Ad Hoc Networks 123 (2021) 102683

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Physical layer authentication for extending battery life

Cem Ayyildiz [a,b], Ramazan Cetin [b], Zulfidin Khodzhaev [c], Taskin Kocak [d], Ece Gelal Soyak [a,*], V. Cagri Gungor [e], Gunes Karabulut Kurt [f]

[a] Computer Engineering, Bahcesehir University, Istanbul, Turkey
[b] GOHM Electronics, Istanbul, Turkey
[c] Department of Physics, Oklahoma State University, OK, USA
[d] Electrical Engineering, University of New Orleans, LA, USA
[e] Computer Engineering, Abdullah Gul University, Kayseri, Turkey
[f] Poly-grames Research Center, Electrical Eng., Polytechnique Montréal, Montréal, Canada

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Smart city
Physical layer security
RF fingerprinting
Battery life
Convolutional Neural Networks (CNN)
Energy efficient

ABSTRACT

Increasing population density in cities, and the increasing demand for efficiency in resource usage call for architectures enabling smart cities, such as the Internet of Things (IoT). In most such scenarios, the data generated by IoT sensors is not confidential, but its integrity is critical. Data integrity can be achieved by establishing certification mechanisms that provide cryptographic message authentication protocols; however, this requires relatively expensive components for storing and processing the encryption key on the sensor and consumes more power while processing and transmitting data, which leads to the renunciation of security issues in cost sensitive deployments. In this paper, we propose a security solution that provides data integrity without draining the batteries of IoT sensors. Our solution consists of, *(i)* differentiating legitimate sensors by taking advantage of their impurities formed during the manufacturing process of the transceiver components, and *(ii)* eliminating the complex components that carry out cryptography as well as the redundant packet header fields, thereby yielding power savings. The testbed implementation of the proposed solution yields power measurement results providing an estimate of 2.52 times improvement in battery life without compromising the integrity of communications in the system, in addition to offering an increase in spectral efficiency and a decrease in the overall IoT device cost.

1. Introduction

The Internet of Things (IoT) is a promising technology that has the potential to tremendously improve the quality and efficiency of healthcare, education, manufacturing, agriculture and transportation [1]. During the last decade, various research studies have been carried out on the use of IoT in urban areas to ensure safety, cleanliness and quality of life, to establish what is referred to as "smart cities" [2]. These applications are facilitated by placing battery-powered sensor devices in various locations in the city for gathering relevant data, which is then sent to a gateway device that locally analyzes, or relays the data to a cloud server where it is processed and stored.

In most smart city applications, the data is not private, but the integrity of data is crucial. For instance, the information regarding the emptiness of a trash bin or the availability of a parking slot is no secret, however, the server must validate that it is a valid sensor generating this data. Traditionally, message integrity is provided by means of digital signatures and cryptography. The additional bandwidth and computational overhead with these schemes is not a burden when it is used by devices with computational capacity and mains powered. When considering sensor communications, however, the primary limiting factor in the design of any protocol is their limited CPU and limited battery. A new approach to providing message integrity without these complex systems is differentiating individual devices using their RF signatures. RF fingerprinting is a method for providing information security by identifying the unique patterns belonging to the RF signals between devices, that exist because of *(i)* the minuscule differences between the hardware components of distinct devices, which is a consequence of the imperfections in the manufacturing of electronic components on the device, as well as *(ii)* the unique propagation path among pairs of devices. Such unique patterns can be considered as unique signatures of each device at the receiver side.

IoT devices are merely electronics with embedded software, with usually some sensor capability. Sensors measure physical phenomena in the environment and send this digital information wirelessly to

* Corresponding author.
E-mail address: ece.gelalsoyak@eng.bau.edu.tr (E.G. Soyak).

https://doi.org/10.1016/j.adhoc.2021.102683
Received 29 March 2021; Received in revised form 30 July 2021; Accepted 9 September 2021
Available online 20 September 2021

other electronics. IoT sensors may face a lack of power where many devices are located in hard-to-reach areas with little access to external power sources. However, these IoT sensors may be used for detecting unforeseeable events e.g., disaster monitoring systems [1], which necessitates them to operate for extended periods of time. It is therefore of fundamental importance to provide solutions that yield an extension of battery life for IoT devices.

In this paper, we propose a method for IoT device authentication using each sensor's RF characteristics as its unique signature. For this, we first employ a Convolutional Neural Networks (CNN) based classification of the sensor RF fingerprints on the data collected from our testbed. Once it is validated that the classification yields accurate results that would enable us to use each sensor's RF characteristics as its unique signature, we proposed SIGN-AUTH, a signature-based authentication framework that eliminates the need for battery- and bandwidth-intensive encryption techniques. We propose modifications in the IEEE 802.15.4 packet format to exclude the device identification which is now obviated thanks to the unique RF signatures. Via testbed measurements and analysis, we demonstrate that our proposed scheme;

- prolongs battery life up to 352% on IoT devices as it obviates the need for standard, memory- and battery-hungry encryption techniques.
- increases the spectral efficiency of the medium up to 1600%, as it enables use of much smaller packet sizes by eliminating the need to encrypt and removing the headers.
- decreases the overall IoT device cost by eliminating extra secure element to save encryption key.

To the best of our knowledge, the challenges related to battery lifespan and security have so far not been optimized together and this is the first work that analyzes battery consumption with and without Physical Layer Authentication (PLA) based security option enabled.

The rest of the paper is organized as follows: Section 2 summarizes related prior art. Our methodology, testbed setup, data analysis procedure are explained in Section 3. Section 4 introduces the SIGN-AUTH framework that utilizes the physical layer fingerprinting based identification for communications. Section 5 evaluates the identification and battery savings impact with the proposed solution. Finally, Section 6 concludes this paper.

2. Related work

In this section we present related prior work on wireless sensor networks, focusing on device authentication, RF fingerprinting, and extending battery life.

2.1. Prior work on security and device authentication

Due to their limited battery, memory, or processor, the protocols that successfully run on high-end devices such as computers or mobile phones cannot be applied on IoT devices to provide security [3]. Most security protocols and device authentication methods for sensor networks are based on symmetric and asymmetric encryption techniques that require high computing power and large amount of memory, both of which are undesirable for power-limited devices [4]. In TinySec framework [5], encryption and decryption are performed using a shared key. The protocol is particularly designed for link-layer cryptography in sensor networks, but it entails a trade-off between battery life and security provided [6]. In both TinyECC [7] and TinyPK [8] authors design cryptographic methods using public–private key encryption, which is more secure compared to symmetric-key schemes; however, it is still costly for low power applications that have extreme battery life requirements.

Besides the encryption techniques, Trust Center model is also used for device authentication in ZigBee-based IoT networks. In [9], authors propose an enhancement to ZigBee Trust Center based authentication mechanism, where node first authenticates using Trust Center, then Trust Center transfers node information over in case of mobility. This method is more energy and memory efficient due to elimination of the extra authentication process.

2.2. Prior work on RF fingerprinting

RF fingerprinting involves the collection of various signal characteristics coming from a transmitter device, in order to uniquely identify the device and differentiate from others. Fingerprints generated by a device can be obtained internally by connecting a hardware to it or by installing a software on it that can present this information. It can also be acquired externally by sniffing the air using an RF receiver or sensors [10]. The authors in [11] evaluate the accuracy of RF fingerprinting against impersonation attacks using low-end transmitters and receivers. The tests, performed using USRP devices, show that no two fingerprints generated with different receivers are alike, due to receivers' own imperfections resulting from their analog components. Similarly, the variations in the USRP RF fingerprints of different devices was also noted in [12]. In [13], a transient-based identification method is performed to authenticate CC2420 wireless sensor nodes. The acquired RF fingerprints from sensor nodes are used to extract sensor features. Proposed system classifies sensor nodes with as low as 0.24% equal error rate; however, it has been observed that, when tested for different distance, antenna polarization and voltage values, device fingerprints may yield a dramatic decrease in the classification accuracy. In [14], random forest classifier is used in order to perform device authentication for different ZigBee devices tested at different signal-to-noise ratio (SNR) values; however, 10% difference is observed in the verification of high-cost receivers (*e.g.* NXI) and low cost receivers (*e.g.* USRP). In [15], RF fingerprints from seven ZigBee devices are extracted for use as training data, and classification accuracy of 90% is achieved at an SNR value of ~10 dB.

One way for device authentication is using Gaussian minimum shift keying (GMSK) as an RF fingerprint for authentication. In [16], authors use RF fingerprints from GSM-GMSK signals to stop malicious activities. Enhanced security is provided by classifying the RF fingerprints from near-transient and midamble regions of GSM-GMSK bursts using multiple discriminant analysis with maximum likelihood estimation (MDA/ML). In [17], carrier frequency offsets are used to identify and authenticate devices, based on the fact that the two clock offsets between every node pairs drift independently and randomly overtime. An alternative approach for device authentication is studied in [18] by using 802.11a signals from four Cisco devices, by classifying the dual-tree complex wavelet transform (DT-CWT) features of the signal using MDA and ML; this approach achieves a classification accuracy of 80%. In [19], power amplifiers are used to identify wireless users. The difference between signals at input and output of the amplifier gives way to signal identification when these characteristics are modeled with Volterra series and analyzed using classical likelihood (CL) and generalized likelihood ratio tests (GLRT). Effective results can be obtained when commercial RF power amplifiers are used. Other papers use Gabor transform RF in discrete form as a Wi-Fi fingerprint, which provides a classification accuracy of at least 90% [20]. Finally, also using Wi-Fi, Internet Control Protocol (ICMP) time stamps of devices were investigated by computing clock skews of Android devices [21].

More recent studies on RF fingerprinting entail advanced data analysis techniques for an accurate association of the impurities with identities. In [22], a deep-learning based classifier has been built in order to learn the hardware imperfections of low-power radios for IoT device authentication. Using Long Short-Term Memory (LSTM) method, the work aims to identify signal imperfections that persist over long durations. [23] uses generative adversarial networks (GANs) for RF fingerprinting for mmWaves at the 60 GHz band. [24] uses deep convolutional neural network architectures to identify a large number of devices, thus focusing on the scalability of the proposed deep learning solution.

2.3. Prior work on extending battery life

Battery life is extremely important for IoT applications due to the challenges around direct intervention to the devices deployed in the field. IoT device lifespan can be prolonged using energy harvesting, wireless energy transfer and energy conservation methods such as radio optimization, cooperative communication schemes, transmission power control, data reduction, data aggregation and data compression [25, 26]. In [27], a wireless charging system is designed to prolong the life of a WSN. The results of the simulations and experiments show that the proposed system can be used in WSNs to increase life of network by using robots to transfer energy to sensors. The battery energy can be saved using wireless energy transfer and energy conservation methods [25], transferring energy to sensors [27], jointly assigning time slots and controlling active times [28], energy-aware sink relocation (EASR) [29]. Energy efficient routing schemes and different sleep procedures (by modifying the idle and active durations of sensors) are also used to increase battery life. In [28], joint routing and sleep scheduling method is used in order to maximize network life and the results show that the proposed method prolongs WSN life by 284% compared to traditional optimal routing and fixed sleep scheduling methods. In multihop networks, sink nodes which are more close to gateway consumes more power and shortens life of network by retransmit incoming packets more frequently. In [29], a sink node relocation method called energy-aware sink relocation (EASR) is proposed for mobile sinks in WSNs. Theoretical analysis showed that EASR can prolong lifespan of WSNs.

2.4. Novelty of this work

Although some of these prior efforts mention the advantages of Physical Layer Authentication (PLA) in terms of power consumption, to the best of our knowledge, this is the first work that analyzes the battery life time of IoT sensors with and without PLA using real life measurements. The main contributions of this paper can be summarized as follows:

- CNN based RF fingerprinting method is used for the identification of legitimate sensors and for improving the integrity of messages for low-cost and battery-operated IoT sensors where the data for the related application is not confidential but the overall data integrity is critical.
- An identification-less message structure is proposed for low-cost battery-operated devices.
- A transfer learning based method is proposed to decrease the number of samples to be collected in the field for obtaining the RF fingerprint of a given sensor–gateway pair.
- Measurements of power consumption and estimations of battery life are carried out for cryptographic based security method using AES-128 and for our proposed physical layer authentication based framework.

3. RF fingerprinting methodology

In this section we explain our methodology for data collection and analysis using the Convolutional Neural Networks (CNN) architecture.

3.1. Our testbed

Our testbed contains a custom designed physical layer security enabled gateway, low-cost sensor nodes, and a high-precision digital multimeter for the measurements.

The gateway is composed of an RF front end board, a software defined radio (SDR) board and an edge computing board, respectively. The samples are collected by the SDR on the gateway. In our tests, RF front end board carries out the communication with the sensor nodes, SDR is used for feature conditioning and extracting fingerprints, and the edge computing board is used for executing the CNN model to identify the sensors.

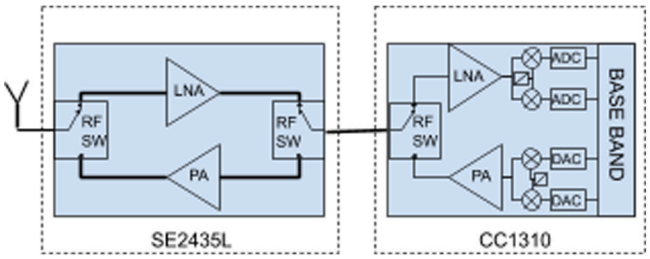


Fig. 1. The hardware structure of the sensors used in our testbed.

Table 1
Wireless parameters of the sensor transceiver.

Parameter Name	Value
Center Frequency	868 MHz
Bandwidth	10 kHz
Modulation	GFSK
Transmission Output power	+10 dBm
Message frequency	10 Hz

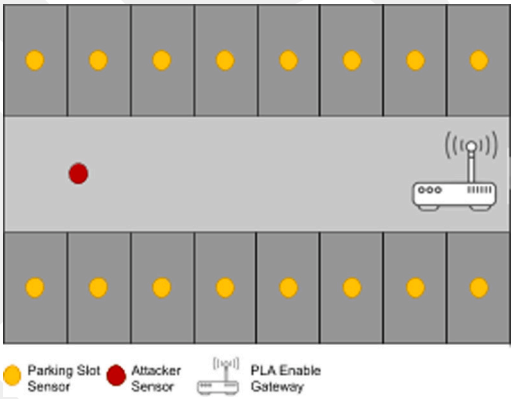


Fig. 2. The parking lot measurement setup.

The sensor nodes consist of low cost TI CC1310 transceivers with Power Amplifier RF stage. The hardware structure of the sensor is shown in Fig. 1. The transceiver on the board operates at the 868MHz ISM band with the parameters shown in Table 1.

For the power measurements, we have used a high precision digital multimeter that is able to measure voltage and current. As the duration of message transmission is very short (10 ms) and the current drained during the transmission is considerably high compared to that during the sleep state, it is not possible to accurately measure the current with normal digital multimeters. Thus, we have carried out our measurements using the multimeter's high frequency digitizer mode that is capable of taking 10 kHz measurements.

3.2. Data collection

Our setup for data collection consists of a gateway node and multiple sensors in a parking lot scenario, as shown in Fig. 2. The sensors are used for detecting and reporting the availability of a parking slot. In the experiments, one of the sensor nodes acts as an attacker while the remaining nodes act as legitimate sensors. All sensors send the same type of messages, where the message headers do not include sensor IDs. Test sensors operate in the ISM band and they transmit fixed-size test data using +10 dBm transmission power and using Gaussian FSK (GFSK) modulation with 5 kHz bandwidth.

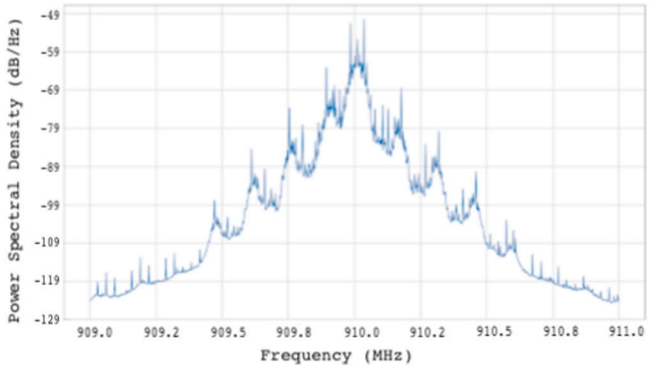


Fig. 3. Power Spectral Density of sensor signal.

Analog test data is collected for approximately 1 h for each sensor using the custom made gateway. Incoming analog data is sampled after passing through the gateway's analog front end using ADC, converted to baseband in 2 MS/s and saved to a file as complex64 float type format, in I/Q form. I/Q form is a complex data type that yields amplitude and phase information about the incoming signal.

Fig. 3 shows the power spectral density of the incoming signal. The sensor signal is located in the receiver's central frequency of 910 MHz and its peak power for represented samples is approximately -50 dBm. It is expected that the impurities due to the analog components of sensors should shift the center frequency of the transmitted signals. These impurities such as the frequency shift and the time duration of the transmitted signal drive the classification achieved by the CNN algorithm.

3.3. Data preprocessing

The collected signals are preprocessed before being input to the CNN algorithm. The collected data set is divided into equal-duration partitions and Short-Time Fourier Transform (STFT) is performed over each part. The digital signals on which STFT is performed are stacked with specific overlap in order to generate spectrograms. A Hanning window is used as the window function to prevent spectral leakage from the edges of the frames. Each window frame roughly corresponds to 60 ms in time domain.

The spectrograms of a legitimate sensor and an attacker for a single transmission are shown in Figs. 4(a) and 4(b), respectively. These images yield the frequency, time and amplitude information of the captured signals, and are used as input to the CNN algorithm upon clipping labels and legends. It can be observed from the images, that the packets from the two sensors have approximately the same frequency and time values. However, analog components of sensors define some impurities that would help CNN to classify sensors.

Fig. 5 depicts the spectrograms of the legitimate and attacker sensors for four transmissions. It can be observed in this figure that the sensors' transmission interval is 100 ms. These images are presented here for visualization purposes only; since the CNN algorithm needs to focus on the details of individual transmission sequences in order to classify tiny differences between sensors, these four-transmissions images are not input to CNN.

During preprocessing, data is also normalized after clipping in order to ensure that all images have a similar distribution. The aim is to increase the convergence speed of the training phase.

3.4. Convolutional neural network (CNN) analysis

In our work, the deep CNN architecture is employed to classify legitimate and attacker sensors with two feature extraction layers that consist of convolutional, batch normalization, max pooling layers and a classification layer that includes two fully connected layers. Input images are RGB images with 3 channels at a size of 128 × 128 pixels. The whole architecture of proposed deep CNN is shown in Fig. 6.

First, the input data set is separated into three distinct parts for training, validation and test. Training and test sets are used for training and prediction, respectively. Validation set is used for hyper-parameter tuning and over-fitting checking. In our study, the training set constitutes 70% of the data set, while validation is 15% and testing is 15%.

In convolutional layers, input image is scanned using different filters to extract an activation map, which is the response of the input image with respect to each filter. While first layers extract simple features, through the last layers more complex features are generated. Convolutional layers basically get a 2D convolution of the images with respect to the filters (Eq. (1)). Here, $x_{m_1\times m_2}$, $\omega_{n_1\times n_2}$, and $S_{l_1\times l_2}$ are the 2D input image, filter matrix and output activation map, respectively [30]. In our architecture, two convolutional layers, which consist of 32 filters with 3 × 3 shape, have been used.

$$S(r,t) = \sum_{k_1=-a}^{a}\sum_{k_2=-b}^{b} \omega(k_1,k_2)x(r-k_1,t-k_2) \tag{1}$$

After the convolutional layer, batch normalization is applied [31]. The aim of applying batch normalization to hidden layers is to keep the mean and variance of mini batches as 0 and 1, respectively. Batch normalization provides faster convergence in back propagation due to prevention of internal covariance shift.

In order to decrease the computational cost and counteract over-fitting, max pooling layer is used after the convolutional layers. Max pooling operation (Eq. (2)) essentially applies maximum filter to non-overlapping sections of the input. In our work, 2 × 2 max pooling filters are used, therefore the output is a 75% downsampled version of the input. This provides significant improvement to network training speed because of decreasing computational intensity.

$$Y(\alpha) = \max(0,\alpha) \tag{2}$$

Classification part of CNN is handled by fully connected layers that consist of hundreds of neurons that produce an output z by using x, ω, b which correspond to the input from the previous layer, the weight of connection and the bias of neuron, respectively (Eq. (3)).

$$z(i) = \sum_i \omega_i x_i + b \tag{3}$$

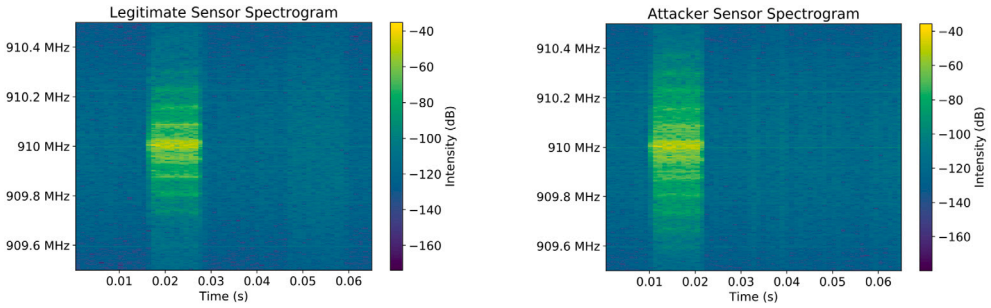
Weights and biases in fully connected layers are trained by optimization algorithms such as Gradient Descent and Adam. Optimization algorithms use partial derivatives of error functions of each output neuron with respect to weights of connections to update each weight. In the proposed work, Mini-Batch Gradient Descent is employed as an optimization algorithm.

In the last layer of CNN, two output neurons are used to represent the legitimate and the attacker sensors. Softmax function is employed here as the activation function due to its simplicity and probabilistic interpretation [32].

4. Signature-based authentication (SIGN-AUTH) framework

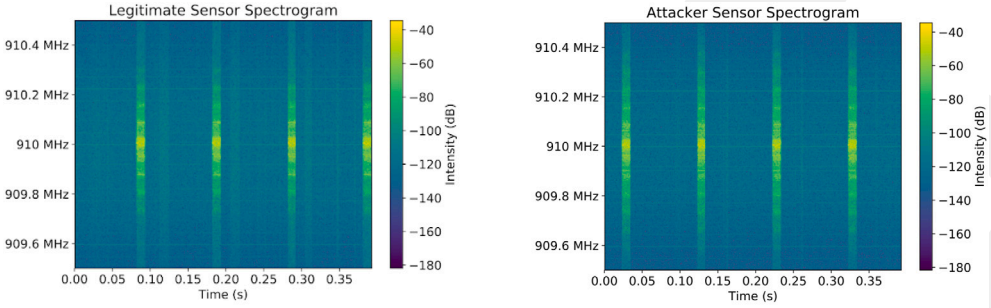
Upon verifying that we can successfully distinguish nodes based on the RF fingerprint of their communication path to a receiver using CNN, we incorporate this mechanism to identify the senders of messages. In the following we explain our proposed SIGNature based AUTHentication (SIGN-AUTH) framework that captures the collection of RF data to construct the fingerprint database, and the adaptations in the network protocols for fingerprint-based message authentication.

The impurities in the RF transmit path of the sensor and the RF receive path of the gateway create a unique fingerprint corresponding to the sensor–gateway pair (Fig. 7). This fingerprint cannot be recreated



(a) Legitimate sensor (b) Attacker sensor

Fig. 4. Legitimate and attacker sensor spectrograms for a single transmission.



(a) Legitimate sensor (b) Attacker sensor

Fig. 5. Legitimate and attacker sensor spectrograms for four transmissions.

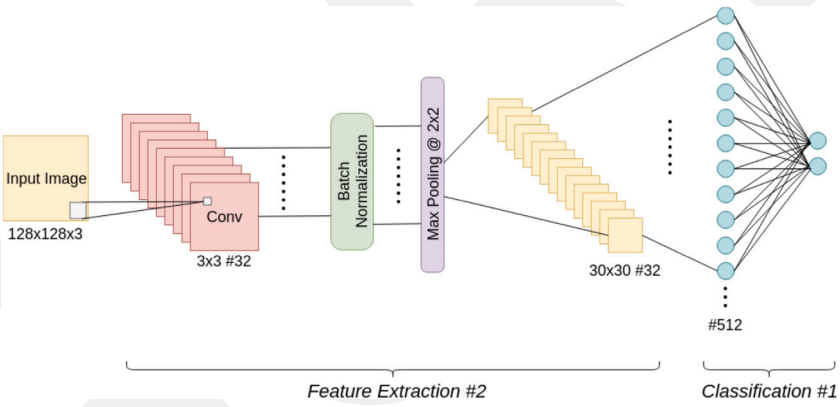


Fig. 6. Proposed CNN architecture.

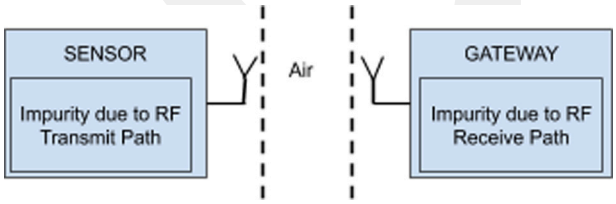
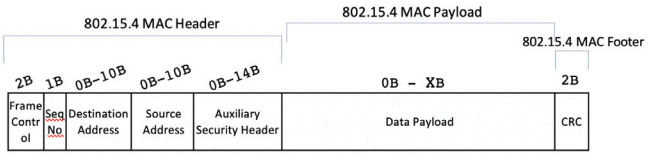


Fig. 7. The impurities in the transmitter sensor and the transmitter–receiver path that create the unique RF fingerprint.

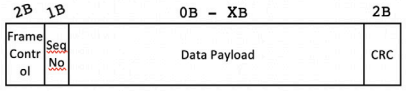
using different receivers [11]. It is these impurities that cause the spectrograms in Figs. 4(a) and 4(b) to be distinguishable.

During the manufacturing process, where the sensors do not have any power restrictions, the impurities of the sensor and the RF transmit path can be learned by collecting data via random transmissions from the sensors. However, the unique RF fingerprint of the sensor depends also on the gateway's receiver RF path (Fig. 7). Thus, the model needs to be trained again on the field. In our work, we propose to use transfer learning, where this can be done via very few new samples of the sensor captured by the gateway, to construct the final fingerprint database.

SIGN-AUTH relies on the premise that the unique fingerprint can be used for the identification of the sender and the authentication of the sender of messages in the air. The frames exchanged for messaging normally include information for the identification of the sender, alongside other useful information identifying the protocol parameters. As an example, the usual packet structure of a widely used 802.15.4 packet is shown in Fig. 8(a). The source address of the message is used to specify the source of the message. A destination address is also included in the header in order to specify the target receiver. These addresses can be MAC addresses, or alternatively, an address distribution procedure can take place before joining the wireless network in order to create a network wide unique address to be used during the session. Both approaches require that a unique sender address is included as part of the messages in the air.



(a) IEEE 802.15.4 packet format



(b) MAC packet for SIGN-AUTH

Fig. 8. Proposed modifications in the IEEE 802.15.4 packet format.

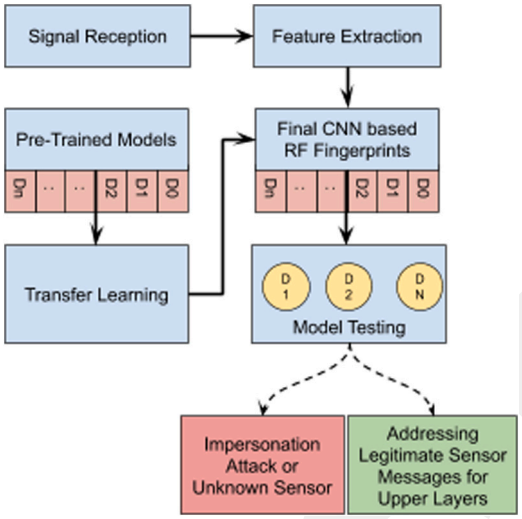


Fig. 9. SIGN-AUTH schema.

Using SIGN-AUTH, it is possible to uniquely identify the sender of each message and thus, the source address field can be removed from the message headers. In the target IoT scenarios where the sensors communicate with the gateway, a further improvement is possible by removing the destination address field from the message header. (It must be noted that multiple such IoT networks can be simultaneously supported by a mechanism such as FDMA.) In this way, it is possible to shorten the message header, which in turn reduces battery consumption. Proposed message structure is shown in Fig. 8(b); it can be seen that the header size shrinks to approximately one tenth.

In the layered communication model, unique labels are needed to specify the parameters for the protocols at each communicating node. With SIGN-AUTH, albeit not needing MAC addresses for the secure communication, unique addresses are needed by the upper layer protocols and applications. Thus, upon receiving an addressless SIGN-AUTH message, after identifying the sender using CNN, the unique address and the required identification prefixes are added to the packet before delivering it to the upper layers. If the sender cannot be identified, the message is discarded and the application is informed about the unidentified message, in order to make a decision on whether it is an impersonation attack or a newly added sensor. Fig. 9 summarizes the proposed framework.

SIGN-AUTH is expected to yield longer battery life, due to eliminating the transmission and processing overhead of additional header fields, and obviating the need to use computationally-intense cryptographic methods on every packet. The impact on battery life is quantified in the next section.

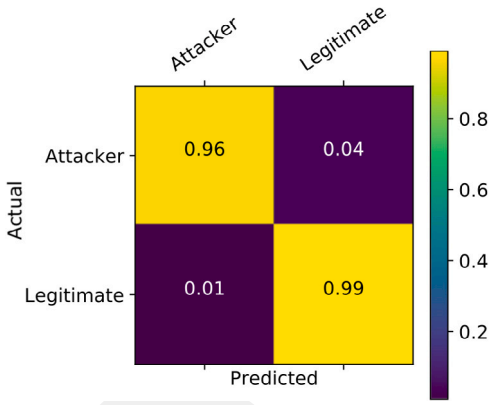


Fig. 10. Confusion Matrix of the proposed classification.

5. Performance evaluation

We evaluate the performance of SIGN-AUTH in terms of sender identification success and reduction in battery consumption.

5.1. Identification performance

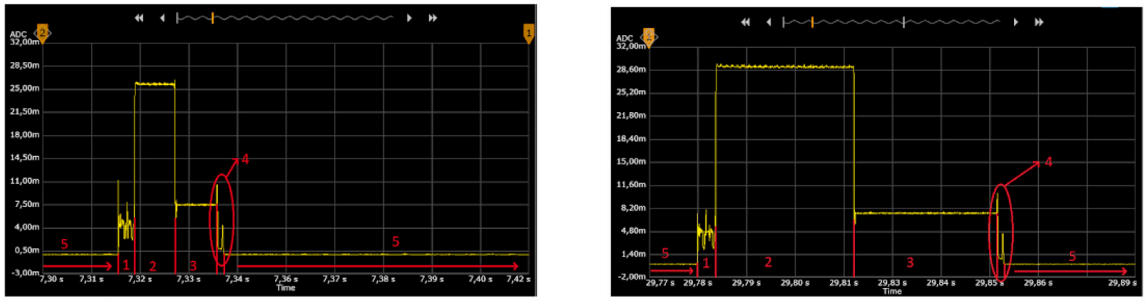
Performance of our CNN architecture is measured on test images collected from two sensors, labeled as *Attacker* and *Legitimate*, by using the method described in Section 3.4. 5-Fold cross-validation is applied in order to find the best CNN model, and the final CNN model is tested using 8000 images.

We capture the RF characteristics of the TX-RX path, in spectrograms. These images yield the frequency, time and amplitude information of the captured signals, and are used as input to the CNN algorithm upon clipping labels and legends. In these images, the discriminative features may appear at any position and for any duration. CNN with convolution and max pooling layers offers shift-invariant classification in this setting and thus yield high accuracies. Fig. 10 depicts that our proposed CNN architecture can classify a given sensor as *Attacker* and *Legitimate*, with accuracies of 96% and 99%, respectively. Given that the RF fingerprinting from the unique features of electromagnetic waves emitted by the transmitter is unique [33], this mechanism can be improved to classify more sensors. As part of our future work, we aim to evaluate the scalability of this architecture for a greater number of nodes, with varying percentage of attacker sensors.

We have also evaluated the footprint of the proposed method on the system resources, specifically, computational complexity, storage complexity and authentication latency. Each raw sample (100 ms in time with 10 kHz bandwidth) occupied around 1.25 MB storage. Given that around 10,000 samples were needed to specify each individual transmitter, approximately 12.5GB of memory was required during training. The fingerprints were stored on the gateway node, wherein each fingerprint occupied ~100 kB space. The delays incurred in each component, namely *(i)* the data preprocessing, *(ii)* CNN based classification (i.e., where the RF fingerprint is obtained using CNN), and *(iii)* threat detection (i.e., where the fingerprint is compared against known fingerprints) are shown in Table 2. In our system, the sensors generate data every second, and thus, the millisecond-grade latencies incurred during sender identification do not impose any critical bottleneck on the IoT communication.

5.2. Power consumption

On the same setup, we also evaluate the impact of SIGN-AUTH on battery consumption. In these tests, identical boards are used in order to get consistent power measurement results. While one board



(a) AES-128 authentication (b) SIGN-AUTH

Fig. 11. Battery consumption using AES-128 versus SIGN-AUTH.

Table 2
SIGN-AUTH delay on different processors.

	GPU (Nvidia RTX 3090)	GPU (Nvidia Jetson AGX Xavier)	CPU (Intel Core i7-10710U)
Pre-processing	300 ms	390 ms	870 ms
Classification	3.8 ms	18.2 ms	9.6 ms
Threat Detection	<1 ms	<1 ms	<1 ms

Table 3
Current and duration values of given mode.

	AES-128 Based Security	SIGN-AUTH
Pre-processing (1)	(4.72 ms) 5.16 mA	(4.18 ms) 4.68 mA
Transmission (2)	(16 bytes, 33.9 ms) 30.31 mA	(1 byte, 9.9 ms) 25.8 mA
Reception (3)	(16 bytes, 34.6 ms) 7.54 mA	(1 byte, 10.2 ms) 7.52 mA
Post-Processing (4)	(1.96 ms) 3.12 mA	(1.76 ms) 2.52 mA
Sleep (5)	(20 s) 320 nA	(20s) 320 nA
Average Current	66.02 μA	18.10 μA
Battery Life with 1.25 Ah	2 years 48 days	7 years 188 days

employs SIGN-AUTH, the other uses encryption and decryption based security method. On this latter board, the AES-128 algorithm is enabled in embedded software and an on-chip AES accelerator is used. The minimum packet size is set to 16 bytes due to the message structure requirements of the AES algorithm. The battery consumption measurement results are shown in Fig. 11. The red numbering indicates the battery consumption in the different states as stated in by the numbering in Table 3. A comparison of Figs. 11(a) and 11(b) indicates an observable reduction of power consumption during transmission and reception.

We also calculate the estimated battery life based on the reported self-discharge values of a 1.25Ah battery. The results are shown in Table 3. Pre-processing phase includes getting sensor measurement from the magnetic sensor and encryption, if security is enabled. Post-processing phase includes the processing of data taken from the gateway and decryption, if security is enabled.

These measurements show that the average power consumption is 3.5 times more for the AES-128 encryption enabled scenario compared to the scenario that implements SIGN-AUTH framework. The estimated battery life is plotted in Fig. 12.

6. Conclusions

In this paper, we propose SIGN-AUTH, a battery-efficient and bandwidth-efficient mechanism to ensure message integrity in IoT systems. First, we experimentally analyze the effectiveness of a CNN-based RF fingerprinting method for authentication of messages on our testbed, where we fuse spectrogram samples from the communication

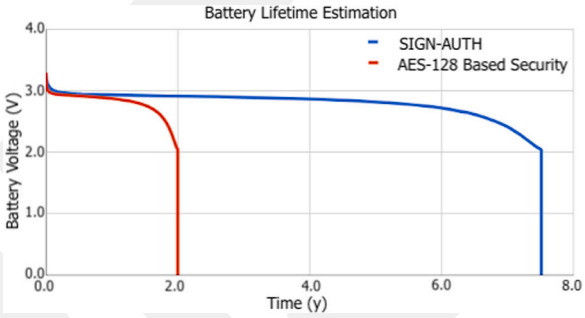


Fig. 12. Battery life analysis.

of another receiver with those of the actual gateway and retrain the CNN-based RF fingerprinting system with the new samples using transfer learning. Our approach achieves device identification accuracy of up to 99%. We then incorporate this identification mechanism in order to eliminate the battery-consuming packet processing and encryption components in a sample IoT communication protocol (IEEE 802.15.4), and show that the battery life is *tripled* using our new message structure.

This work is an initial step in our ongoing investigation of application areas for RF fingerprinting. Our results suggest that practical deployment of RF fingerprinting enabled gateways have a great potential for prolongation of battery life as well as improving the integrity of data by protecting the system against impersonation attacks. Our future work will include the investigation of the scalability of this framework with varying number of attackers. We also aim to develop RF fingerprinting-based authentication protocols for other communication technologies.

Declaration of competing interest

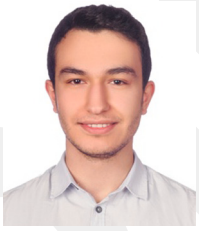
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.
[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of Things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[3] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501.
[4] M. Bhalla, N. Pandey, B. Kumar, Security protocols for wireless sensor networks, in: International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1005–1009.
[5] C. Karlof, N. Sastry, D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, in: International Conference on Embedded Networked Sensor Systems (SenSys), 2004, pp. 162–175.

[6] G. Sharma, S. Bala, A.K. Verma, Security frameworks for wireless sensor networks-review, Proc. Technol. 6 (2012) 978–987.
[7] A. Liu, P. Ning, TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks, in: International Conference on Information Processing in Sensor Networks (IPSN), 2008, pp. 245–256.
[8] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, P. Kruus, TinyPK: securing sensor networks with public key technology, in: ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004, pp. 59–64.
[9] K. Lee, J. Lee, B. Zhang, J. Kim, Y. Shin, An enhanced trust center based authentication in ZigBee networks, in: Advances in Information Security and Assurance, 2009, pp. 471–484.
[10] G. Baldini, G. Steri, A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components, IEEE Commun. Surv. Tutor. 19 (3) (2017) 1761–1789.
[11] S.U. Rehman, K.W. Sowerby, C. Coghill, Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers, J. Comput. System Sci. 80 (3) (2014) 591–601.
[12] S.U. Rehman, K. Sowerby, C. Coghill, Analysis of receiver front end on the performance of RF fingerprinting, in: IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), 2012, pp. 2494–2499.
[13] B. Danev, S. Capkun, Transient-based identification of wireless sensor nodes, in: 8th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2009.
[14] H. Patel, M.A. Temple, B.W. Ramsey, Comparison of high-end and low-end receivers for RF-DNA fingerprinting, in: IEEE Military Communications Conference (MILCOM), 2014, pp. 24–29.
[15] C.K. Dubendorfer, B.W. Ramsey, M.A. Temple, An RF-DNA verification process for ZigBee networks, in: IEEE Military Communications Conference, 2012, pp. 1–6.
[16] D.R. Reising, M.A. Temple, M.J. Mendenhall, Improved wireless security for GMSK-based devices using RF fingerprinting, Int. J. Electron. Secur. Digit. Forensics 3 (1) (2010) 41–59.
[17] M.M.U. Rahman, A. Yasmeen, J. Gross, PHY layer authentication via drifting oscillators, in: IEEE Global Communications Conference (GLOBECOM), 2014, pp. 716–721.
[18] R. Klein, M. Temple, M. Mendenhall, Application of wavelet-based RF fingerprinting to enhance wireless network security, J. Commun. Netw. 11 (2009) 544–555.
[19] S. Dolatshahi, A. Polak, D.L. Goeckel, Identification of wireless users via power amplifier imperfections, in: Asilomar Conference on Signals, Systems and Computers, 2010, pp. 1553–1557.
[20] D.R. Reising, M.A. Temple, J.A. Jackson, Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints, IEEE Trans. Inf. Forensics Secur. 10 (6) (2015) 1180–1192.
[21] M. Cristea, B. Groza, Fingerprinting smartphones remotely via ICMP timestamps, IEEE Commun. Lett. 17 (6) (2013) 1081–1083.
[22] R. Das, A. Gadre, S. Zhang, S. Kumar, J.M.F. Moura, A deep learning approach to IoT authentication, in: IEEE International Conference on Communications (ICC), 2018, pp. 1–6.
[23] N. Wang, L. Jiao, P. Wang, W. Li, K. Zeng, Machine learning-based spoofing attack detection in MmWave 60GHz IEEE 802.11ad networks, in: IEEE Conference on Computer Communications (INFOCOM), 2020, pp. 2579–2588.
[24] T. Jian, B.C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, S. Ioannidis, Deep learning for RF fingerprinting: A massive experimental study, IEEE Internet Things Mag. 3 (1) (2020) 50–57.
[25] C. Wang, J. Shih, B. Pan, T. Wu, A network lifetime enhancement method for sink relocation and its analysis in wireless sensor networks, IEEE Sens. 14 (6) (2014) 1932–1943.
[26] F. Engmann, F.A. Katsriku, J.-D. Abdulai, K.S. Adu-Manu, F.K. Banaseka, Z. Chu, Prolonging the lifetime of wireless sensor networks: A review of current techniques, Wirel. Commun. Mob. Comput. (2018).
[27] Y. Peng, Z. Li, W. Zhang, D. Qiao, Prolonging sensor network lifetime through wireless charging, in: IEEE Real-Time Systems Symposium (RTSS), 2010, pp. 129–139.
[28] F. Liu, C. Tsui, Y.J. Zhang, Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks, IEEE Trans. Wirel. Commun. 9 (7) (2010) 2258–2267.
[29] J. Men, W. Wang, J. Liu, Z. Han, Designing mutual authentication protocols in industrial wireless network, in: International Conference on Data Intelligence and Security (ICDIS), 2018, pp. 153–158.
[30] O.A. Topal, S. Gecgel, E.M. Eksioglu, G. Karabulut Kurt, Identification of smart jammers: Learning-based approaches using wavelet preprocessing, Phys. Commun. 39 (2020).
[31] S. Ioffe, C. Szegedy, Batch normalization: Accelerating deep network training by reducing internal covariate shift, in: International Conference on Machine Learning (ICML) - Volume 37, 2015, pp. 448–456.
[32] W. Liu, Y. Wen, Z. Yu, M. Yang, Large-margin softmax loss for convolutional neural networks, in: International Conference on Machine Learning (ICML) - Volume 48, 2016, pp. 507–516.
[33] N. Soltanieh, Y. Norouzi, Y. Yang, N.C. Karmakar, A review of radio frequency fingerprinting techniques, IEEE J. Radio Freq. Identif. 4 (3) (2020) 222–233.

Cem Ayyildiz received his B.Sc. degree in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey in 2006, M.Sc. degree in Microelectronics from Bremen University of Applied Sciences, Bremen, Germany in 2008 and Ph.D. degree in Computer Engineering from Bahcesehir University, Istanbul, Turkey in 2019. He has over 12 years of R&D engineering experience and he is currently the managing director in GOHM Electronics, İstanbul, Turkey. His research interests include wireless communications, and physical layer security in mobile networks and the Internet of Things.



Ramazan Cetin received his B.Sc. degree in Electronics and Communication Engineering from Yildiz Technical University, Istanbul, Turkey, in 2016 and an M.Sc. degree from Bogazici University, Istanbul, Turkey, in 2019. He has been working as an embedded software engineer since 2016 in a range of applications such as physical layer communication design, outdoor positioning, machine learning, and mesh networks.

Zulfidin Khodzhaev received a B.S. degree with a double major in physics engineering and electronics communication engineering (ABET-accredited program) from the Istanbul Technical University, Turkey. He is currently pursuing a Ph.D. degree at the Oklahoma State University (OSU). His undergraduate research included machine learning applications in wireless communication networks: interference detection and authentication aspects. His Ph.D. research focus is in spintronics: ultrafast electron, spin, phonon dynamics, topological spin textures, e.g., dynamics of hopfions, and skyrmions and superdiffusive spin currents. His research interests include machine learning and deep learning applications. His unique skill includes technology development and technology transfer, especially, high-tech with a demonstrated history of successful technology implementation in Riata's business plan competition.

Taskin Kocak received a Ph.D. degree in Electrical and Computer Engineering from Duke University, Durham, NC in 2001. He is currently the Dean of the College of Engineering and a Full Professor in Electrical and Computer Engineering at the University of New Orleans, LA. Recently, he served as the Dean of the College of Engineering and Natural Sciences at Bahcesehir University (BAU), Istanbul, Turkey (2014–2017) and before that as the Head of Computer Science and Engineering at BAU (2009-2014). Previously, he was on the faculty of University of Bristol, England and the University of Central Florida (UCF), Orlando, FL. Before joining the academia, he worked as a design engineer at Mitsubishi Electronic America's Semiconductor Division in Raleigh-Durham, NC.

Taskin Kocak's broad research interests and expertise span the areas of computer systems, computer networks, and GPU parallel computing. His research activities have been supported by external grants from American, British, Turkish and Japanese funding agencies, and have produced over 120 peer-reviewed publications, including 45 journal papers. He served as an associate editor for the Computer Journal, and as a guest editor for the ACM Journal on Emerging Technologies in Computing Systems.

Ece Gelal Soyak received the Ph.D. degree in Computer Science and Engineering from the University of California, Riverside, in 2009. From 2010 to 2012 she worked in Microsoft Redmond, USA and from 2012 to 2018 she worked in AirTies Wireless Networks, Istanbul, Turkey; in these industry positions she did research and software development. In 2018 she joined the Computer Engineering department in Bahcesehir University, Istanbul as Assistant Professor. Her research interests are in the field of wireless networks, with emphasis on the scalability and security of the Internet of Things, and use of machine learning for solving wireless networking problems.

V. Cagri Gungor received his B.S. and M.S. degrees in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey, in 2001 and 2003, respectively. He received his Ph.D. degree in electrical and computer engineering from the Broadband and Wireless Networking Laboratory, Georgia Institute of Technology, Atlanta, GA, USA, in 2007. Currently, he is a Full Professor and Chair of Computer Engineering Department, Abdullah Gul University (AGU), Kayseri, Turkey. His current research interests are in smart grid communications, machine-to-machine communications, next-generation wireless networks, wireless ad hoc and sensor networks, cognitive radio networks.

Gunes Karabulut Kurt received the Ph.D. degree in electrical engineering from the University of Ottawa, Ottawa, ON, Canada, in 2006. Between 2005 and 2008, she was with TenXc Wireless, and Edgewater Computer Systems, in Ottawa Canada. From 2008 to 2010, she was with Turkcell R&D Applied Research and Technology, Istanbul. She was with Istanbul Technical University between 2010 to 2021. G. Karabulut Kurt is with the Department of Electrical Engineering, Polytechnique Montreal, Montreal, Canada. She is also an Adjunct Research Professor at Carleton University. She is serving as an Associate Technical Editor of IEEE Communications Magazine.