LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks

Junejo, A. K., Benkhelifa, F., Wong, B. & McCann, J.

Original citation & hyperlink:
Junejo, AK, Benkhelifa, F, Wong, B & McCann, J 2021, 'LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks', IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4110-4124.
https://dx.doi.org/10.1109/JIOT.2021.3103009

DOI 10.1109/JIOT.2021.3103009
ISSN 2327-4662

Publisher: IEEE

LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks

Aisha Kanwal Junejo, Fatma Benkhelifa, Boon Wong, and Julie A. McCann

***Abstract*—Physical layer security (PLS) schemes use the randomness of the channel parameters, namely, channel state information (CSI) and received signal strength indicator (RSSI), to generate the secret keys. There has been limited work in PLS schemes in long-range (LoRa) wide area networks (LoRaWANs), hindering their widespread application. Limitations observed in existing studies include the requirement of having a high correlation between channel parameter measurements and the evaluation in either fully indoor or outdoor environments. The real-world wireless sensor networks (WSNs) and LoRa use cases might not meet both requirements, thus making the current PLS schemes inappropriate for these systems. This paper proposes LoRA-LiSK, a practical and efficient shared secret key generation scheme for LoRa networks to address the limitations of existing PLS schemes. Our proposed LoRa-LiSK scheme consists of several preprocessing techniques (timestamp matching, two sample Kolmogorov Smirnov tests, and a Savitzky-Golay filter), multi-level quantization, information reconciliation using Bose–Chaudhuri–Hocquenghem (BCH) codes, and finally, privacy amplification using secure hash algorithm SHA-2. The LoRa-LiSK scheme is extensively evaluated on real WSN/IoT devices in practical application scenarios: 1) indoor to outdoor and 2) long range static and mobile outdoor links. It outperforms existing schemes by generating keys with channel parameter measurements of low correlation values (0.2 to 0.6) while still achieving high key generation rates and low key disagreement rates ($10\% - 20\%$). The scheme updates a key in one hour approximately using an application profile with a high transmission rate compared to three hours reported by existing works while still respecting the duty cycle regulation. It also incurs less communication overhead compared to the existing works.**

***Index Terms*—Security, Key Generation, LPWAN, LoRaWAN, Wireless Sensor Networks**

I. Introduction

THE broadcast nature of wireless transmission enables all devices in the range of a sender to receive a message. Taking advantage of such cases, adversaries can eavesdrop and monitor the network traffic to carryout active attacks, namely, modification, jamming, spoofing, replaying, and Denial of Service (DoS) [1]. These attacks violate the confidentiality, integrity, and availability of wireless sensor networks (WSNs) and therefore robust security mechanisms are essential. Encryption has always been used as a tool to protect information during rest and transit. However, the classical encryption schemes, namely asymmetric and symmetric, have several limitations when applied to sensor networks. Asymmetric schemes are computationally heavy due to operations on large prime numbers and finite fields. They also require a public key infrastructure (PKI) for the generation and verification of keys and certificates. Likewise, in symmetric schemes, the generation and management of shared secret keys in the large-scale WSNs are challenging problems. Each sensor node requires $(n-1)$ keys to securely communicate with its neighbouring nodes. The management of these many keys is not a trivial process, thus making symmetric schemes an impractical solution. The challenges mentioned above are precisely why classical encryption schemes are not suitable for battery-powered and resource constrained sensor devices. Additionally, the nature of continuously evolving wireless technologies and their security issues necessitate the devising of novel and lightweight encryption schemes.

Recently, low power wide area network (LPWAN) technologies, namely long range (LoRa), SigFox, and narrowband Internet-of-Things (NB-IoT), have widely been used in many sensor-based applications such as healthcare, smart cities, manufacturing, agriculture, etc. [2]. In contrast to the other LPWAN technologies, LoRa has captured particular research and industrial interest for several reasons such as operating over unlicensed spectrum (sub-GHz band), transmitting over long range distances, consuming low power, etc. The LoRaWAN specification supports end-to-end security based on a 128-bit application key (App key) generated from the advanced encryption standard (AES) [3]. Each device uses the App key to generate two session keys; network session key and application session key. LoRaWAN defines two joining procedures for end-devices; over the air activation (OTAA) and activation by personalization (ABP). The latter is vulnerable to security attacks as the devices use preshared keys for encryption/decryption. Additionally, predistributed secret keys can also be compromised by a node capture attack [4].

The physical layer security (PLS) is an alternative approach to the secret key generation. PLS key generation has several advantages over classical schemes. The most notable advantage is how it is more lightweight and more efficient compared to asymmetric cryptography. As reported in [5], the elliptic curve Diffie-Hellman (ECDH) consumes 98 times more energy and imposes 1289 times higher complexity than PLS key generation, when both are implemented on an 8-bit Intel MCS-51 microcontroller. The PLS key generation also does not rely on a trusted key generation authority (KGA), making it suitable for decentralized or device-to-device sensor applications. Another key advantage of PLS key generation is how it is able to address the problem with key predistribution.

PLS schemes use channel state information (CSI) and

A. K. Junejo, F. Benkhelifa, B. Wong, and Julie A. McCann are with the Adaptive Emergent System Engineering Group, Department of Computing, Faculty of Engineering, Imperial College London, London, SW7 2AZ, e-mail: {a.junejo,f.benkhelifa,b.wong18,j.mccann}@imperial.ac.uk.

Manuscript received January, 2021

received signal strength indicator (RSSI) as the randomness sources for secret key generation. However, acquiring CSI knowledge is quite challenging for some network technologies as it requires developing customized driver packages which inform about channel properties such as scattering, fading, and power decay with distance. RSSI is the most commonly employed channel parameter in wireless networks. Key generation in LPWAN faces challenges such as channel reciprocity, key refreshment, and low randomness that are typical characteristics of the static environments. Additionally, the correlation between RSSI measurements at the end device and gateway can be low due to the low signal-to-noise ratio and the high delay time between uplink and downlink packets.

There is limited work on PLS schemes in LPWAN, and the existing studies [6]–[8] are exploratory and inconclusive. They are not feasible for real LPWAN applications due to the following reasons. Firstly, the application scenarios presented in the above studies are based on fully indoor or outdoor modes with static and mobile configurations. Realistic scenarios however do not always follow a fully indoor or outdoor network topology. LoRaWAN is the enabler technology of smart cities as it provides ubiquitous connectivity in disparate endpoints. In such large-scale network ecosystems, gateways can only be deployed in a few locations. The use cases namely public transport (specifically the underground network), indoor monitoring, waste management and agriculture farming can be based on indoor-to-outdoor topologies where gateways are located on roof tops and nodes are either inside or outside the buildings [9]. The sensor nodes may be outside in an agriculture farm or deployed on vehicles, whereas the base station may be indoors in a junction box. Likewise, for indoor monitoring, the base station can be around the city, which is the case of The Things Network (TTN) having multiple base stations all around Europe.

Secondly, a high correlation between RSSI channel measurements of end devices and the gateway is a prerequisite of the existing key generation schemes. However, the correlation can be low in some practical use cases such as indoor to outdoor, and deep indoors where the end devices could be located indoor but the gateway located outdoors and vice versa. In these cases, the propagation channels cannot be perfectly symmetric; that is where the uplink channels are assumed to be exactly the same as downlink channels and vice versa. Our work also focuses on indoor to outdoor scenarios where the propagation channel between the nodes and the gateway is not perfectly symmetric. The low correlation can be due to obstacles, walls, large-scale path loss fading, and short-scale multi-path fading. Moreover, it is well known that multi-path fading channels are time-varying and randomly distributed meaning that it is impossible to have the same channel quality during the uplink and downlink transmission.

A. Contributions

Considering the security challenges of LoRaWAN and the limitations of existing works, in this paper, we propose a lightweight shared secret key generation scheme for LoRa networks (LoRa-LiSK). The contributions of this paper are three-fold, 1) The proposed scheme enables key generation using RSSI channel measurements with a low correlation value (down to 0.2 in some cases). The generation of secret keys with channel parameter measurements of low correlations enables securing information in all use cases including those mentioned above. 2) The scheme is experimentally evaluated over several devices and in realistic application scenarios. The first scenario is based on multiple end-devices located deep in-building and an outdoor gateway. Precisely, four end devices are located indoor and one gateway is located outdoor on a different building. The motive behind the evaluation on more than one device is to benchmark the performance in different deep-indoor locations with varying channel randomness. To the best of our knowledge, this is the first study which is simultaneously evaluated on four end devices and in which optimal results are produced. In the second scenario, the scheme is evaluated in a dense urban environment involving a long distance outdoor LoRaWAN link between one end device and a gateway. 3) An extensive attacker model was designed and implemented on a separate end device acting as a passive eavesdropper overhearing two end devices located nearby in a bid to generate similar keys with any one of them. The eavesdropper fails to generate a shared secret key highlighting the effectiveness of our proposed scheme.

The rest of this paper is organized as follows. The related work is presented in section II. The proposed LoRa-LiSK scheme is discussed in section III. The experimental results are discussed in section IV. The conclusion and future work are presented in section V.

II. Related Work

In this section, the recent studies on PLS based security are discussed. The wireless key generation process is well established and consists of four steps, namely channel probing, quantization, information reconciliation, and privacy amplification [10]. Existing studies differ from each other based on the methods used in the steps mentioned above to achieve high key generation rate (KGR) and low key disagreement rate (KDR). Following this, we discuss PLS schemes proposed for different wireless technologies namely, WI-FI, bluetooth, and LPWAN. Due to the limited amount of literature about LoRa key generation. we extended our review to cover the schemes used for other technologies.

We will first start with the secret key generation schemes proposed for other wireless technologies such as IEEE 802.11, IEEE 802.15.4, and LTE. Zenger et al. [5] propose an authenticated key establishment scheme for resource constrained devices. The scheme uses a notion of vicinity pairing (VP) in which the authenticated and trusted nodes authenticate other nodes. VP is based on time and frequency-varying channel profiles. VP uses the correlation between channel profiles in physical proximity for authentication and extraction of shared secret keys. The study in [11] proposes a scheme for establishing an encrypted wireless link between two body-worn sensor nodes integrated on the textile antenna platforms. The scheme utilizes CSI for the key establishment. The works in [5] and [11] are not suitable for LoRa networks because of the

short-range communication involved. Liu et. al [12] propose a key generation scheme for IEEE 802.11, Wi-Fi networks based on the channel measurements from multiple Orthogonal Frequency-Division Multiplexing (OFDM) subcarriers achieving high KGR. The problems of channel non-reciprocity and low correlation are addressed by introducing a notion of Channel Gain Complement (CGC). The study in [13] proposes a RSSI based key generation scheme for IEEE 802.11 multiple input multiple output (MIMO) WSNs. Significant limitations of the scheme are the use of a computationally heavy Cascade-based information reconciliation, and evaluation on Google Nexus One phone, which is not a lightweight device.

Ali et al. [14] propose a secret key scheme for wearable health monitoring devices. The bit mismatches in RSSI measurements of the base-station and the device are removed by using Savitzky-Golay (SG) filtering and therefore does not require information reconciliation step in key generation. Xi et al. [15] propose a CSI based group key generation scheme for IEEE 802.11n Wi-Fi networks. S-boxes are generated after channel sampling, and parity check bits are used for removing the mismatches. The scheme enables the devices located in the proximity to generate the shared secret key and therefore are not suitable for LPWAN networks which cover long distances. The nodes are close to each other and this setting does not fit the LPWAN networks. The study in [16] proposes a key generation scheme using RSSI for 802.11b passive Wi-Fi technology. The system model is similar to the RFID, consisting of tag and passive reader. The scheme is not suitable for LPWAN networks with long distances. The study in [17] explores the secret key generation in In-Band Full-Duplex Communication. Siavoshani et al. [18] propose a group key scheme shared among many nodes. The scheme does not follow the formal key generation process. For key generation, a state-dependent wireless broadcast channel is converted into several independent erasure channels. Additionally, an optimal key generation rate is achieved by solving a non-convex power allocation problem over the erasure channels. Huang et al. [19] propose a channel frequency response based key for underwater acoustic systems. The correlation is increased by using adaptive weighted probing signaling. Additionally, block-sliced key verification is employed to handle channel dynamics and increase the KGR probability.

Next, the existing studies [6]–[8] for secret key generation in LPWAN are discussed. Xu et al. [6] propose a key generation protocol for LoRa networks. This work employs filtering and interpolation techniques to generate the missing values and achieve high KGR. Additionally, compressive sensing is used to reduce the mismatches between the node and the gateway's RSSI measurements. The scheme achieves a KGR of 18 bits/sec in stationary and 31 bits/sec in mobile scenarios. However, the results of key update time and the communication overhead are not presented. In other words, the complexity of the key generation process is not discussed. The use of several techniques, namely, SG filter, linear interpolation, multi-level quantization, and compressive sensing indicate a higher level of communication and computational complexity. The scheme's evaluation in fully indoor and outdoor use cases also underlines its unsuitability for practical scenarios. Additionally, in the threat model, the attacker is put at a distance of 1 m from the gateway. It is believed that the threat model is quite simplistic and the presence of an unknown/malicious node in such a short distance can easily be detected and blocked from overhearing. Ruotsalainen et al. [7] propose a secret key generation scheme for LPWAN. They have addressed limited randomness due to static channel conditions in LoRa networks by using an electrically steerable parasitic array of radiators (ESPARs) antenna. The proposed scheme is evaluated with LoRa signalling and LoRaWAN. The scheme uses single-bit quantization to convert analog RSSI values to bits. Additionally, BCH code is used in the information reconciliation step. The study has several limitations as discussed below. Mounting an ESPARs antenna to enhance the channel randomnesses is not viable for small sensor devices and incur additional hardware costs. The schemes takes 3 hours to generate a shared secret key. Such long update times are not suitable for mission critical sensor networks wherein a key update is required for every new message. Also, the evaluation was done in constrained network topologies, either fully indoor or outdoor, which may not be compatible with realistic scenarios where the gateway is outdoor and the nodes are indoor or where the gateway is indoor and the nodes are outdoor. They never tried deep indoor to outdoor. The outdoor scenario is also not tried in a dense city like London. Lastly, the attacker node is just 5 cm from the legitimate node which is a very short distance. It is believed that malicious nodes can be identified by employing some radio identification techniques thus rendering the current threat model ineffective. Zhang et al. [8] also propose a key generation scheme for LoRa networks which employs differential quantization for extracting high level of randomness from wireless channels. Similar to other LPWAN key generation schemes, this scheme is also evaluated in fully outdoor urban and indoor environments. These are the limitations of existing works (experimental scenarios, network topology, and location) that we are trying to address in this paper.

From the literature review, it is clear that the current LPWAN key generation schemes in [6]–[8] cannot fulfil the requirements of realistic and practical use cases such as agriculture, smart grid, and transportation where nodes can be located indoor and gateway can be located outdoor or vice versa. Besides that, they require highly correlated RSSI measurements to generate the secret keys, which can be another limitation of the real-world application scenarios. Moreover, in terms of experimental evaluation, the existing schemes are not consistent, and different values for parameters, namely, indoor/outdoor distance, channel parameters, and attacker model specifications are applied. The prevailing inconsistency makes it difficult to evaluate the performance of new schemes against a well-defined criteria. However, considering the limitations of the existing studies, in this paper, we proposed an efficient and lightweight scheme, named LoRa-LiSK. This scheme is evaluated in real-world WSNs use cases, and can generate keys with low correlation but still maintaining a high level of security from a passive eavesdropper. Our choice of experimental parameters for this scheme (i.e., location, distance, SF, attacker model) is also in line with this approach and produce

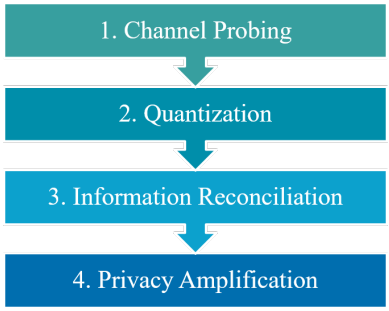


Fig. 1: Key Generation Process

optimal results.

III. Shared Secret Key Generation Process

In this section, we present our proposed LoRa-LiSK scheme. As discussed previously, all PLS schemes follow the same standard key generation process. The process consists of fours steps namely, channel probing, quantization, information reconciliation, and privacy amplification as shown in Fig. 1. Any two LoRa devices can generate a shared secret key by following the process shown in Fig. 1. However, the choice of techniques applied in each of the subprocesses varies among different studies and is mainly motivated by improving the performance metrics, namely, KGR, KDR, randomness, and security. In line with this approach, we are discussing the techniques and methods that are used in each of the subprocess in our LoRa-LiSK scheme. Additionally, we also discuss the attacker model and the performance evaluation metrics.

A. Channel Probing

As discussed in section I, the keys are generated from the channel parameters. In the LoRa-LiSK scheme, RSSI is chosen as the source of randomness because the current LoRa driver specifications do not provide CSI measurements. In other words, the only measurements available at both sides, end device and the gateway are RSSI values. This is the first step of secret key generation in which both parties need to record each other's RSSI measurements.

For a shared key generation, the gateway and sensor devices need to collect at least 128 RSSI measurements each. This may pose a challenge if a gateway connected to The Things Network (TTN) is used since a sensor device (class A) connected to the TTN is only able to receive up to 10 downlinks per day due to the fair access policy. TTN is not used by most LoRa networks and it does not have uniform global coverage. TTN has 18534 gateways in 151 countries worldwide with more than 9000 gateways in West Europe alone [20]; while LoRa has 152 operators spread over 167 countries covering all continents [21].

LoRa supports bi-directional communication with three device classes A, B, and C. In low powered LoRa operations, class A end devices are configured to send uplink packets to the gateway (in compliance with the legal requirements for duty-cycling), whereas the downlink packets are not so frequent. In Class A devices, after each uplink transmission, two consecutive downlink windows of limited duration (1 or 2 s) open. We are examining class A end devices because they consume lower power compared to their class B and C counterparts which have more frequent downlink windows [2]. LoRa was designed to have bi-directional communications, TTN restricts the number of downlink transmission to 10 per 24 hours for class A devices. For that reason, TTN cannot perform bi-directional communications as it was designed by LoRa networks. This scheme or any other existing PLS based scheme such as [6], [7] will require enough bi-directional communications in order to generate one key. Therefore, in our study, the gateway is connected to the ChirpStack, open-source LoRaWAN network instead where a downlink is sent to the end device for every uplink packet transmitted by the same end device. This ensures that the LoRa-LiSK scheme is able to take place within a reasonably short amount of time in a practical use case.

In the LoRaWAN class A standard, the end devices first send an uplink packet and then open up downlink windows at two specified times, typically at 1 second and 2 seconds after the uplink packet is transmitted.

$$T_d = T_u + \tau, \tag{1}$$

where T_d and T_u are the downlink and uplink time durations and τ is the delay between them.

After channel probing, generally some signal processing and filtering techniques are employed to reduce the asymmetry which is introduced by the non-simultaneous RSSI measurements and the inherent noise in the hardware platforms. In the existing studies, the noise in the measurements is reduced by employing different preprocessing techniques such as low pass filtering [6], and statistical methods based on mean and standard deviation of the RSSI measurements [7], [12]. However, none of the already proposed schemes gave us the same results, and for this reason a systematic study is carried out to find the best fit of techniques for this scheme. Precisely, three techniques namely, time stamp matching, two-sample test, and Savitzky–Golay (SG) Filter are used in the LoRa-LiSK scheme.

1) Timestamp Matching: The timestamp matching technique is used to correctly identify a downlink packet corresponding to an uplink packet. Three time stamps, uplink sending time T_u, uplink arrival time at gateway $T_u +$ air time, and downlink receiving time T_d at the end device are recorded to ensure the RSSI measurements match. Care is also taken to ensure the time required to send and receive packets is in the coherence time limit, T_c, the time during which propagation channels remain unchanged. T_c is comprised of a transmit time T_t, propagation time T_p, and operation delay τ.

2) Two Sample Test: Next, the collected RSSI measurements are divided into several subsets. A two-sample Kolmogorov-Smirnov (KS) test [22] is carried out for each subset to ascertain that they belong to same density distribution using eq. 2

$$D_n = sup_x |F_{1,n}(x) - F_{2,n}(x)|, \tag{2}$$

where n is the size of samples, $F_{1,n}$ and $F_{2,n}$ are the empirical distribution functions (EDF) of two RSSI samples taken at

different time periods, and sup_x is the supremum function which functions like a threshold to filter out a range of samples. The RSSI values within the range of supremum are considered for quantization while the rest of them are dropped.

3) Savitzky–Golay Filter: The noisy discrepancies in RSSI measurements taken from uplink and downlink packets have been smoothed out by using a SG filter [23]. SG filter is a low pass data smoothing method based on a local least-squares polynomial approximation which reduces noise while maintaining the shape and height of bandwidth fluctuation caused by multi-path environment.

B. Multi-level Quantization

The next step of the LoRa-LiSK scheme is to convert analog RSSI values to their binary representation. The number of bits generated from each RSSI sample depends upon the quantization levels, namely single-bit and multi-bit. The number of quantization levels are bounded by the entropy of the RSSI measurements. The channel measurements recorded in our experiments have high entropy and are therefore suitable for multi-level quantization. We adopt [24]'s scheme, consisting of two steps namely, finding quantization levels and intervals.

1) Quantization Levels: The quantization levels are bounded by the mutual information between the end devices and gateway. In other words, the bit length (i.e., 1, 2 or 4 bits) of quantization is directly proportional to the shared randomness. However, both the parties cannot find the mutual information before hand and subsequently infer it based on the estimated entropy given as

$$H(R) = -\sum_{i=1}^{n} P(r_i) \log P(r_i), \tag{3}$$

where $H(R)$ is the entropy of a subset R of RSSI measurements, $P(r_i)$ is the frequency of ith measurement in R. The maximum quantization level, η is bounded by the estimated entropy, $\eta \leq 2^{H(R)}$. Each level in the quantization is assigned an n–bit code, $n = \log_2 \eta$. For instance, the code would be two bits long in 4-level quantization.

2) Quantization Intervals: Once the quantization levels are defined, the next step is to find out the number of RSSI measurements that will fall into each of the levels based on their probability distribution f_r. A robust quanitzation technique ensures that all the levels are equiprobable. The bit agreement ratio between two consecutive intervals is increased by using guard bands. With η quantization levels, the quantization intervals are given as:

$$I_0 = (q_0, q_1 - g_1), I_1 = (q_1, q_2 - g_2), ..., I_{\eta-1} = (q_{\eta-1}, q_\eta) \tag{4}$$

where q_0 and q_η are the minimum and maximum RSSI values in R, g_i is the size of guard band between the ith level and $(i-1)$th level, and q_i is the lower bound of the ith level . The size of interval of each level is calculated using eq 5

$$\int_{q_i-1}^{q_i-g_1} f_r d_r = \frac{1-\alpha}{\eta}, \qquad \int_{q_i-g_1}^{q_i} f_r d_r \quad = \frac{\alpha}{\eta - 1} \tag{5}$$

where, q_i and g_i are the ith quantization level and guard band respectively. Likewise, $1 \leq i \leq \eta - 1$ and α denotes the guard band to data ratio, which are the excluded measurements in all the guard bands over the total measurements in R. Equations 4 and 5 are translating the aim of achieving equiprobable RSSI values in the quantization levels. The guard bands are complementing the process by increasing the bit agreement ratio between two quantization levels.

C. Information Reconciliation

After quantization, both the end device and the gateway generate a key which might not always be same and can have some mismatching bits due to non-simultaneous channel measurements. The information reconciliation in the LoRa-LiSK scheme addresses this issue by employing some error correction code (ECC) technique, namely Bose–Chaudhuri–Hocquenghem (BCH) code [25], Reed-Solomon code [26], low-density parity-check (LDPC) [27], Turbo, and Golay code [28]. Other ECC techniques include compressive sensing [29] and Cascade protocol [30]. In the LoRa-LiSK scheme, BCH codes are used for correcting the mismatched bits as they are lightweight compared to other error correcting codes. The BCH codes are constructed from polynomials defined over a finite Galois field (GF) having linear complexity and thus suitable for low powered devices. The error correction capacity t of BCH codes (n, k, t) is defined using eq. 6, where n and k are the lengths of codeword and message respectively

$$\zeta = \frac{t_{max}}{n} = \frac{2^{m-2} - 1}{2^m - 1}. \tag{6}$$

where $m \geq 3$ is a positive integer. ECC schemes are used in conjunction with secure sketches [31] to securely transmit the encoded data over unauthenticated channels. A secure sketch produces public information about the key without revealing it to an eavesdropper. The main advantage of using secure sketches is to recover key given another value that is close to key. In the LoRa-LiSK scheme, the end device transmits a secure sketch towards gateway and gateway decodes the sketch to correct the errors in the quantized key bits.

D. Privacy Amplification

As the secure sketch is transmitted over an unprotected channel, it may still leak some information about the secret key. The privacy amplification step in the LoRa-LiSK scheme is introduced to prevent the leakage about the shared secret key such that an adversary cannot generate the same key. Cryptographic Hash functions namely, SHA-1, SHA-2, and SHA-3 are generally used for privacy amplification. In this work, SHA-256 from the family of SHA-2 is used for privacy amplification.

E. Attacker Model

The proposed LoRa-LiSK scheme follows Dolev-Yao threat model [32]. In Dolev-Yao adversarial model, adversaries can overhear and intercept any message that is exchanged between two or more parties in the network. Besides that, in some cases, the eavesdroppers can just overhear the exchanged messages for learning about the network entities and may later use this information for active attacks.

F. Performance Evaluation Metrics

The performance of a key generation scheme can be evaluated based on four key metrics namely, randomness and entropy, KGR, KDR, and key update time.

1) Randomness and Entropy: The security of cryptographic algorithms is based on a good source of randomness, and it is achieved by using large security parameters and prime numbers. Randomness of the key sequences is the prerequisite of PLS based schemes because otherwise the adversary can easily guess the shared secret key. NIST statistical test suite [33] is used to test the randomness of random number generators (RNGs) and pseudo random number generators (PRNGs). Every secret key must pass the NIST randomness test prior to be used in any crytographic algorithm. The tests are conducted before the privacy amplification step. Additionally, entropy is the quantification of randomness of the shared secret key and lies between $[0, 1]$. A high entropy indicates a truly random key.

2) Key Generation Rate: The KGR defines the rate at which the secret key bits produced from RSSI measurements. KGR is defined using eq. 7

$$KGR = \frac{n_r}{n_k}, \tag{7}$$

where n_r is the number of RSSI measurements and n_k is the number of quantized key bits. In case of 4-level multi quantization, two bits are generated from each measurement. Other factors namely channel parameters (RSSI, CSI), spreading factor, channel probing rate, and quantization scheme also impact the KGR.

3) Key Disagreement Rate: KDR defines the number of mismatching bits between two parties and is calculated using eq. 8

$$KDR = \frac{n_m}{n_k} \tag{8}$$

where n_m is the number of mistmatching bits in the quantized vectors of the two parties and n_k is the number of key bits, which is generally 128 for a 128 bit AES key. If the KDR is higher than the error correction capability t of BCH code then the mismatches cannot be corrected and the key generation fails.

4) Key Update Time: To obtain the timing results, we adopt the technique in [7]. Additionally, we assumed that the KDR of the Eve is readily available and/or derived from experiments. The time T_{key} required for generating a new key depends upon a number of factors, 1) the mismatches (KDR) between the keys of Alice and Bob, and Eve, 2) quantization algorithm, and 3) spreading factors. T_{key} is inversely proportional to the KDR, meaning that key update time would be shorter with a larger KDR and vice versa. T_{key} is calculated based on the minimum number of quantized bits n_{min} and total measurements n_t required for generating a 128-bit AES key. n_{min} is calculated using eq. 9

$$n_{min} = \frac{128}{KDR_{Eve} - KDR_{AB}}, \tag{9}$$

where KDR_{Eve} and KDR_{AB} are the KDR of Eve, and Alice and Bob respectively. Next, n_t is calculated using eq. 10

$$n_t = \frac{n_{min}}{KGR}. \tag{10}$$

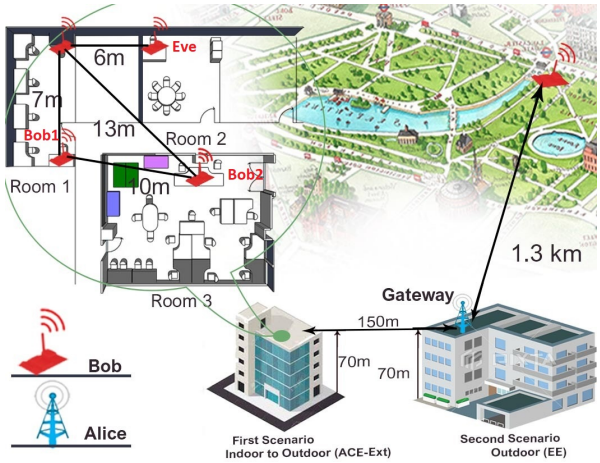


Fig. 2: Indoor and Outdoor Scenarios

TABLE I: Experiment Parameters

Parameter	Value
Bandwidth	125 kHz
Power	20 dBm
Frequency	868 MHz
No: of End Devices	Total 4 3 with ADR 1 with SF = 12
No: of Gateway	1
Duration	7 Days

Lastly, T_{key} is calculated using eq. 11

$$T_{key} = n_t T_a, \tag{11}$$

where T_a is the airtime for an uplink packet with a fixed payload and specific SF.

IV. Experimental Results

In this section, the performance of the LoRa-LiSK scheme is evaluated. The results has two parts: 1) the first part presents the performance of the scheme in benign and attacking scenarios, and 2) the second part presents a comparative analysis with existing state-of-the-art works.

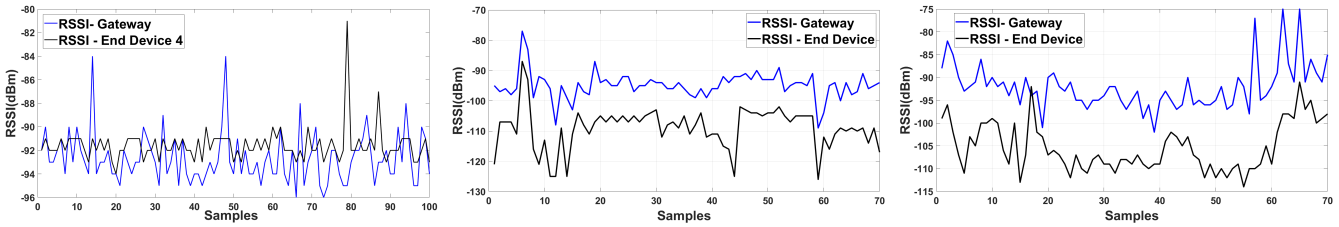
A. Experimental Setup

In our experiments, the LoRa end device is represented by a customized node made up of a Pycom FiPy development board and Raspberry Pi Model Zero, as shown in Fig. 3(a). The FiPy module [34] is used as the primary LoRa end device the Raspberry Pi acts as the observer which sends the setup parameters to configure the LoRaWAN stack running on the FiPy besides performing node-side datalogging for both the uplinks and downlinks.

The MultiConnect Conduit MTCDTIP-LEU1-266A-915 is used as the LoRa gateway in our experiments. As mentioned earlier, the gateway is connected to the Chirpstack, an open-source LoRaWAN network server. Our choice of the packet transmission rate of 1 packet/minute is motivated by our intention to challenge the upper performance limit of the LoRaWAN network in continuous infrastructure monitoring while abiding by the 1% duty cycle regulation as part of the

(a) LoRa End Device (b) Outdoor Static (c) Outdoor Distance

Fig. 3: Experimental Setup



(a) Indoor-to-Outdoor (b) Static Outdoor (c) Mobile Outdoor

Fig. 4: RSSI Channel Measurements

TABLE II: Pre-processing and Filtering

KDR	Node 1	Node 2	Node 3	Node 4
Raw RSSI				
$\alpha = 0$	0.72	0.11	0.88	0.61
$\alpha = 1$	0.16	0.2	0.67	0.33
Filtering 1 - Moving average window (Size=15) and CGC				
$\alpha = 0$	0.72	0.27	0.75	0.67
$\alpha = 1$	0.38	0.05	0.66	0.16
Filtering 2 - Low Pass Golay (5,9)				
$\alpha = 0$	0.23	0.19	0.31	0.21
$\alpha = 1$	0.17	0.04	0.14	0.12

fair access policy of LoRa. By keeping the packet size at 20 bytes or below, we are able to keep the uplink airtime within the bounds of 1% duty cycle regulation while still committing to our choice of packet transmission rate.

The experiments were run in two very challenging conditions in the dense city of London and COVID-19 restrictions (brought further experimentation challenges). Table I lists the parameters used in the experiments. Adhering to security algorithm terminology, the notions of Alice, Bob and Eve are used to represent the gateway, node (end device), and eavesdropper, respectively. We successfully managed to conduct experiments for two scenarios, 1) static indoor to outdoor, and 2) static and mobile long range outdoor.

First experimental scenario: As shown in Fig. 2, it consists of four nodes (Bob) and one gateway (Alice). The four nodes are located in three different rooms at the same level in one building (ACE extension). They are located deep indoors. Rooms 1 and 3 have windows, while Room 2 has no window and is located at the heart of the building. The gateway is outdoor on the rooftop of another building, Electrical Engineering (EE) building. The two buildings (ACE building and EE building) are not in line of sight (LoS) of each other. Three nodes are setup on adaptive data rate (ADR) while one is on a fixed spreading factor (SF $=$ 12). ADR adapts the SF value assigned to the end device depending on the channel quality [3]. We configure one of the nodes to SF-12, an edge-case, that analyzes the performance of the proposed scheme on the largest spreading factor that is used when the channel conditions are at their worst, introducing longer on air times and hence longer off times due to the duty cycle restrictions. This experiment was run for 9 days and 10K RSSI measurements are collected for each node.

Second experimental scenario: As shown in Figs. 2 and 3, the end device and the gateway are approximately 1.3 km apart which represent the long range outdoor link. This scenario is used to evaluate the performance of our proposed scheme in a fully outdoor long range condition covering both static and mobile end devices. The end device in both the static and mobile modes of the scenario have been configured to transmit in spreading factor 12 assuming worst channel conditions. Both the experimental modes for the mentioned fully outdoor long range condition involve the movement or placement of the end device in Hyde Park in Central London

and the gateway located in the same position as that in the first experimental scenario. In the static setup as shown in Fig. 3(b), the end device was placed on a wooden bench in Hyde Park where randomness was introduced by mainly the winds, trees and the activities of the people in the park. As for the mobile setup shown in Fig. 3(c), the end device was carried by a team member who was walking in the compound of Hyde Park at a speed of approximately 1m/s. This mode of experiment introduced disparity/fluctuations between the channel measurements of both the end device and the gateway due to path loss, shadow-fading and small-scale fading. Although the duration of these outdoor experiments were limited to only two hours due to COVID-19 restrictions, the application profile used by the end devices enabled us to collect sufficient RSSI measurements to validate our proposed shared key generation scheme. Next, the attacker model setup is discussed.

The attacker model consists of one Alice (gateway), two Bob nodes, and one Eve. Fig. 2 shows the positioning of the nodes. Two Bob nodes are purposefully used to evaluate the robustness of the proposed scheme under two different attacking configurations. The node 1 and node 4 in rooms 1 and 3 are the two Bob nodes. Node 1 is near the window closer to the gateway than the other nodes, whereas Node 4 is located deep indoors in room 3. An Eve node is put close (8 m away) to the Bob nodes. Node 3 in room 2 is the eve. It is also located close to the window. From here onwards, node 1 is referred to as Bob1 and node 4 is referred as Bob2. The Eve is programmed as LoRa Class C device to overhear both uplink and downlink channels simultaneously. The LoRa Class C applies no restriction for reception, which is helpful for low latency communication. The SF for Eve is changed once every two days because it is unable to operate in ADR. The channel (frequency) for Bob nodes and Eve is fixed to 868.1 MHz by using channel blacklisting, because otherwise eavesdropping may not be possible. In real life, when a Bob node operates in LoRaWAN mode with no channel blacklisting and using ADR, it would almost be impossible for Eve to eavesdrop as the channel is random and the SF is unknown.

B. Performance Analysis

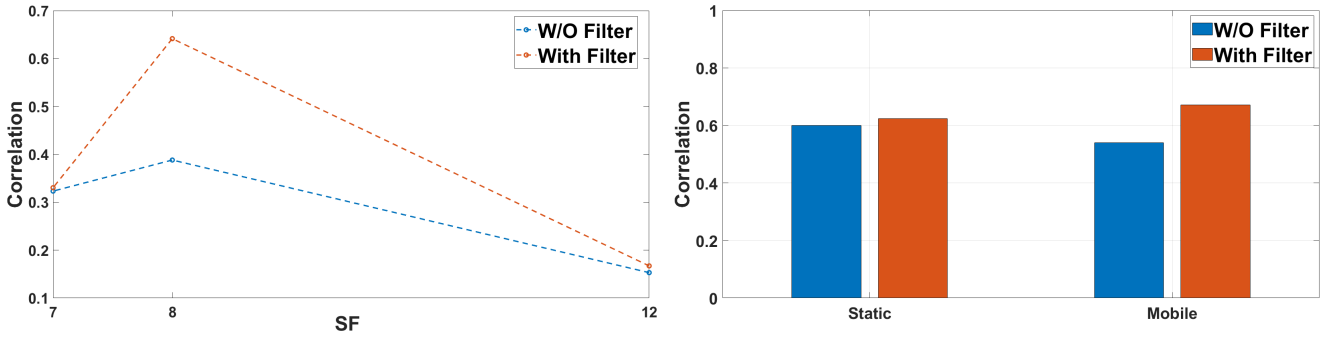
In this section, the results of the proposed LoRa-LiSK scheme are presented. We will first discuss the results of correlation and KDR of both scenarios and then move to KGR and entropy.

First Scenario Results

There are four nodes in the first scenario and all nodes are evaluated based on four metrics namely, randomness and entropy, KGR, KDR and key update time discussed in section IV-B. As there are multiple nodes located in different locations, so there were variations in the RSSI samples of each node. To handle these variations and to reduce the KDR, several preprocessing and filtering techniques were evaluated. Table II lists the KDR obtained with different techniques. At first, the raw RSSI is used directly for key generation but as can be seen, the KDR is very high with $\alpha = 0$ for all nodes but node 2. KDR decreases with $\alpha = 1$, however KDRs of 33% and 67% are still high for nodes 3 and 4. Henceforth, two filtering techniques are applied to test which one decreases the KDR. The techniques would be referred as Filtering 1 and Filtering 2 in the following paragraphs. Filtering 1 is a combination of two preprocessing techniques, namely, moving average window (with window size $= 15$) and channel gain complement (CGC) used in [12]. CGC is applied to reduce the disparity of channel measurements between Alice and Bob. CGC is based on the mean and variance of RSSI samples. As can be observed from Table II, this filtering also did not yield any conclusive results and the KDR remained high for all nodes and in fact it increases from 11% to 27% for node 2 with $\alpha = 0$. Different sizes 10, 15 and 25 of moving average window were also tried but none gave conclusive results. In Filtering 2, three different techniques, namely, time stamp matching, KS-two sample test, and SG low pass filter are applied together. For the KS-two sample test, a threshold of 0.5 is defined. Moreover, the Golay filter is also tested with different polynomial orders and frame lengths. The $sgolayfilt(5, 9)$ function (from MATLAB) produces the most optimal results and is therefore chosen. It can be observed that our chosen techniques significantly reduce the KDR. Henceforth, we proceed to use Filtering 2 with three techniques (i.e., time stamp matching, KS-two sample test, and SG low pass filter) for achieving low KDR. The results of the complete key generation process are presented in what follows.

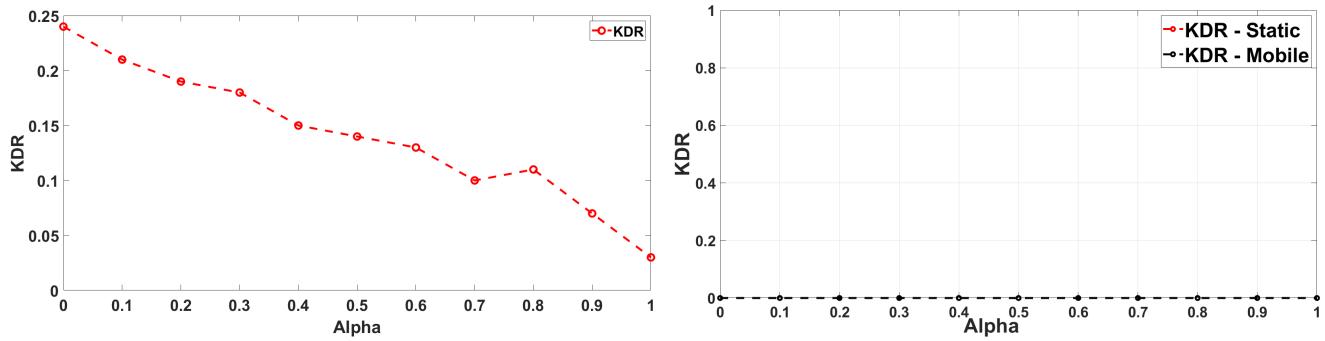
1) Correlation: All nodes have shown good performance, however the results of one of the nodes are presented here to omit redundancy. Fig. 4(a) shows the raw RSSI values (before preprocessing) of Alice and Bob (Node 4) in Fig. 2. It can be observed that the values are close to each other but with some spikes in the gateway samples. Fig. 5(a) shows the correlation between RSSI values of Alice and Bob with respect to different spreading factors in the indoor-to-outdoor experimental scenario. As discussed in section IV-A, three nodes have been setup with the ADR activated. In particular, the node 4 operated on three SFs (i.e. 7, 8 and 12), while the other two nodes operated on ($SF = 7$, 8, 9, 10, and 12). In our experimental data sets, the nodes were never assigned to the whole range of the SF values $\{7, 8, \ldots, 12\}$. This restriction is due to the ADR as the selection of SF is based on environmental conditions. Under stable channel conditions, the end device may not operate with all SFs. It can be observed that the correlation of the raw RSSI is low, and the highest is 0.38. The SG filtering has significantly improved the correlation and for $SF = 8$, it has increased from 0.35 to 0.65. Additionally, in both outdoor scenarios, the correlation is generally good for raw RSSI and slightly improved by filtering. Next, the results of KDR are presented.

2) Key Disagreement Rate: Fig. 6(a) shows the KDR between Alice and Bob. It can be observed that KDR is decreasing with increasing values of α in equation 5. The highest KDR is 0.23 when $\alpha = 0$, and the lowest is 0.03 with $\alpha = 1$. This is an expected behaviour of multi-level quantization, and as the guard band to data ratio is increasing the RSSI measurements are being quantified to the same levels/values based on their probability distributions. Additionally, a BCH code $(255, 63, 30)$ is used in the information reconciliation step meaning that it can correct up to 30 errors in a codeword



(a) Indoor-to-Outdoor Scenario (b) Outdoor Static and Mobile Scenarios

Fig. 5: RSSI Correlation between Gateway and End Devices versus Spreading Factor for Node 4



(a) Indoor-to-Outdoor Scenario (b) Outdoor Static and Mobile Scenarios

Fig. 6: KDR versus α in Indoor and Outdoor Experiments for Node 4

of length 255. The message/key length is 63.

The ECC code is carefully chosen after experimenting with several BCH code lengths. Since the experimental evaluation involves multiple end devices with different KDR with the gateway. For instance, in case of node 1, more than 70% of the RSSI measurements have mismatches in the range of 1 to 15, which can be easily corrected by applying a BCH code of $(127, 29, 21)$ with a syndrome of just 98 bits. Likewise, for nodes 2 and 4, approximately 60% to 70% RSSI measurements have mismatches in the range of 3 to 15. The mismatches for node 3 were slightly higher, and the smallest number of error bits was 12. However, more than 40% of measurements have mismatches between 13 and 30. Henceforth, we must choose a BCH code that can correct mismatches resulting in the lowest possible KDR and uniform success ratio for all devices and not give Eve freedom to derive the key. In other words, we have to select an optimal ECC code that does not compromise the security of the proposed scheme. So, we have decided to use the BCH $(255, 63, 30)$ code. The key blocks of node 3 having mismatches ≥ 30 would be dropped, and the channel probing would start again. The same applies to other nodes.

Second Scenario Result

Next, the results of outdoor LoRaWAN scenarios are discussed. Figures 4(b) and (c) show the RSSI measurements in static and mobile outdoor setups. It can be observed that compared to static indoor to outdoor scenario, there are more fluctuations in RSSI in both outdoor setup. Also, the mobile outdoor has more variations than static outdoor. Figures 5(b) and (c) show the correlation of end device and gateway in outdoor static and mobile setups, respectively. In static outdoor environment, the correlation is 0.6 which is remarkably greater than the highest correlation (0.38) observed in first scenario. Likewise, the correlation in outdoor mobile environment is 0.55 which has further improved to 0.68 after Golay filtering. Precisely, before filtering, the correlation of static environment was higher than mobile. However, after filtering the correlation of mobile environment is higher than static. Fig. 6(b) shows the KDR of both outdoor setups. It can be observed that KDR is 0% meaning that the RSSI measurements of Alice and Bob are quantized to same bits. Even if there were some mismatches they are successfully corrected by our chosen BCH code.

3) Key Generation Rate: In this section, KGR with respect to the spreading factor is discussed. With Multi-level quantization (4-level in our case), one RSSI measurement is always converted into two bits. However, the KGR varies with the spreading factor. The channel coherence time T_c increases with a high spreading factor as the symbols take longer to be transmitted from sender to receiver. In our experiments, when a node is running on ADR, the spreading factor is selected based on the environmental conditions. Fig. 7(a) shows the KGR achieved by node 1 in the first scenario for different spreading factors. In the second scenario, the KGR is 0.5. Due to COVID-19, the outdoor experiments were run for shorter time period and with a fixed $SF = 12$. It can be observed

TABLE III: P Values of NIST Statistical Test

NIST Test	Value
Frequency	0.99
FFT	0.53
Longest Run	0.21
Linear Complexity	0.73
Block Frequency	0.91
Cumulative Sums	0.35
Approximate Entropy	0.73
Non Overlapping Template	0.53

that all spreading factors achieve a KGR of 0.5 at least. The KGR is the highest with $SF = 12$ and the lowest 0.52 with $SF = 10$. It is underlined that all other nodes also achieve similar KGR but the number of spreading factors they adapt to varies.

4) Randomness and Entropy: Another property that is essential for generating robust secret keys is the randomness. A secret key must be truly random and the randomness is calculated based on the Shannon's information entropy. The entropy is calculated before and after the last step, privacy amplification of key generation process. Fig. 7(b) shows the entropy of secret key shared between node 2 and Alice in the first scenario. The entropy values before and after privacy amplification are plotted. One entropy value represents the entropy of one shared secret key. It can be observed that entropy of secret key before privacy amplification is between 0.6 and 1 meaning that the key is random and cannot be guessed by an adversary. Overall, the entropy for most of the keys is between 0.75 to 0.99 which indicates that our proposed scheme can generate the keys with high entropy. Additionally, SHA-256 (SHA-2) hash function is used in privacy amplification step for generating the final secret key. It can be seen that the chosen hash function is further increasing the entropy and it is approaching 1 for some keys. It is underlined that the hash function does not decrease the key generation rate. SHA-256 produces an output of 32 bytes, so first 16 bytes can be used as the secret key.

Apart from entropy, the secret keys are also tested for randomness based on the statistical test suite proposed by NIST [33]. This test is also carried out before privacy amplification step. A truly random sequence must pass the recommended tests namely, frequency, block frequency, cumulative sum, linear complexity, approximate entropy, etc. Each test returns a p-value indicating the probability of randomness and to pass the test, it must be greater than 1%. Table III lists the p-values in the indoor to outdoor scenario for each of the tests obtained from the secret keys generated from LoRa-LiSK scheme. It can be seen that p-values of all tests except longest run and cumulative sums are greater than 50%. The values for these tests are also 21% and 35%, respectively, meaning that they also passed the set randomness criteria of 1%.

C. Security Analysis

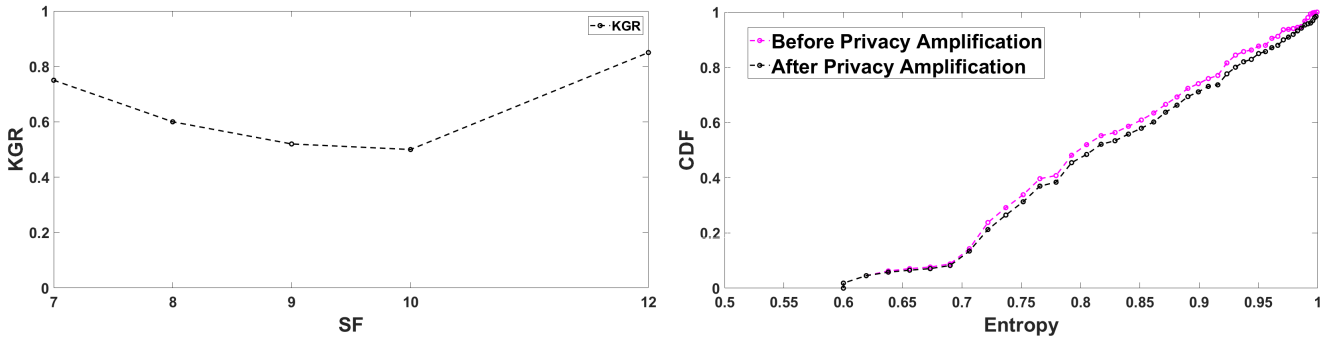
In this section, the security of the LoRa-LiSK scheme is evaluated by analysing if a passive eavesdropper (Eve) can obtain the same key as the Alice and Bob. It is underlined that the attacker model is only evaluated in the first scenario, static indoor-to-outdoor. The security analysis is based on three overhearing scenarios. All attacking scenarios are run for 7 days to collect the overhearing logs. In the first two overhearing scenarios, Alice, Bob1, and Eve are configured to run on $SF = 7$ and $SF = 12$ respectively. In the third scenario, Alice and both Bob nodes are configured to run on ADR and Eve is configured to run on one specific SF for one day. The spreading factor of Eve is changed every day. It is underlined that in ADR mode, Bob1 operates on SF = $\{8, 9, 12\}$, while Bob2 operates on SF = $\{7, 8\}$. The operation in a few spreading factors is due to the static environmental conditions. Due to Covid-19, the offices were empty and the randomness that could be introduced due to moving people was also missing. It is underlined that Eve can hardly overhear Bob2 and therefore the logs could only be collected for SF = $\{7, 8\}$. For $SF = 9$ and $SF = 12$, Eve did not overhear enough packets required to generate a key.

Figures 8(a) and (b) show the RSSI values of Alice, Bob1, and Eve in $SF = 7$ and $SF = 12$, respectively. It can be observed that the RSSI measurements of Alice and Bob1 are close to each other. Additionally, the RSSI of Bob1 and Eve uplink are also correlated to each other. However, the downlink of Eve is highly uncorrelated to all other RSSI measurements. The same pattern can be observed in case of $SF = 12$. However, there are a bit more fluctuations this time. These figures also explain the reasons of low correlation between the Alice and Eve, and Bob1 and Eve.

TABLE IV: Correlation in Attacking Model

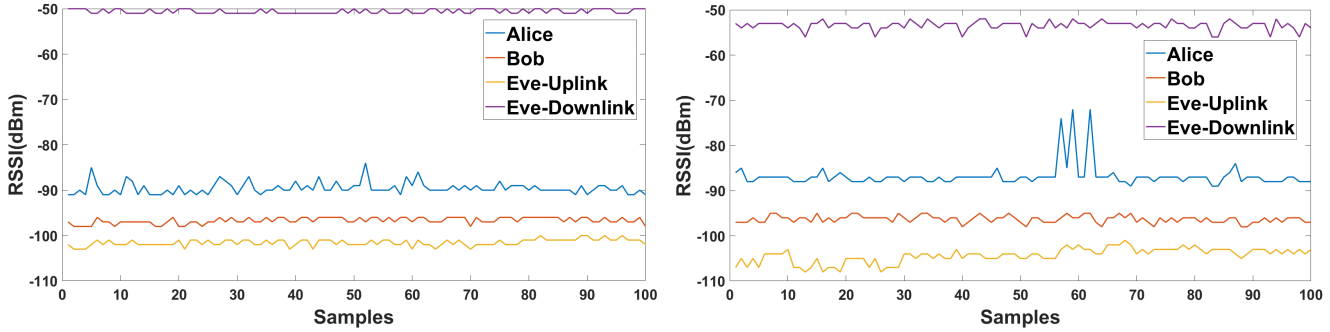
Eve Setup	SF-7	SF-8	SF-9	SF-12
Eve Overhearing Alice and Bob1 - ADR				
Alice-Bob	N/A	0.12	0.11	0.04
Alice-Eve	N/A	0.05	-0.01	0.2
Bob -Eve	N/A	-0.03	-0.05	0.01
Eve Overhearing Alice and Bob2 - ADR				
Alice-Bob	0.039	0.04	N/A	N/A
Alice-Eve	0.083	0.15	N/A	N/A
Bob -Eve	-0.03	0.17	N/A	N/A

Table IV lists the correlation between the real RSSI measurements of Alice and Bob nodes and those overheard by Eve. It is noted that none of the Bob nodes operated with SF = $\{10, 11\}$, as there are no results for them. First, the correlation results of Bob1 node with respect to different SFs are discussed. Bob1 did not operate in SF=7. For SF=8, the correlations between Alice and Bob1, Alice and Eve, and Bob1 and Eve, are 0.12, 0.05, and -0.03, respectively. Likewise, in case of SF=9, the correlation values are 0.11, -0.01, and -0.05. For SF=12, the correlations are 0.04, 0.2, and 0.01. Similarly, when Eve is overhearing Bob2 for $SF = 7$, the correlations between Alice and Bob2, between Alice and Eve, and between Bob2 and Eve, are 0.03, 0.083, and -0.03, respectively. The correlation values of Bob2 in SF=8 are 0.04, 0.15, and 0.17. These values are comparatively higher than the other correlation values. Overall, the correlation is very low as expected. Table V lists the bitwise KDR between the keys generated from Alice and Bob, and from Alice and Eve. The KDR values are obtained before privacy amplification. It can be observed that in case of Bob1, the KDR is $22\%, 32\%$ and 35% for SF=8, SF=9, and SF=12, respectively. For Bob1, the



(a) KGR versus SF (b) Information Entropy

Fig. 7: KGR and Entropy in Indoor-to-Outdoor Experiment



(a) $SF = 7$ (b) $SF = 12$

Fig. 8: RSSI values of Alice, Bob, and Eve in different attacking scenarios

TABLE V: KDR in Attacking Model

Eve Setup	SF-7	SF-8	SF-9	SF-12
Bob1 and Eve	N/A	22%	32%	35%
Bob2 and Eve	30%	25%	N/A	N/A

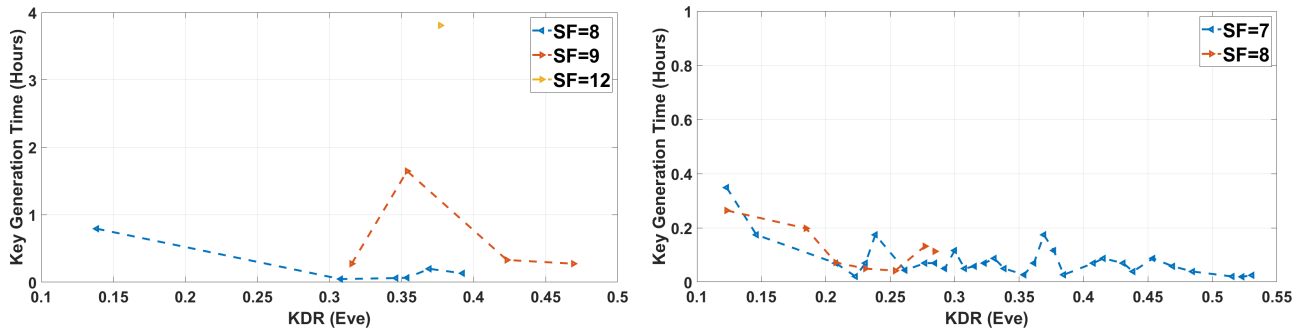
KDR is increasing with increasing spreading factor. The KDR for Bob2 and Eve is also listed in Table V. KDR is 30% and 25% for SF=7 and SF=8, respectively. The KDR further increases after privacy amplification and henceforth, the Eve cannot generate the same key as Alice and Bob. The above results highlight the robustness of our proposed LoRa-LiSK scheme.

D. Key Update Time and Communication Overhead

In section I, we discussed that existing symmetric and asymmetric schemes are not suitable for large scale WSNs. Additionally, the security vulnerabilities in the ABP joining procedure of LoRaWAN are also discussed. These challenges underpin the need of proposing lightweight and robust security schemes such that new keys can be generated without incurring additional overhead. Frequent key updates guarantee that sensor data is secure and cannot be corrupted by malicious adversaries. In this section, the timing and memory overhead of the key generation process are discussed.

T_{key} is computed using eq. 11 presented in section III-F4. As T_{key} is computed based on the KDR, so the attacker model is exploited for it. Figures 9 (a) and (b) show T_{key} for Bob1 and Bob2 nodes versus KDR. It can be observed that T_{key} increases while decreasing KDR. Additionally, T_{key} also increases with a high SF value. The highest T_{key} for $SF = 8$ is 0.79 hours (47 mins) with $KDR = 0.13$. Likewise, T_{key} for $SF = 9$ is 1.64 hours (98 mins). Bob1 takes the highest $T_{key} = 3.8$ hours when $SF = 12$. T_{key} results for Bob2 can be observed in Fig. 9 (b). The highest T_{key} happens for $SF = 7$ and is 0.34 hours. Overall, it is concluded that T_{key} obtained in this study are low and better than reported by other studies [7]. Without the attacker model, the average T_{key} is approximately one hour with duty cycle. T_{key} depends upon the frequency of uplink and downlink packets, a high frequency can result into low key update time and vice versa.

Next, the communication overhead of each step in the key generation process is discussed. The channel probing does not introduce any communication overhead as the probe and request packets are exchanged as part of the normal LoRaWAN operation. The packet synchronization is achieved by the time stamp matching technique introduced in section III-A. The end device records both T_u and T_d, if the downlink is received within one or two seconds of sending the uplink, the downlink is marked as matching with the uplink packet otherwise the packet is retransmitted. T_u and T_d enable packet synchronization without incurring any communication overhead. Additionally, for the KS-two sample test, a fixed threshold of 0.5 is defined and agreed. Both end device and



(a) Bob1 (b) Bob2

Fig. 9: Key Update Time versus ADR

gateway utilize only those measurements which meet the set criteria. The SG filter is also executed on predefined parameters and does not require any packet exchange. The multi-level quantization is also executed individually and does not incur any communication overhead. After the quantization, the end device will encode the key bits and send the generated code word to the gateway. Sometimes there were more mismatches between the quantized key bits so, a BCH code $(255, 63, 30)$, with a higher t is used. At this stage, the communication overhead is determined based on the packet payload and the packet delivery ratio (PDR). The overhead for both scenarios is discussed below. Each packet has a payload of 20 bytes and the PDR in the first scenario is approximately between 90% to 95%, henceforth 4 to 5 packets (72 to 76) bytes are sent. In the second scenario, the PDR is 70% meaning that 5 to 6 uplink packets (75- 80) bytes are sent. This overhead estimation is the upper bound and represents the worst case scenario with a high number of mismatches. Lastly, in privacy amplification, a hash function is applied that does not incur any overhead.

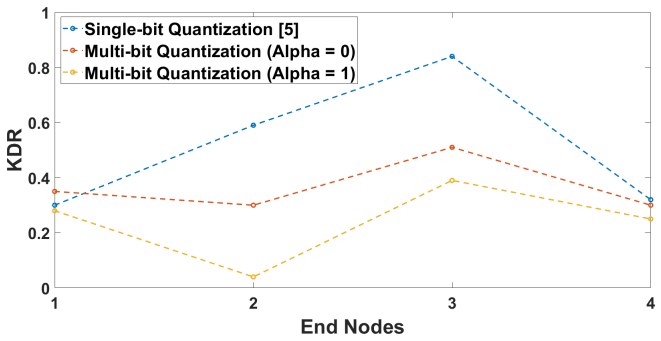


Fig. 10: Comparison of Quantization Techniques

E. Comparative Analysis

In this section, LoRa-LiSK is compared with relevant existing schemes [6]–[8] to show the compatibility with the state of the art. Firstly, the above mentioned schemes including the proposed are compared based on their experimental configurations, and secondly the LoRa-LiSK scheme is compared with an existing work [7]. Table VI lists the parameters, namely, deep in-building penetration, outdoor range, spreading factors, bandwidth, transceivers, antennas, signalling, communication scenarios, quantization, and preprocessing techniques chosen for comparison. It can be observed that the LoRa-LiSK scheme is evaluated on same parameters as used by other studies, thus making it compatible with the state of the art. Besides that it can be analyzed that the LoRa-LiSK scheme is tested in all possible configurations whereas the other schemes are not. For instance, it is evaluated in deep in-building scenario but [6] is not. Additionally, this scheme is evaluated in both static and mobile scenarios whereas [7] and [8] are not. All above schemes require high correlation for secret key generation whereas the LoRa-LiSK scheme can generate keys with low correlations. Our first experimental scenario is based on indoor-to-outdoor configuration making it more practical than fully indoor or outdoor scenarios. It is underlined that LoRa-LiSK is the only scheme which is evaluated in indoor to outdoor scenarios which is more challenging and also more typical of real-world scenarios. Lastly, compared to the other schemes, our scheme uses ADR for selection of SF based on environmental conditions rather than fixing it initially. ADR informs about the channel conditions namely reciprocity, randomness, and signal-to-noise ratio, which in turn assist in evaluating the performance of the secret key generation. The LoRa-LiSK scheme is evaluated by activating the ADR. Precisely, the ADR is deactivated in other schemes.

Next, the LoRa-LiSK scheme is compared with [7] based on low correlation and KDR. The work in [7] is based on highly correlated RSSI vectors. However, the correlation between RSSI measurements of the end devices and the gateway in our dataset is low. The efficiency of the LoRa-LiSK scheme to generate the secret key from low correlated channel measurements has already been demonstrated in section IV-B. Next, both the schemes are compared based on KDR. Fig. 10 shows the KDR obtained by applying the single-bit quantization scheme introduced in [7]. The single-bit quantization is different from the multi-bit quantization and is based on the mean (μ) and standard deviation (σ) of the RSSI measurements [10]. The measurements are quantized as follows.

$$\eta+ = \mu + \alpha \times \sigma$$
$$\eta- = \mu - \alpha \times \sigma$$

All measurements $\geq \eta+$ are quantized to 1 while those

TABLE VI: Comparative Analysis with Existing Studies

Parameters	[6]	[7]	[8]	Our Scheme
Deep in-building Penetration	No	Yes	Yes	Yes
Outdoor Range	4 km	7 km	500 m	1.3 km
Spreading Factors	7	12	7	ADR - SF = {7,8,9,10,11,12}
Bandwidth	500	125	125	125
Transcievers	2xSX1276	SX1276, SX1301 and SX1257	2xSX1276	FiPy with LoRa Transceiver
Antennas	Monopole	ESPAR and Monopole	Monopole	Monopole
Signalling	LoRa	LoRaWAN	LoRa	LoRaWAN
Communication Scenarios	Static and Mobile	Static	Mobile	Static and Mobile
Quantization Technique	Multi-lbit	Single-bit	Single-bit	Multi-bit
Preprocessing Techniques	SG Filter and Linear Interpolation	KS Test, Packet Number Matching, and DCT	None	Time Stamp Matching, KS Test, and SG Filter
Correlation Requirements	High	High	High	Low

$\leq \eta-$ are to 0. The comparative analysis is based on the first scenario consisting of four nodes. It can be observed that KDR is much higher with single bit quantization with node 3 having 80% key disagreement. Comparing the results with our multi-bit quantization, it can be observed that LoRa-LiSK scheme is performing better even with $\alpha = 0$, with the highest KDR being 42% for node 3. The proposed scheme shows the best performance with $\alpha = 1$. The lowest KDR is approximately 5% and the highest being 30% for nodes 2 and 3 respectively. Overall, the KDR of node 3 is always higher than the other nodes. Study in [7] uses a BCH code (127, 23,22) in the information reconciliation step. Having less mismatches between quantized key bits, the chosen code can correct up to 23 bits in a code word of 127 bits. However, in our case, there were more mismatches and therefore a $BCH(255, 63, 30)$ code with $t = 30$ is selected. The above results exhibit that the LoRa-LiSK scheme is performing better than all the existing state-of-art schemes.

V. Discussion and Conclusion

In this paper, a secret key generation scheme is proposed for LoRaWAN networks. The scheme outperforms the existing schemes in several important ways; low correlation, low KDR, and high KGR. In LoRa-LiSK scheme, secret keys can be generated with low correlation meaning that its feasible to secure information in deep indoor to outdoor and long range link scenarios wherein the highly correlated RSSI measurements might not readily available. The evaluation is carried out in real-world practical application use cases, with four end devices covering indoor-to-outdoor, and long range outdoor configurations. This scheme achieves low KDR compared to existing studies. With high KDR, the key generation process can fail because a large number of mismatching bits cannot be corrected in information reconciliation step. Additionally, the code size has a trade off with the correction capability t of the BCH code (n, k, t). These factors put constraints on the choice of error correction techniques and also impact the communication overhead. Precisely, a larger BCH code can correct more mismatches but it adds to the communication overhead which is undesirable for resource constrained and low latency sensor systems. Our LoRa-LiSK scheme worked with BCH code with $t = 30$. Additionally, the attacker model is designed to challenge the LoRa-LiSK scheme to its upper bound by testing it in different experimental configurations. The Eve is configured as a class C LoRa device running on ADR (changed every other day) and allowed to eavesdrop on both uplink and downlink channels. It is placed at a distance of 8 meters from two Bob nodes and has the freedom to listen to any Bob node of its choice in a bid to generate the same key as Alice and the Bob node. We are aware that this scenario is beyond what can happen in reality but our goal was to challenge our scheme to its extremity. Fortunately, the inability of Eve to generate the same key as Alice and Bob gives us the confidence about the robustness of the proposed scheme.

The above advantages underline that our proposed LiSK scheme is not only efficient and lightweight, but also robust and universal. To further analyze the strengths of our scheme, we aim to evaluate it in a few other scenarios, 1) with large number of static and mobile nodes in outdoor locations, 2) under different attacking configurations, and 3) with other LPWAN technologies. The low KDR of 0% in our static and mobile outdoor experiments guarantees that the LoRa-LiSK scheme will produce similar results with larger datasets. The scheme will be further evaluated in outdoor experiments over longer duration (e.g. one to two weeks) with large number of static and mobile nodes. The impact of other channel parameters, namely, randomness, ADR, path loss, and shadow fading for long range outdoor links will be analyzed. The results of current attacker model give us the confidence that it will perform well in outdoor modes with varying environmental and experimental configurations. In line with this, the attacker model will also be evaluated in outdoor scenarios with larger number of static and mobile nodes. Lastly, we aim to propose security schemes for other LPWAN technologies, namely, NB-IoT and Sigfox. Our LoRa-LiSK scheme can be directly applied to the other LPWAN technologies as long as the source of randomness (RSSI values) is the same or has similar probabilistic behavior. If the source of randomness has a different type of distribution, our scheme needs revision only at the level of channel probing and the preprocessing techniques. For the other steps of quantization, information reconciliation and privacy amplification, we believe they are robust enough to adapt to other LPWAN technologies.

ACKNOWLEDGMENT

This work is partially supported by two EPSRC grants, Science of Sensor Systems (S4) programme (EP/N007565/1), and PETRAS Logistics 4.0 project (EP/S035362/1). The authors would like to thank the anonymous reviewers for their helpful and constructive comments.

REFERENCES

[1] "Dynamic key management algorithms in wireless sensor networks: A survey," *Computer Communications*, vol. 134, pp. 52 – 69, 2019.

[2] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 855–873, Secondquarter 2017.

[3] L. Alliance. Lorawan® specification v1.1. [Online]. Available: https://lora-alliance.org/resource-hub/lorawanr-specification-v11

[4] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of lora," in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, 2017, pp. 1–6.

[5] C. T. Zenger, M. Pietersz, J. Zimmer, J. Felix Posielek, T. Lenze, and C. Paar, "Authenticated key establishment for low-resource devices exploiting correlated random channels," *Computer Networks*, vol. 109, pp. 105 – 123, 2016, special issue on Recent Advances in Physical-Layer Security.

[6] W. Xu, S. Jha, and W. Hu, "Lora-key: Secure key generation system for lora-based network," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6404–6416, 2019.

[7] H. Ruotsalainen, J. Zhang, and S. Grebeniuk, "Experimental investigation on wireless key generation for low-power wide-area networks," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1745–1755, 2020.

[8] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: Lora-based key generation in low power wide area networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12 462–12 466, 2018.

[9] L. Alliance. (2020) Why lorawan is the connectivity platform for smart city applications. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/LA-WhitePaper-SmartCities-0520-v1.pdf

[10] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[11] P. Van Torre, T. Castel, and H. Rogier, "Encrypted body-to-body wireless sensor node employing channel-state-based key generation," in *2016 10th European Conference on Antennas and Propagation (EuCAP)*, 2016, pp. 1–5.

[12] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *2013 Proceedings IEEE INFOCOM*, 2013, pp. 3048–3056.

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

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

[15] W. Xi, C. Qian, J. Han, K. Zhao, S. Zhong, X.-Y. Li, and J. Zhao, "Instant and robust authentication and key agreement among mobile devices," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 616–627.

[16] M. H. Chinaei, V. Sivaraman, and D. Ostry, "An experimental study of secret key generation for passive wi-fi wearable devices," in *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2017, pp. 1–9.

[17] A. Sadeghi, M. Zorzi, and F. Lahouti, "Analysis of key generation rate from wireless channel in in-band full-duplex communications," in *2016 IEEE International Conference on Communications Workshops (ICC)*, 2016, pp. 104–109.

[18] M. Jafari Siavoshani, S. Mishra, C. Fragouli, and S. N. Diggavi, "Multi-party secret key agreement over state-dependent wireless broadcast channels," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 323–337, 2017.

[19] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Channel frequency response-based secret key generation in underwater acoustic systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 5875–5888, 2016.

[20] TTN. (2021) Building a global open lorawan network. [Online]. Available: https://www.thethingsnetwork.org

[21] L. Alliance. (2021) Lora alliance. [Online]. Available: https://lora-alliance.org/

[22] *Kolmogorov–Smirnov Test*. New York, NY: Springer New York, 2008, pp. 283–287.

[23] A. Savitzky and M. J. E. Golay, "Smoothing and differentiation of data by simplified least squares procedures." *Analytical Chemistry*, vol. 36, no. 8, pp. 1627–1639, 1964.

[24] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *2010 Proceedings IEEE INFOCOM*, 2010, pp. 1–9.

[25] "9 bch codes," in *The Theory of Error-Correcting Codes*, ser. North-Holland Mathematical Library, F. MacWilliams and N. Sloane, Eds. Elsevier, 1977, vol. 16, pp. 257 – 293.

[26] I. S. Reed and X. Chen, *Reed-Solomon Codes*. Boston, MA: Springer US, 1999, pp. 233–284.

[27] *Low-Density Parity-Check Codes*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 37–59.

[28] M. F.J. and S. N.J.A., *An Introduction to the binary Golay Code*. North Holland: Elsevier Science, 1983, pp. 1–782.

[29] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[30] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol cascade," *Quantum Info. Comput.*, vol. 15, no. 5–6, p. 453–477, apr 2015.

[31] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometricsand other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, p. 97–139, 2008.

[32] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, p. 198–208, Sep 2006.

[33] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Tech. Rep., 2013.

[34] P. Ltd. (2018) Fipy datasheet. [Online]. Available: https://pycom.io/wp-content/uploads/2018/03/Pycom 002-Specsheets-FiPyv2.pdf

A. K. Junejo is a Research Associate in the AESE research group at Imperial College London, UK. She received her PhD degree in Computer Science from City, University of London, UK in 2019. She is currently researching the security of sensor based systems as part of the Logistics 4.0 and S4 projects funded by Petras and EPSRC. Dr Junejo is interested in designing lightweight security solutions for resource-constrained sensors and Internet of Things (IoT) devices. She has been working on physical layer security (PLS) encryption schemes. Her research interests include but not limited to the security, privacy and trust of cyber-physical systems, wireless sensor networks, cloud computing, fog computing, and applied cryptography.

F. Benkhelifa Dr. Fatma is a research fellow in the AESE research lab at Imperial College London since 2018. She obtained her PhD in Electrical Engineering in 2017 from King Abdullah University of Science and Technology (KAUST), Saudi Arabia. She also obtained her Master of Science from KAUST in January 2013. She graduated as a Polytechnician engineer from "Ecole Polytechnique de Tunis" with major in Signals and Systems. Her research interests include, but not limited to, the scalability and coverage of low power wide area networks via resource management algorithms, stochastic geometry-based analysis, and spatiotemporal modelling of wireless sensor networks.

B. Wong Boon Wong is a PhD student under the supervision of Prof. Julie A. McCann. Under the Land and Liveability National Innovation Challenge (L2NIC) Research Programme funded by Singapore Ministry of National Development and the National Research Foundation, he is involved in the development of smart city solutions to enhance the performance of key electrical and mechanical services, optimise maintenance regimes and minimise service disruptions. His works are mostly focused on devising robust low-cost sensor networks in built environment to expand the capabilities of sensor networks and predictive analytics in densely populated housing estates.

Julie A. McCann (M'16) is a Professor in Computer Systems with Imperial College London. Her research centres on decentralized and self-organizing schemes for spatial computing e.g., Wireless Sensor systems, Internet of Things, or Cyber-physical systems. She leads the Adaptive Embedded Systems Engineering Research (AESE) Lab , is Deputy Director for the UK-wide PeTraS Centre for IoT Cyber-security, and until recently co-directed the Intel Collaborative Research Institute for Sustainable Cities. She has received significant funding though national and international bodies such as the UK's EPSRC, EU FP7/H2020 funding and Singapore NRF; she has a sub-lab in Singapore with I2R and HDB. Prof McCann is an Elected Peer for the EPSRC, serves on/chairs/AE for the top international conference committees and journals in the field, and is a Fellow of the BCS and Chartered Engineer.