Design of an Efficient OFDMA-Based Multi-User Key Generation Protocol

Junqing Zhang, Ming Ding, *Senior Member, IEEE,* David López-Pérez, *Senior Member, IEEE,* Alan Marshall, *Senior Member, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Secret key generation exploits the unique random features of wireless channels, hence it is eminently suitable for the resource constrained Internet of Things applications. However, it has only been involved for single links between a pair of users, whilst there is a paucity of literature on group and multi-user key generation. This paper proposes an orthogonal frequency-division multiple access (OFDMA)-based multi-user key generation protocol to efficiently establish keys in a star topology. The uplink and downlink multi-user access facilitated by OFDMA allows the central node to simultaneously communicate with multiple users, which can significantly reduce the channel probing overhead. In particular, we provide a compelling case study of multi-user secret key generation by designing a prototype based on IEEE 802.11ax, a new Wi-Fi standard to be released. Our simulation results have demonstrated that the OFDMA-based multi-user key generation protocol incurs low interference amongst the users, whilst benefiting from channel reciprocity and generating unique random keys.**

***Index Terms*—Physical layer security, group key generation, multi-user key generation, multi-user access, OFDMA, IEEE 802.11ax**

I. Introduction

The Internet of Things (IoT) has significantly transformed our lives with ubiquitous connections among devices, the environment and people, which has triggered many exciting applications such as smart homes, smart cities, healthcare, etc. While the IoT brings convenience to our everyday life, it also introduces potential problems, since it is prone to the lack of data confidentiality. Secure connections are thus essential to the provision of reliable and confidential communications [1].

Wireless communications are usually protected by conventional cryptography, which requires a common key shared between the communication parties, e.g. by using public key cryptography (PKC). PKC is widely used to protect communications and computer networks, but its application in the future IoT may be challenging for several reasons. Firstly, PKC is computationally demanding, which is not suitable for low-cost devices. Moreover, PKC is designed based on computationally complex mathematical problems, such as integer factorization and discrete logarithms, which may be cracked by the emerging quantum computers [2].

Automatic key generation based on the randomness of wireless channels has been identified as a promising alternative to establishing cryptographic keys [3]. This technique generates keys between a pair of legitimate users with no assistance from a third party. Using a lightweight procedure, compared to the popular elliptic curve-based Diffie-Hellman (ECDH) PKC scheme, the results in [4] indicate that an ECDH protocol dissipates about 100 times more energy and imposes about 1000 times higher complexity than the key generation counterpart, when both are implemented by an 8-bit Intel MCS-51 micro-controller. Key generation has also been proved to be information theoretically-secure, as it relies on the unpredictable random wireless channels [5]. Thus, this technique is particularly suitable for low-cost and resource-constrained devices.

Network nodes can be arranged in different topologies, e.g. star and mesh topologies, depending on their specific applications. However, the star topology has become more popular, since it is easy to maintain, and hence has been used in numeral networks, such as Wi-Fi, cellular, LoRaWAN, etc., where a central controller[1] coordinates the connections of a number of devices.

In the considered star topology, the central controller may want to broadcast securely to all the network nodes, which requires a common group key shared among all the communication parties. In other scenarios, the controller may have to transmit unicast messages securely to each device, which will require different private session keys established between the controller and each device. Key generation has been mainly applied to pairs of users [4], [6]–[16]. Substantial research efforts have been invested in designing group key generation [17]–[21], but channel probing still has to be carried out in a pairwise manner, which imposes substantial cost in terms of the number of transmissions and channel occupation. How to assign these keys in an efficient and secure manner at a low communication overhead is still an open question.

Manuscript received xxx xx, 2019; revised xxx xx, 2019; accepted xxx xx, 2019. Date of publication xxx xx, 2019; date of current version xxx xx 2019. The work of L. Hanzo was supported by the EPSRC projects EP/N004558/1, EP/P034284/1, the Royal Society's GCRF Grant as well as the European Research Council's Advanced Fellow Grant QuantCom. The associate editor coordinating the review of this paper and approving it for publication was xxx xxx.

J. Zhang and A. Marshall are with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk; alan.marshall@liverpool.ac.uk)

M. Ding is with Data61, CSIRO, Australia (e-mail: Ming.Ding@data61.csiro.au)

D. López-Pérez is with Nokia Bell Labs, Ireland (email: david.lopezperez@nokia-bell-labs.com)

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (email: lh@ecs.soton.ac.uk).

Digital Object Identifier xxx

[1]The name of the controller will differ according to the specific techniques, such as access point (AP), base station, and gateway in the Wi-Fi, cellular, and LoRaWAN systems, respectively.

To address this open problem, we consider multi-user key generation in a star topology. Multi-user access can be realized in the code, frequency and spatial domains. In particular, code-division multiple access (CDMA) allocates user-specific orthogonal codes to different users as in 3G UMTS, while orthogonal frequency-division multiple access (OFDMA) allocates orthogonal frequency resources to different users as in 4G LTE. Instead, IEEE 802.11ac, based on orthogonal frequency-division multiplexing (OFDM), uses neither code- nor frequency-domain user separation, but multi-antenna technology and allocates unique user-specific spatial streams for supporting downlink (DL) multi-user transmissions. However, key generation requires bidirectional transmissions to obtain correlated channel measurements, which poses some challenges/restrictions for the above multi-user techniques, when it comes to key generation.

IEEE 802.11ax [22] constitutes a new Wi-Fi standard amendment to be released in 2019, which supports both DL and uplink (UL) multi-user transmissions by using OFDMA in the same channel. In this paper we design for the first time an efficient OFDMA-based key generation protocol to simultaneously establish keys between the AP and a number of stations[2], whilst relying on the IEEE 802.11ax features. In particular, our contributions are as follows.

- An efficient multi-user key generation protocol is proposed by employing OFDMA. The UL and DL multi-user access supported by OFDMA allows multiple channel measurements to be carried out at the same time, which significantly reduces the channel probing overhead.
- An IEEE 802.11ax-based case study is carried out and extensive simulation results are presented. The proposed protocol can be implemented in the context of the standard IEEE 802.11ax system, with no standard modifications required. The simulation results demonstrate that the proposed multi-user key generation protocol has a good performance in terms of imposing low interference on the users, whilst benefiting from a high degree of channel reciprocity as well as from a unique key.

The rest of the paper is organized as follows. Section II introduces the related work on multi-user/group key generation protocols. Section III proposes an OFDMA-based multi-user key generation protocol, while an IEEE 802.11ax-based case study is given in Section IV. Our simulation results are provided in Section V while Section VI concludes the paper.

II. Related Work

As shown in Fig. 1, a key generation protocol usually involves four steps, including channel probing, quantization, information reconciliation and privacy amplification [3]. The majority of key generation protocols run between a pair of legitimate users, namely Alice and Bob. In order to obtain correlated channel observations, key generation is usually studied with the aid of systems operating in time division duplexing (TDD) mode, e.g. Wi-Fi [6]–[9], ZigBee [4], [10]–[12], Bluetooth [13], and LoRa [14]–[16], etc.

[2]A station is a device that supports Wi-Fi functions in the Wi-Fi terminology. This paper uses station and user interchangeably.

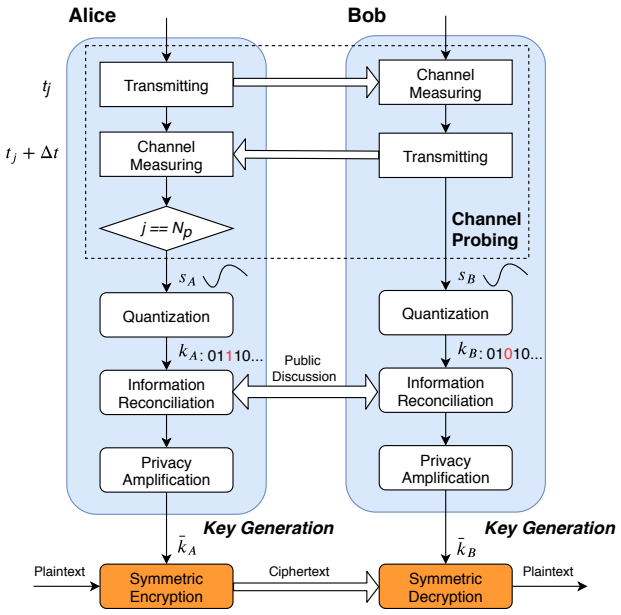

Fig. 1. Key generation protocol and symmetric encryption.

During the channel probing stage, at time t_j and $t_j + \Delta t$, Alice and Bob transmit alternately to each other and obtain measurements, s_A and s_B, respectively. They will repeat the bidirectional measurements N_p times to obtain sufficient data for key generation. Channel reciprocity implies that the channel responses at each end of the link are similar [9], [23], provided that both the transmitting and receiving front-ends are calibrated. Therefore, the channel measurements at Alice and Bob will be highly correlated when the sampling interval, Δt, is kept shorter than the channel's coherence time. At the quantization stage, Alice and Bob will independently convert the channel measurements into binary sequences, k_A and k_B, respectively, by comparing the received signals to some thresholds. The unsynchronized sampling, interference and noise at the receiver will result in mismatch between the quantized key bits. Hence, information reconciliation is then adopted to correct this mismatch by exploiting the correction capability of error correction codes [24]. Finally, privacy amplification is used to remove any possible leakages of the keying information to eavesdroppers and to enhance the security of the key sequences generated, e.g. by using a hash function.

Alice and Bob will then get the same keys, i.e., $\bar{k}_A = \bar{k}_B$. The keys can be used for symmetric encryption to provide secure and confidential data communications [25]. Among the four steps of the key generation, channel probing is the key step of harvesting entropy from the environment and supporting secure communications. Hence we focuses our attention on the design of an efficient channel probing protocol to obtain channel measurements from multiple users at a minimum overhead.

Many wireless networks require secure data exchange among a number of users. There have been a good number of group key generation protocols designed for different network topologies [17]–[21]. Liu *et al.* proposed protocols

for star topologies in order to share a common secret among nodes [17]. Specifically, a central node is first selected and a reference channel, p_{ref}, is calculated between the central node, n_c, and another randomly selected node, n_{ref}. The central node transmits to all the other nodes while the received signal strength at the u^{th} node is p_u^f. The nodes then respond to the central node via the reverse channels, where the signal strength at the central node is p_u^r. Finally, the central node calculates the difference of signal strengths (DOSS) between the reverse channels and the reference channel, $\Delta p_u = p_u^r - p_{ref}$, and transmits the corresponding DOSS to the nodes, which can extract the common secret, namely the reference channel, calculated as $p_u^f - \Delta p_u$. Note that even if the DOSS was observed by an eavesdropper, he or she fails to infer the common secret, since he/she is oblivious of p_u^f. The scheme of Xiao *et al.* [18] was also designed for star topologies but differs from that in [17] in its last step. Instead of calculating the DOSS, the central node calculates the exclusive-OR between the reverse channels and the reference channel to share the common secret. Wei *et al.* proposes a variety of group key generation protocols for different star topologies, including single cluster, independent multi-cluster and overlapped multi-cluster [19]. Finally, Jin *et al.* analyzed the average time that a user has to spend on waiting and completing the key generation process when a central node serves random arrival users [26].

Group key generation protocols have also been conceived for other network topologies. Thai *et al.* proposed a multiple antenna-based protocol for mesh topologies [20]. A pairwise channel sounding is performed between different mesh nodes. Wang *et al.* designed roundtrip channel phase-based group key generation, where the nodes form a circle and channel probing is carried out on a pairwise basis [21]. However, its practical application remained limited because attaining accurate phase estimation is rather challenging.

It is important to note that all the above research efforts have mainly focused on sharing the common secret across a group. However, channel probing still has to be carried out in a pairwise manner. Thus, when there are N_u users, the number of user pairs is $\frac{N_u(N_u-1)}{2}$, and the total number of transmissions is

$$N_t^{\text{pairwise}} = \frac{N_u(N_u-1)}{2} \cdot 2N_p, \tag{1}$$

where N_p denotes the number of times the channel is probed. The resultant complexity is thus in the order of $\mathcal{O}(N_u^2)$ [19].

It is desirable to design an efficient channel probing mechanism for group key generation, in order to reduce communications and timing overhead. This subject has not been extensively investigated in the open literature. Invoking simultaneous multi-user transmission allows a central node to transmit to a number of users at the same time, which alleviates the transmission overhead. The algorithm proposed in this paper significantly mitigates the probing complexity by exploiting OFDMA, namely to $\mathcal{O}(N_u)$.

III. OFDMA-Based Multi-User Key Generation

As shown in Fig. 2(a), OFDM allocates all the available subcarriers to a single user, which can then achieve a high data rate within the given bandwidth. Duplexing is handled in a TDD mode. Therefore, OFDM has been employed for improving the key generation rate by exploiting the randomness both in the time- and in the frequency-domains [27]–[30].

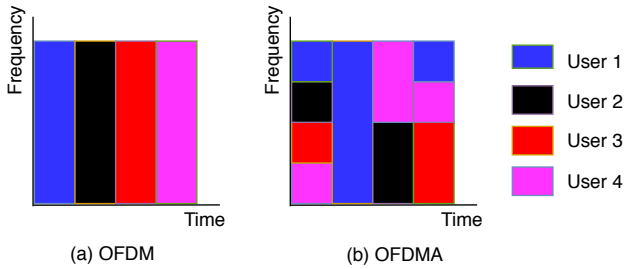

Fig. 2. Comparison of OFDM and OFDMA.

On the other hand, OFDMA allows multiple users to simultaneously access the spectrum by transmitting in orthogonal non-overlapping bands, as illustrated in Fig. 2(b). Since the OFDM subcarriers are orthogonal, there is no interference amongst them. This allows the AP to simultaneously obtain channel measurements of multiple users. Surprisingly, however, this feature has never been exploited for key generation, mainly because OFDMA has never been adopted in Wi-Fi standardization until the recent advent of 802.11ax.

In this paper, we fill the gap and design an efficient multi-user key generation protocol among an AP and multiple users by exploiting this beneficial OFDMA feature.

A. Channel Model

This paper investigates an OFDMA-based star topology network, where an AP simultaneously generates keys with multiple users based on their random wireless channels. The system model exemplified by four stations is illustrated in Fig. 3. We assume that the wireless channels between the AP and each user are independent where the channel between the AP and the u^{th} user, $h_u^{dir}(\tau,t)$, experiences time-varying multi-path fading, which is given by

$$h_u^{dir}(\tau,t) = \sum_{l=0}^{L-1} h_u^{dir}(\tau_l,t)\delta(\tau-\tau_l), \tag{2}$$

where $dir = \{dl, ul\}$, represents the DL or the UL, respectively, $\delta(\cdot)$ is the Dirac delta function, L is the number of paths, τ_l is the the delay of the l^{th} path, and $h_u^{dir}(\tau_l,t)$ is the corresponding attenuation.

Given $h_u^{dir}(\tau,t)$, the channel's frequency response can be calculated as

$$H_u^{dir}(f_k,t) = \sum_{l=0}^{L-1} h_u^{dir}(\tau_l,t)e^{-j2\pi f_k \tau_l}. \tag{3}$$

The DL and UL channels are assumed to be reciprocal, thus we have

$$h_u^{dl}(\tau_l,t) = h_u^{ul}(\tau_l,t). \tag{4}$$

Their corresponding channel frequency responses are also reciprocal.

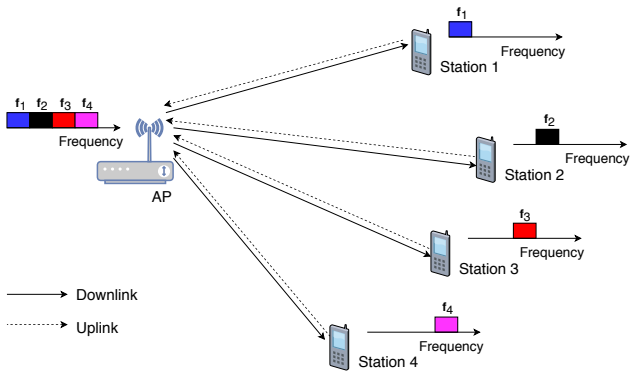

Fig. 3. System model.

The AP allocates orthogonal and non-overlapping subcarriers to different users, i.e.

$$\mathbf{f}_u \cap \mathbf{f}_v = \emptyset, u \neq v, \tag{5}$$

where $\mathbf{f}_u$ is the subcarrier set allocated to the u^{th} user.

When the eavesdroppers are located several wavelengths[3] away from the legitimate users, they tend to experience uncorrelated channel fading [9]. Whenever the eavesdroppers are very close to the legitimate users, we assume that they can be spotted, and the legitimate users will pause the key generation process to maintain security.

B. Protocol

Here we design an efficient OFDMA-based channel probing scheme, which allows the AP to simultaneously communicate with multiple users, thus reducing overhead. Key generation requires bidirectional transmissions to facilitate for the AP and stations to estimate their common and reciprocal channels. The system thus operates in the TDD mode, and the AP coordinates the channel access. The protocol is formulated in Algorithm 1, and it is detailed in the following.

In the DL and at time t_j^{dl}, the AP will first transmit a message, $X(f, t_j^{dl})$, and the signal received by the u^{th} station can be expressed as

$$Y_u^{dl}(\mathbf{f}_u, t_j^{dl}) = H_u^{dl}(\mathbf{f}_u, t_j^{dl}) X(\mathbf{f}_u, t_j^{dl}) + w_u^{dl}, \tag{6}$$

where w_u^{dl} is the noise at the user u. Once the message is received, each station can separately carry out channel estimation as

$$\widehat{H}_u^{dl}(\mathbf{f}_u, t_j^{dl}) = \frac{Y_u^{dl}(\mathbf{f}_u, t_j^{dl})}{P_u(\mathbf{f}_u)}, \tag{7}$$

where $P_u(\mathbf{f}_u)$ is the pre-defined frequency-domain pilot pattern, which is part of the transmitted signal $X(\mathbf{f}_u, t_j^{dl})$, and it is known by both the AP and the stations. Since OFDM systems require frequency domain channel estimation for channel equalization, $\widehat{H}_u^{dl}(\mathbf{f}_u, t_j^{dl})$ is already available in commercial products, and can be reused for key generation. Therefore, no additional channel estimation operations are required in the proposed protocol.

[3]The wavelength is 6 cm when the carrier frequency is 5 GHz.

Algorithm 1 An OFDMA-based multi-user key generation protocol

INPUT: $\{\mathbf{f}_u\}$: Subcarrier allocation to users.
INPUT: N_p: Number of probing.
OUTPUT: $\bar{k}_u^{\text{AP}}$, $\bar{k}_u$: Session key for the AP and the u^{th} user.
OUTPUT: k_G: Group key for the AP and users.

% *Channel Probing*
for $j \leftarrow 1$ **to** N_p **do**
  At t_j^{dl}: AP transmits downlink message to users; users estimate their channel state information (CSI), $\widehat{H}_u^{dl}(\mathbf{f}_u, t_j^{dl})$.
  At $t_j^{ul} = t_j^{dl} + \Delta t$: The users transmit UL messages simultaneously to the AP; AP estimates the CSI, $\widehat{H}_u^{ul}(\mathbf{f}_u, t_j^{ul})$.
end for
% *Quantization*
AP quantizes the channel measurements into keys: $\widehat{H}_u^{ul}(\mathbf{f}_u, t^{ul}) \rightarrow k_u^{\text{AP}}$.
The u^{th} user quantizes the channel measurements into keys: $\widehat{H}_u^{dl}(\mathbf{f}_u, t^{dl}) \rightarrow k_u$.
% *Information reconciliation and privacy amplification*
AP: $k_u^{\text{AP}} \rightarrow \bar{k}_u^{\text{AP}}$.
The u^{th} user: $k_u \rightarrow \bar{k}_u$.
% *Group key generation*
AP calculates the group key as $k_G = \bar{k}_1^{\text{AP}} \oplus ... \oplus \bar{k}_u^{\text{AP}} \oplus ... \oplus \bar{k}_{N_u}^{\text{AP}}$.
The AP encrypts k_G using $\bar{k}_u^{\text{AP}}$ and sends it to the u^{th} user.
The u^{th} user obtains the group key by decryption with $\bar{k}_u$.

The UL transmission is more complex. The stations should not transmit on all the OFDM subcarriers, because it would impose interference at the AP side. Instead, the user-specific subcarrier allocation information will be first determined by the AP and then sent to all the stations. Again, there will be no overlapping amongst the OFMDA subcarriers allocated to different stations. Additionally, all stations should commence and complete their transmissions at the same time, in order to not cause intra-cell interference. In this case, the DL transmission can be treated as a trigger message for informing all the stations to initiate their UL transmissions. At time instance $t_j^{ul} = t_j^{dl} + \Delta t$, all stations simultaneously transmit their packets with the same length using their allocated OFDMA subcarriers. The waveform received at the AP in the frequency-domain can be expressed as

$$\begin{aligned} Y^{ul}(f, t_j^{ul}) &= \sum_{i=1}^{N_u} Y_u^{ul}(\mathbf{f}_u, t_j^{ul}) \\ &= \sum_{i=1}^{N_u} H_u^{ul}(\mathbf{f}_u, t_j^{ul}) X_u(\mathbf{f}_u, t_j^{ul}) + w_{\text{AP}}^{ul}, \end{aligned} \tag{8}$$

where w_{AP}^{ul} is the noise at the AP. Since these subcarriers are orthogonal and non-overlapping, the AP can separate the signals received in the frequency-domain according to the

OFDMA subcarrier allocations, and estimate the CSI between itself and the u^{th} station as

$$\widehat{H}_u^{ul}(\mathbf{f}_u, t_j^{ul}) = \frac{Y_u^{ul}(\mathbf{f}_u, t_j^{ul})}{P_u(\mathbf{f}_u)}. \tag{9}$$

The above DL and UL transmissions complete a pair of channel probing actions. The AP and the stations will continue such probing until they obtain sufficient measurements, $\{\widehat{H}_u^{ul}(\mathbf{f}_u, t_j^{ul}), \widehat{H}_u^{dl}(\mathbf{f}_u, t_j^{dl})\}$. There should be time separation, namely sampling period T_s, between any two adjacent samplings. The frequency-domain response of any subcarrier, $H_u^{dir}(f_k, t)$, is subject to a similar Doppler spectrum, as well as similar coherence time [28], unless there is a large difference between the lowest and highest OFDMA subcarrier frequencies. We can thus design the sampling period according to the Doppler frequency, or equivalently to the coherence time.

Once the channel probing is completed, we then use a mean value-based quantization as an example, which converts the measurements s to 1, when they are above the mean value μ_s, or 0 otherwise, which can be mathematically expressed as

$$k(i) = \begin{cases} 1, & \text{if } s(i) > \mu_X; \\ 0, & \text{if } s(i) \leq \mu_X. \end{cases} \tag{10}$$

The AP and the u^{th} user can then generate a pair of keys, $\{k_u^{\text{AP}}, k_u\}$, which usually do not match because the channel measurements of the AP and of the stations are unlikely to be identical due to their unsynchronized sampling and noise. Information reconciliation and privacy amplification will then enable the AP and stations to agree on the same keys, yielding

$$\bar{k}_u^{\text{AP}} = \bar{k}_u. \tag{11}$$

These two steps can use the mechanisms as in other key generation systems [3], which is out of the scope of this paper.

It is important to note that each pair of channel probing actions only occupies a pair of time slots, which significantly mitigates the channel's occupation time. The total number of transmissions can be expressed as

$$N_t^{\text{mu}} = (1 + N_u) \cdot N_p, \tag{12}$$

and the resultant complexity is $\mathcal{O}(N_u)$, which is much lower than that of the pairwise group key generation systems, $\mathcal{O}(N_u^2)$. The transmission reduction ratio of our multi-user protocol is

$$G = \frac{N_t^{\text{mu}}}{N_t^{\text{pairwise}}} = \frac{N_u + 1}{N_u(N_u - 1)}, \tag{13}$$

which is quite significant. For example, when there are $N_u = 4$ stations, our protocol only needs a fraction of $\frac{5}{12}$ transmissions compared to those required by the pairwise-based group key generation protocol.

As shown in Fig. 1, the keys generated can serve as the seed for the upper layer cryptographic schemes and protocols, such as the Wi-Fi Protected Access 2 (WPA2) at the medium access control (MAC) layer of Wi-Fi. To elaborate, WPA2 is based on advanced encryption standard (AES), which supports key lengths of 128, 192, and 256 bits. The length of the channel probing, N_p, will thus be determined by the cryptographic applications, which is selected for ensuring that the AP and the stations obtain sufficient channel measurements for key generation.

Following the key generation process, the AP establishes a unique key, $\bar{k}_u^{\text{AP}}$, with the u^{th} station, which can be used as the private session key for encrypting unicast transmissions. Additionally, the AP can generate a group key by calculating

$$k_G = \bar{k}_1^{\text{AP}} \oplus ... \oplus \bar{k}_u^{\text{AP}} \oplus ... \oplus \bar{k}_{N_u}^{\text{AP}}, \tag{14}$$

where $\oplus$ is the exclusive-OR operation. The AP will then encrypt the group key, k_G, using $\bar{k}_u^{\text{AP}}$ and send it to the u^{th} station, which will receive the ciphertext and obtain the group key by decryption using $\bar{k}_u$. The group key can then be used for securely broadcasting messages to all stations.

C. Metrics

In the following, we present the key performance indicators used in our analysis.

1) Channel Reciprocity: The similarity of two variables, s_u and s_v, can be quantified by Pearson's cross-correlation coefficient, which is defined as [3]

$$\rho(s_u, s_v) = \frac{\sum_{i=1}^{N_p}(s_u(i) - \mu_{s_u})(s_v(i) - \mu_{s_v})}{\sqrt{\sum_{i=1}^{N_p}(s_u(i) - \mu_{s_u})^2}\sqrt{\sum_{i=1}^{N_p}(s_v(i) - \mu_{s_v})^2}}. \tag{15}$$

After the analog measurements are converted to binary sequences, we can also use the key disagreement rate (KDR) for quantifying their similarity, defined as

$$\textit{KDR}(k_u, k_v) = \frac{\sum_{i=1}^{l_k} |k_u(i) - k_v(i)|}{l_k}, \tag{16}$$

where l_k is the length of the key, k_u.

Approximate channel reciprocity ensures that the keying parties generate similar keys. In a TDD system, the accuracy of channel reciprocity is limited by the non-simultaneous sampling and noise. We use the correlation coefficient between the channel measurements of the AP and that of the u^{th} user, $\rho[\widehat{H}_u^{ul}(\mathbf{f}_u, t_j^{ul}), \widehat{H}_u^{dl}(\mathbf{f}_u, t_j^{dl})]$, as well as the KDR between the keys at the AP and that of the u^{th} user, $\textit{KDR}(k_u^{\text{AP}}, k_u)$, to quantify the performance.

2) Key Uniqueness: The session keys between the AP and each user should be unique as they are used to encrypt their unicast transmissions, i.e. k_u^{AP} should differ significantly from k_v^{AP}, $u \neq v$. We still use the cross-correlation and KDR to quantify the difference. Without loss of generality, we only compare the channel measurements and corresponding keys of the UL transmissions, i.e. the results at the AP side. We use the correlation coefficient of the channel measurements between the AP and the u^{th} station and that between the AP and the v^{th} station, $\rho[\widehat{H}_u^{ul}(\mathbf{f}_u, t_j^{ul}), \widehat{H}_v^{ul}(\mathbf{f}_v, t_j^{ul})]$, as well as the KDR between the AP and the u^{th} station and that between the AP and the v^{th} station, $\textit{KDR}(k_u^{\text{AP}}, k_v^{\text{AP}})$, to quantify the performance.

3) Key Randomness: The keys generated are used for the cryptographic applications, which require a random key. A non-random key will render the cryptographic scheme vulnerable to brute force attacks [25]. The National Institute of Standards and Technology (NIST) randomness test suite [31] is a popular tool for evaluating the randomness of the output of the random number generator (RNG) and pseudo random number generator (PRNG). It has been widely used in the key generation research area [8]–[10], [12]–[14], [17], [21], [28], [30], and it is also adopted in this paper.

The test suite provides 15 randomness tests, each of which will return a p-value. When the p-value is larger than a threshold, e.g. 0.01, then we declare that the sequence passes a test. The sequence is deemed random, if it passes all the available tests.

We used the above metrics for evaluating the raw keys, k_u^{AP} and k_u, rather than the final keys, $\bar{k}_u^{\text{AP}}$ and $\bar{k}_u$. Firstly, the raw key is intuitively required to evaluate the channel reciprocity. Secondly, the uniqueness between k_u^{AP} and k_v^{AP} will lead to the conclusion of the uniqueness of $\bar{k}_u^{\text{AP}}$ and $\bar{k}_v^{\text{AP}}$, because $\bar{k}_u^{\text{AP}}$ is hashed from k_u^{AP}. Finally, because the output of a hash function is usually randomized, it is necessary to evaluate the randomness of the raw key, k_u^{AP}.

IV. Case Study with IEEE 802.11ax

In this section, we tailored the proposed algorithm to IEEE 802.11ax standard.

A. IEEE 802.11ax Protocol

IEEE 802.11ax is a new Wi-Fi standard amendment, which is going to be released in the late 2019 [32]. It extends its predecessors, namely IEEE 802.11ac/n/g/a, by numerous beneficial new features, including DL and UL multi-user access supported by OFDMA and MU-MIMO, higher-order modulation (1024-QAM), reduced power consumption, extended long range for outdoor communications, target wakeup time, basic service set colouring, etc. IEEE 802.11ax is suitable for enterprise office and stadium scenarios, as well as for outdoor operation and IoT scenarios. It aims for improving the average user throughput by a factor of at least four in high-density environments w.r.t. 802.11ac. This section briefly introduces the new features relevant to key generation. Readers who are interested in further details are referred to the standard amendment [32] for more information.

1) Physical Layer: Table I shows the new features of the IEEE 802.11ax physical layer compared to those of the legacy IEEE 802.11ac. IEEE 802.11ax uses both OFDMA and MU-MIMO as physical layer technologies for supporting multi-user access. The multi-user OFDMA and DL MU-MIMO will be implemented in the IEEE 802.11ax wave 1, but UL MU-MIMO will be deferred to the wave 2. Similarly to IEEE 802.11ac, IEEE 802.11ax DL multi-user MIMO uses explicit feedback for feeding back the CSI. The transmit beamformer sends a sounding frame/null data packet (NDP), and the receive beamformee exploits it for estimating the CSI, which is then quantized and fed back to the beamformer [33]. However, it has been experimentally demonstrated that even when the CSI feedback is encrypted, attackers may still be able to infer the CSI [34]. Therefore, the IEEE 802.11ax multi-user MIMO framework is not directly suitable for key generation, hence this paper relies on exploiting OFDMA.

TABLE I
Physical Layer Enhancement of IEEE 802.11ax compared to IEEE 802.11ac

	IEEE 802.11ac	IEEE 802.11ax
Carrier Frequency (GHz)	5	2.4 or 5
Bandwidth (MHz)	20, 40, 60, 80, 80+80, or 160	20, 40, 60, 80, 80+80, or 160
FFT Size	64, 128, 256, 512	256, 512, 2014, 2048
Subcarrier Spacing (kHz)	312.5	78.125
OFDM Symbol Duration (μs)	3.2	12.8
OFDM Cyclic Prefix (μs)	0.8/0.4	0.8/1.6/3.2
Multi-user Access	DL, MIMO	DL and UL, OFDMA and MIMO

In IEEE 802.11ax, there are more OFDM subcarriers than that in IEEE 802.11ac, hence a higher data rate can be supported. Additionally, IEEE 802.11ac only supports single-user OFDM, but IEEE 802.11ax extends it to multi-user OFDMA transmissions, for both the DL and UL, which is suitable for dense environments.

The IEEE 802.11ax amendment defines a resource unit (RU) (or subcarrier) allocation table, which describes RU assignment to stations. For example, there are 256 subcarriers in total for the 20 MHz bandwidth; when the allocation index is 112, the AP can serve four stations simultaneously through four RUs, each having 52 non-overlapping subcarriers. The rest of the subcarriers are used as guard band. The full RU allocation table is defined in Table 28-24 of [32].

It should be noted time and frequency synchronization is very important in IEEE 802.11ax, which will be affected by the transmission time delay, clock frequency offset and timing errors. IEEE 802.11ax tackles this issue by using accurate time synchronization, as detailed in [32].

2) MAC Layer: The MAC layer protocol coordinates the channel access of different users in order to avoid collisions. IEEE 802.11ax supports multi-user access by employing OFDMA and MIMO. Regarding the UL multi-user transmissions, it is important to ensure that all stations are synchronized so that they simultaneously commence their transmissions, because asynchronous transmissions would cause interference at the AP side.

IEEE 802.11ax tackles this challenge by introducing a new scheme, namely the high efficiency (HE) trigger-based (TB) UL transmissions, which is illustrated in Fig. 4. The AP first sends a DL trigger packet to the stations which have data requests. The trigger packet informs the stations when they can start transmitting and the duration of the transmission to ensure that all the stations start and complete their transmissions at the same time. After a specified short interframe space (SIFS) time interval ($t_{\text{SIFS}} = 10$ μs in the 2.4 GHz band and $t_{\text{SIFS}} = 16$ μs in the 5 GHz band), the stations will simultaneously transmit to the AP. After the reception, the AP will echo an acknowledge

(ACK) frame to the stations to indicate a positive packet reception. By contrast, the lack of an ACK frame indicates negative reception. This completes the HE TB transmissions.

At first glance, the spectrum efficiency is not improved compared to the single-user OFDM systems, since the total spectral resources remain the same. However, the IEEE 802.11 MAC layer uses carrier-sense multiple access with collision avoidance (CSMA/CA) to negotiate channel access among stations, which requires a number of packet exchanges, such as the classic Request to Send (RTS)/Clear to Send (CTS). The stations, which have transmission request will back off for a random interval, whenever the channel is sensed to be busy. CSMA/CA will become less efficient when the number of stations increases, since there is a higher probability of channel collisions. The multi-user transmission feature of IEEE 802.11ax allows multiple stations to simultaneously transmit, which reduces the overhead of channel sensing and improves the spectral efficiency, especially in a dense deployment [35]. Considering road traffic systems as an analogy, the CSMA/CA operates in a similar manner to a round-about, which is efficient when the network traffic is low. On the other hand, the central scheduling relying on a traffic light is more efficient when the traffic load is high.

B. Key Generation Prototype

The multi-user transmission feature is ideal for designing an efficient multi-user key generation protocol. An IEEE 802.11ax-based key generation system is thus designed as follows, assuming the allocation index to be 112 as an example. The AP transmits a trigger packet to four stations modulated using DL multi-user OFDMA. Upon receiving the trigger, the stations will estimate the channel using the preamble in the HE TB frame. After an interval of t_{SIFS}, they will separately and simultaneously send their packets to the AP at their allocated subcarriers, without causing interference to each other. These packets will arrive at the AP at the same time, and the AP can carry out the channel estimation for each station using the respective preambles in their UL frames. After waiting for a sampling period T_s, the AP and stations will repeat the above processes until they collect sufficient channel measurements. Afterwards, the AP and stations will carry out quantization, information reconciliation as well as privacy amplification, and finally generate the same keys locally.

It is worth noting that key generation can be carried out along with the normal data transmission, and hence dedicated communications are not mandatory. Whenever the AP initiates the HE TB UL mode, the AP and stations will exploit the existing channel estimation information, obtained by data and trigger packets, respectively. Therefore, key generation does not introduce additional energy consumption for the channel probing stage, which is a very attractive feature, especially for power-constrained IoT devices.

V. Simulation Study

In this section, we provide simulations result for demonstrating the efficiency of the proposed scheme.

TABLE II
Configuration Parameters

Bandwidth	20 MHz
FFT Size	256
DL	OFDMA
UL	HE trigger-based
Allocation index	112
Number of users	4
Number of subcarriers each user	52

TABLE III
Channel Parameters

Sampling frequency	20 MHz
Carrier frequency, f_c	5.25 GHz
Delay Profile	Model-B
Environmental speed, v	5 km/h
Distance between the AP and users	10 m
SNR	0:2:20 dB

A. Setup

We built the transceiver simulation models of both the AP and station based on the IEEE 802.11ax examples and functions provided by the Matlab WLAN toolbox [36]. The WLAN toolbox implements all the necessary functions, including waveform construction, channel modelling, receiver processing, etc.

The detailed configuration parameters of the AP and stations are shown in the Table II. In order to focus on the benefits provided by the multi-user OFDMA feature, we consider a single input single output (SISO) system.

In order to emulate realistic environments, a practical IEEE 802.11ax channel model is used [37]. We assume that the stations are located at different places, but their channel models and statistical parameters are the same. An indoor mobile environment is considered with the main channel parameters shown in Table III. The station speed is 5 km/h, which is a typical walking speed. The Saleh-Valenzuela channel model is used, where there are two clusters and nine taps in the Model-B. Please refer to the Matlab help file for detailed explanation [38].

Because the channel frequency is 5.25 GHz, $t_{\text{SIFS}} = 16$ μs, then the sampling interval is set as $\Delta t = 16$ μs. The channel coherence time is in the order of

$$T_c \propto \frac{1}{f_d} = \frac{c}{v f_c} = 41 \text{ ms}, \tag{17}$$

where c is the speed of light. The sampling period is thus set as $T_s = 50$ ms. Sampling interval and sampling period is illustrated in Fig. 4. Similar to the main trend in key generation research, this paper also considers a slow fading channel. A fast fading environment encountered in vehicular communications will impact the measurements' correlation [39], which is set aside for our future research.

Based on the above configurations, we have carried out extensive simulations, and collected $N_p = 3,000$ pairs of channel probing. As the key required by the cryptographic applications, e.g. AES, is only 128/192/256 bits, it is not necessary to perform so many channel probing realizations in real applications. However, increasing the number of channel

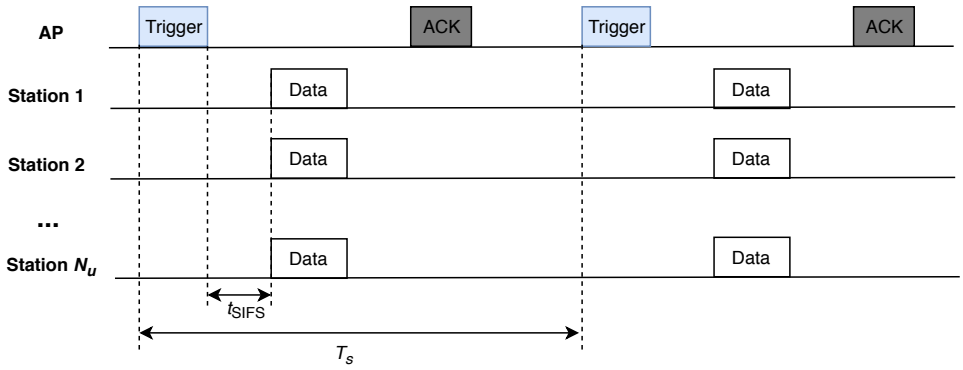

Fig. 4. Trigger-based UL multi-user transmission in IEEE 802.11ax.

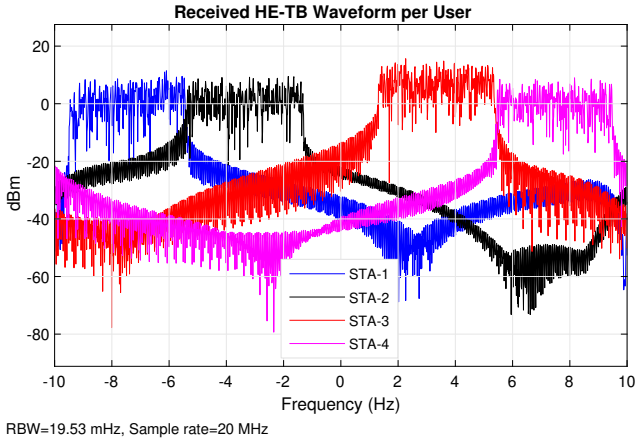

Fig. 5. The UL power spectrum of the received waveforms at the AP of the HE TB mode.

TABLE IV
NIST RANDOMNESS TEST RESULTS OF KEY SEQUENCES OF THE FOUR STATIONS, k_u^{AP}. SNR = 20 DB.

Test	Station 1	Station 2	Station 3	Station 4
Frequency	0.073	0.684	0.166	0.034
Block frequency	0.415	0.937	0.86	0.107
Runs	0.48	0.051	0.868	0.241
Longest run of 1s	0.842	0.803	0.54	0.025
DFT	0.262	0.708	1	0.025
Serial	0.63 0.487	0.878 0.877	0.559 0.554	0.066 0.48
Appro. entropy	0.245	0.403	0.174	0.029
Cum. sums (fwd)	0.121	0.971	0.284	0.021
Cum. sums (rev)	0.121	0.837	0.242	0.045

probing realizations will help to get a more accurate statistical analysis.

B. Results

It is essential to ensure that the transmitted signals of different stations do not interfere with each other at the AP during the UL HE TB transmissions. Although in reality the waveforms of different stations are combined at the AP, the simulation model allows us to separately save the waveforms of each station, and to analyze their individual power spectrum, which is shown in Fig. 5. It can be observed that each station only occupies its allocated subcarriers, and the intra-cell interference is quite low, at least 20 dB lower than the useful signal power.

The channel responses of the first subcarriers of the first fifty received packets of the four stations, i.e. $\widehat{H}_u^{dir}(\mathbf{f}_u(1), t^{dir})$, are shown in Fig. 6 as examples, for both the UL and DL. When the channel condition is good, providing a 20 dB SNR, the UL and DL channel estimates match quite well, which is indicating a high correlation. Additionally, the channel responses of each station are different and uncorrelated, which is a necessary condition in order to generate unique keys for the stations.

Moreover, the detailed results of the channel reciprocity are shown in Fig. 7. Intuitively, the higher the SNR, the higher the cross correlation. On the other hand, the KDR decreases as the SNR increases. The correction capability of the information reconciliation is determined by the error correction code selected. A Reed-Solomon (RS) (n, k, t) code is capable of correcting $\left\lfloor \frac{n-k}{2} \right\rfloor$ errors out of n symbols. For example, an RS $(63, 31, 16)$ code is capable of correcting 16 errors and the correction capacity is about 25%. As shown in Fig. 7, when the SNR is higher than 8 dB, the KDRs of all four stations are always lower than 25%. Therefore, the mismatch can be corrected and key generation can be successfully executed.

The results of the key uniqueness are shown in Fig. 8. The correlation coefficients of different pairs of the channel measurements are close to zero, indicating the absence of similarity between them. The corresponding KDRs are around 0.5, which is no better than a random guess. Therefore, the session keys, k_u^{AP}, are significantly different from each other, and can be used securely.

Finally, the results of randomness tests of the key sequences at the four stations, $\{k_u^{\text{AP}}\}$, are given in Table IV. All the p-values are above the threshold, i.e. 0.01, which means that all the session keys pass the selected randomness tests. In summary, our proposed multi-user key generation protocol is capable of generating unique keys with good channel reciprocity and key randomness, which is suitable for cryptographic schemes.

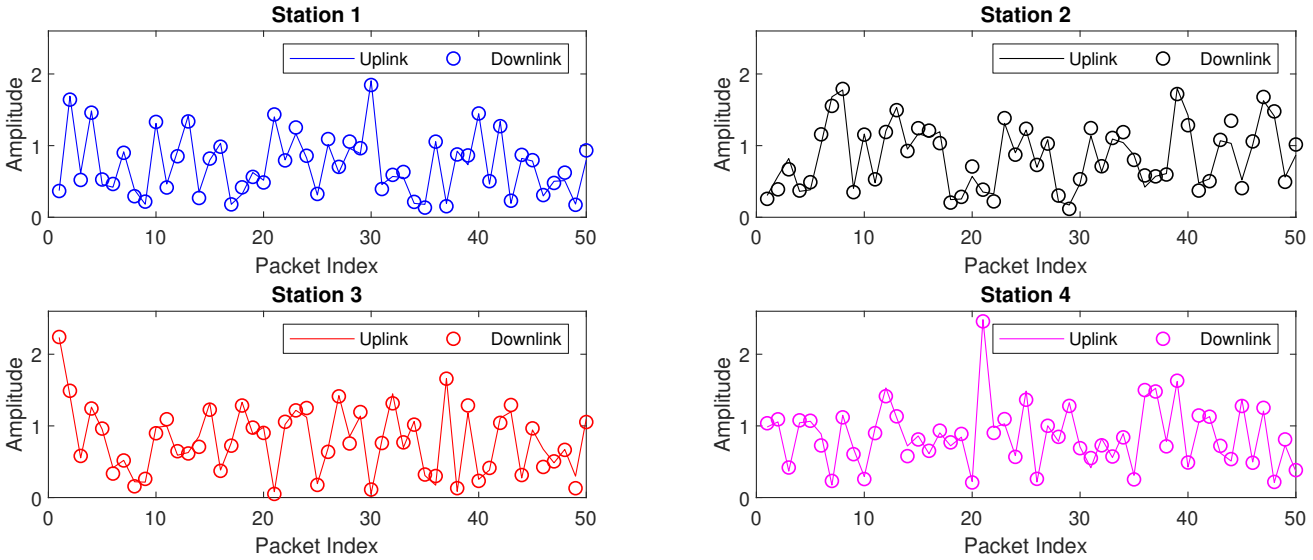

Fig. 6. Channel responses of the first subcarrier of different stations. SNR = 20 dB.

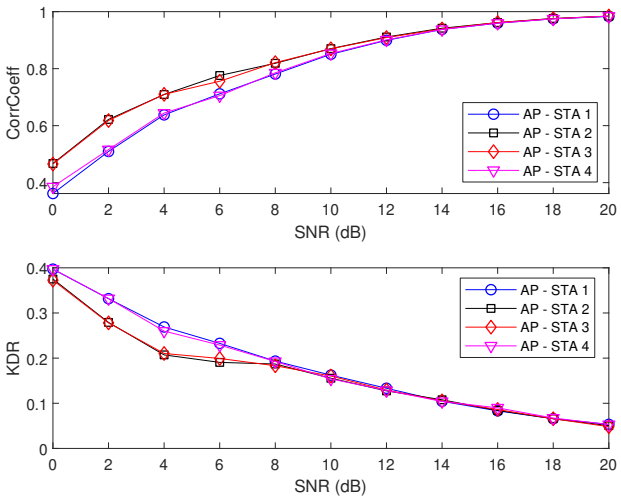

Fig. 7. Channel reciprocity: correlation coefficient and KDR between the channel measurements of the AP and that of the users versus SNR.

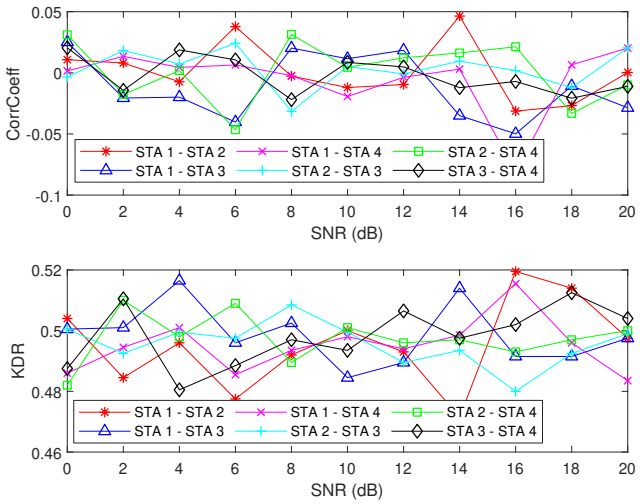

Fig. 8. Key uniqueness: correlation coefficient and KDR channel measurements of different users versus SNR.

VI. Conclusions

This paper proposed an efficient OFDMA-based multi-user key generation protocol, which is achieved by simultaneous channel measurements among multiple users on both the UL and DL. A prototype of the new Wi-Fi standard amendment IEEE 802.11ax was investigated as a case study. We simulated the full IEEE 802.11ax AP and station transceivers models based on the Matlab WLAN toolbox. Based on that, we carried out extensive simulations, and demonstrated that the proposed multi-user key generation protocol has a good performance in terms of low interference among users, high channel reciprocity and good key uniqueness and randomness, while being able to substantially reduce the key generation overhead. Our future work includes the implementation of the proposed protocol using software defined radio platforms and evaluation of its performance in various real-life scenarios.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, 2017.

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

[4] C. T. Zenger, M. Pietersz, J. Zimmer, J.-F. 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.

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

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

[7] B. Zan, M. Gruteser, and F. Hu, "Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4020–4027, 2013.

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

[9] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.

[10] O. Gungor, F. Chen, and C. Koksal, "Secret key generation via localization and mobility," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2214–2230, Jun. 2015.

[11] D. Kreiser, Z. Dyka, S. Kornemann, C. Wittke, I. Kabin, O. Stecklina, and P. Langendoerfer, "On wireless channel parameters for key generation in industrial environments," *IEEE Access*, vol. 6, pp. 79 010 – 79 025, 2018.

[12] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 802–817, 2018.

[13] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using Bluetooth wireless signal strength measurements," in *Proc. 11th Annual IEEE Int. Conf. Sensing, Communication, and Networking (SECON)*, Singapore, Jun. 2014, pp. 293–301.

[14] 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 Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12 462–12 466, 2018.

[15] H. Ruotsalainen and S. Grebeniuk, "Towards wireless secret key agreement with LoRa physical layer," in *Proc. Int. Conf. Availability, Reliability and Security*, Hamburg, Germany, Aug. 2018, p. 23.

[16] W. Xu, S. Jha, and W. Hu, "LoRa-Key: Secure key generation system for LoRa-based network," *IEEE Internet Things J.*, p. Early Access, 2019.

[17] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, 2014.

[18] S. Xiao, Y. Guo, K. Huang, and L. Jin, "Cooperative group secret key generation based on secure network coding," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1466–1469, Jul. 2018.

[19] Y. Wei, C. Zhu, and J. Ni, "Group secret key generation algorithm from wireless signal strength," in *Proc. Int. Conf. Internet Computing for Science and Engineering*, Zhengzhou, China, Apr. 2012, pp. 239–245.

[20] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 18–33, Jan. 2019.

[21] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1422–1430.

[22] Q. Qu, B. Li, M. Yang, Z. Yan, A. Yang, J. Yu, M. Gan, Y. Li, X. Yang, O. Aboul-Magd *et al.*, "Survey and performance evaluation of the upcoming next generation WLAN standard-IEEE 802.11 ax," *arXiv preprint arXiv:1806.05908*, 2018.

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

[24] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, "Information reconciliation schemes in physical-layer security: A survey," *Computer Networks*, vol. 109, pp. 84 – 104, 2016.

[25] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, 2017.

[26] R. Jin, X. Du, K. Zeng, L. Huang, L. Xiao, and J. Xu, "Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2526–2535, 2017.

[27] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[28] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, p. 2578 – 2588, Jun. 2016.

[29] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, 2017.

[30] L. Peng, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, "An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation," *IEEE Trans. Mobile Comput.*, vol. 18, no. 3, pp. 507 – 519, 2019.

[31] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Tech. Rep. Special Publication 800-22 Revision 1a, Apr. 2010.

[32] *Draft Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Enhancements for High Efficiency WLAN*, IEEE Std. IEEE P802.11ax™/D3.0, Jun. 2018.

[33] B. Bellalta and K. Kosek-Szott, "AP-initiated multi-user transmissions in IEEE 802.11 ax WLANs," *Ad Hoc Networks*, vol. 85, pp. 145–159, 2019.

[34] X. Zhang and E. W. Knightly, "CSIsnoop: Inferring channel state information in multi-user MIMO WLANs," *IEEE/ACM Trans. Netw.*, p. Early Access, 2019.

[35] "802.11 ax," Aruba, White Paper, accessed on 23 Mar., 2019. [Online]. Available: https://www.arubanetworks.com/assets/wp/WP_802.11AX.pdf

[36] Matlab WLAN Toolbox. Accessed on 23 Mar., 2019. [Online]. Available: https://uk.mathworks.com/help/wlan/index.html

[37] J. Liu, R. Porat, N. Jindal *et al.*, "IEEE 802.11 ax channel model document," IEEE, Tech. Rep. 802.11–14/0882r3, Sep. 2014.

[38] wlanTGaxChannel System object. Accessed on 23 Mar., 2019. [Online]. Available: https://uk.mathworks.com/help/wlan/ref/wlantgaxchannel-system-object.html

[39] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, 2017.