Bhatti *et al. J Wireless Com Network (2024) 2024:66*
https://doi.org/10.1186/s13638-024-02396-y

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A dynamic symmetric key generation at wireless link layer: information-theoretic perspectives

David Samuel Bhatti[1], Shahzad Saleem[2,3], Heung-No Lee[1] and Ki-Il Kim[4*]

*Correspondence:
kikim@cnu.ac.kr

[1] School of Electrical Engineering and Computer Science, Gwangju Institute of Sciences and Technology, Gwangju 61005, Republic of Korea
[2] Department of Cybersecurity, College of Computer Science and Engineering, Jeddah University, Jeddah, Kingdom of Saudi Arabia
[3] School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, Pakistan
[4] Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Republic of Korea

Abstract

The expansion of wireless communication introduces security vulnerabilities, emphasizing the essential need for secure systems that prioritize confidentiality, integrity, and other key aspects of data protection. Since computational security acknowledges the possibility of breaches when adequate computational resources are available, that is why information-theoretic security is being explored, which suggests the existence of unbreakable cryptographic systems even in the presence of limitless processing power. Secret key exchange has traditionally relied on RSA or DH protocols, but researchers are now exploring innovative approaches for sharing secret keys among wireless network devices, leveraging physical or link layer characteristics. This research seeks to revolutionize secure multi-party key acquisition in wireless networks, capitalizing on information-theoretic security and collaborative data extraction. The proposed secret key generation framework comprehensively organizes and explains the information-theoretic aspects of secret key generation within the lower layers of wireless networks, especially the link layer, proposes a novel information-theoretic SKG framework for the dynamic acquisition of symmetric secret keys, and responds to contemporary information security challenges by relying on information-theory principles rather than vulnerable mathematical relationships in the post-quantum period. A new cryptographic key can be generated using a straightforward method, and when it is combined (XORed) with the previous key, it creates a continuously changing secret for encryption and decryption. This approach enhances security because, as attackers attempt to break the encryption, the system generates fresh, dynamic keys, making it progressively more challenging for them to succeed. The research work in question integrates key renewal, or how often keys are updated (dynamic keys), with a security off-period. It introduces a framework for determining the best key refresh rate based on the anticipated rate at which keys might be compromised. Furthermore, the proposed framework is scalable, allowing new nodes to quickly join the existing network. The system was tested with multiple nodes equipped with IEEE 802.11 interfaces, which were set in monitor mode to capture frames at the link layer. Nodes map their on-time frames onto their Bloom filters. Nodes exchange these Bloom filters in a feedback mechanism. Nodes extract those frames from their .pcap files, which are present in all Bloom filters; these are common frames among all nodes. These frames are used to form a shared secret that is passed to HMAC Key Derivation Function by each node to acquire the final encryption key of the required length. The validation of this encryption key is performed using a simple challenge-response protocol; upon successful validation, encrypted communication begins. Otherwise, the key generation process is restarted.

Keywords: Information-theoretic security, One Time Frames, Multi-path fading, Principle of reciprocity, Spatial variation, Temporal variation

1 Introduction

The communication world is increasingly becoming wireless due to the rapid adoption of wireless and cordless networks in various activities of life. Wireless technologies like WiFi, Bluetooth, and WBANs are used for short-range communications, while networks like WiMAX, cellular, microwave, and satellite are being used in various industries for long range [1–3]. However, being widely used, these technologies pose a risk of security breaches due to their broadcast nature. Therefore, it is crucial to protect these transmissions from both external and internal threats. Secure communication system design requires confidentiality, integrity, availability, authentication/authorization, and non-repudiation [4]. Presently, there are two schools of thought with respect to information security, which address these security features: computational security and information-theoretic security. Computational security is also known as conditional security, meaning an adversary with a sufficient amount of computing power can breach the cryptosystems which are based on computational security. For instance, DH, RSA, and PKI are computationally secure and can be compromised if adversaries have large computational resources [5]. Mostly, current solutions focus on security, neglecting resource issues like memory, processing, and bandwidth. Even some SKG solutions also neglect these aspects. Information-theoretic security, also known as unconditional security, assumes adversaries are not limited in processing power; that is why, cryptosystems based on information theory are unbreakable, even if the attacking system is provided with adverse processing power. They are secured through information-theoretic arguments that exploit natural wireless physical layer communication phenomena in the form of random processes, making them suitable for wireless communication systems.

Traditionally, secret keys used for encryption and decryption are exchanged using RSA or DH protocols. However, with the rise of wearables, WBANs, and IoTs, traditional methods are not productive. Researchers are exploring new paradigms for secret key sharing among devices in resource-limited ad hoc network scenarios. They proposed that natural phenomena from the physical or link layers can be leveraged to establish symmetric secret keys between network nodes. Among the pioneer researchers from this domain are Hassan et al. [6], Amigo [7], Ensemble [8], Towsly et al. [9], David et al. [10], Linh et al. [11], Yara et al. [12], Rushan et al. [13], Nasser et al. [14], François et al. [15], Jingqi Zhou [16] who proposed different secret key acquisition schemes while exploiting the characteristics of wireless physical or link layer processes.

Among the above-mentioned researches, [6–10] have investigated wireless radio channels' physical layer characteristics. They found that wireless nodes can establish identical secret keys by exploiting channel reciprocity and randomness. Channel reciprocity means that eavesdroppers located more than $\lambda/2$ away from the transmitter or receiver cannot access the same symmetric channel state as legitimate nodes. This symmetric state remains identical for a brief period known as the coherence time, emphasizing the importance of timely key establishment in secure wireless communication [6–8, 11]. It is stated that there is no direct relationship between the proposed scheme and the principle of channel reciprocity, but rather an indirect one. The principle of channel reciprocity exists at the physical layer, where backward and forward channels remain the same for a short period of time (coherence time), during which channel measurements made by the transmitter and receiver are identical, but those of eavesdroppers differ from both. This characteristic is inherited by the link layer, where nodes within $\lambda/2$ have a probability of precisely listening to exactly the same transmission, but not the eavesdropper, who is positioned at different locations. Because it is highly improbable for an eavesdropper to be very close to the legitimate receiver within $\lambda/2$, that is why, it is unlikely for the eavesdropper to hear exactly the same transmission as that of the legitimate receiver.

At wireless link layer, it is commonly believed that two nodes cannot hear the exact same transmission unless they are within $\lambda/2$ distance [5, 9, 10, 17–20]. Practical observations revealed discrepancies due to wireless errors and environmental factors like multi-path fading and interference. During experimenting WiFi (2.4 GHz) behavior, it was observed, even when nodes are closer than 6.25 cm ($\lambda/2$), they do not always capture identical frames. However, they consistently intercept the ACKs and re-transmitted frames. This is because control frames use simpler modulation, and retransmissions increase capture probability in feedback scenarios. Thus, for secret key generation, using only One Time Frames (OTFs) of data type is recommended [21, 22]. The keys contributions of the proposed work are

1. This study aims to organize and provide insights into the information-theoretic aspects of secret key generation within the physical and link layers processes of wireless networks.
2. Our proposal includes a complete framework for the acquisition of dynamic symmetric secret keys leveraging the random process of frame losses at the link layer.
3. A new key can be generated easily using the same method, and when it is XORed with the previous key, that creates a dynamic secret for encryption and decryption. This key is strong because, as attackers try to crack it, the system keeps generating new dynamic keys, making it increasingly difficult for attacker to succeed.
4. This research work combines key renewal with the security off-period that helps a framework for determining the optimal key refresh rate based on the known key compromise rates.
5. This innovative framework represents a response to post-quantum information security concerns, as it relies on information theory principles rather than potentially vulnerable mathematical relationships, which are susceptible to cryptanalysis.

The manuscript is organized into different sections, such as 1-Introduction, 2-SKG Principles, Theoretical Basis, and Information-theoretic Perspectives, 3-Secret Key Generation Methods, 4-Proposed SKG Method: Information-theoretic Approach , 5- Experimentation, 6-Protocol for New Node Joining 7-Analysis and Optimization of Bloom Filter False Positives, 8-Probabilistic Analysis Frame Loss, 9-Results and Discussion, 10-SKG Comparison, 11-Limitation & Challenges, and 12-Conclusions.

2 SKG principles, theoretical basis, and information-theoretic perspectives

2.1 Principle

Radio frequency, a frequency range from 20 to 100 GHz, is crucial for transmitting signals through enclosed mediums like cables or cable-less devices. It combines electric and magnetic fields to create a *"Radio Wave"* that can travel at a speed equal to light (3 x 10^8 m/s). The antenna's receiving sensitivity extracts the signal from noise. Wireless networks use these electromagnetic waves to transfer messages, eliminating the need for physical connections like wired networks. These waves, also known as radio waves, are superimposed on a carrier frequency in wireless communication, allowing data to be transferred between wireless nodes. The superimposition of radio signals creates a composition of multiple radio frequencies, known as a radio channel or channel.

Wireless communication is a broadcast medium, due to which it is vulnerable to attacks. Attackers can eavesdrop radio traffic, monitor and jam signals, and perform statistical analysis. However, the wireless medium has been studied for its potential to establish symmetric keys between wireless nodes. This is achieved through three basic characteristics: temporal variation, spatial variation, and the principle of reciprocity [23]. These channel characteristics exist because of multi-path propagation which occurs due to multi-path fading, reflection, diffraction, scattering, and shadowing. These characteristics factors create a baseline for exploiting wireless physical and link layers for information-theoretic security [24–26]. Multi-path prorogation occurs when multiple copies of the same signal are received by the receiver at different times with varying phases. This addition can be destructive, causing a decrease in signal-to-noise ratio (SNR) and making radio signal detection more challenging. On the other hand, it can be constructive, resulting in better SNR. Furthermore, inter-symbol interference is a direct consequence of multi-path propagation [26]. Multi-path fading occurs when a signal is received from different paths with varying degrees of delay, causing changes in the relative phase and strength of the signal. This can be due to atmospheric changes, mobility caused by the transmitter or receiver, or other objects moving in the same environment. Reflection occurs when the propagated signal hits a flat surface larger than the signal's wavelength (λ), such as walls, earth surfaces, or buildings. Diffraction occurs when the signal comes into contact with the sharp edge of a non-penetrating surface, blocking the signal's path and generating secondary waves. Scattering is the projection of the transmitted signal when it hits an obstacle in its path. Large-scale fading also leads to shadowing. With the wavelength of IEEE 802.11 (2.4 GHz) being very small, that is, 0.15 m, there is a very high chance of these phenomena occurring. This wavelength is calculated in Eq. 1.

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{2.4 \times 10^9} = 0.15\,\mathrm{m} \tag{1}$$

All these concepts can be comprehended from Fig. 1. In this figure, we have shown a base station and a mobile, but these principles apply to all types of wireless communication.

2.2 Principle-I: temporal variation

Temporal variation is a wireless communication phenomenon in which reflection, scattering, and refraction of the channel path happen to be changed due to atmospheric

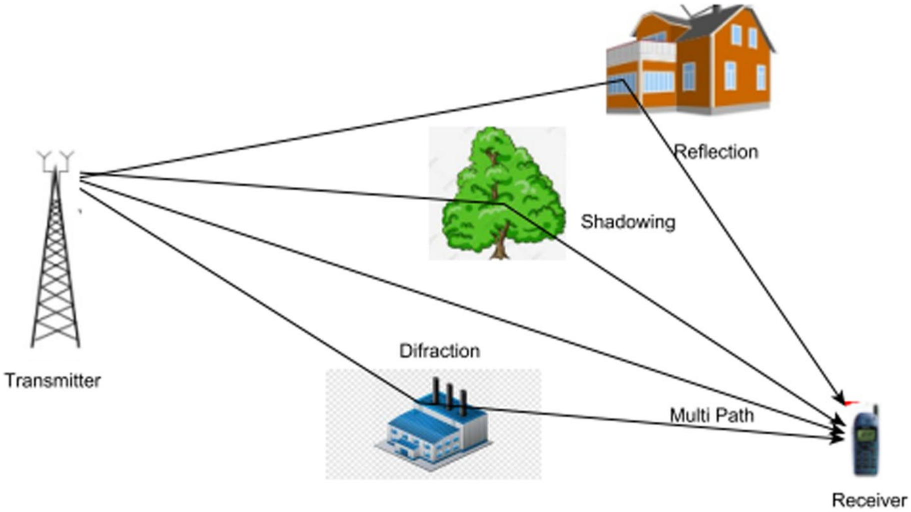


Fig. 1 Multi-path Fading. This figure demonstrates how signals reach their destination by striking, reflecting, and penetrating different objects

changes such as mobility, which may be caused by the transmitter, receiver, or any other object that is moving in the same environment. So, the randomness created in this case is uncertain or unpredictable, and it can be reaped to generate identical or symmetric secret keys at the transmitter and receiver [5, 24]. The use of temporal variation has been exercised by [25] for the purpose of authentication [27].

2.2.1 Principle-II: spatial variation

If the eavesdropper is away from the transmitter by a distance of $\lambda/2$, then it experiences a different and uncorrelated version of the same signal compared with the signal that is received by the legitimate receiver. This difference in the observations of the same signal is due to multi-path fading. This feature has been claimed to be used for the acquisition of alike secret keys between a legitimate transmitter and a receiver [5, 24]. This characteristic of radio channels has been used in wireless systems for authentication algorithms as well [25].

2.2.2 Principle-III: principle of reciprocity

It states that the state of a multi-path fading channel remains the same at the wireless transmitter and receiver for a short instance of time that is termed “coherence time” in literature. But this state is observed non-symmetric (or different) at the eavesdropper site when compared with the observations made at legitimate receiver nodes. So, symmetric observations made by transmitting and receiving nodes can be leveraged to establish identical secret keys between them. This principle of channel reciprocity is feasible only in Time-Division Duplex Systems (TDD). In these systems, channel measurements can be made simultaneously. These measurements remain the same at both nodes (the transmitter and receiver) in the TDD system. But in systems where these measurements cannot be made simultaneously, channel observations (or measurements) remain no more symmetric. In such scenarios, to mitigate the effects of factors concerning non-simultaneous measurements or mismatches, different signal pre-processing techniques

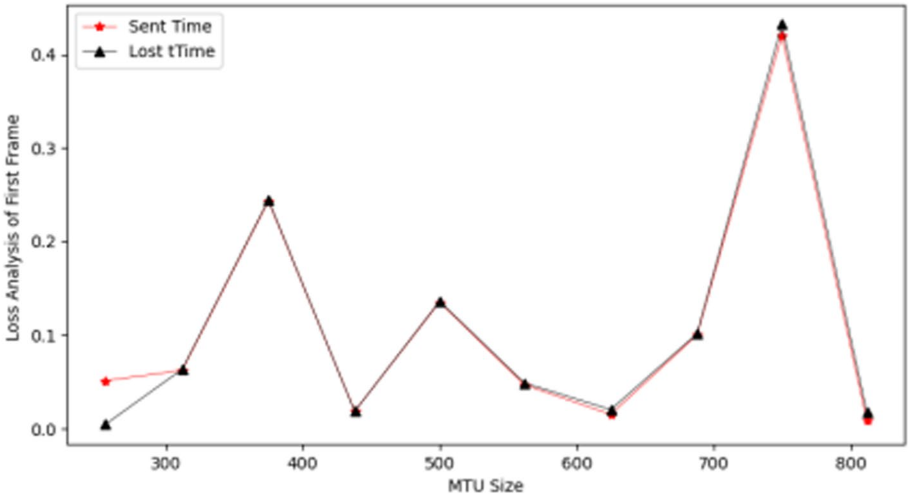


Fig. 2 When First Frame Lost. The figure presents results for different MTUs of frames and their time of loss, observed to be less than 0.5 s

like interpolation, filtering, and noise cancellation are used to improve the cross-correlation between transmitted and received signals [5, 24]. One of the studies that advocate this principle for secret key generation is [27]. The randomness that exists at the physical layer is inherited by the link layer. This concept has been used in different researches for establishing symmetric or identical secret keys between two or multiple nodes in different scenarios of wireless networks [9, 28, 29].

2.3 Theoretical basis for proposed SKG

At the wireless link layer, principle of spatial variation, temporal variation, and principle of reciprocity are inherited and applicable at frames. The concept gives rise to a phenomenon that states, *"it is not possible for the eavesdropper to listen the transmission between a legitimate transmitter and a receiver without error for a very long period of time, provided the eavesdropper is away from the transmitter by a distance of* $\lambda/2$". It implies that two nodes distanced by $\lambda/2$ cannot hear exactly the same transmission taking place in their range. But they share significant number of frames. The reason behind this incapability is the impossibility of two nodes being located at the same place at the same time. Due to this, they receive and drop different sets of wireless frames that are flying in the air. It has already been reported that the adversary who is eavesdrops the wireless link layer frames drops the first frame within a very short period of time that is less than 0.5 s. Such frame dropping is because of inevitable losses in wireless transmissions, which are the direct result of the erroneous nature of the wireless transmission medium [9]. We verified validity of the first frame loss reported in [9]. We made different transmissions with variable sizes of IEEE 802.11 frames. We found that the first frame was lost within half a second. These results are shown in Fig. 2.

From this fact, it can be concluded that if the transmitting and receiving nodes are provided with the capability to exchange knowledge of the correctly received frames without leaking information about them, then these transmitting and receiving nodes, based on their common frames, can generate identical secret keys. Fortunately, there exists an Oracle, which is a probabilistic data structure that can provide such a capability to wireless nodes. From the detailed review of probabilistic data structures, we came to know that wireless nodes, with the help of Bloom filters [30], can efficiently exchange the knowledge of their captured frames in a very compact manner with very little or no information leakage to an adversary [31–33]. Moreover, for the first time, these data structures were proposed by Hannes et al. [34] in the context of web engineering to find pages that are associated with comments saved at "Common-Knowledge Server" [35].

2.4 Information-theoretic support

The computationally secure systems like DES, RSA, DH, and AES demand impractical processing power for breaches, relying on unsolvable hard problems, and their effectiveness depends on limited adversary resources. Cryptographic research often emphasizes computational security, but the ideal computational model remains unproven [36]. On the other hand, information-theoretically secure systems, exemplified by the One-Time-Pad (OTP), rooted in information theory, remain resistant to attacks with unlimited computing resources [37, 38]. This is the reason, our research advocates the practicality of information-theoretic approaches, proposing their application in wireless lower layers for developing secure crypto-systems. The purpose of adding this section to the manuscript is to create a link between information theory, information-theoretic security, and wireless communication. The section proves the authenticity of proposed secret key generation framework from the perspective of information-theoretic security under wireless communication systems. It lays down a solid baseline for accepting the fact that the wireless communication processes at lower layers of the network stack (physical and data link layers) can be exploited for establishing a cost-effective secret key sharing solution for low-resource scenarios. The section starts with the contributions of renowned researchers who played a valuable role in the direction of wireless information-theoretic security, the secret key sharing.

2.4.1 Claude E. Shannon 1949

In the early days of information theory, information-theoretic security was considered to be impractical because the model presented by Claude E. Shannon was hard to achieve [39]. It was a simple communication model that consists of Alice, Bob, and an eavesdropper Eave, as shown in Fig. 3.

According to Shannon's model, the system is perfectly secure if it meets the following condition of information theory, given in Eq. 2.

$$I(M; C) = 0 \tag{2}$$

In Eq. 2, I(.,.) is the mutual information and *M* is the message. This means that the mutual information between the message and its cipher is zero. In other words, the eavesdropper having access to cipher *C* is unable to know Message *M*. This system can only be designed if and only if $H(K) \geq H(M)$; it means the entropy or length of the Key *K* should be greater than the length of the message *M* or equal to it. This is only possible with Vernam One-Time-Pad [40]. Due to these conditions, Shannon's model of perfect secrecy could not gain much popularity at that time. Moreover, his assumption of noiseless channels made it further less attractive.

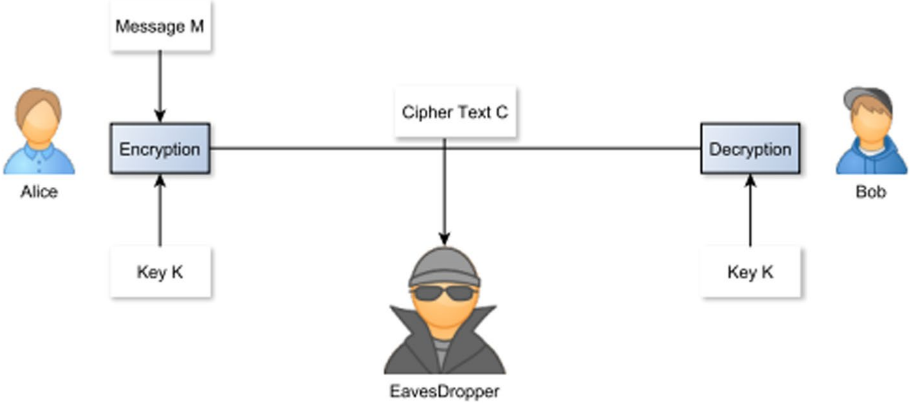


Fig. 3 Shannon model. This figure outlines the communication model assumed by Claude E. Shannon, consisting of Alice, Bob, and Eve. According to Shannon, the crypto-system is secure if $H(Key) \geq H(Message)$

2.4.2 A. D.Wyner 1974

A. D. Wyner did not accept the noiseless assumption of communication channels that was made by Shannon. Wyner proposed the concept of a noisy channel named wiretap channel [41]. It can be elaborated more specifically if we take J as the transmitted signal by Alice, K, L as the received versions of J at Bob and Eavesdropper, respectively. If this is the case, then J-K-L forms a Markov chain. Furthermore, Wyner slightly relaxed the assumption of perfect secrecy with the assumption that some information can be leaked at the eavesdropper. But the information leakage (I_{Leak}) may approach zero when this information is normalized by the total block size of the transmitted information. It can be expressed as given in Eq. 3.

$$I_{Leak} = \frac{1}{N} I(M; L) = 0 \tag{3}$$

Here N is the total length of the message block, and L is the observation of the wiretap channel that is made by Eave. Similarly, Wyner also gave the secrecy rate called the capacity of the wiretap channel, which is given by Eq. 4. This secrecy rate, or capacity (C), is the measure of secret bits per channel, observation, or measurement. It can also refer to secrets bits per second and is evaluated using Eq. 4.

$$C = Max_{P_J}\ I(J; K) - I(J; L) \tag{4}$$

In Eq. 4, P_J represents the probability distribution function of the transmitted signal J and $I(.; .)$ is the way in information theory to represent the mutual information between two signals that are transmitted and received. This model proves that we can acquire a positive secrecy rate without having the shared cryptographic keys in advance.

2.4.3 Choeng et al. in 1978

These wiretap channels can be created using the AWGN channel model proposed by Choeng et al. in 1978 [42]. AWGN is one of the simple communication models that provides a natural extension or application of Wyner's wiretap channel. The concept of using a wiretap channel is a scenario in which the sender encodes his private information in such a way that the intended legitimate recipient can extract meaningful information from it correctly, but not the adversary. There are so many ways to create this phenomenon. For instance, if the sender knows in advance the sensitivity of the eavesdropper and legitimate receiver to receive the signal, he can send a message whose RSS value is higher than that of the legitimate user but lower than that of the adversary. In this scenario, the legitimate user can decode this message correctly, but not the eavesdropper. The reason for such incapability is that for a legitimate user, the encoded message acts as the intended one, but for the eavesdropper, the same message acts as noise. In this way, a message is securely received and decoded by the legitimate receiver. This means that whenever the SNR of the adversary is less than the SNR of the legitimate receiver, the encoded message will not be comprehended by the eavesdropper. We also believe the removal of the noiseless assumption of the Shannon channel model is important concerning practical scenarios. In reality, we observe that wireless channels are prone to error. That is why the model proposed by Choeng et al. [42] in 1978 is an information-theoretically secure communication model. It consists of two channels; the first is the main channel that exists between two legitimate nodes (Alice-Bob) and is expressed using Eq. 5.

$$C_{\text{main}} = \frac{1}{2}\log\left(1 + \frac{W}{\sigma_1^2}\right) \tag{5}$$

The second channel is the wiretap channel that exists between legitimate and adversary nodes (Alice-Eave, Bob-Eave) and is modeled as Eq. 6.

$$C_{\text{wiretap}} = \frac{1}{2}\log\left(1 + \frac{W}{\sigma_1^2 + \sigma_2^2}\right) \tag{6}$$

Main and wiretap channels are modeled as i.i.d random processes. The outputs of these processes are those random variables whose measurements can generate a common or shared secret key between Alice and Bob. But this key will differ from the one that is computed at Eave. More specifically, it can be realized that if noise at the main and wiretap channels is treated as a result of some random process, then it is i.i.d over the main and wiretap channels. Under some transmission power W with which the signal is transmitted, the maximum secrecy rate can be expressed using Eq. 7.

$$\begin{aligned} C_{\text{AWGN}} &= C_{\text{main}} - C_{\text{wiretap}} \\ C_{\text{AWGN}} &= \left[\frac{1}{2}\log\left(1 + \frac{W}{\sigma_1^2}\right)\right] - \left[\frac{1}{2}\log\left(1 + \frac{W}{\sigma_1^2 + \sigma_2^2}\right)\right] \end{aligned} \tag{7}$$

where C_{AWGN} represents the secrecy capacity in an AWGN channel, C_{main} is the capacity of the main channel, C_{wiretap} is the capacity of the wiretap channel, W is the transmit power, σ_1^2 is the variance of the main channel noise, and σ_2^2 is the variance of the wiretap channel noise. $[\frac{1}{2}\log(1 + \frac{W}{\sigma_1^2})]$ is the rate of secret bit generation (secrecy rate) at the main channel. Similarly, the secrecy rate of the wiretap channel can be represented by $[\frac{1}{2}\log(1 + \frac{W}{\sigma_1^2+\sigma_2^2})]$. This implies that a positive secrecy rate can be attained whenever the SNR of the eavesdropper is below the SNR of the legitimate receiver. This equation calculates the secrecy capacity by taking the difference between the capacity of the main channel and the capacity of the wiretap channel. It measures how much secret information can be reliably transmitted over the main channel while keeping the wiretapper's information leakage minimal. Beside that it is well-known that differences in entropy are useful to expressing them mutual information $H(J) - H(J|K) = I(J; K)$. If J is the transmitted signal and K, L are its observations at eavesdropper and legitimate receiver, respectively, then we can express mutual information between legitimate transmitter and receiver in the presence of an eavesdropper as $I(J; K|L) = H(J|K) - H(J|K, L) = H(J|L) - H(J|K)$. Since J is conditionally independent on L given K then mutual information expression can be rephrased as $I(J; K|L) = H(J|L) - H(J|K, L)$, which implies that L provides no additional information about J when K is measured. So, in this case, $I(J; K|L) = 0$, indicates that knowing L provides no additional information about J beyond what is already known from K. But at link layer where the frames losses are independent at legitimate receiver and eavesdropper, which are transmitted by the transmitter, in the scenario where the eavesdropper has limited knowledge about the frames received by Bob or the frames transmitted by Alice such as at link layer where the frames losses are independent at legitimate receiver and eavesdropper, which are transmitted by the transmitter, we express mutual information expression as $I(J; K|L) \leq 1 - \epsilon$, where L represents the frames captured by the eavesdropper. Here, ϵ indicates the degree of uncertainty or information leakage to the eavesdropper. A smaller ϵ implies greater privacy in the communication between Alice and Bob.

2.4.4 Csiszar and Korner in 1978

Csiszar and Korner in their study toward transmitting confidential messages over the broadcast channel, further extended the work of Wyner, but they removed the assumption of wiretap channel [43]. Their research is highly suitable for wireless channels where a transmitter uses a transmission medium that is inherently public or broadcast in nature, and the transmitted message is received by the legitimate node as well as by the adversary. Thus, if *J* is a transmission made by a legitimate node (Alice) and *K*, *L* are the received versions of this transmission at honest user (Bob) and an eavesdropper (Eave), then the secrecy rate *Cs* can be given as Eq. 8

$$C_s = \mathrm{Max}_{P_J} I(J; K) - I(J; L) \tag{8}$$

Because *J*-*K*-*L* is a Markov chain, that is why main and eavesdropper channels are AWGN. So, it is highly probable to transmit the secret bits from Alice to Bob whenever Bob's SNR is better than Eave's.

2.4.5 Maurer, Csiszar 1990–2006

For a long period, Shannon's notion of a perfectly secure crypto-system was considered unrealistic, and it did not gain popularity. But the 1990s was the time when Maurer, in his outstanding research work, knocked out Wyner's wiretap channel model. He criticized that Wyner's model cannot be implemented in a real environment [44]. Logically, in practical scenarios, it is difficult to know the signal receiving sensitivity of the attacker in advance. He supported Shannon's notion of a perfectly secure communication system. Maurer proposed that a common secret can be shared between two wireless nodes even if the channel observed by the eavesdropper is equally good or even healthier than the channel that exists between two legitimate nodes (e.g., Alice and Bob). His model for secure secret key acquisition is based on the commonly correlated randomness that exists between the wireless transmitter and receiver. This shared randomness can be exploited to acquire a symmetric key at Alice and Bob in wireless setups. Maurer work was equally acknowledged by Ashlewede, Csizer, and Naryan for computing the secret key rate or secret key capacity in wireless domains [45, 46]. The model used by these authors consists of two legitimate nodes and one malicious node. This model is based on the commonly correlated randomness that exists inherently between two wireless devices. But it decorrelates instantly. More precisely, it exists only for a very small amount of time known as co-coherence time. It is independently distributed at legitimate and malicious nodes due to the spatial and temporal variations that exist in the state of a radio channel (path). These variations are the effects of multi-path fading, reflection, diffraction, scattering, and shadowing. These phenomena are already discussed in Sect. 2. If the transmitter (Alice) and receiver (Bob) measure their channels within coherence time, then their observations will be alike due to reciprocity, but the eavesdropper's (Eave) observation will be different. This means Alice and Bob can agree upon a common key, but Eve cannot do this. Information-theoretically, we shall see how these authors proposed this model to acquire the symmetric keys at the two legitimate nodes in the presence of an eavesdropper. So let us take two legitimate nodes, Alice and Bob, and one malicious node, Eave (eavesdropper). Let n observations made by Alice be $\{J_1, J_2, J_3 \ldots J_n\} = J$, Bob's are $\{K_1, K_2, K_3 \ldots K_n\} = K$ and Eave's are $\{L_1, L_2, L_3 \ldots L_n\} = L$. These are the observations of i.i.d random variables J, K, and L. At any instance of time, the observations J_i and K_i are statistically highly dependent or correlated if they are measured within the coherence time. But these observations instantly decorrelate and are not observed symmetric by Eave due to the effects of multi-path propagation. If Alice and Bob exchange some message symbols with the help of communication system X, then based on dependent observation of the channel, Alice and Bob can generate a symmetric secret key $S = \{S_1, S_2, S_3 \ldots S_n\}$. If this is the case, then according to information theory, this system must hold the following four properties of information-theoretic security, which are discussed in the subsequent subsection.

2.5 Information-theoretic arguments

2.5.1 Property 1: $P(S = S_a = S_b \geq 1 - \epsilon)$

If there exist two functions such that $f_a(J_n, X) \to S_a$ and $f_b(K_n, X) \to S_b$, then this implies they could generate symmetric secret keys S_a and S_b from the commonly observed randomness. This means that for any ϵ, there is a high probability that the condition $P(S_a = S_b = K \geq 1 - \epsilon)$ will be satisfied. It is worth mentioning that in mathematics, ϵ represents a very small number, better understood as infinitesimally small. To gain a better understanding of ϵ, it is stated that ϵ is less than any real number, but not exactly zero at the same time [47, 48].

2.5.2 Property 2: $H(S) \geq \log|S| - \epsilon$

Another important property concerning information-theoretic security exhibited by such communication models is that any key instance S_i obtained in each observation or measurement has no dependency over the past generated instances of the secret key. Moreover, the acquired symmetric key S_i at both sides (Alice and Bob) is uniformly distributed over the entire key range or length of the secret key $\{S_1, S_2, S_3 \ldots S_n\} \in K$.

2.5.3 Property 3: $H(S) \geq n(R - \epsilon)$

A further property held here is that a reasonable number of secret bits can be obtained per channel observation. This is also called the secrecy rate R or secret key capacity. Moreover, the bits acquired are highly random in nature.

2.5.4 Property 4: $\frac{1}{n}H(S) \geq n(R - \epsilon)$

This property states that if a large number of observations are made over the transmission of a large message of size n, then the secret key S of a reasonable size can be acquired. Moreover, for sufficiently large n, the generated key leaks no or very little information to the eavesdropper, that is, $I(S, X) = \epsilon$ or 0.

2.5.5 Property 5: $I(S; X) \leq \epsilon$

Finally, these communication systems claim that for the eavesdropper, it is difficult to extract knowledge about the secret key from the communication system. This implies that Eve knows nothing about the secret key or knows too little to have complete information about the entire length of the key.

Because communication processes occurring at the link and physical layers of the wireless transmission system are random, their observations or measurements are modeled as i.i.d. random variables that form Markov chains. From this model, secret key capacity or secrecy rate (secret bits per observation) can be defined using the following Eq. 9:

$$\text{Key Capacity} = R(J; K|L) = \min[I(J; K), I(J; K|L)] \tag{9}$$

Therefore, due to these properties, information-theoretically secure cryptographic systems are difficult to break for adversaries, regardless of how much computing power they possess. Wireless communication at physical and link layer is suitable to share secret keys using shared randomness that exist in different forms such as “channel state information” at physical layer and in the form frames at the link layer whose loss and reception at two nodes are identically independent and distributed reception is identically distributed and can be modelled as random variables.

3 Related secret key generation methods

It is believed that discussing physical and link layer approaches for generating symmetric keys in wireless networks can greatly help readers understand the SKG model. So, in this section, secret key generation from sources like RSS/RSSI, CIR, CFR, channel phase, amplitude/gain, AOA, TOA, and BER is discussed.

3.1 Physical layer

In the literature, multiple secret key generation methods are proposed that are based on the characteristics of wireless channels and successfully acquire information-theoretic security. These techniques capitalize on inherent shared randomness, reciprocity, and spatial-temporal decorrelation within fading channels. This unique characteristic ensures that the fading experienced by attackers differs from that of legitimate users. Wireless physical layer secret key generation techniques are extensively investigated using wireless channels as they offer simple, lightweight security solutions for wireless communication systems. The channel-based secret key acquisition techniques exploit channel reciprocity, spatial decorrelation, and temporal variation of wireless channels, enabling two legitimate users to generate and update secret keys using steps like channel estimation, quantization, information reconciliation, privacy amplification, and key validation. However, in wireless frequency division duplex systems, the principle of channel reciprocity does not hold due to differences in the observations of uplink and downlink channels as they experience different fading. This results in a discrepancy between the uplink and downlink channels, making the shared random sources such as RSS, CIR, and CFR significantly different from those in TDD systems. Various research efforts have been made to address these issues. For instance, leveraging spatial reciprocity, some research studies have focused on frequency-independent parameters for secret key generation. In one of the SKG approaches that use wireless channels, the angle and delay of each path were used to generate shared keys. Another approach used the channel covariance matrix's slow variability while proposing a SKG technique based on the eigenvectors of this matrix. However, despite their effectiveness, these SKG solutions often involve complex path extraction algorithms in addition to specific antenna configurations, which are impractical for low-power devices. Additionally, a loopback mechanism-based SKG scheme was suggested. However, this method is vulnerable to attacks by passive eavesdroppers, raising security concerns [49].

3.1.1 SKG from channel state information (CSI)

Channel state information is a superior parameter for acquiring symmetric secret keys due to its large amount of information about the radio channel. Its most valuable parts are Channel Impulse Response (CIR) and Channel Frequency Response (CFR), which study channel effects in the time and frequency domains, respectively [5]. Hassan et al. [6] research is one of the earliest works in this direction, which proposed to establish shared secret keys from the differential of channel phases. Phase-based SKG is advocated based on research findings reported by Ren et al. [24]. The research claimed that the radio signal phase is uniformly distributed over 360^o, resisting path power loss. Current hardware devices allow for fine-grained channel phase estimation, resulting in a high key generation rate. These estimated phases can be combined to investigate group-key solutions. But at the same time, it cannot be ignored that phase-based SKG schemes are more hypersensitive to noise, synchronous clock drifts, and frequency shifts (offsets) at the receiver. Other techniques based on the phase of the radio signal are ProxiMate [50], Qian et al. [51], and Cheng et al. [27]. AOA, or the angle of arrival, is the angle from which a signal is received at a receiver's antenna in a wireless radio system. The SKG scheme, proposed by Badawy et al. [52], estimates AOA for symmetric key acquisition. The authors found that two angles estimated from a common reference point are equivalent at both nodes, indicating high accuracy even at lower signal-to-noise ratios. The channel gain is a complex number. It is the magnitude of the attenuation of a radio signal. The popular techniques that are based on channel reciprocity and exploit the gain of a wireless radio channel are [53–56].

3.1.2 SKG from RSS/RSSI

RSS is the amount of energy in the signal a receiver receives from the transmitter. RSS-based SKG techniques involve sender and receiver exchanging symbols and recording RSS values at different intervals. Once sufficient RSS values are collected, secret key bits are created using Eq. 10.

$$T(m) = \begin{cases} 1, & \text{if } x > t+; \\ 0, & \text{if } x < t-; \\ e, & \text{else} \end{cases} \tag{10}$$

In Eq. 10, x is the sample value; e is the undefined state; and $t+$ and $t-$ are the upper and lower thresholds of the quantization method. Multiple RSS-based SKG schemes have been proposed in the literature. Among the pioneers, Jana et al. [23] used common randomness to establish a symmetric key between two wireless nodes, proving the existence of shared randomness at the transmitter and receiver. They concluded that the entropy of secret bits acquired using RSS can be increased through mobility or channel variation. Ensemble, a combination of DH and Amigo, is a good secret key sharing and device authentication protocol. They used the RSS values of wireless radio signals to achieve key sharing and device authentication based on proximity. Ensemble [8] aimed to answer the question "Are we close to each other?" and focused on handheld devices like mobiles and smartphones. It is a combination of DH [57] and Amigo [7]. Jeff and Tsouri investigated the RSS parameter of wireless signals to generate identical secret keys in wireless body-worn (WBAN) devices. They proposed measuring RSS values at the transmitter and receiver through packets sent and received in a feedback mechanism such as ACK (acknowledgment) of ARQ protocols. Taha et al. [58] exploited the RSS feature using mobile scenarios of WBAN devices, believing that mobility is one of the sources to achieve more uncertainty and randomness in RSS-based SKG solutions. This randomness results in the projection of more resistance for adversaries, who aim to guess the bits of security keys used by two BAN devices for encryption and decryption purposes. Van Torre [59] suggests RSS-based secret key acquisition. Katerina et al. [60] proposed a new idea for secret exchange. They suggested that if a secret is transmitted with a signal-to-noise ratio (SNR) greater than the SNR of the legitimate transmitter but less than the eavesdropper's, then a legitimate transmitter can decode it, but not the eavesdropper. This is because the message behaves as noise for the eavesdropper receiver. Theoretically, it looks attractive, but practically, it is hard to know the attacker's SNR in advance.

3.1.3 SKG from BER

The bit error rate (BER) is the rate at which errors occur in digital communication. Kitano et al. [61] proposed that fluctuations in BER can be exploited for acquiring symmetric keys between two wireless nodes. They successfully generated 128 secret bits from 138 observations of BER, with ten values of BER ignored as erroneous. The researchers also found that other parameters like phase, amplitude, and AOA can also be used to acquire symmetric keys.

3.1.4 UCFH-based techniques

Un-Coordinated Frequency Hopping (UCFH) is a modified form of FHSS that addresses secret sharing issues in the presence of jammers. In UCFH, nodes communicate messages without knowing the pattern of frequency hopping in advance. The transmitter and receiver randomly hop over the available range of frequencies, arriving at points where secret bits are successfully received by the receiver. These points can be used to transmit secret keys. However, this technique has a problem as it requires a lot of retransmissions in a feedback channel, which can take a long time for complete message exchange. Strasser et al. [62] divided the bigger DH message (DH Key) M into smaller chunks of bits called fragments f_i in such a way that $f_i = f_i + hash(f_{i+1})$, means frame f_i is concatenated with the hash of frame f_{i+1}. The transmitter node transmits these smaller messages using UCFH on a feedback channel. The receiver receives these smaller messages and using pre-shared hash function generates the original DH message. This original message is actually the DH secret key that was sent by transmitter in small chunks. This improvement decreases the frames' retransmissions. But, still, this technique results in the degradation of efficiency and overall performance of the network [63]. We also believe, this scheme is not appropriate for the battery-powered wireless devices because it may drain the battery quickly due to such large number of retransmissions. Other researchers who contributed in this area are [62], Liu et al. [64] Manjola et al. [65], Sona et al. [66]. Naive fragmentation of the DH message into smaller chunks in UCFH (Uncoordinated Frequency Hopping) scenario used for secret sharing in the presence of jammer may lead to a DOS attack. The reason for such a denial of service is the application-level signature verification that is carried out for every candidate message.

3.2 Link layer

One of the most popular areas for the extraction of secret keys is the wireless MAC/Link layer. Different researchers have proposed various approaches for acquiring similar secret keys. Well-known researchers among them are I. Safaka, Christina Fragouli, Katrina Agyraki, and Suhas Diggavi, who have all made significant contributions to the process of establishing secret keys by harnessing wireless MAC layer frames. This is an active research team from AT &T, whereas S. Mathur is at WIN-Labs. Likewise, this list also includes the writers of Elsabagh et al. [67], Towsley et al. [9], and Yara et al. [12]. Towsley et al. [9] pioneered dynamic secret generation for secure communication using OTF windows. Their technique links secret key updates with communication, resulting in fast renewals with minimal bandwidth, storage, and processing overheads. They exploited the SAW protocol as a link layer feedback mechanism to generate symmetric secret keys. Yaha et al. [68] first assumed correlated receiver and eavesdropper channels in feedback ARQ systems, using the SAW protocol for OTF windows and the universal hash function to acquire high-entropy symmetric secret keys. Similarly, Iris et al. [28] made use of feedback mechanisms in wireless communication for establishing the pairwise as well as the group secret keys. Other researchers who proposed to acquire secret keys from the wireless MAC layer frames are [29, 69, 70].

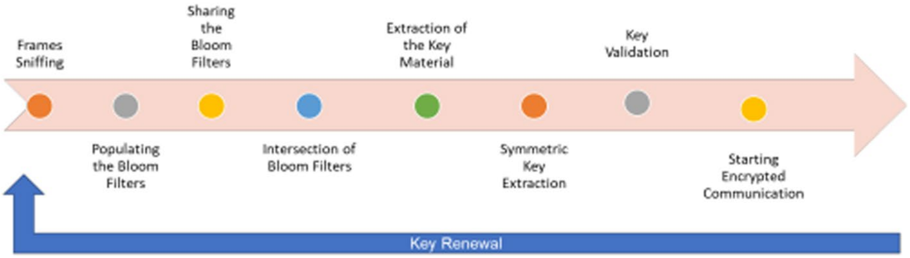

Frames Sniffing
Sharing the Bloom Filters
Extraction of the Key Material
Key Validation
Populating the Bloom Filters
Intersection of Bloom Filters
Symmetric Key Extraction
Starting Encrypted Communication
Key Renewal

Fig. 4 SKG Stages. The figure illustrates that the proposed SKG model comprises the following stages: (i) sniffing, (ii) bloom filter population, (iii) exchange of bloom filters, (iv) intersection of bloom filters, (v) key extraction, (vi) key validation, (vii) encrypted communication, and (viii) key renewal

4 Proposed method: information-theoretic SKG model

In an era where wireless communication is ubiquitous, the security of transmitted data remains paramount. Traditional cryptographic methods often rely on pre-shared keys or centralized authorities, which may not be scalable or resilient against emerging threats. In light of this, our research aims to propose an innovative solution for multi-party secret key acquisition, capitalizing on the principles of information-theoretic security within wireless networks. The primary objective of this proposed model of SKG is to design, implement, and evaluate a robust multi-party secret key generation scheme that harnesses the inherent characteristics of wireless communication. By exploiting the phenomenon that no two nodes can hear the same information if they are distanced by $\lambda/2$, we intend to establish a secure and scalable framework for secret key acquisition among multiple parties in the wireless domain.

The proposed SKG model consists of (i) sniffing, (ii) bloom filter population, exchange, intersection, (iii) key extraction, (iv) key validation, and (v) renewal, as shown in Fig. 4.

4.1 Frames capturing

Wireless networks use sniffing, tapping, and capturing to listen to wired or wireless frames from networks. Wireless adapters can work in three modes: network mode (normal mode), promiscuous mode, and monitor mode. Network mode, or normal mode, allows wireless nodes to capture only packets destined to their network. Promiscuous Mode captures all frames belonging to the network but does not contain radio or physical layer information. This mode is easily available in Microsoft Windows and Linux-based operating systems. Monitor Mode is set in Linux-based operating systems, but is not easily available in Microsoft Windows. Kali Linux is a popular choice for this purpose, as it captures 802.11 frames at the link layer with complete information and radio information. This mode is suitable for conducting research and investigation at almost all layers of the network stack, except for the physical layer, which only renders partial information. Two nodes were set in the normal mode to send and receive a file in the feed-back mechanism, which is TCP using socket programming. Other nodes were set in monitor mode to capture all frames from the air in.pcap files. We used WireShark and tcpdump, both of which have almost the same level of performance. The.pcap files were processed, and the one-time data frames (OTF) exchanged between sender and receiver were obtained.

4.2 Inserting OTFs in bloom filter

4.2.1 Bloom filter

Probabilistic data structures offer memory-efficient solutions for handling large data volumes. In wireless communication, they can be used to handle a large number of networks. They provide approximate answers compared to deterministic structures [71]. The Bloom filter is a compact probabilistic data structure that is used for membership queries, meaning whether a data item is present in a set or not. It operates as a bit-array and does not support element modification or deletion. Being small in size, it can be implemented in hardware and software and even transmitted in IP packet headers. Despite being limited by false positives, it is extensively being used in network security applications [32]. The false positives can be fixed to a tolerable threshold at the cost of negligible memory bytes. The false positive rate is significant and can be computed using Eq. 11 [33].

$$P_{FP} = \left(1-(1-1/m)^{kn}\right)^{k} \approx \left(1-e^{-kn/m}\right)^{k} \tag{11}$$

In the present scenario, ’k’ is the number of hash functions, ’m’ is the size of the Bloom filter, and ’n’ is the number of frames to be inserted. Adjusting ’k’ and ’m’, false positives can be significantly reduced [72]. Thus, if the given input size of frames is ’n’ and the desired false positive rate is FPR, then the estimated number of hash functions ’k’ and length/size of the Bloom filter can be derived from Eqs. 12 and 13, respectively.

$$k = \log 2 \times m/n \tag{12}$$

$$m = -n \log P_{FP}/(\log 2)^{2} \tag{13}$$

For the optimal value of k, the false-positive-rate is given by Eq. 14.

$$\left(\frac{1}{2}\right)^{k} = (0.6185)^{\frac{m}{n}}. \tag{14}$$

The derivation of these equations is not the purpose of this study but can be examined from Mitzenmacher and others [31, 73]. Equation (14) shows that the value of K must be an integer less than the optimal to lessen the processing overheads because the length m of Bloom filter *B[]* grows higher as the number of elements to be inserted increases [73, 74]. Since the Bloom filters aim to reduce disk space usage and query time, they require faster hash functions like Murmur and FNV over slower MD5 and SHA hashes. Alternatives like HashMix and Jenkins have efficient solutions and security domain applications. [75].

4.2.2 Insertion and exchange

The one-time data frames (OTFs) filtered in the sniffing stage were inserted in the Bloom filter. Each node exchanged their Bloom filters with one another using reliable protocols such as TCP. Each node queried its captured OTFs, and the frames that mapped on all Bloom filters were separated.

Table 1 Specification of WiFi adapters

Sr. No	Device	IEEE 802.11	USB ports	Gain/sensitivity
1	Dell D620 (Latitude),Kali Linux, Processor (Intel 1.83GHz (core 2 Dou)), RAM (2GB DDR2 SDRAM)), Hard Disk (5400RPM ,160 GB SATA)	a/b/g	4	Tx-Power 15 dBm
2	Compaq 610,Kali Linux,Processor (Intel 2GHz (Core 2 Dou)), RAM (800MHz, DDR2, (2GB)), Hard Disk (5400RPM ,80GB)	b/g/n	3	Tx-Power 20 dBm
3	Compaq 6710b, Kali Linux, Processor (Intel 2.4GHz (Core 2 Dou)), RAM (800MHz, DDR2, (1GB)), Hard Disk (7200RPM ,80GB)	a/b/g/n	4	Tx-Power 14 dBm
4	Haier 7G5H, Kali Linux, Processor (Intel 2.4GHz (Core i3 4Generation)), RAM (4GB), Hard Disk (7200RPM,500GB)	802.11 b/g/n	4	Tx-Power 16 dBm
5	Alpha AWUS036NH	b/g/n	NA	-92 dBm(802.11 b),-76 dBm (802.11 g)
6	Alpha AWUS036H	b/g	NA	5dBi Antenna
7	LB-Link BL-WN150AH	b/g/n	NA	5dBi Antenna
8	Operating Systems: Kali Linux, AirCrackNG, tcpdump, WireShark, Python, MySQL	NA	NA	NA

4.3 Symmetric key extraction

Each common frame was passed to the shared universal hash function; the outputs were XORed to the shared secret. The shared secret as an input is passed to the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) to generate a 128/256-bit symmetric key [76]. This symmetric is used for encrypted communication between nodes A, B, and C using a block cipher like AES.

4.4 Symmetric key validation

Challenge/response protocols are used for validating the symmetric keys and are discussed in detail in a later section named Experimentation-5.

5 Experimentation

We considered the deployment of a controlled experimental setup involving six IEEE 802.11 nodes in an ad hoc mode. Two nodes were given the task of transmitting and receiving a designated file using WiFi data frames. Three were configured to operate in monitor mode [77, 78], enabling the interception and analysis of WiFi frames exchanged exclusively between the transmitting nodes for group key acquisition, and one node acts as an attacker that attempted to acquire the same key as the other three legitimate nodes. The information about devices used in the experimentation is given in Table 1.

To achieve multi-party secret key acquisition, each monitoring node **captures frames** and stores them in the Bloom filter. Three nodes that are designated to acquire an identical symmetric key by exchanging their Bloom filters with one another lay the foundation for shared data extraction. Frames that are successfully queried at all Bloom filters are used as sources of shared secret. Bloom filters are shared publicly, yet they possess an irreversible nature, making them resistant to reverse engineering even when accessed by potential attackers. The attacker's capability is limited to query operations, preventing their ability to extract specific elements from the Bloom

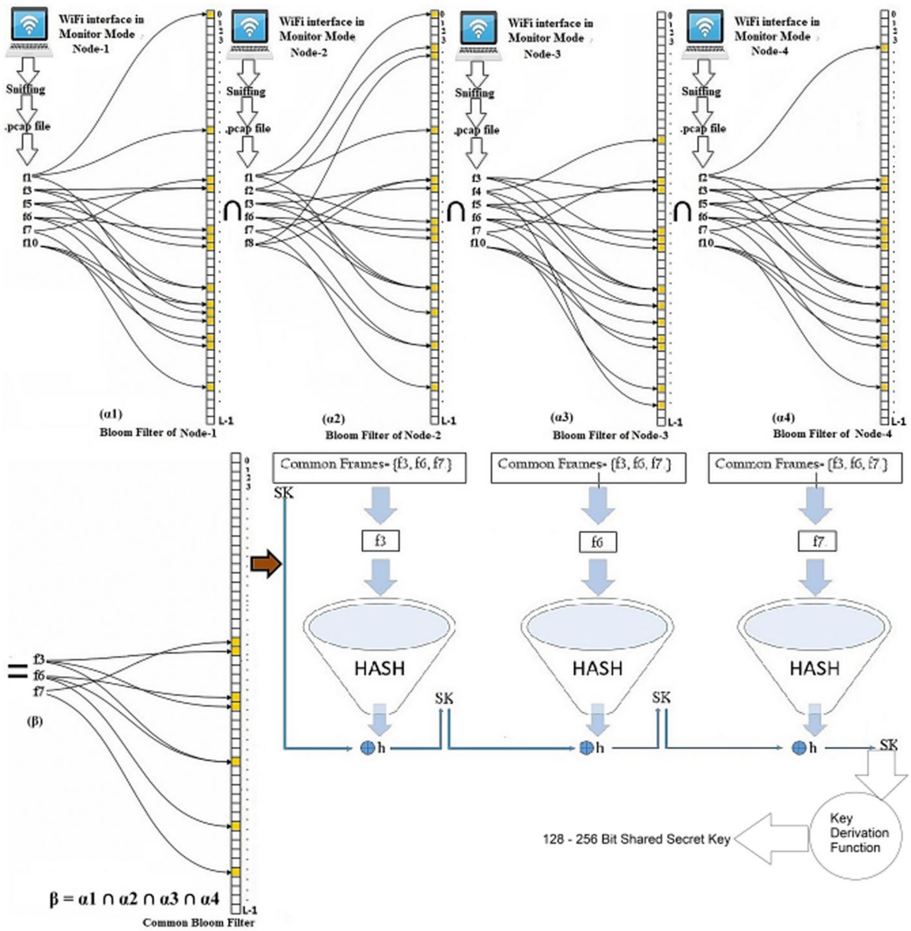
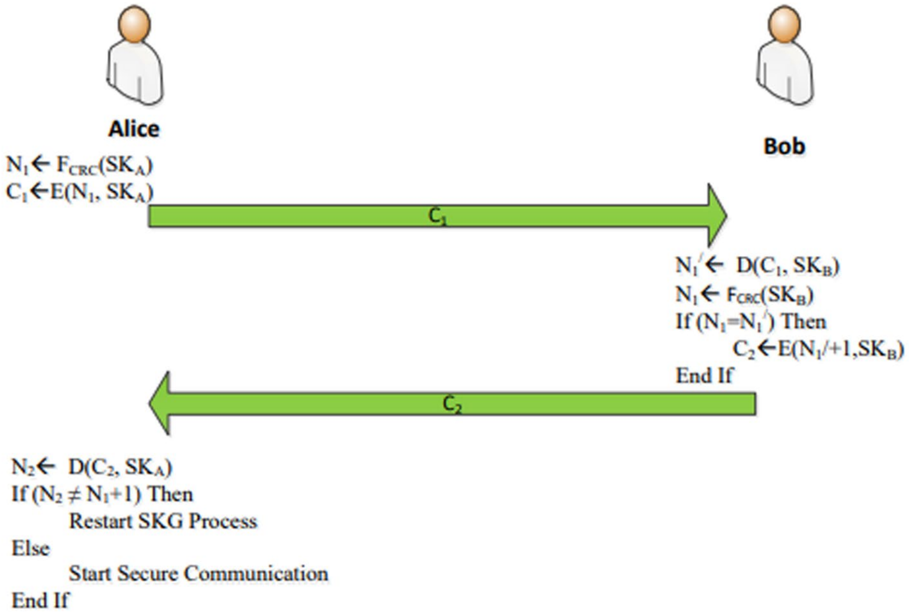


Fig. 5 Complete SKG Model. This figure depicts WiFi interfaces set in monitor mode capturing Wi-Fi frames from the surrounding. These frames are then mapped onto bloom filters, exchanged, and common frames are derived through the intersection of bloom filters. Each node processes common frames through a hash function, generating a shared secret key

filter. Notably, the absence of a single frame in the attacker's query can suffice to generate a shared secret, particularly if the omitted frame is commonly shared among legitimate groups of nodes.

Our proposed SKG protocol hinges on the identification of a set of frames that are consistently present in the Bloom filters of all participating nodes. This common Bloom filter is the intersecting point of various Bloom filters, enabling the identification of frames important for secret key derivation, as can be seen from Fig. 5. In this figure, four nodes are shown, which, on exchange of their Bloom filters with one another, compute the intersection of all received Bloom filters ($\alpha 1$, $\alpha 2$, $\alpha 3$, and $\alpha 4$), and the resultant bloom $\beta{=}\alpha_1 \cap \alpha_2 \cap \alpha_3 \cap \alpha_4$ is obtained. When nodes query Bloom filter β at their ends, they find that frames f3, f6, and f7 are present in it. The contents of these frames are obtained from the.pcap file. The frames are passed to standard hash functions, and the outputs are XORed. This shared secret is passed to the key derivation function such as HKDF to generate an encryption key of the required length. This final output can be used for protected communication.



```
N1 ← FCRC(SKA)
C1 ← E(N1, SKA)
```

```
N1/ ← D(C1, SKB)
N1 ← FCRC(SKB)
If (N1=N1/) Then
    C2 ← E(N1/+1,SKB)
End If
```

```
N2 ← D(C2, SKA)
If (N2 ≠ N1+1) Then
    Restart SKG Process
Else
    Start Secure Communication
End If
```

Fig. 6 Key Validation. The figure illustrates the use of a simple and cost-effective CRC algorithm, modified into a challenge/response protocol, for validating the shared key

The key validation in the proposed secret key generation (SKG) model involves using a simple and cost-effective algorithm, the Cyclic Redundancy Check (CRC). As illustrated in Fig. 6, Alice computes the CRC of her key SK_A as N_1, encrypts N_1 with SK_A as C_1, and sends it to Bob. Bob decodes C_1 with his key SK_B as $N_1^{/}$, computes the CRC of SK_B, and compares it with N_1. If they match, Bob increments $N_1^{/}$, sends it back to Alice as C_2. Alice decrypts it, and if the result matches $N_1 + 1$, key validation is successful for encrypted communication initiation using symmetric key cryptography protocols such as AES, TwoFish, BlowFish, Serpent, and 3DES.

To enhance the security of the system, we can renew the encryption key by combining the old key with a newly acquired key through a process called XORing. The formula for generating the new key is: $Key_{new} = Key_{old} \oplus Key_{new}$. This updated key can then be used for subsequent encryption and decryption processes. So, the strength of this approach lies in its ability to dynamically renew the key. While an attacker is attempting to crack the key, our proposed System Key Generator (SKG) generates a new dynamic key, making the cracking attempt more challenging.

6 Protocol for new node joining

In the context of symmetric secret key generation, the concept of scalability is addressed to seamlessly integrate new nodes into a growing communication network. When a new node wishes to join, it engages in a handshake with an existing node to obtain a group key. Both nodes quickly analyze 802.11 frames in monitor mode, exchanging filled Bloom filters. They then execute the SKG method, including key validation. After validating the newly generated keys, the existing node encrypts the old key with the new one, transmitting the encrypted key to the new node. Upon decryption using the acquired pairwise key, the new node obtains the group key already used by existing nodes, enabling secure communication within the network. We have carefully investigated new node

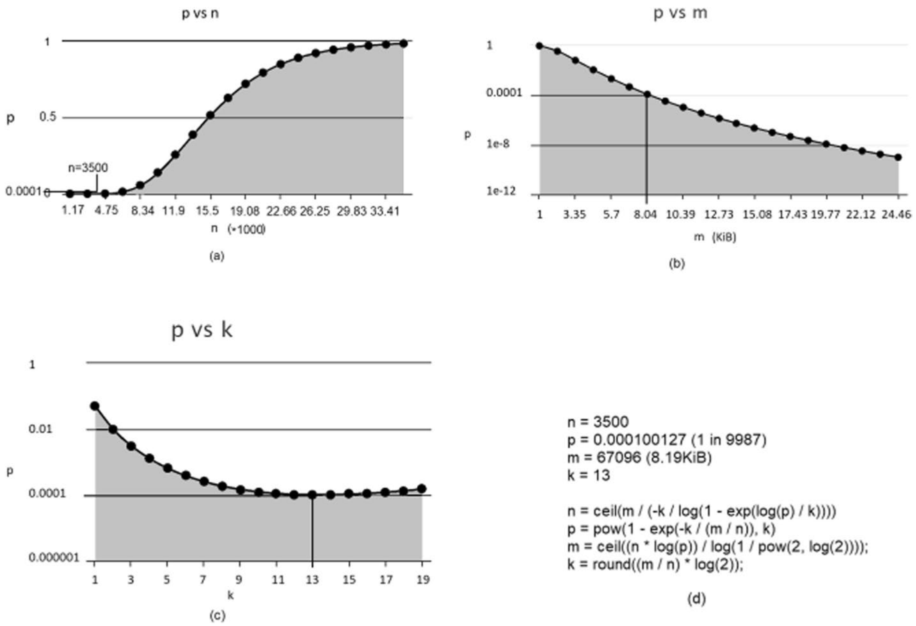
Table 2 Optimizing bloom filter in terms of its size, FPR, and hash functions

n (number of frames)	*p* (FPR)	*m* (length of Bloom filter)	*k* (hash functions)
100000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{469, 410, 352, 293\}$	$\{27, 23, 20, 17\}$
90000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{423, 369, 315, 264\}$	$\{27, 23, 20, 17\}$
80000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{374, 328, 281, 235\}$	$\{27, 23, 20, 17\}$
70000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{328, 287, 246, 205\}$	$\{27, 23, 20, 17\}$
60000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{281, 246, 211, 176\}$	$\{27, 23, 20, 17\}$
50000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{235, 205, 175, 147\}$	$\{27, 23, 20, 17\}$
40000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{187, 163, 140, 88\}$	$\{27, 23, 20, 17\}$
30000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{140, 122, 105, 52\}$	$\{27, 23, 20, 17\}$
20000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{94, 81, 70, 59\}$	$\{27, 23, 20, 17\}$
10000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{46, 40, 35, 30\}$	$\{27, 23, 20, 17\}$
1000	$\{1^{-8}, 1^{-7}, 1^{-6}, 1^{-5}\}$	$\{5, 4.1, 3.5, 3\}$	$\{27, 23, 20, 17\}$

joining protocol process. It is established that there is no significant but rather a negligible chance of sniffing old and new keys because the principle of generating keys remains the same in case when two nodes want to communicate securely or when a new node wants to join the group. The principle is that it is hard for the attacker to capture all OTF frames correctly, which are received by a legal node due to resting away from legal node by the distance $\lambda/2$ and difference in experience in multi-path fading.

7 Analysis and optimization of bloom filter false positives

Bloom filters are highly useful data structures, and they let us trade-off between false positive rate (FPR) p, length or size of Bloom filter m and hash functions k. Table 2 gives the optimum theoretical values of m, k for p at given n. m is been expressed in KiB, where $0.976562KiB = 1KB$. From such an analysis of information, the designer of the secure communication system can derive optimum values of m and k for its systems. Different online tools are available to find these values quickly. One of these tools is available on [79]. Moreover, we provide a real example that answers, what values of m and k are required to maintain and process the given number of input frames n for a desired value of FPR p?. It is suggested that the designer himself has to figure out the values of m and k rather than just relying on the theoretical values obtained from the standard equations of the Bloom filter. The equations given in Fig. 7d have been extracted from [79]. Similarly, the designer cannot rely on the values obtained from online tools such as [79]. It does not mean that these sources are useless. These sources are very useful. The values obtained from these sources lead us to the nearest values of the above-mentioned variables. The values of the above-mentioned variables may vary with the nature (collision-resistant factor) of the hash functions being used. Strong collision-resistant hash functions can reduce FPR. Our results are based on the Python library of Murmer hash functions. The results given in Table 2 lead us to the nearest optimum values of m and k. This means, we cannot rely on the theoretical claims provided in this table. There is a need to go toward more robust values. Thus, n, m, and k can be adjusted for the desired value of FPR using Bloom filter equations discussed in Sect. 4.2.1 and online source [79]. The results given in Table 2 have been equally verified using the spreadsheet software



```
n = 3500
p = 0.000100127 (1 in 9987)
m = 67096 (8.19KiB)
k = 13

n = ceil(m / (-k / log(1 - exp(log(p) / k))))
p = pow(1 - exp(-k / (m / n)), k)
m = ceil((n * log(p)) / log(1 / pow(2, log(2))));
k = round((m / n) * log(2));
```

Fig. 7 Bloom Filter Optimization. The figure illustrates how Bloom filters are tuned to adjust the desired rate of false positives while maintaining an optimal length of the Bloom filter and number of hash functions for a known number of elements

Open Office Calc on Kali Linux. From Fig. 7, we found that the value of k increases in a linear fashion with bits per frame m/n. It means that if we increase the number of hash functions, it will demand more processing cycles from the underlying microprocessor. Similarly, bigger Bloom filters ask for more storage space. These two parameters are critical in deciding the acceptable rate of false positives. Thus, in low-resource wireless systems, these parameters must be handled with great care.. For the validity of values in Table 2 claimed by Bloom filters, we took 3500 as the number of input frames n and set the value of FPR p to 0.0001. The theoretical values of m and k obtained using the online calculator [79] were 67096 and 13, respectively. Figure 7 shows how a Bloom filter can be optimized. The graphs in this figure have been produced using the online Bloom filter calculator [79]. Figure 7a helps to decide the number of input frames for the acceptable rate of false positives for the known values of p and k. Similarly, Fig. 7b, c helps to choose the optimum values of m and k provided the values of n and p are known in advance. Figure 7d just shows the respective equation used to find $m, n, k,$ and p. For $n \leq 3500$, the selected.csv files were made to contain a similar number of frames. The frames of these files were successfully mapped onto their respective Bloom filters. The nodes exchanged their Bloom filters. The frames of these.csv files were queried successfully with an error probability equal to 0.0001. The frames were queried and subsequently used for common secret key generation. Practically, we found that desired FPR p can be achieved with $\mathrm{k} = 7$ instead of $\mathrm{k} = 13$ (theoretical) and $\mathrm{m} = 60000$ Bits instead of $\mathrm{m} = 67096$ Bits (theoretical). The reader is requested to refer to Table 2 for the theoretical values. The output number of common frames was equally verified through the intersection of SQL tables of the.csv files. SQLlite on the Kali Linux platform is used for SQL operations in this research. The variation between practical and theoretical values of k

and *m* is due to the choice of hash functions. For example, high collision-resistant hash functions provide more optimized values of *p, m, k*, and *n*. So, we have concluded that the designers of the security system must be aware of the fact that the theoretical values of these parameters are not fully optimized and reliable. But these values are very close to optimized ones. By increasing/decreasing the values of *k* and *l*, a Bloom filter can be optimized for some acceptable value of error probability (FPR).

8 Probabilistic analysis of IEEE 802.11 frame losses

We have tried our level best to carry out a probabilistic analysis of the resiliency of the proposed model. It is well known that wireless medium is erroneous in nature and causes bit errors and frame losses. Theoretically, a frame transmitted by the sender has only two options: Either it will be received correctly or incorrectly by the receiver. The incorrectly received frames are re-transmitted using a feedback mechanism until they are received correctly by the receiver at its link layer. This feedback mechanism is also used at higher layers for the reliable delivery of data. This feature is implemented at the transport layer using TCP protocols. Here, we are interested in the probability of frame loss at the attacker node at its MAC layer. The performance analysis of transmission errors of 802.11 DCF has been done in [80], where the probability of frame collision or the probability that a frame is received in error is given as $P_{fl} = 1 - (1 - \tau)^{D-1}(1 - P_{BE})^{l}$, where D is the number of nodes and l is the length of the frame. Since in ad hoc mode RTS/CTS is disabled, that is why the component $(1 - \tau)^{D-1})$ can be omitted from this equation. This component is the inability of the station to transmit a frame in a randomly chosen slot. A similar study on bit error has been carried out by Gustave Anderson in his PhD research work [81]. The probability of error rate (P_{BE}) in 802.11 networks has been reported as 0.27 [82]. But it varies from scenario to scenario. If P_{BE} is the bit error probability and l is the frame length, then the frame loss probability can be expressed as $P_{fl} = 1 - (1 - P_{BE})^{l}$. If the attacker is intended to capture a large number of frames (n) distributed over a longer span of time (t), it will definitely result in an increased probability of frame loss at the attacker. Here n and t are interchangeable. Thus, P_{fl} will become $1 - (1 - P_{BE})^{l \times n}$. The increase in distance d and data rate r also increases the probability of bit errors [82]. So, now $P_{fl} = 1 - (1 - P_{BE})^{l \times n \times d \times r}$. But, from the experiments, we have seen that when two or three attackers project the joint attack, their collective probability of incorrectly receiving the frame or the probability of frame loss decreases. Similarly, mobility v also affects the correct receiving of the frames. The final form of the P_{fl} can be given by the following Eq. (15). It is important to clarify that our current focus is not on analyzing the partial impact of the mentioned parameters. Instead, we are examining the broader trend or consensus regarding the factors influencing the probability of frame loss. This is why specific weights are not assigned to these parameters in our evaluation.

$$P_{fl} = 1 - (1 - P_{BE})^{\left(\frac{l \times n \times d \times v \times r}{a}\right)} \tag{15}$$

Figure 8 shows that the probability of a frame missed or lost by the attacker increases with the capturing time, number of frames, and size of the frame. But it decreases with the number of attackers. This is because if two or more attackers combine their captured

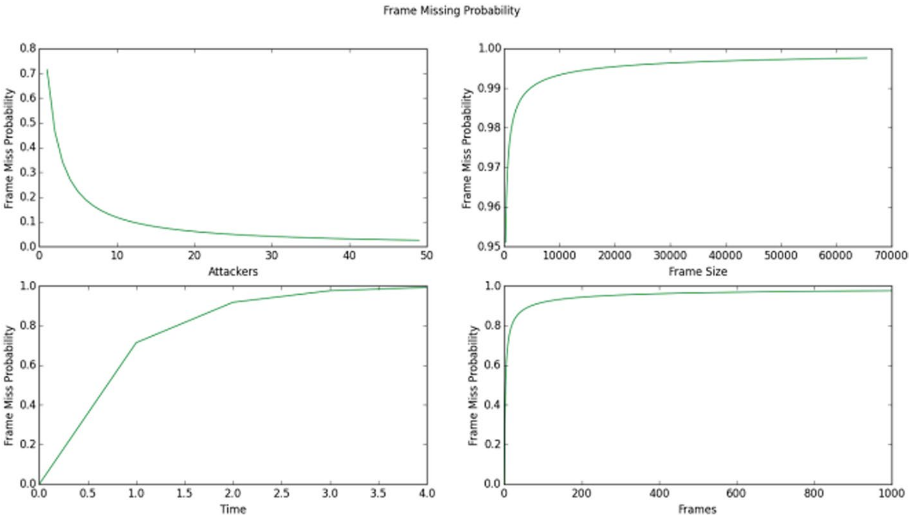


Fig. 8 Frame Lost Probability by Attacker. This graph demonstrates that the probability of frame loss by an attacker with frame size, number of frames, and frame size but decreases with an increase in the number of attackers

frames, then their probability of frame loss becomes reduced. The individual effects of these parameters on the probability of frame loss are shown in Fig. 8. The parameters such as distance, mobility, and the data rates of modulation schemes affect the probability of frame loss in the same way.

9 Results and discussion

The matter of concern is not the probability of frames being lost by the attackers. Rather, concern is the probability of a frame lost by the attacker but received at the legitimate node. For simplicity, we took two capturing files from a test case. One file belongs to a legitimate node named B4, whereas the other belongs to an attacker named AA37. The average capture file size is about 80 MB. The total number of frames captured by B4 is 231469, and that of AA37 is 292617. These numbers contain all types of frames available in the air. We found in raw form that there were about 68571 frames that were missed by AA37 but received by B4. A file of size 11 MB was also transmitted from one node to another during the process of capturing. So, about 14634 OTF TCP data packets were sent by the sender. AA37 captured 9273, and B4 captured 8645. The captured.pcap files were converted into.csv files and.csv files to SQL tables for similarity or overlap analysis. Then the SQL query operations were carried out to find the number of frames that were missed by AA37 but received by the legitimate node. It was observed that there are about 2094 frames that are missed by the attacker but received by the legitimate node. The reason for loss of frame is that reception and loss are independent at the legitimate and attacker nodes. It was observed that 5989 frames were missed by the legitimate node and 5451 by the attacker. Thus, the probability of a frame being missed or lost by the attacker Pas is $\frac{5451}{14634} = 0.37$, and the probability of a frame being lost by the legitimate node Pns is $\frac{5989}{14634} = 0.4$. Similarly, the probability ($Pnsas$) of a frame being lost by the attacker but correctly received by the legitimate node is $\frac{2094}{8645} = 0.24$. The probabilities of frames missed and correctly received are equally probable at the legitimate node and the

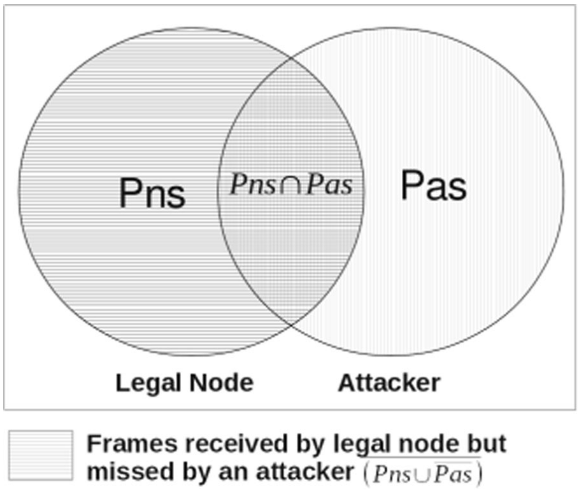

Pns
$Pns \cap Pas$
Pas
Legal Node
Attacker
▤ Frames received by legal node but missed by an attacker $\overline{(Pns \cup \overline{Pas})}$

Fig. 9 Probability of Frame Received by a Legal Node But Missed by the Attacker. This figure highlights the probability of an attacker missing a frame that is successfully captured by a legitimate node, showing a significant probability in this context

attacker node because these events occur randomly and independently. This probability is modeled in Fig. 9. This model, along with Eq. (16), validates the findings, or vice versa [83].

$$Pnsas = \overline{(Pns \cup \overline{Pas})} = \overline{Pns} \cap Pas = 0.4 \times 0.633 = 0.25 \tag{16}$$

From this analysis, we can conclude that there is an $\approxeq$ 25% chance that the packet received by the legitimate node has been missed or lost by the attacker. This value of probability seems to be very small, but it is the probability of one frame. While calculating it over a large number of frames can provide us with a more realistic picture of the scenario, for this purpose, we have used Poisson distribution for modeling the events of frame losses at legitimate nodes and eavesdroppers that are independent [84]. The basic form of Poisson distribution has been given in Eq. (17).

$$P_P(\lambda, k) = e^{-\lambda} \frac{\lambda^k}{k!} \tag{17}$$

In this equation, λ is the average rate of events or mean observed after many trials. k is the exact number of events we want to observe. With little mathematics, we can find the frame loss probability for $k = 1$ over many frames. If

$$e^{-0.25} \frac{0.25^1}{1!}$$

is the probability of missing a single frame over one frame, then

$$\left(1 - e^{-0.25} \frac{0.25^1}{1!}\right)$$

is the probability of not missing that frame. Thus,

$$1-\left(1-e^{-0.25}\frac{0.25^{1}}{1!}\right)^{110}$$

is the probability of a single frame being missed over 110 frames received at the receiver; this probability approaches 1 with the given parameters that are shown in the above expression. It means that if a node has captured about 110 frames, then there is probably a 100% chance that one of the 110 frames has been missed by the attacker. Additionally, the longer the capture duration, the higher the likelihood that the attacker will lose a frame.

9.1 Key refresh rate

The designer of a crypto-system must define the refresh rate of the encryption key. It means how many times a day, month, or year a secret key is reset or refreshed. This time gap might be seconds, minutes, hours, transactions, or even transmission sessions. We believe the secret key must be refreshed in a timely manner because if it is not done in a defined way, it can be compromised. In reality, the user is unaware that its key has been compromised. Sometimes a user comes to know that its key has been compromised when a substantial loss has already occurred. In most cases, these losses become hard to reverse.

A qualitative model can be used for the analysis of secret key security. We can say that either the secret key is completely safe or completely compromised. Key safety and compromise are always independent of one another. It means that if the key is not reset, it can be compromised. It can be compromised even if it is reset. But the regular reset can reduce the time in which the attacker can perform some malicious activity. Thus, the secret key can be reset regardless of whether it is in a safe state or compromised. Thus, the period of a key in which it is safe and in which it is compromised is also independent. Safe key periods are also random; the same is true of compromised periods. The safety of a secret key can be measured in terms of entropy H_{key}. Here entropy means how many bits are required to know the entire secret key. So in the beginning of any crypto-system, $H_{key} = Length_{key}$ means none of the key bits are known to an adversary. Key safety and compromise both have the characteristics that fulfil the conditions of Poisson processes. In crypto-systems, key leakages may appear on different occasions, and it cannot be claimed that there is no secret key leakage. The adversary can exploit every leakage to have complete knowledge of the secret key. If we assign the key reset job to the network administrator, then the safety time period of the key can be increased. But, in the event of administrator absence or when he or she forgets to reset the secret key, the compromised time span may increase to an unexpected level. Thus, key reset and leakage can be modelled as a Poisson distribution in the form of binary events. Poisson process or Poisson distribution can be used to model the events independently (singly and randomly) over a series of time [85]. It also assumes that the rate of occurrence of events remains the same and that future occurrences of these events exhibit memory-less properties. It means the events occurring in the future are not dependent on past events. For simplicity, we would like to use a parameter L_r for the leakage events and S for the time periods in which the key is set or refreshed periodically by the network administrator.

The time period in which the key is not refreshed or reset is S_{off}. In other words, S_{off} is the time duration in which the crypto-system is no more secure. Since one leakage event is not related to the other, that is why they also exhibit a memory-less property. Thus, if the leakages are memory-less then S_{off} can be modelled using Eq. 18 [9].

$$S_{\text{off}} = \frac{S}{1 - e^{-L_r S}} - \frac{1}{L_r} \tag{18}$$

Thus, if the key is reset once an hour and leakage takes place once a day, that is, $\frac{1}{L_r} = 24S$, then from our model of key compromise given in Eq. (18), we can derive a period in which the system is vulnerable to the adversary using Eq. (19).

$$\begin{aligned} \text{Since,}\ \ S_{\text{off}} &= \frac{S}{1 - e^{-L_r S}} - \frac{1}{L_r} \\ S &= 1/24L_r \\ S_{\text{off}} &= \frac{S}{1 - e^{-1/24}} - 24S \\ S_{\text{off}} &= S\left(\frac{1}{1 - 2.7182818284590452353602874713527^{-1/24}} - 24\right) \end{aligned} \tag{19}$$

Key refreshment rate can be defined using Eq. 20.

$$K_r = \frac{\text{key resets}}{\text{unit time}}. \tag{20}$$

For $K_r = \frac{5}{1\,\text{h}}$, the security off-period can be calculated using Eq. 21.

$$S_{\text{off}} = \frac{\left(\frac{S}{1-e^{-1/24}} - 24S\right)}{K_r} \approxeq 0.10069442435513935S \tag{21}$$

It means that, on average, the adversary has about 0.1 h or 6 min to carry out some vicious operation. In the above derivation, the value of e is 2.7182818284590452353602874713527, which is a universal constant. In this scenario, we have assumed that the time period S is in hours. Furthermore, we have taken a very short time frame of 24 h. If we increase this time span and the key refresh is also not very regular or the administrator forgets to update the secret key according to the mentioned schedule, then the time frame to perform the malicious activity becomes larger. In other words, if we increase the frequency of key refreshment, then the time to perform the malicious activity or leakage becomes reduced. This trend is shown in Fig. 10. The graph in this figure is drawn between key refreshment rate ($K_r = \frac{\text{key resets}}{\text{unit time}}$) and $S_{\text{off}} = \frac{\left(\frac{S}{1-e^{-1/24}} - 24S\right)}{K_r}$. The trend shows that by increasing the rate of secret key resets, we can reduce the secret key unsafe time span or leakage rate.

After all that analysis, we have decided to suggest that secret keys must be ephemeral. Ephemeral secret keys are those where a separate key is used for every new transmission session. Since our model is quick at generating symmetric keys, that is why there is no harm in adopting this model for acquiring ephemeral secret keys for new secure transmission sessions. In addition to all that was discussed above, wireless communication at the link layer cannot exist without frame losses. These

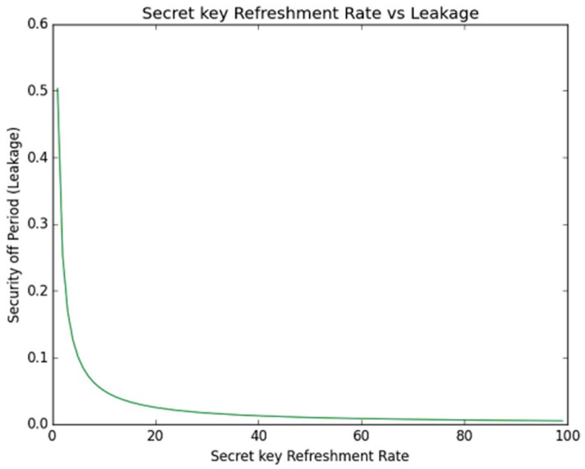


Fig. 10 Secret Key Refresh Rate versus Leakage. The figure indicates that the rate of secret key leakage decreases with an increase in its renewal rate

losses are random and independent of one another. The secret keys obtained from the sniffed frames at any stage of capture are equally random, and their safety is fully maintained, provided that every capturing duration is at least more than half a second [9]. The reason for this condition is that a single frame loss takes place within half a second. Thus, $H_k(t_o = 0.5) = length(frame_i)$ means key entropy is at least equal to the length of the secret bit-string because missing one frame by the adversary is enough to generate a random string of bits for the secret key. The $Frame_i$ is any of the frames that get lost during capture. The longer capturing will result in more losses at the adversary. This means, the key generated at time $t_o + \tau$ will be more difficult for the adversary to guess. This means that to compromise the system, he must have knowledge of all those frames that he has missed, but the legitimate nodes have received and used them in the SKG process. If the adversary has lost n frames, then $H_k(t_o + \tau) = length(frame_{i=1\rightarrow n}) >= H_k(t_o = 0.5)$. Since frame loss occurs within a half second, that is why this feature is a good candidate to be recommended for dynamic secret keys for wireless ad hoc networks.

9.1.1 Key refresh rate in real scenarios

Key renewal is very important in networks, but unfortunately, it requires a balance between security needs and operational efficiency. So, it has to be set vigilantly, considering multiple factors such as network susceptibility to network attacks, network topology, traffic patterns, sensitivity of the data, and computational overheads of the key refresh rate. But the key refresh rate should align with security requirements and the level of perceived threats, ensuring that the key will be updated before the vulnerability is exploited. For instance, in scenarios where data integrity and confidentiality are critical, such as WSNs in power or unclear plants, shorter life times of security keys are necessary because frequent key updates ensure a low impact on the risk of key compromise. In some cases, the availability of the service is crucial, such as when creating a hotspot network in a train or coffee shop for quick data exchange. In these scenarios, key refresh rates might be kept longer because, in such cases, the user network experience and its performance and availability are more important than strict security measures. Similarly, key refreshes are also monitored by regulatory and industry requirements. We have to change our bank login password and university login password after a defined period of time. WPA security default key life is 3600 s [86]. In WiMax networks the key life time more than 12 h is not recommended [87]. To play content on commercially available BD video software, we may need to renew the AACS encryption key. The key, which expires in 12–18 months, is used to protect copyrighted content on Blu-ray movies. By updating the system software to the latest version and the key will automatically be renewed [88, 89]. We cannot decide the key refresh rate of the reader's networks, but we can say that determining the key refresh rate in wireless networks requires network administrators to consider security needs, operational constraints, regulatory requirements, and industry requirements to achieve a balance between security and usability. Periodic risk analysis and security auditing help validate the efficacy of the chosen rate and its alignment with operational security requirements [90].

10 SKG comparison

Worst-case complexity analysis is a cost analysis of an algorithm when it performs the maximum number of operations or steps to process a given input of size N. Best-case complexity is the lower bound on the algorithm's running time, while average-case complexity considers the average number of steps required to compute the input. It is essential to know the time complexities of certain mathematical operations and processing algorithms before discussing the complexities of SKG schemes. For example, matrix multiplication, matrix inversion, and polynomial multiplication have time complexities of $O(N^3)$, $O(N^3)$, and $O(N^2)$ [91]. For example Primality test is the heart of DH and RSA algorithms, with Miller Rabin primality test running in $O(RN^3)$ bit operation, here R is the number of rounds and N is the number that has to be tested for primality [92]. Wireless physical layer SKG schemes, which are based on CSI, have various costs, including channel estimation (LSE, MMSE), reconciliation (error correcting codes), and privacy amplification (universal hash functions, extractors). The existing state-of-the-art schemes for computing CSI are expensive due to the complexity of least square channel estimation methods. The cost of channel state estimation using LSE is $O(N^3)$, which is unacceptably high. The length of training bits or pilot symbols also plays an important role in the computational complexity of estimation algorithms. The complexity of estimation techniques such as LS, MMSE, and OLR-MMSE has been well studied by Jaap et al., who found that LS, MMSE, and OLR-MMSE have low, high, and moderate complexities, respectively. LSE, LMMSE, and LMMSE-SV are widely practiced as channel estimation techniques in data communication. Asymptotic space/time complexity analysis of these techniques has been carried out by Zhang et al., with time complexities of LSE, LMMSE, and LMMSE-SV reported as $O(N)$, $O(N^4)$, and $O(N^2)$, respectively. In addition to the complexities mentioned above, channel-based SKG schemes also require error detection and correction codes for reconciliation, which demand extensive computing resources. This makes channel estimation-based techniques unsuitable for low-resource wireless devices. Channel parameters are not available at higher layers, and specialized hardware and software are required to acquire channel parameters at the software layers of the network stack. Analog-to-digital converters are also required for working at Nyquist rate for single-tone carrier frequency.

RSS calculation can be performed in $O(N^2)$, but secret key agreement incurs additional costs of reconciliation and amplification. The minimum computational cost of naive error correction procedures is $O(M^3)$, which is low in Wozencraft Ensemble Codes and Reed Solomon Codes. The space complexity for RSS-based techniques is $O(N^2)$, as they require additional bandwidth and multiple antennas for high bit generation due to key mismatches. RSS values are readily available at higher layers using off-the-shelf devices, but due to key mismatches, error correction codes are necessary. Secret bit leakage at this phase requires key amplification functions like universal hash functions or extractors. The complexities of RSS-based techniques contribute to the space complexity.

The computation of BER is a complex process with a complexity of $O(KN^3)$ in CDMA scenarios, where K represents the number of concurrent transmissions and N is the size of the chip/sequence per data bit. A reduced cost algorithm for BER calculation has been proposed, but its software development is time-consuming. For 2D constellation systems in Rayleigh fading channel, the computation complexity is $O(KN^2)$. The worst case requires $O(K)$ memory space, as the BER value is recorded against every transmission. For better results, a large number of transmissions are required to generate a longer secret key, and excessive re-transmissions cause excessive power drainage.

The application-level signature verification in UFH scenarios, used for secret sharing in the presence of a jammer, can lead to a denial of service (DOS) attack due to the exponential workload complexity at the receiver. This complexity is on average $\sim((N/l)+1)^l$, where N is the number of packets successfully arrived at the receiver and M is the number of fragments divided by the sender. This complexity can be reduced to a linear time complexity through cryptographic linking of individual packets using hash links or chains. One way hash chains have $O(N)$ time and space complexity. The total cost of UFH-based techniques is given in Eq. (22),

$$complexity{\sim}(N/l+1)*l+(N/l+1) \tag{22}$$

where $\sim(N/l+1)*l$ is the cost of hash verification and $(N/l+1)$ is the cost of signature verification.

The proposed SKG scheme focuses on capturing a large number of frames, focusing only on the data frames. Reduction is applied to select only the OTFs for secret key generation, reducing storage requirements by storing data bytes only. The space complexity of the solution is $O(\log(N)+L)$, where L is the size of a Bloom filter and N is the number of frames. This linear space complexity can be expressed as *O(L)*. The time complexity of the solution is $O((K)+\log(N))$, where K is the number of independent hash functions. If parallelized, this complexity can be lowered to $O(\log(K)+\log(N))$. K does not increase significantly with the increase in input N, and it does not reach higher values. It can also be reduced to a linear time complexity of $O(1)$, making the time complexity of the proposed approach $O(\log(N))$. The intersection or overlapping of Bloom filters can be processed using bit-wise binary operations that are faster than higher language comparison operations. A summarized view of the observation is given in Table , allowing readers to easily compare the complexities of different SKG schemes. The proposed simple SKG solution is within the reach

Table 3 Comparison of SKG techniques

Technique	Features	KGR	Key Mismatch	Computation	Memory	Band width	1	2	3	4
{CSI,CIR} [53, 54, 56, 93, 94]	Average information measure, low probability of symmetric secret key generation, subject to hardware mismatches, practically not possible to measure CSI at both nodes at the same, high key bit mismatches, Shehadeh et al. [56] is the advanced version of Shehadeh et al. [93]	75% [54], 68 bits per single-channel and 6793 bits per' second [56]	10% [54], less than 10^{-3} [56]	$O(M^3)$ [95–97]	$O(N)$	High	✓	✓	✓	X
RSS [23, 98–100]	Can be validated using off-the-shelf devices like USRP, not much hardware changes are required, robust to synchronization, RSSI accessible at higher layers, require reconciliation and amplification [101].	KGR with single-bit extraction is 16%, but error correction codes (gray codes) and multiple bit extraction it is 67% [23], achieves bit rate of 800 bps, generates 128 secret bits in 160 milliseconds [100]	Mismatch rate is 11% in the case of heterogeneous devices, 50% in static environment with single-bit extraction which with multiple bit extraction [23], 100% key agreement [100]	$O(N^2)$ [102]	$O(N)$	High	✓	✓	✓	X
FHSS [103]UFH [62, 63] [65]	FH and UFH both resist jamming, eaves-dropping, and traffic analysis with no key mismatches, but FH is hopping sequence dependent, whereas UFH encounters too much re-transmissions	100%	0%	FH is $O(N)$ [104], UFH is $(N/l+1)*l+(N/l+1)$ [105]	$O(N)$	Very High	X	X	X	✓
BER [61]	Average information measure, low probability of symmetric secret key generation, symmetric BER fluctuations at both ends may not be accurate in real networks, high key mismatches	128 bits per 12.42 second per 90 millisecond, but 20 millisecond is enough to generate shared secret that significantly shortens the key generation time	Key agreement is 100% with error correction and 70% without error correction codes	$O(KN^3)$ reduced to $O(KN^2)$ [106–108],	$O(K)$ fluctuations	High	✓	✓	✓	X

Table 3 (continued)

Technique	Features	KGR	Key Mismatch	Computation	Memory	Band width	1	2	3	4
Proposed SKG Scheme	Used space/time efficient data structures Bloom filters that needs small amount of memory, computing power and bandwidth.{ where K is the number of hash functions, L is the size of Bloom filter in bits, and N is number frames to mapped; does not need to load whole list of frames in memory}	Key generation rate is adaptable, even a single shared is enough to generate secret key of any size	Adjustable, depends upon size and number of hash functions of the bloom filter. For example key error 0.0001 is achieved with $k = 7$ m = 60000, and $n = 3500$ frames	*O(log(N))*	*O(L)*	Small	X	X	✓	✓

1 = Key Reconciliation Required?; 2 = Key Amplification Required?

3 = Key Validation Required?; 4 = Support Group Key?

of resource-constrained wireless devices, with a computational complexity of $O(\log(N))$ and a space complexity of $O(L)$ (Table 3).

In addition, proposed link layer secret key generation systems are valid in real-world scenarios where quick protected communication is required. For example WSNs, wireless communications, IoT devices, ad hoc networks, military and defense applications. It is well-known that WSNs operate in hostile environments where classic cryptographic key distribution methods may not be feasible. Link layer SKG methods can establish secret keys quickly based on randomly shared frames. So, wireless communications systems can enhance security and privacy by using off-the-shelf devices, or built-in wireless radio interfaces, which are accompanied with most of the today devices without altering physical layer. Proposed framework is valid in IoT devices that are often low in resources and make traditional key management protocols challenging to implement. Ad hoc networks can also establish secure communication links using proposed approach without relying on pre-existing key distribution infrastructures, which are not scalable. Proposed link layer SKG methodology provides an additional layer of security, making it harder for adversaries to intercept or compromise protected communication channels. The proposed link layer SKG framework is designed to cater to a variety of scenarios, including WBAN, wearables, and hotspots. These scenarios involve the creation of short-term hotspot networks for information or internet sharing, while individuals are on the move, such as during train travel or while enjoying coffee in cafes. Additionally, the framework addresses the need for secure communication in contexts like making payments at ticketing booths.

11 Limitation & challenges

1. The proposed model operates with the assumption that wireless nodes are configured for key acquisition in monitor/promiscuous, which may result in a slight increase in energy consumption compared to normal operation. However, the substantial benefits of this approach outweigh the associated energy expenditure. This is because nodes will promptly revert to normal mode once they converge on a shared secret key.
2. Some wireless interfaces do not support monitor mode, necessitating a driver update for the hardware. This requirement involves a software update and is not a significant impediment to the adoption of the solution.
3. The community of computational security (RSA, DH, AES, etc.) is very large; replacing it with unconditional security is one of the greatest challenges.
4. As far as potential attackers are concerned, there is a possibility of intercepting shared frames. It has been noted that as the number of WiFi interfaces utilized by attackers rises, the instances of shared frames being captured by legitimate nodes but eluding attackers decrease. The threat can be addressed with longer captures and multiple interfaces.

12 Conclusion

Computational is conditional, meaning that with large enough computing resources, the security of the crypto-system can be breached. So, the replacement for the issue is information-theoretic security, which does not depend on the computing power of the adversary. Furthermore, quantum computing is going to become a reality, and if it does happen, the entire space will probably be unprotected. That is why, from the present study, it is concluded that in the case of wireless networks, secret key generation from natural and random processes of physical layer communication is one of the most suitable options. The proposal presents a detailed methodology poised to deliver valuable insights and practical progress. The outlined Secret Key Generation (SKG) solution offers cost-effective, adaptable, and secure key establishment, yielding ephemeral secrets that greatly enhance wireless communication security. But it cannot be ignored that configuring nodes to operate in monitor/promiscuous mode for key generation and renewal can lead to higher energy consumption. This could be a significant drawback for battery-powered devices. Fortunately, devices are set to monitor mode only for the time of shared key generation, and then they can switch to normal mode. So, the key renewal period needs to be set carefully. Similarly, the effectiveness of the key generation process relies on the physical and environmental conditions of the wireless channel, which can vary widely. This variability can impact the reliability of the key generation process. In a highly noisy environment, there is a high chance of quickly generating the key by capturing fewer frames, as there is a high probability that an attacker will quickly miss the frame. However, in low-noise scenarios, it is better to capture more frames for the key generation process to avoid the attacker capturing similar frames to the legal nodes. In the same way, the process of frequent key renewal and validation can introduce additional latency into the communication process, which might be undesirable for time-sensitive applications. Thus, the network administrator is supposed to set key renewal and validation periods carefully. In the future, we would like to implement the proposed framework for secret key generation on real USRP devices. In addition to the Bloom filter, there is also another probabilistic data structure called the Cuckoo filter, which is slightly more expensive than the Bloom filter but generates a lesser number of false positives [109, 110]. We would like to compare both data structures to validate their performance in real-life scenarios. Furthermore, Map Reduce is one of the key technologies that efficiently finds commonality among different sets of elements. We would like to exploit it to find the group shared secret in less computational time.

Abbreviations

ACK	Acknowledgment
AOA	Angle of arrival
ARQ	Automatic Repeat reQuest
AWGN	Additive White Gaussian Noise
BER	Bit error rate
CFR	Channel frequency response
CIR	Channel impulse response
CDMA	Code division multiple access
CSI	Channel state information
DCF	Distributed coordination function
FHSS	Frequency-hopping spread spectrum
GHz	Giga Hertz
GPS	Global positioning system
HMAC	Hash-based message authentication code
HKDF	HMAC-based key derivation function
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
LMMSE	Linear minimum mean square error
LMMSE-SV	Linear minimum mean square error with singular value decomposition
LSE	Least squares estimation
LS	Least squares

MAC Layer	Media access control layer
MMSE	Minimum mean square error
OLR-MMSE	Ordered likelihood ratio minimum mean square error
OTF	One Time Frames
PKI	Public key infrastructure
RSA	Rivest Shamir Adleman
RSS	Received signal strength
RTS/CTS	Request to send/clear to send
SKG	Secret key generation
SNR	Signal-to-noise ratio
SQL	Structured Query Language
TCP	Transmission control protocol
TDD	Time division duplex
TOA	Time of arrival
UCFH	Un-coordinated frequency hopping
UFH	Ultra-wideband frequency hopping
USRP	Universal software radio peripheral
WBAN	Wireless body area networks
WiFi	Wireless fidelity
WPA	Wi-Fi-protected access
WSN	Wireless sensor network

Acknowledgements

The authors express their deep gratitude to Dr. T. Ali (National University of Sciences & Technology (NUST), Pak) for his insightful discussions and constructive feedback on the experimental setup, which significantly influenced their final SKG model.

Author contributions

All authors contributed equally.

Funding

This work was supported in part by the National Research Foundation of Korea (NRF) Grant funded by Korean Government, Ministry of Science and ICT (MSIT), under Grant RS-2022-00144000 and Grant RS-2022-00165225, and Basic Science Research Program through the NRF funded by the Ministry of Education (RS-2023-00237300).

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Competing interests

There is no conflict of interest.

Received: 19 February 2024 Accepted: 4 August 2024
Published online: 27 August 2024

References

1. D.S. Bhatti et al., A survey on wireless wearable body area networks: a perspective of technology and economy. Sensors (2022). https://doi.org/10.3390/s22207722
2. I. AlShourbaji, An overview of wireless local area network (WLAN). CoRR arXiv:1303.1882 (2013)
3. Y. Xiao, Y. Pan, *Emerging Wireless LANs, Wireless PANs, and Wireless MANs: IEEE 802.11, IEEE 802.15, 802.16 Wireless Standard Family*, 1st edn. (Wiley Publishing, New York, 2009)
4. B. Rong, Security in wireless communication networks. IEEE Wirel. Commun. **30**, 10–11 (2023). https://doi.org/10.1109/MWC.2023.10077227
5. J. Zhang, T.Q. Duong, A. Marshall, R. Woods, Key generation from wireless channels: a review. IEEE Access **4**, 614–626 (2016). https://doi.org/10.1109/ACCESS.2016.2521718
6. A.A. Hassan, W.E. Stark, J.E. Hershey, S. Chennakeshu, Cryptographic key agreement for mobile radio. Digital Signal Process. **6**, 207–212 (1996). https://doi.org/10.1006/dspr.1996.0023
7. A. Varshavsky, A. Scannell, A. LaMarca, E. de Lara, Amigo: Proximity-based authentication of mobile devices, in *UbiComp Ubiquitous Computing*, pp. 253–270. (Springer, Berlin, 2007)
8. A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, A. LaMarca, Ensemble: Cooperative proximity-based authentication, in Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, MobiSys '10, pp. 331–344 (ACM, New York, 2010). https://doi.org/10.1145/1814433.1814466
9. S. Xiao, W. Gong, D. Towsley, Secure wireless communication with dynamic secrets, in *Proceedings of the 29th Conference on Information Communications*, INFOCOM'10, p. 1568–1576 (IEEE Press, Piscataway, 2010)
10. D.S. Bhatti, S. Saleem, Ephemeral secrets: multi-party secret key acquisition for secure IEEE 802.11 mobile ad hoc communication. IEEE Access **8**, 24242–24257 (2020). https://doi.org/10.1109/ACCESS.2020.2970147
11. D.V. Linh, V.V. Yem, Key generation technique based on channel characteristics for MIMO-OFDM wireless communication systems. IEEE Access **11**, 7309–7319 (2023). https://doi.org/10.1109/ACCESS.2023.3238573

12. Y. Abdallah, M.A. Latif, M. Youssef, A. Sultan, H. El Gamal, Keys through ARQ: Theory and practice. IEEE Trans. Inf. Forensics Secur. **6**, 737–751 (2011). https://doi.org/10.1109/TIFS.2011.2123093
13. R. Lin, L. Xu, H. Fang, C. Huang, Efficient physical layer key generation technique in wireless communications. EURASIP J. Wirel. Commun. Netw. **2020**, 13 (2020). https://doi.org/10.1186/s13638-019-1634-7
14. N. Aldaghri, H. Mahdavifar, Physical layer secret key generation in static environments. IEEE Trans. Inf. Forensics Secur. **15**, 2692–2705 (2020). https://doi.org/10.1109/TIFS.2020.2974621
15. F. Rottenberg, T.-H. Nguyen, J.-M. Dricot, F. Horlin, J. Louveaux, CSI-based versus RSS-based secret-key generation under correlated eavesdropping. IEEE Trans. Commun. **69**, 1868–1881 (2021). https://doi.org/10.1109/TCOMM.2020.3040434
16. J. Zhou, X. Zeng, Physical-layer secret key generation based on domain-adversarial training of autoencoder for spatial correlated channels. Appl. Intell. **53**, 5304–5319 (2023). https://doi.org/10.1007/s10489-022-03777-w
17. L. Czap, V.M. Prabhakaran, C. Fragouli, S. Diggavi, Secret message capacity of erasure broadcast channels with feedback, in 2011 IEEE Information Theory Workshop (ITW), pp. 65–69. https://doi.org/10.1109/ITW.2011.6089579 (IEEE, Paraty, 2011)
18. A. Puri, S. Kumar, Error control codes: a novel solution for secret key generation and key refreshment problem. Int. J. Comput. Appl. **92**, 1–6 (2014). https://doi.org/10.5120/15970-4720
19. Y. Zhang, Y. Xiang, X. Huang, Password-authenticated group key exchange: a cross-layer design. ACM Trans. Int. Technol. **16**, 241–2420 (2016). https://doi.org/10.1145/2955095
20. N. Saxena, S. Grijalva, Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication. IEEE Trans. Ind. Inf. **13**, 1482–1491 (2017). https://doi.org/10.1109/TII.2016.2610950
21. Riihikallio, P. Tuning your Wi-Fi by adjusting transfer rates. Last updated: 17th Sept.. 2018, Accessed on Dec. 2019
22. Ergen, M. IEEE 802.11 tutorial (2002)
23. S. Jana, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments, in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, pp. 321–332. https://doi.org/10.1145/1614320.1614356 (ACM, New York, 2009)
24. K. Ren, H. Su, Q. Wang, Secret key generation exploiting channel characteristics in wireless communications. IEEE Wirel. Commun. **18**, 6–12 (2011). https://doi.org/10.1109/MWC.2011.5999759
25. L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels. IEEE Trans. Wireless Commun. **7**, 2571–2579 (2008)
26. T. Mazloum, A. Sibille, Analysis of secret key randomness exploiting the radio channel variability. Int. J. Antennas Propag. (2015). https://doi.org/10.1155/2015/106360
27. L. Cheng et al., Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase. Mob. Inf. Syst. **1**(13), 2017 (2017). https://doi.org/10.1155/2017/7393526
28. I. Safaka, C. Fragouli, K. Argyraki, S. Diggavi, Creating shared secrets out of thin air, in *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, HotNets-XI, pp. 73–78 (ACM, New York, 2012). https://doi.org/10.1145/2390231.2390244
29. M.J. Siavoshani, et al. Exchanging secrets without using cryptography. CoRR arXiv:1105.4991 (2012)
30. B.H. Bloom, Space time trade-offs in hash coding with allowable errors. Commun. ACM **13**, 422–426 (1970). https://doi.org/10.1145/362686.362692
31. A. Broder, M. Mitzenmacher, A.B.I.M. Mitzenmacher, Network applications of bloom filters: a survey, in *Internet Mathematics*, pp. 636–646 (2002)
32. S. Geravand, M. Ahmadi, Survey bloom filter applications in network security: a state-of-the-art survey. Comput. Netw. **57**, 4047–4064 (2013). https://doi.org/10.1016/j.comnet.2013.09.003
33. D. Randall, Bloom filters and hashing (2006). Lecture and notes by: Alessio Guerrieri and Wei Jin on CS 6550 Design and Analysis of Algorithms: Accessed on 15th Oct. 2018
34. H. Marais, K. Bharat, Supporting cooperative and personal surfing with a desktop assistant, in *Proceedings of the 10th Annual ACM Symposium on User Interface Software and Technology*, UIST '97, pp. 129–138 (ACM, New York, 1997). https://doi.org/10.1145/263407.263531
35. L. Fan, P. Cao, J. Almeida, A.Z. Broder, Summary cache: a scalable wide-area web cache sharing protocol. IEEE/ACM Trans. Netw. **8**, 281–293 (2000). https://doi.org/10.1109/90.851975
36. D. Jost, U. Maurer, J. Ribeiro, *Information-Theoretic Secret-Key Agreement: The Asymptotically Tight Relation Between the Secret-Key Rate and the Channel Quality Ratio: 16th International Conference, TCC 2018*, Panaji, India, November 11–14, 2018, Proceedings, Part I, pp. 345–369 (2018)
37. N. Smart, *Cryptography: An Introduction,3rd Edition*, chap. 5 (Mcgraw-Hill College (December 30, 2004); eBook (3rd Edition, 2013), 2013)
38. M. Hirt, U. Maurer, V. Zikas, Mpc vs. sfe: Unconditional and computational security, in *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '08, 1–18 (Springer, Berlin, 2008). https://doi.org/10.1007/978-3-540-89255-7_1
39. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
40. G.S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications. Trans. Am. Inst. Electr. Eng. **XLV**, 295–301 (1926). https://doi.org/10.1109/T-AIEE.1926.5061224
41. A. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**, 1355–1387 (1974)
42. S. Leung-Yan-Cheong, M. Hellman, The gaussian wire-tap channel. IEEE Trans. Inf. Theory **24**, 451–456 (1978). https://doi.org/10.1109/TIT.1978.1055917
43. I. Csiszar, J. Korner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**, 339–348 (1978). https://doi.org/10.1109/TIT.1978.1055892
44. M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**, 733–742 (1993). https://doi.org/10.1109/18.256484
45. R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans. Inf. Theory **39**, 1121–1132 (1993). https://doi.org/10.1109/18.243431

46. I. Csiszar, P. Narayan, Common randomness and secret key generation with a helper. IEEE Trans. Inf. Theory **46**, 344–366 (2006). https://doi.org/10.1109/18.825796
47. P. Hoffman, The man who loved only numbers: The story of Paul Erdos and the search for mathematical truth (1998)
48. D.T. Murphy, What, if anything, is epsilon? (2014). https://pdfs.semanticscholar.org/da63/9bc5e88d1ab31da1fb80f020f95e986792b4.pdf. Accesses on: 16th August 2019
49. Z. Wan, K. Huang, Y. Lou, Y. Chen, Channel covariance matrix based secret key generation for low-power terminals in frequency division duplex systems. Electron. Lett. **57**, 324–327 (2021). https://doi.org/10.1049/ell2.12123
50. S. Mathur, R. Miller, A. Varshavsky, W. Trappe, N. Mandayam, Proximate: Proximity-based secure pairing using ambient wireless signals, in *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, pp. 211–224 (ACM, New York, 2011). https://doi.org/10.1145/1999995.2000016
51. Q. Wang, H. Su, K. Ren, K. Kim, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, in 2011 Proceedings IEEE INFOCOM, pp. 1422–1430 (2011). https://doi.org/10.1109/INFCOM.2011.5934929
52. A. Badawy, et al. Secret key generation based on AoA estimation for low SNR conditions, vol. 2015 (2015). https://doi.org/10.1109/VTCSpring.2015.7146072
53. R. Wilson, D. Tse, R.A. Scholtz, Channel identification: Secret sharing using reciprocity in ultra-wideband channels. IEEE Trans. Inf. Forens. Secur. Part **1**(2), 364–375 (2007). https://doi.org/10.1109/TIFS.2007.902666
54. M.G. Madiseh, M.L. McGuire, S.S. Neville, L. Cai, M. Hori, Secret key generation and agreement in UWB communication channels, in *2008 IEEE Global Telecommunications Conference (GLOBECOM' 08)*, pp. 1–5 (IEEE, New Orleans, 2008). https://doi.org/10.1109/GLOCOM.2008.ECP.356
55. M. Guillaud, D.T.M. Slock, R. Knopp, A practical method for wireless channel reciprocity exploitation through relative calibration, in *Proceedings of International Symposium on Signal Processing and its Applications (ISSPA '05)*, pp. 403–406 (IEEE, 2005). https://doi.org/10.1109/ISSPA.2005.1580281
56. Y.E.H. Shehadeh, O. Alfandi, D. Hogrefe, Towards robust key extraction from multipath wireless channels. J. Commun. Netw. **14**, 385–395 (2012). https://doi.org/10.1109/JCN.2012.6292245
57. W. Diffie, M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (2006). https://doi.org/10.1109/TIT.1976.1055638
58. S.T. Ali, D. Ostry, V. Sivaraman. Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks, in *2010 IEEE IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)* pp. 644–650 (2011)
59. P. Van Torre, Channel-based key generation for encrypted body-worn wireless sensor networks. Sensors **16**, 1453 (2016). https://doi.org/10.3390/s16091453
60. K. Argyraki et al., Creating secrets out of erasures, pp. 429–440 (2013). https://doi.org/10.1145/2500423.2500440
61. T. Kitano, A. Kitaura, H. Iwai, H. Sasaoka, A private key agreement scheme based on fluctuations of BER in wireless communications, in *The 9th International Conference on Advanced Communication Technology (Volume: 3)*, ICACT'07, pp. 1495–1499. https://doi.org/10.1109/ICACT.2007.358651 (IEEE, 2007)
62. M. Strasser, C. Pöpper, S. Capkun, M. Cagalj, Jamming–resistant key establishment using uncoordinated frequency hopping, in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, SP '08, pp. 64–78 (IEEE Computer Society, Washington, 2008). https://doi.org/10.1109/SP.2008.9
63. J.S. Sousa, J.P. Vilela, A characterization of uncoordinated frequency hopping for wireless secrecy, in *7th IFIP Wireless and Mobile Networking Conference, WMNC 2014, Vilamoura, Portugal, May 20–22, 2014*, pp. 1–4 (IEEE, 2014). https://doi.org/10.1109/WMNC.2014.6878885
64. A. Liu, P. Ning, H. Dai, Y. Liu, USD–FH: Jamming-resistant wireless communication using uncoordinated frequency hopping with uncoordinated seed disclosure, in *The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010)*, pp. 41–50 (IEEE, San Francisco, 2010). https://doi.org/10.1109/MASS.2010.5663968
65. P. Manjola, S. Sharmila, Anti-jamming broadcast communication using un-coordinated frequency hopping. Int. J. Appl. Innov. Eng. Manag. (IJAIEM) **2**, 26–28 (2013)
66. G. Sona, P. Annapandi, A. Shinney, Establishing adversary resistant communication in wireless network. Int. J. Innov. Res. Comput. Commun. Eng. **2**, 2053–2058 (2014)
67. M. Elsabagh, Y. Abdallah, M. Youssef, H. El Gamal, ARQ security in wi-fi and rfid networks, in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1212–1219 (2010). https://doi.org/10.1109/ALLERTON.2010.5707052
68. Y.S. Khiabani, S. Wei, ARQ-based key scheduling algorithm over correlated erasure channels, in *31st IEEE Military Communications Conference, MILCOM 2012, Orlando, FL, USA*, October 29–November 1, 2012, pp. 1–6 (2012). https://doi.org/10.1109/MILCOM.2012.6415667
69. Jafari Siavoshani, M., Fragouli, C., Diggavi, S., Pulleti, U. & Argyraki, K. Group secret key generation over broadcast erasure channels, in *2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers*, pp. 719–723 (2010). https://doi.org/10.1109/ACSSC.2010.5757657
70. L. Czap, C. Fragouli, Secure key exchange in wireless networks, in *2011 International Symposium on Networking Coding*, pp. 1–6. https://doi.org/10.1109/ISNETCOD.2011.5978921 (2011)
71. A. Gakhov, *Probabilistic Data Structures and Algorithms for Big Data Applications* (Books on Demand, 2019)
72. J. Lu et al., Low computational cost bloom filters. IEEE/ACM Trans. Netw. **26**, 2254–2267 (2018). https://doi.org/10.1109/TNET.2018.2869851
73. J. Honorof, An examination of bloom filters and their applications. https://cs.unc.edu/~fabian/courses/CS600.624/slides/bloomslides.pdf (2006)
74. L. Carrea, A. Vernitski, M. Reed, Yes-no bloom filter: a way of representing sets with fewer false positives. CoRR arXiv:1603.01060 (2016)
75. D. Clayton, C. Patton, T. Shrimpton, Probabilistic data structures in adversarial environments, pp. 1317–1334. https://doi.org/10.1145/3319535.3354235 (2019)

76. H. Krawczyk, P. Eronen, HMAC-based extract-and-expand key derivation function (HKDF), in Request for Comments (RFC) 5869. IBM Research and Nokia (Internet Engineering Task Force (IETF), 2010)
77. A.B. Cloud, The master, managed, ad-hoc, and monitor modes of the wireless network adapter (2018). https://topic.alibabacloud.com/a/the-master-managed-ad-hoc-and-monitor-modes-of-the-wireless-network-adapter_8_8_32140912.html. Last accessed on 30 June 2022
78. Parth. Difference—promiscuous vs. monitor mode (wireless context) (2008). http://lazysolutions.blogspot.com/2008/10/difference-promiscuous-vs-monitor-mode.html. Last Accessed on 30 June 2018
79. T. Hurst, Bloom filters calculator. Last updated: 15th 2018. Accessed on Dec. 2018
80. P. Chatzimisios, A.C. Boucouvalas, V. Vitsas, Performance analysis of IEEE 802.11 DCF in presence of transmission errors, in *2004 IEEE International Conference on Communications* IEEE *(Cat. No.04CH37577)*, vol. 7, pp. 3854–3858 (2004)
81. G. Anderson, *Bit Error Rate and Capacity Estimation in Wireless Networks*. Ph.D. dissertation, Drexel University, Philadelphia (2011). http://hdl.handle.net/1860/3430
82. W. Jiang, Y. Ma, Bit error rate analysis of wi-fi and Bluetooth under the interference of 2.45 ghz RFID. J. China Univ. Posts Telecommun. **14**, 89–93 (2007). https://doi.org/10.1016/S1005-8885(08)60019-9
83. ck12. Probability using a venn diagram and conditional probability. URL https://www.ck12.org/probability/venn-diagrams/lesson/Probability-Using-a-Venn-Diagram-and-Conditional-Probability-ALG-II/. Accessed 20th Jan 2020
84. W.J. Thompson, Poisson distributions. Comput. Sci. Eng. **3**, 78–82 (2001)
85. M343:applications of probability, modeling events in time and space (2012). https://www.open.edu/openlearn/ocw/pluginfile.php/1118700/mod_resource/content/3/Modelling%20events%20in%20time_m343_1.pdf. Accessed 20th Jan 2020
86. Stone_Horse. Group key renewal (2022). TP-Link (Home Network Community), Last edited on 2022-12-03 21:59:33. Access on 20th March, 2024
87. F. Falcone, P. Trimintzios, G. Georgiou, Wifi and wimax secure deployments. J. Comput. Syst. Netw. Commun. **2010**, 423281 (2010). https://doi.org/10.1155/2010/423281
88. Renewing the aacs encryption key. Online. © 2022 Sony Interactive Entertainment Inc
89. P. McHenry, Wpa2 default key renewal (2012). Last edited on 2021-07-03 10:50 PM, Access on 20th March, 2024
90. S. Posea, Renewal Periods for Cryptographic Keys. Master's thesis, Eindhoven University of Technology (2012). Master's Thesis, Access on 20th March, 2024
91. K. S. do Prado Kelvin Salton do Prado, Understanding time complexity with python examples (2019). An electronic medium publication sharing concepts, ideas, and codes, Accessed on 20th Aug. 2020
92. T.H. Cormen, C. Stein, R.L. Rivest, C.E. Leiserson, *Introduction to Algorithms*, chap. 31. Number Theoretic Algorithms, 2nd edn., pp. 849–896 (McGraw-Hill Higher Education, 2001)
93. Y.E.H. Shehadeh, O. Alfandi, K. Tout, D. Hogrefe, Intelligent mechanisms for key generation from multipath wireless channels, in *2011th Wireless Telecommunications Symposium (WTS)*, pp. 1–6 (IEEE, New York City, 2011). https://doi.org/10.1109/WTS.2011.5960848
94. G. Merline; R. C. Porselv, Addressing the temporal correlation in wireless channel for secure communication, in *2013 International Conference on Communications and Signal Processing (ICCSP)*, pp. 428–432 (IEEE, Melmaruvathur, 2013). https://doi.org/10.1109/iccsp.2013.6577089
95. Y. Dong, Y. Tang, K.Z. Shenzhen, Improved joint antenna selection and user scheduling for massive MIMO systems, in *16th IEEE/ACIS International Conference on Computer and Information Science, ICIS 2017, Wuhan, China*, May 24–26, 2017, pp. 69–74. https://doi.org/10.1109/ICIS.2017.7959971 (2017)
96. S. Chen, Accurate acquisition of MIMO channel state information: How big the problem. University of Southampton lecture in ELEC6014 AWCNSs: Advanced Topic Series (2014)
97. D.F.S. Murga, *Feedback of Channel State Information in Multi-Antenna Systems Based on Quantization of Channel Gram Matrices*. Ph.D. dissertation, Universitat Polit'ecnica de Catalunya (UPC) (2012)
98. M.N. Hemavathi, V.K. Annapurna, A survey on secret key extraction using received signal strength in wireless networks. Int. J. Recent Innov. Trends Comput. Commun. **2**, 209–213 (2014)
99. A. Zanella, Best practice in RSS measurements and ranging. IEEE Commun. Surv. Tutor. **PP**, 1 (2016). https://doi.org/10.1109/comst.2016.2553452
100. G. Revadigar, C. Javali, H.J. Asghar, K.B. Rasmussen, S. Jha, iARC: Secret key generation for resource constrained devices by inducing artificial randomness in the channel, in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, Singapore*, April 14–17, 2015, p. 669 (2015). https://doi.org/10.1145/2714576.2714644
101. G. Margelis, et al. Efficient DCT-based secret key generation for the internet of things. *Ad Hoc Netw.* **92**, 101744 (2019). https://doi.org/10.1016/j.adhoc.2018.08.014. Special Issue on Security of IoT-enabled Infrastructures in Smart Cities
102. S. Hegde, *Introduction to Computational Complexity Theory*. Department of Computer Science and Automation, Indian Institute of Science, India (2014). http://drona.csa.iisc.ernet.in/~chandan/courses/complexity14/notes/lec1.pdf. Accessed on 25th Aug 2017
103. J. Boer, Direct sequence spectrum: Physical layer specification IEEE 802.11. Tech. Rep., New Jersey, USA (1996)
104. M. Strasser, *Novel Techniques for Thwarting Communication Jamming in Wireless Networks*. Ph.D. dissertation, ETH ZURICH (2009)
105. M. Cagalj, Jamming-resistant key establishment using uncoordinated frequency hopping (2009). feihu.eng.ua.edu/NSF_CPS/year2/W5_3_slides.ppt. Accessed on 18th August 2017
106. R. Morrow, J. Lehnert, Packet throughput in slotted ALOHA DS/SSMA radio systems with random signature sequences. IEEE Trans. Commun. **40**, 1223–1230 (1992)
107. J. Robert, K. Morrow, Accurate CDMA BER calculations with low computational complexity. IEEE Trans. Commun. **46**, 1413–1417 (1998)
108. L. Szczecinski, H. Xu, X. Gao, R. Bettancourt, Effcient evaluation of BER for arbitrary modulation and signaling in fading channels. IEEE Trans. Commun. **55**, 2061–2064 (2007)

109. Y. Zhao et al., A review of cuckoo filters for privacy protection and their applications. Electronics **12**, 2809 (2023)
110. B. Fan, D.G. Andersen, M. Kaminsky, M.D. Mitzenmacher, Cuckoo filter: practically better than bloom, in *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, pp. 75–88 (2014)

Publisher's Note

David Samuel Bhatti is working as a postdoc researcher in the InfoNet lab. School of Electrical Engineering and Computer Science, GIST, Republic of Korea. Previously, he was associated with the University of Central Punjab (UCP) in Lahore, Pakistan. He earned his Ph.D. in Computer Science with a specialization in Information Security from the School of Electrical Engineering and Computer Science (SEECS) at the National University of Sciences and Technology (NUST) in Islamabad, Pakistan, in 2020. Dr. Bhatti's research interests span various domains, with a focus on networks, mobiles, and smartphones security. His expertise extends to secure routing protocols, secret key establishment, and device authentication, particularly in low-resource devices like wearables, body-worn devices, and WBANs. His current research endeavors involve the design of security protocols using probabilistic data structures. The aim is to optimize time and space complexity in low-resource devices, enhancing their efficiency and robustness in the realm of information-theoretic security.

Shahzad Saleem formerly associated with the School of Electrical Engineering and Computer Science (SEECS) at the National University of Sciences and Technology (NUST) in Islamabad, Pakistan, is currently on an extended leave from SEECS. He is actively engaged in research at the Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, KSA, focusing on Information Security with a keen interest in Digital Forensics. Dr. Saleem holds an MS in Information and Communication Systems Security from The Royal Institute of Technology, Sweden, and a Ph.D. in Digital Forensics from the Department of Computer and Systems Sciences, Stockholm University, Sweden. His expertise includes extensive work with industry-standard digital forensics tools such as i2 Analyst Notebook, EnCase, FTK, XWays, UFED, XRY, and Device Seizure.

Heung-No Lee received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of California at Los Angeles, CA, USA, in 1993, 1994, and 1999, respectively. He was a Research Staff Member with the HRL Laboratories, LLC, Malibu, CA, USA, from 1999 to 2002. From 2002 to 2008, he was an Assistant Professor with the University of Pittsburgh, PA, USA. In 2009, he joined the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju, South Korea. He is currently with the Gwangju Institute of Science and Technology. His research interests include information theory, signal processing theory, blockchain, communications/networking theory, and their application to wireless communications and networking, compressive sensing, future internet, and brain-computer interface. He has received several prestigious national awards, including the Top 100 National Research and Development Award, in 2012, the Top 50 Achievements of Fundamental Research Award, in 2013, and the Science/Engineer of the Month, in January 2014.

Ki-Il Kim received the MS and PhD degrees in computer science from Chungnam National University, Daejeon, Korea, in 2002 and 2005, respectively. He is affiliated with the Department of Computer Science and Engineering at the Chungnam National University, Daejeon, Korea. He has been with the Department of Informatics at Gyeongsang National University since 2006. His research interests include machine learning for networks, wireless/mobile networks, fog computing, MANET, QoS for wireless, and wireless sensor networks.