishop, "An introduction to the Kalman filter," University of North Carolina at Chapel Hill, USA, Tech. Rep., 1995.

[55] K. Nishiyama, "An H_∞ optimization and its fast algorithm for time-variant system identification," *IEEE Transactions on Signal Processing*, vol. 52, no. 5, pp. 1335–1342, 2004.

[56] C. K. Chui and G. Chen, *Kalman Filtering with Real-Time Applications*. Germany: Springer, Berlin, Heidelberg, 1987.

[57] P. Hinterseer, E. Steinbach, and S. Chaudhuri, "Perception-based compression of haptic data streams using Kalman filters," in *2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings*, vol. 5, 2006, pp. V–V.

[58] D. Trudnowski, W. McReynolds, and J. Johnson, "Real-time very short-term load prediction for power-system automatic generation control," *IEEE Transactions on Control Systems Technology*, vol. 9, no. 2, pp. 254–260, 2001.

[59] M. Mitev, A. Chorti, E. V. Belmega, and H. V. Poor, "Protecting physical layer secret key generation from active attacks," *Entropy*, vol. 23, no. 8, 2021.

[60] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *15th Annual Int. Conf. Mobile Computing Netw.*, ser. MobiCom '09. New York, NY, USA: Assoc. Computing Machinery, 2009, p. 321–332.

[61] M. Shakiba-Herfeh and A. Chorti, "Comparison of short blocklength slepian-wolf coding for key reconciliation," in *IEEE Stat. Signal Process. Workshop SSP 2021*, 2021.

[62] S. Balakrishna and M. Thirumaran, "Semantic interoperable traffic management framework for IoT smart city applications," *EAI Endorsed Transactions on Internet of Things*, vol. 4, p. 155482, 09 2018.

[63] P. Spachos and K. N. Plataniotis, "BLE beacons for indoor positioning at an interactive IoT-based smart museum," *IEEE Systems J.*, vol. 14, no. 3, pp. 3483–3493, 2020.

[64] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. USA: Prentice Hall PTR, 2001.

[65] I. Domuta and T. P. Palade, "On-line estimation of base station location," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 331–335, 2020.

[66] F. M. Alsalami, Z. Ahmad, S. Zvanovec, P. A. Haigh, O. C. L. Haas, and S. Rajbhandari, "Indoor intruder tracking using visible light communications," *Sensors*, vol. 19, no. 20, 2019.

[67] L. Ljung, M. Morf, and D. Falconer, "Fast calculation of gain matrices for recursive estimation schemes," *International Journal of Control*, vol. 27, no. 1, pp. 1–19, 1978.

[68] D. Falconer and L. Ljung, "Application of fast Kalman estimation to adaptive equalization," *IEEE Transactions on Communications*, vol. 26, no. 10, pp. 1439–1446, 1978.

[69] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, 1995.

[70] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: Assoc. Computing Machinery, 2008, p. 128–139.

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

[72] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*, 1st ed. Springer Publishing Company, Incorporated, 2016.

[73] Y. Gao, Y. Su, L. Xu, and D. C. Ranasinghe, "Lightweight (reverse) fuzzy extractor with multiple reference puf responses," *IEEE Trans. Inf. Forens. Secur.*, vol. 14, no. 7, pp. 1887–1901, 2019.

[74] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, "Helper data algorithms for puf-based key generation: Overview and analysis," *IEEE Trans. Computer-Aided Design Integr. Circuits Systems*, vol. 34, no. 6, pp. 889–902, 2015.

[75] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb 2019.

[76] H. Yıldız, M. Cenk, and E. Onur, "Plgakd: A puf-based lightweight group authentication and key distribution protocol," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5682–5696, 2021.

[77] V. C. Patil and S. Kundu, "Realizing robust, lightweight strong pufs for securing smart grids," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 5–13, 2022.

[78] M. Bhargava and K. Mai, "An efficient reliable puf-based cryptographic key generator in 65nm cmos," in *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2014, pp. 1–6.

[79] B. Colombier, L. Bossuet, V. Fischer, and D. Hély, "Key reconciliation protocols for error correction of silicon puf responses," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1988–2002, 2017.

[80] J. Petit, "Analysis of ecdsa authentication processing in vanets," in *2009 3rd International Conference on New Technologies, Mobility and Security*, 2009, pp. 1–5.

[81] J. Petit and Z. Mammeri, "Authentication and consensus overhead in vehicular ad hoc networks," *Telecommunication Systems*, vol. 52, pp. 1–14, 04 2011.

[82] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev, J. Hajny, J. Niutanen, and Y. Koucheryavy, "Feasibility characterization of cryptographic primitives for constrained (wearable) iot devices," in *2016 IEEE Int. Conf. Perv. Computing Commun. Workshops (PerCom Workshops)*, March 2016, pp. 1–6.

[83] V. K. Sarker, T. N. Gia, H. Tenhunen, and T. Westerlund, "Lightweight security algorithms for resource-constrained iot-based sensor nodes," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[84] J. Cho and W. Sung, "Efficient software-based encoding and decoding of bch codes," *IEEE Trans. Computers*, vol. 58, no. 7, pp. 878–889, July 2009.

[85] T. Eisenbarth, Z. Gong, T. Güneysu, S. Heyse, S. Indesteege, S. Kerckhof, F. Koeune, T. Nad, T. Plos, F. Regazzoni, F.-X. Standaert, and L. van Oldeneel tot Oldenzeel, "Compact implementation and performance evaluation of block ciphers in attiny devices," in *Progress in Cryptology - AFRICACRYPT 2012*, A. Mitrokotsa and S. Vaudenay, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 172–187.

[86] I. Ullah, N. Meratnia, and P. J. M. Havinga, "imac: Implicit message authentication code for iot devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1–6.

[87] A. R. Chowdhury and S. DasBit, "Lmac: A lightweight message authentication code for wireless sensor network," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–6.

[88] G. Saldamli, L. Ertaul, and A. Shankaralingappa, "Analysis of lightweight message authentication codes for iot environments," in *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2019, pp. 235–240.

[89] J. Balasch, B. Ege, T. Eisenbarth, B. Gérard, Z. Gong, T. Güneysu, S. Heyse, S. Kerckhof, F. Koeune, T. Plos, T. Pöppelmann, F. Regazzoni, F.-X. Standaert, G. Van Assche, R. Van Keer, L. van Oldeneel tot Oldenzeel, and I. von Maurich, "Compact implementation and performance evaluation of hash functions in attiny devices," in *Smart Card Research*

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3187967

and Advanced Applications, S. Mangard, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 158–172.

[90] N. Aviram, K. Gellert, and T. Jager, "Session resumption protocols and efficient forward security for TLS 1.3 0-RTT," Cryptology ePrint Archive, Report 2019/228, 2019.

[91] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[92] G. T. Becker, "Robust fuzzy extractors and helper data manipulation attacks revisited: Theory versus practice," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 5, pp. 783–795, 2019.

[93] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.

[94] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *Proc. Computer Security Foundations Workshop VI*, 1993, pp. 147–158.

[95] M. Mitev, "Verification of the security properties of a PUF-based authentication protocol," https://github.com/Miroslav-Mitev/Tamarin-prover-PUF-Authentication-protocol, 2021.

[96] B. Fuller, L. Reyzin, and A. Smith, "When are fuzzy extractors possible?" *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 5282–5298, 2020.

[97] C. Huth *et al.*, "Securing systems with indispensable entropy: LWE-based lossless computational fuzzy extractor for the internet of things," *IEEE Access*, vol. 5, pp. 11 909–11 926, 2017.

[98] C. J. F. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Computer Aided Verification*, A. Gupta and S. Malik, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 414–418.

[99] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," in *Proceedings. 14th IEEE Computer Security Foundations Workshop, 2001.*, 2001, pp. 82–96.

[100] D. Basin, C. Cremers, J. Dreier, and R. Sasse, "Symbolically analyzing security protocols using tamarin," *ACM SIGLOG News*, vol. 4, no. 4, p. 19–30, nov 2017. [Online]. Available: https://doi.org/10.1145/3157831.3157835

[101] J. Dreier, C. Duménil, S. Kremer, and R. Sasse, "Beyond subterm-convergent equational theories in automated verification of stateful protocols," in *Principles of Security and Trust*, M. Maffei and M. Ryan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 117–140.

[102] C. Jacomme, S. Kremer, and G. Scerri, "Symbolic models for isolated execution environments," in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, 2017, pp. 530–545.

[103] V. Cortier, S. Delaune, and J. Dreier, "Automatic generation of sources lemmas in tamarin: Towards automatic proofs of security protocols," in *Computer Security – ESORICS 2020*, L. Chen, N. Li, K. Liang, and S. Schneider, Eds. Cham: Springer International Publishing, 2020, pp. 3–22.

[104] M. Mitev, "Physical layer security for IoT applications," Ph.D. dissertation, University of Essex, 2020.

MIROSLAV MITEV obtained the Ph.D from the University of Essex, UK with his thesis in the area of physical layer security. Next (2020), he joined the École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA) in France, working in collaboration with Nokia Bell Labs on interference management. Since 2021, he is with the Wireless Connectivity group at the Barkhausen Institute, Germany. His research interests include wireless communications, physical layer security and link adaptation for industrial IoT.

MAHDI SHAKIBA-HERFEH received his B.Sc. degree from the University of Tehran, Tehran, Iran, in 2011, M.Sc. degree from Middle East Technical University, Ankara, Turkey, in 2014, and Ph.D. degree from Bilkent University, Ankara, Turkey, in 2019. Next, as a post-doctoral researcher, he joined ENSEA, Cergy, France. His research interests include various topics in information theory, wireless communications, and wireless security with a particular focus on coding techniques.

ARSENIA (ERSI) CHORTI is a Professor at the École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Joint Head of the Information, Communications and Imaging (ICI) Group of the ETIS Lab UMR 8051 and a Visiting Scholar at Princeton and Essex Universities. Her research spans the areas of wireless communications and wireless systems security for 5G and 6G, with a particular focus on physical layer security. Current research topics include : context aware security, multi-factor authentication protocols, 5G / 6G and IoT, anomaly detection, machine learning for communications, new multiple access techniques and scheduling. She is a Senior IEEE Member, member of the IEEE INGR on Security and of teh Sterring Committee of the Competitive Pole Systematic and of the PhD Thesis GdR ISIS Award Committee in France. Since October 2021 she is chairing the IEEE Focus Group on Physical Layer Security.

MARTIN REED is a full professor in the School of Computer Science and Electronic Engineering at the University of Essex, UK. He has been awarded research funding by UK research councils, Industry and EU research programmes in areas such as network/communication security, IoT security, future Internet architectures, optical network control planes and media transportation over networks, leading to over 100 peer-reviewed papers. His work has resulted in patents, international impact and inclusion in standards by ITU, IETF and 3GPP.

SAJJAD BAGHAEE is a Ph.D. candidate at the Department of Electrical and Electronics Engineering in the Middle East Technical University (METU), Ankara, Turkey. He received an M.Sc. degree in Electrical and Electronics Engineering from METU in 2012. From 2010 to 2020, he has been a research assistant in the Communication Networks Group (CNG) of Department of Electrical and Electronics Engineering at METU. Currently, he is a senior IoT system engineer in JEOIT, Ankara, Turkey, and before that he worked as a Machine Learning and Artificial Intelligence Engineer in TEKNOS, Ankara, Turkey. Mr. Baghaee has participated in numerous research projects as a researcher funded by The Scientific and Technological Research Council of Turkey (TUBITAK) and serves as a reviewer for various IEEE journals/conferences. His current research interests concentrate on Internet of Things (IoT), Age of Information (AoI), future Internet architectures and protocols with an emphasis on age-aware communications.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/