ACCEPTED FROM OPEN CALL

Physical Layer Security for the Internet of Things: Authentication and Key Generation

Junqing Zhang, Sekhar Rajendran, Zhi Sun, Roger Woods, and Lajos Hanzo

Abstract

A low-complexity, yet secure framework is proposed for protecting the IoT and for achieving both authentication and secure communication. In particular, the slight random difference among transceivers is extracted for creating a unique radio frequency fingerprint and for ascertaining the unique user identity. The wireless channel between any two users is a perfect source of randomness and can be exploited as cryptographic keys. This can be applied to the physical layer of the communications protocol stack. This article reviews these protocols and shows how they can be integrated to provide a complete IoT security framework. We conclude by outlining the future challenges in applying these compelling physical layer security techniques to the IoT.

Introduction

Our life is being fundamentally transformed by the Internet of Things (IoT), which allows ubiquitous connection of people, machines and environments. IoT applications are being applied in smart cities and homes, intelligent transportation, healthcare, and so on. For example, implantable medical devices such as pacemakers, or wearables, for example, Fitbit, can provide 24/7 monitoring of our physiological conditions, promoting a healthier life style and enabling timely medical intervention whenever necessary. IoT applications look to make our lives much smarter and more personalized and convenient.

Most IoT devices are connected wirelessly as exemplified by WiFi, IEEE 802.15.4 (ZigBee), Bluetooth, Narrowband IoT (NB-IoT), LoRa, and Sigfox. For any IoT systems, data confidentiality and authenticity are paramount as many IoT applications carry private, sensitive or confidential data. For example, healthcare data such as heart rate from wearable devices is personal and therefore highly confidential and needs to be secure.

A secure wireless communication system involves authentication and secure transmission [1]. Authentication verifies the user's identity and prevents malicious users from accessing the network, while secure transmission protects data integrity and confidentiality using encryption schemes. Conventional authentication and confidentiality schemes are mainly cryptography-based, and are handled in different communication layers of the protocol stack. For example, LoRaWAN authentication uses a network and an application session key during its over-the-air-activation process. ZigBee exchanges both network- and link-keys, while Bluetooth uses the Elliptic Curve Diffie-Hellman (ECDH) public-private key exchange for authentication. Regarding secure communications, legitimate parties employ symmetric encryption such as the advanced encryption standard (AES), which relies on a secret key shared between them beforehand. Public key cryptography (PKC) is the de facto key distribution protocol.

Although cryptographic schemes have been efficient in protecting modern communication and computer networks, their applications in IoT have been challenged. First, conventional schemes are based on complex mathematical problems and protocols. These schemes work well for devices having powerful capabilities, such as smartphones. On the other hand, there are a large amount of IoT devices that are of low cost, small size, and battery-powered, such as Fitbit. These lightweight devices may not be able to support computationally complex algorithms needed to perform complex cryptography. Second, conventional cryptographic schemes are computationally secure as their security is achieved when the attacker fails to decipher the protection within a certain amount of time. Traditional PKC is mathematically complicated and difficult to solve, for example, relying either on employing integer factorization or discrete logarithm algorithms. However, it may be compromised due to developments in quantum computing, which has the potential to have a severe impact on public key cryptography. Finally, conventional authentication schemes are based on the MAC or IP addresses, which can be easily tampered with by attackers employing malware.

Because of the limited protection, there have been increasingly notorious IoT cyberattacks. The transformative revolution that IoT aims to bring about is thus compromised by the lack of secure connectivity. All of these attacks have compromised societal trust in IoT services. Therefore, it is necessary to develop new security primitives for vulnerable IoT applications.

There are emerging techniques that exploit the unique features and characteristics of the transceiver hardware and wireless channels for security purposes. The received signal $r(t)$ can be formulated as

$$r(t) = F_u[x(t)] * h(t) + n(t), \quad (1)$$

where $F_u[\cdot]$ is the transceiver effect imposed on user u, $x(t)$ is the transmitted signal, $h(t)$ is the wireless channel, and $n(t)$ is the noise. Due to the

Digital Object Identifier:
10.1109/MWC.2019.1800455

Junqing Zhang is with the University of Liverpool; Sekhar Rajendran and Zhi Sun are with the University at Buffalo, the State University of New York; Roger Woods is with Queen's University Belfast; Lajos Hanzo is with the University of Southampton.

1536-1284/19/$25.00 © 2019 IEEE

imperfections of the manufacturing process, there are subtle differences between the radio frequency components of the transceivers, which will result in slight feature variations among them. These features of each transceiver, that is, $F_u[\cdot]$, are unique and can be observed from the electromagnetic waves that are emitted by it. This signature exploits the individual characteristics of the transceiver's analog circuitry and is obtained from the wireless physical layer. This is termed *radio frequency fingerprinting (RFF)* and results in a fingerprint that can be used to authenticate the individual device's identity. Explicitly, the process of differentiating and measuring the fingerprints of the analog circuitry is RFF identification [2]. The channel between any two users, that is, $h(t)$, is determined by the propagation environment, which is also affected by the user/object movements. The random nature of the wireless channel between users can be exploited as common information and employed as the cryptographic key, which is termed as *key generation from wireless channels* [3].

RFF identification and key generation are eminently suitable for IoT. First, neither of these two techniques is energy-hungry, hence they can be applied for power-constrained IoT devices. As will be discussed later, RFF identification does not involve complex computations at the devices; the results in [4] demonstrate that the energy required by an ECDH protocol, a popular PKC scheme, is 98 times higher than that needed by key generation. In addition, RFF identification and key generation can be implemented in the context of a real system by exploiting the existing data transmissions, without incurring modification to the standard procedures. RFF identification and key generation thus have attracted much research interest (see [2, 3] and references therein). The authors have carried out extensive work in these areas including RFF identification for ZigBee [5, 6], key generation for WiFi [7, 8] and LoRa [9]. This article first reviews the RFF identification protocol, and then gives a tutorial on the design of key generation. In particular, the key generation implementation and performance in short-range (WiFi) and long-range (LoRa) environments is compared for the first time. Authentication and secure transmission are usually handled separately and independently. Based on the fact that both RFF identification and key generation occur in the physical layer of the communication stack, this article goes beyond and proposes a new and integrated security framework for IoT by combining these two techniques. The article finally concludes with visions of future research challenges.

Radio Frequency Fingerprinting, Authentication by Hardware Variation

Hardware variations in analog circuitry appear in individual circuits as a result of the manufacturing process. These imperfections are universal, distinctive and permanent, and can act as the unique fingerprint for the device. These fingerprints manifest as RFFs, extracted from the electromagnetic waves that are generated when the devices communicate with each other.

Protocol

As shown in Fig. 1, the authenticator aims to classify the N intended users by analyzing their received signals, and carrying out feature extraction and classification. The protocol is explained in detail as follows.

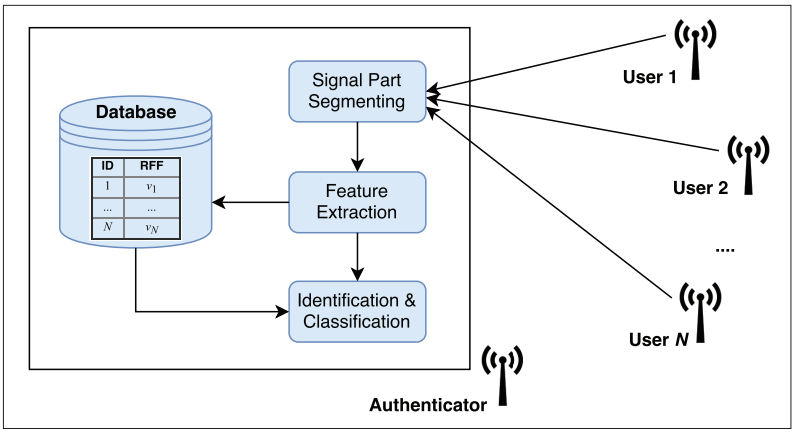

FIGURE 1. RFF identification protocol.

Signal Part Segmenting: After receiving signals from each user, the authenticator partitions them into segments and then identification signals will be extracted from them. The segments that have been applied for RFF identification include the following.

Transient Part: When the frequency synthesizer attempts to lock on to the transmission frequency assigned to the user, the authenticator will separate the turn-on transient part, transition observed when the device is turning on, for identification.

Near-Transient Part: This part includes both the turn-on transient and some segments of the stable signal.

Preamble Part: The power spectral density of the preamble part of the signal may be computed to extract uniquely identifiable features. Both the frequency and phase characteristics of the preamble can be used to create the RFF.

The Entire Signal: The frequency, phase, amplitude and I/Q samples can all be evaluated in the entire signal to extract the RFF features.

RF Burst: For radio-frequency identification (RFID) based systems, the out-of-band emissions of a sinusoidal carrier outside its intended frequency can also be utilized to obtain a fingerprint.

Feature Extraction: The distinct characteristics that are extracted from the signal segments are termed *features*. The features that have been used to represent the RFF include wavelets, FFT spectra, modulation constellation variations, clock skew, transient length and timing errors, to name but a few. The features are related to definitive parts of the transmitter, such as the power amplifier, frequency synthesizer, modulator circuitry, oscillator and the antenna.

Identification and Classification: The objective is to find a function ϕ, which projects the feature space of N users, $V = \{v_1, v_2, v_3 ... v_N\}$, to the so called class space, $C = \{c_1, c_2, c_3 .... c_N\}$, which is formulated as $\phi : V \rightarrow C$, where the function ϕ belongs to a hypothesis space Φ. After the projection, the feature of the specific user is classified to the corresponding class. This hypothesis space can also be mapped on to a real number $\mathbb{R}$ using a so called scoring function, $s : V \times C \rightarrow \mathbb{R}$, which returns a value corresponding to the highest score and can be expressed as

$$\phi(v) = \arg\max_{c} s(v,c). \quad (2)$$

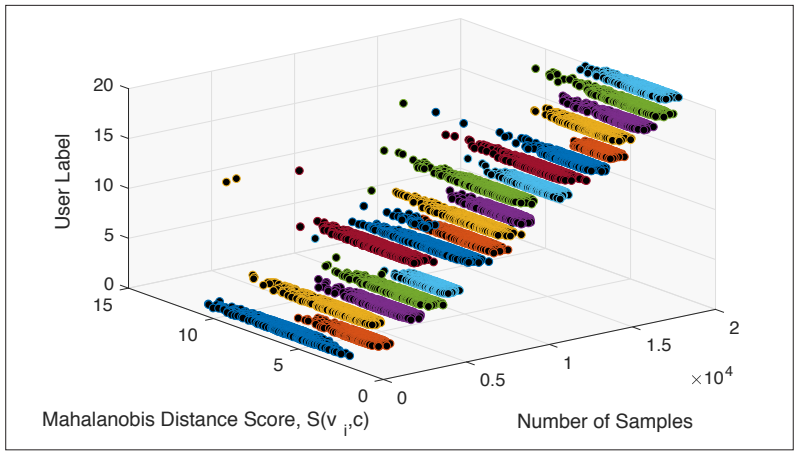

FIGURE 2. ZigBee-based RFF identification.

When $s(v, c)$ is translated to joint probability models, $s(v, c) \rightarrow P(v, c)$ becomes the foundation of the probabilistic classifiers, for example, naive Bayes and linear discriminant analysis.

Let us now consider an input signal received by the authenticator having a feature vector v_i and let the computed score be $s(v_i, c)$. Identification is performed when the score $s(v_i, c)$ exceeds a set threshold value, λ. By contrast, if the computed score is below λ, then the incoming signal is deemed to be from an unauthorized user and its authentication is refused. If the calculated score is above λ, then $\phi(v)$ is computed and the device identity (corresponding class) is inferred.

When the classifier is trained to map the feature space V to the class space C, we have to measure the mapping. A loss function $L(c, \hat{c})$ can be defined, where $\hat{c}$ is the estimated class. The expected loss of ϕ can be estimated by training, using a so-called empirical risk function R_{emp}, formulated as

$$R_{emp}(\phi) = \frac{1}{N} \sum_{i} L\left[c_i, \phi(v_i)\right] \tag{3}$$

This measure helps us to avoid over-fitting and under-fitting scenarios while training. After the classifier is trained, the classified features of the enrolled users are then stored in a database. When a new incoming signal is received, its feature is extracted and its score is computed using the features saved in the database; this is then used for authentication.

In our previous work [6], 20 user scenarios were created, each with two ZigBee devices. These 40 nodes were various ZigBee sensors, such as MicaZ, Imote2 and TelosB, and a USRP N210 connected to a PC, which was used as the authenticator node. The specific feature used in the experiments was the 512-point FFT of the baseband preamble, and 2000 samples per device were collected. The feature classification was carried out by projecting features into a subspace using the Fisher Linear discriminant analysis and then their Mahalanobis distance was measured. The classification error rate was found to be as low as 0.47 percent. Figure 2 characterizes the RFF identification method, where 20 different users were classified versus their Mahalanobis distance score against the number of samples used. In the dataset used as input, 0 to 1000 · n test samples were meant for user n, which is represented as the X axis in the figure. For each test sample, the Mahalanobis distance has been computed and a corresponding color has been allocated to the point, so that the reader can match it with its corresponding user label in the Z-axis.

Applications

RFF identification has been tested on several wireless protocols that are predominantly used in IoT applications. Most IoT networks follow a star network topology and many devices connect to a central hub, which can act as the authenticator.

WiFi uses the WiFi Protected Access (WPA) scheme for authentication which employs the temporal key integrity protocol (TKIP) for its key exchange. Attacks like the TKIP Michael Attack and its variations have already identified severe weaknesses in the WPA scheme, since the MAC address in the WiFi frame is easy to forge (MAC spoofing). By contrast, the RFF of the WiFi network interface cards is difficult to forge, and can hence be employed to strengthen network security [10]. The popular LoRaWAN protocol faces a similar issue, since it uses a network as well as application session key and employs the AES-128 scheme for encryption. Because of the relatively short key length, the network can suffer from multiple potential attacks, and hence the unique device address may be easily spoofed. Along with the state-of-the-art cryptographic-based authentication scheme used in LoRa, the addition of RFF identification can reduce the vulnerability [11]. ZigBee and Bluetooth use variants of the Diffie-Hellman algorithm to exchange keys for authentication. Furthermore, ZigBee uses plain text instead of a cipher text for transmission, which allows the devices to be easily cloned, and the network becomes vulnerable to replay attacks. RFF identification has the potential to enhance the authentication of ZigBee [5].

There are also applications in the context of RFID systems. As the terminology suggests, the nature of RFID is an identification technology, which consists of a reader and RFID tags. Authentication can only happen in an RFID system if they possess a micro controller both in the tag and in the reader, which is not economically feasible given the extremely low cost needs of the application domains. The current authentication for RFID is achieved with the aid of microchips that use hard-wired logic, designed to perform simple authentication and encryption. Unfortunately, even with this modification, RFID can still be easily sniffed, after which an attacker can carry out a replay attack and gain access. This signal replay attack can be prevented by using RFF identification, because the attacker can only copy the data but not the RFF itself [12].

Wireless Key Generation, Secure Communication by Channel Randomness

The wireless channel is intrinsic to the environment, affected by the environment layout, scatterer distribution and materials, as well as by the movement of users or scatterers, and so on. Therefore, the characteristics of wireless channels tend to be unique and unpredictable. The randomness exhibited by the wireless environment between any two users can be exploited to generate cryptographic keys for secure communications [8].

Protocol

Key generation usually works in a pairwise mode between two users, namely Alice and Bob. Without loss of generality, Alice is selected as the initiator and Bob is a legitimate user, who can be authorized by the RFF identification introduced above. As shown in Fig. 3, the process usually includes four stages, namely channel probing, quantization, information reconciliation and privacy amplification.

Channel Probing: The users communicate in a time division duplex (TDD) mode at the same carrier frequency. Bidirectional channel measurements are required for the channel probing stage. During the i^{th} probing at time t_i, Alice sends a packet to Bob, which allows Bob to get the channel measurement $X^B(t_i)$. After time τ, Bob transmits a packet to Alice who can obtain the channel measurement $X^A(t_i + \tau)$. According to the channel reciprocity, when τ is shorter than the coherence time, the channel is highly correlated and the measurements obtained by Alice and Bob will be similar. Alice and Bob repeat the above channel sampling for a certain time to collect sufficient measurements. It is worth noting that in key generation, users are not transmitting keys secretly, but extract keys from the wireless channel by employing a public pilot. No dedicated packet transmissions are required, as the channel measurements can be carried out along with the normal data transmission [13].

Any channel measurement parameter which can reflect the variation is applicable for key generation. The parameters suitable for key generation include:

- *Received signal strength (RSS):* RSS (received power) is the most popular candidate because it is available in almost all the wireless protocols, including WiFi, ZigBee, Bluetooth, LoRa, and so on. However, RSS is the averaged power of a packet which is coarse-grained, thus much randomness information is lost.
- *Channel state information (CSI):* CSI is the channel gain in time, frequency and spatial domains, including both amplitude and phase, which is fine-grained. The estimated CSI can be obtained by diverse wireless techniques. For example, ultra-wideband systems can get the channel impulse response, while orthogonal frequency-division multiplexing (OFDM) and multiple-input and multiple-output (MIMO) can obtain the channel gains in the frequency and spatial domain, respectively. However, the CSI is not made public in many commercial transceivers, which limits its application in key generation.

We have carried out RSS-based key generation experiments using WiFi in an indoor office [8] and using LoRa in an urban environment, representing short-range and long-range environments, respectively. In both cases, the device was carried by a pedestrian, moving at a walking speed, so the channel underwent slow fading. Parts of the results are shown in Figs. 4a and 4b, respectively. A detailed comparison and analysis will be given later. The cross correlation coefficients between the received power of Alice and Bob in the WiFi-based and LoRa-based key generation are 0.9646 and 0.9582, respectively, which indicate a strong reciprocity.

Quantization: Cryptographic applications require a binary sequence as the key, but the channel measurements, X^u, are analog. Quantization can be adopted to convert analog measurements, X^u, to digital ones, K^u, which can be categorized into the absolute-value-based quantizer and differential-value-based quantizer.

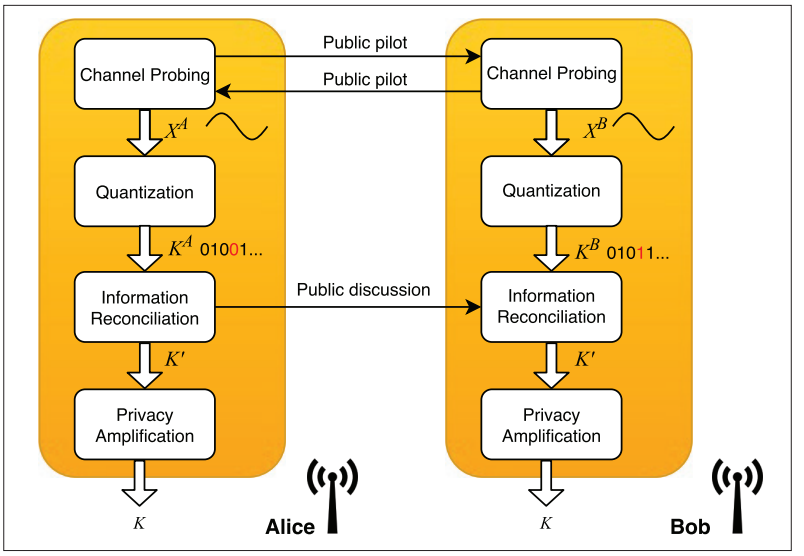

FIGURE 3. Key generation protocol.

The absolute-value-based quantizer works in a similar manner to an analog-to-digital converter. The user will first calculate the quantization thresholds, and then assigns a binary result when it is compared to the channel measurements. The output of such a mean-value-based quantizer example is shown in Fig. 4a. Alice and Bob calculate their mean values as their own thresholds, respectively. All the analog values above the threshold are considered as 1, while the measurements below the threshold are converted to 0.

The differential-value-based quantizer is completed by comparing the difference between adjacent measurements. As shown in Fig. 4b, a 0 is assigned when $X^u(i + 1) \le X(i)$ and a 1 is assigned when $X^u(i + 1) > X^u(i)$.

Information Reconciliation and Privacy Amplification: The channel measurements of Alice and Bob are generally not identical because of the noise and non-simultaneous sampling, which will result in mismatches between the quantized key sequences, K^A and K^B. The percentage of the number of errors over the key length is defined as the key disagreement ratio. As illustrated in Fig. 4a, even if there is only a very slight difference between the measurements of Alice and Bob, it still results in a mismatch after quantization. Information reconciliation is adopted to correct these discrepancies, which can be achieved by employing an error correction code such as BCH or LDPC code. Provided that the number of errors is not excessive, Alice and Bob will then both get the same keys, K'. For example, a (n, k, t) BCH code can correct t out of n errors. For example, a BCH (15, 3, 3) code can correct 20 percent mismatch. The KDR in Fig. 4a is 4.03 percent, which can be corrected. Some public discussion will be required during this stage, for example, exchanging the syndrome, which can be heard by the attackers as well. Finally, privacy amplification is used to remove the information leakage by using the hash function, which completes the key generation process.

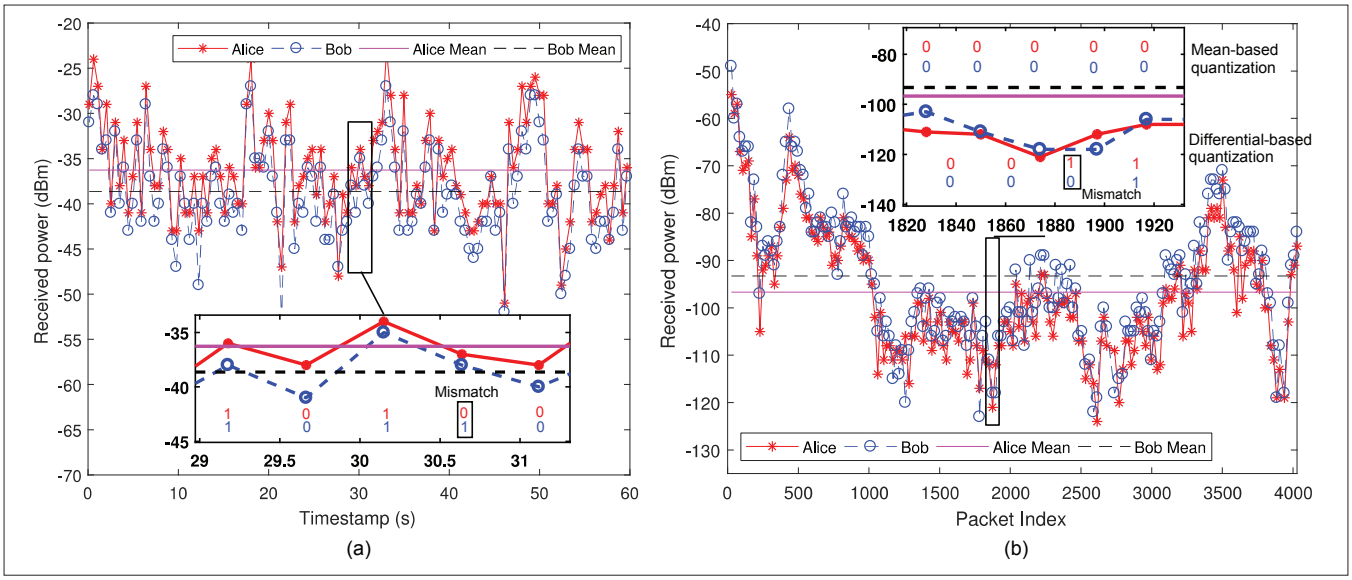

FIGURE 4. a) Key generation using WiFi in an indoor office environment; b) key generation using LoRa in an urban environment.

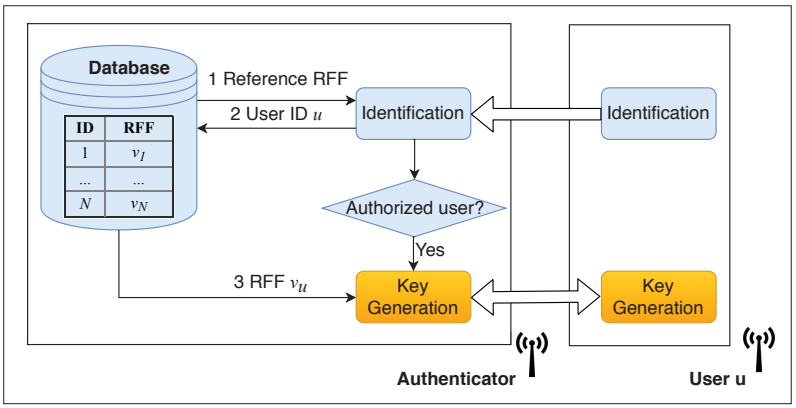

FIGURE 5. An integrated IoT security framework using RFF identification and key generation.

Applications

Key generation has been prototyped for wireless IoT protocols and tested in various environments, demonstrating the practicality of this promising technology. This section reviews key generation applications based on different channel conditions.

Many IoT applications are running in indoor environments, including the smart home. For example, you may want to control home appliances using a smartphone by sending the signals securely. The indoor environment is indeed ideal for key generation, because first it has a slow fading channel as the variation is usually introduced by the movement of people, walking at a speed of 1-2 meter per second. This will lead to highly correlated channel measurements because the channel remains almost the same during the bidirectional sampling. Second, there are many scatterers and reflectors in the indoor environment, for example, cabinets, chairs, etc., which can create rich multipath. Multipath usually degrades the system performance, requiring a complex receiver design. However, it acts as a beneficial source of randomness for key generation. Finally, an indoor office usually involves short-range communications only because of the limited space. Both IEEE 802.15.4 (ZigBee) and Bluetooth are popular personal area network standards, hence they are available in many home appliances, consumer and industrial equipment. Key generation has been demonstrated to work well with them [4, 13, 14]. Since the first conception of the WiFi-based prototype and its experimental exploration reported in [15], numerous key generation prototypes and experiments have been created for WiFi operating in indoor environments. We also carried out WiFi-based experiments in a dynamic indoor office environment and the communication range was limited to 20 meters. The received power variation in Fig. 4a is only about 25 dBm because of the short-range communication. The absolute-based quantizer, for example, mean-based quantizer, can be adopted.

In contrast to indoor scenarios, massive IoT applications, for example, smart cities and environment monitoring, will predominantly operate in outdoor environments, which may involve long-range transmission, for example, in the order of km. We prototyped a LoRa-based key generation system and carried out experiments in an urban environment with a maximum distance between users about 500 meters. As shown in Fig. 4b, because of the long-range environment and the effects of path loss and shadowing in urban environment, there was a much larger variation in the received power, namely 70 dBm, than the 25 dBm variation in the WiFi example. In this case, the absolute-value-based quantization, such as the mean-value-based scheme, will produce long runs of 1s and 0s, which is not random and unsuitable for key generation, as shown in Fig. 4b. This can be tackled by the differential-value-based quantizer. To the best knowledge of the authors, this is the first time to compare the key generation performance and design in short-range and long-range environments.

An Integrated Security Framework

As discussed in the previous two sections, RFF identification can be used for authentication. For a legitimate user, the authorized user will then start the key generation process and extract keys for the cryptographic scheme to achieve secure transmission. Both RFF identification and key generation offer numerous advantages for IoT. First, both techniques exhibit low complexity as they

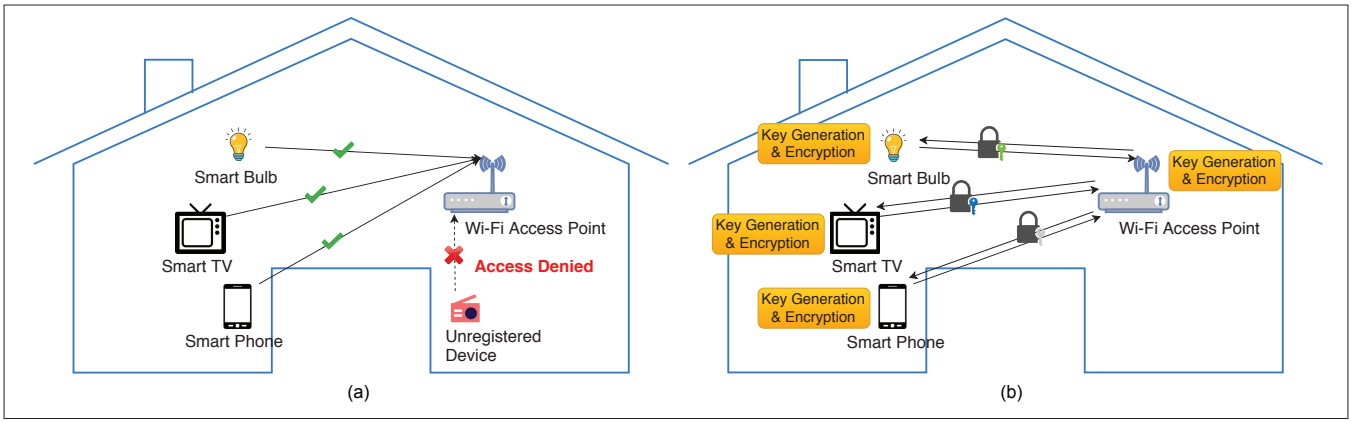

FIGURE 6. Application scenario, a secured smart home: a) authentication; b) secure communications.

do not involve the computation of sophisticated mathematical problems, such as factorization, and hence they are extremely suitable for IoT. Second, both are information-theoretically secure. Both RFF identification and key generation exploit the inherent randomness residing in the physical world, such as the hardware imperfections imposed by the manufacturing process and the wireless channel affected by the movement of users and objects. The randomness is intrinsic and cannot be tampered with or predicted easily.

Since both techniques rely on the physical layer of the wireless communications protocol stack, there is clearly a need for an integrated security framework, which combines the RFF identification and key generation, as shown in the block diagram in Fig. 5. As shown in Eq. 1, the hardware imperfections and channel effects are combined at the receiver and generally difficult to separate. However, the channel quality is very good and hence the receiver becomes capable of more accurate feature extraction during the training stage. The RFF database constructed can then be exploited to enhance the key generation performance. After the authenticator successfully validates the identity of the user, it will access the RFF of that particular user stored in the database and use this information for key generation.

This interaction can significantly improve the key generation performance in terms of the channel reciprocity and security. The correlation of channel measurements is impaired both by frequency and phase offsets, resulting from the hardware imperfections. With the aid of calibration assisted by the reference RFF, the receiver can compensate for the non-linear nature of the hardware imperfections and get a more accurate channel estimate. On the other hand, key generation may suffer from passive eavesdropping, when the attackers are in close proximity. However, the attackers do not have access to the reference RFF and their channel measurements will deviate from the calibrated channel estimation of the legitimate users, especially when the phase information is also exploited.

An application scenario is shown in Fig. 6, portraying a smart home as an example. The smart devices, including phone, TV and bulb, are connected to the WiFi access point (AP), which acts as the authenticator. The legitimate smart devices are registered at the AP and can gain access to the network, but any unregistered devices will be denied access. The legitimate users will then carry out key generation in collaboration with the AP and the keys generated will be used for encryption and decryption. Note that many smart home devices, for example, TV and bulbs, will be fixed and stationary, but there will always be people moving around and the channel variation incurred is sufficient by random for key generation.

Future Vision and Challenges

Both RFF identification and key generation have been demonstrated to be suitable for IoT. However, as for all emerging techniques, there are still research challenges to be addressed for conceiving a more mature and robust framework.

Resisting an attack is a common challenge both in RFF identification and in key generation [3]. Because both techniques rely on the received wireless signals, attackers can perform passive eavesdropping and endeavor to extract useful information. However, when the attackers are very close to the legitimate users, for example, located within one wavelength (12 cm when the carrier frequency is 2.4 GHz), they would be easily spotted; when the distance is larger, the channel will be uncorrelated and the attackers cannot get useful information. Therefore, these two techniques are generally robust to passive eavesdropping. Having said that, further research efforts are required to identify potential security risks and to design corresponding countermeasures.

RFF Identification

The RFF-based authentication should be robust to channel effects, since they degrade the fingerprint. When building a noise-resistant physical layer identification system, the existing methods tend to degrade the spoofing resistance. Hence, there is a need for more robust RFF identification systems, which can be achieved, for example, by basing the RFF on non-linear features such as the power amplifier non-linearity, because most of the channel effects are linear in nature. Furthermore, training an RFF system and storing the parameters in a user database requires additional resources. Hence, reducing the cost of RFF is another challenge that has to be addressed. Additionally, it is seen that narrowband IoT protocols such as LoRa, NB-IoT, and so on, and ultra narrowband protocols such as Sigfox, and Weightless-N are becoming more popular. These protocols have a very low bandwidth and transmit their information in energy-conserving short bursts. This results in a smaller input vector space (compared to the number of users) in both the time domain and

Our framework offers low complexity and is information-theoretically secure. It circumvents the limitations of the conventional cryptography-based schemes. In particular, the RFF of the transceiver is employed for authenticating the user identity and the wireless channel is exploited to generate cryptographic keys.

frequency domain, which makes classification more challenging. More research needs to be carried out to identify which physical layer features would be best suited for creating a more secure and robust RFF identification system. Finally, the specific causes of imperfections in the devices that generate the RFFs also have to be further investigated. A deeper and more thorough understanding of the particular imperfections and their causes will indeed help synthesize fingerprints and design a more secure RFF identification scheme.

Key Generation

At the time of this writing, indoor environments are the most popular investigated scenarios which exhibit promising properties for secure key generation. However, many IoT applications may be operated in an unfriendly environment, which requires special attention. For example, there will be lots of noise and interference in smart manufacturing scenarios, which may result in poor-quality channel measurements. In some scenarios such as environmental monitoring, the environment may remain static over a long period, where no channel randomness is encountered. Entropy harvesting in this kind of quasi-static environment has to be tackled.

Key generation is usually applied in the context of TDD systems because it requires reciprocal channel measurements. While many IoT wireless standards operate in a TDD mode, including WiFi, ZigBee, LoRa, and so on, there are also others operating in the frequency-division duplexing (FDD) mode, for example, NB-IoT, where channel reciprocity does not hold. Since NB-IoT is standardized by the 3rd Generation Partnership Project (3GPP), it is becoming one of the dominant IoT standards and expected to lead to widespread deployment. A feasible way to design FDD-based key generation will thus be paramount, for example, constructing equivalent channel gains with high correlation.

Conclusions

IoT security is of the utmost importance in promoting compelling IoT applications and services, given the confidential nature of IoT data. We have conceived a physical layer security-based framework for authentication and secure communications. Our framework offers low complexity and is information-theoretically secure. It circumvents the limitations of the conventional cryptography-based schemes. In particular, the RFF of the transceiver is employed for authenticating the user identity and the wireless channel is exploited to generate cryptographic keys. Their protocols and applications have also been reviewed. Since both techniques are based on the physical layer of the communication protocol stack, they constitute a self-contained security framework. The article concludes with a vision of the future and research challenges of this promising technique.

Acknowledgment

The work of L. Hanzo was supported by the EPSRC projects EP/N004558/1 and EP/P034284/1, the Royal Society's GCRF Grant, and the European Research Council's Advanced Fellow Grant QuantCom.

References

[1] Y. Zou *et al.*, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proc. IEEE*, vol. 104, no. 9, 2016, pp. 1–39.
[2] Q. Xu *et al.*, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, 2016, pp. 94–104.
[3] J. Zhang *et al.*, "Key Generation from Wireless Channels: A Review," *IEEE Access*, vol. 4, Mar. 2016, pp. 614–26.
[4] C. T. Zenger *et al.*, "Authenticated Key Establishment for Low-Resource Devices Exploiting Correlated Random Channels," *Computer Networks*, vol. 109, 2016, pp. 105–23.
[5] W. Wang *et al.*, "Wireless Physical Layer Identification: Modeling and Validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, 2016, pp. 2091–2106.
[6] W. Wang *et al.*, "User Capacity of Wireless Physical-Layer Identification," *IEEE Access*, vol. 5, 2017, pp. 3353–68.
[7] J. Zhang *et al.*, "Efficient Key Generation by Exploiting Randomness from Channel Responses of Individual OFDM Subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, June 2016, pp. 2578–88.
[8] J. Zhang *et al.*, "Experimental Study on Key Generation for Physical Layer Security in Wireless Communications," *IEEE Access*, vol. 4, 2016, pp. 4464–77.
[9] J. Zhang, A. Marshall, and L. Hanzo, "Channel-Envelope Differencing Eliminates Secret Key Correlation: LoRa-Based Key Generation in Low Power Wide Area Networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, 2018, pp. 12 462–66.
[10] V. Brik *et al.*, "Wireless Device Identification with Radiometric Signatures," *Proc. 14th ACM Int'l. Conf. Mobile Computing and Networking*, San Francisco, California, USA, Sept. 2008, pp. 116–27.
[11] P. Robyns *et al.*, "Physical-Layer Fingerprinting of LoRa Devices Using Supervised and Zero-Shot Learning," *Proc. 10th ACM Conf. Security and Privacy in Wireless and Mobile Networks (WiSec)*, Boston, USA, July 2017, pp. 58–63.
[12] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-Layer Identification of RFID Devices," *Proc. 18th Conf. USENIX Security Symposium*, Montreal, Canada, 2009, pp. 199–214.
[13] S. Ali, V. Sivaraman, and D. Ostry, "Eliminating Reconciliation Cost in Secret Key Generation for Body-Worn Health Monitoring Devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, Dec. 2014, pp. 2763–76.
[14] S. N. Premnath *et al.*, "Secret Key Extraction Using Bluetooth Wireless Signal Strength Measurements," *Proc. 11th Annu. IEEE Int. Conf. Sensing, Commun. Networking (SECON)*, Singapore, Jun. 2014, pp. 293–301.
[15] S. Mathur *et al.*, "Radiotelepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," *Proc. 14th Annu. Int. Conf. Mobile Computing Networking (MobiCom)*, San Francisco, California, USA, Sept. 2008, pp. 128–39.

Biographies

Junqing Zhang received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China in 2009 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from Queen's University Belfast, UK in 2016. From February 2016 to January 2018, he was a postdoctoral research fellow at Queen's University Belfast, UK. Since February 2018, he has been a tenure track fellow at the University of Liverpool, UK. His research interests include Internet of Things, wireless security, physical layer security, key generation and radio frequency fingerprinting identification.

Sekhar Rajendran is a Ph.D. student in the Department of Electrical Engineering at the University at Buffalo. Previously, he was an assistant professor at the Rajagiri School of Engineering and Technology (India). He has a Master degree in signal processing and control systems from the NIT Hamirpur (2014) and a Bachelor degree from CUSAT, India (2008). Rajendran has also spent over two years as a network subsystem engineer at Sasken Technologies, India.

Zhi Sun received the Ph.D. degree from Georgia Institute of Technology in 2011. Currently he is an associate professor at the University at Buffalo, SUNY. He was the recipient of the NSF CAREER Award in 2017, the UB Exceptional Scholar Award in 2017, Best Demo Award at IEEE Infocom 2017, and Best Paper Award at IEEE Globecom 2010. His research interests include wireless communication and networking, physical-layer security, and cyber physical systems.

Roger Woods [M'95, SM'01] received the B.Sc. and Ph.D. degrees from Queen's University Belfast, United Kingdom, in 1985 and 1990, respectively. He is a professor, research director of the Systems and Sensors cluster at the University and Chief Scientist at Analytics Engines Ltd. His research interests include the heterogeneous programmable systems for data, signal, and image processing, and telecommunications.

Lajos Hanzo [F'04] FREng, FIEEE, FIET, Fellow of EURASIP, DSc, received his degree in electronics in 1976 and his doctorate in 1983. He holds an honorary doctorate from the Technical University of Budapest (2009) and from the University of Edinburgh (2015). He is a member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He is a Governor of both IEEE ComSoc and of VTS.