IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 30, 2020, accepted April 28, 2020, date of publication April 30, 2020, date of current version May 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2991649

Passive and Active Wireless Device Secure Identification

OSCAR DELGADO[1], (Member, IEEE), LOUAI KECHTBAN[2], SÉBASTIEN LUGAN[2], (Member, IEEE), AND BENOÎT MACQ[2], (Fellow, IEEE)

[1]Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0G4, Canada
[2]Institute of Information and Communication Technologies, Electronics, and Applied Mathematics (ICTEAM), Université Catholique de Louvain, 1348 Louvain-la-Neuve, Belgium

Corresponding author: Oscar Delgado (oscar.delgadocollao@mail.mcgill.ca)

ABSTRACT Secure wireless device identification is necessary if we want to ensure that any transmitted data reach only a desired receiver. However the fact that wireless communications are by nature broadcast creates unique challenges such as identity theft, eavesdropping for data interception, jamming attacks to disrupt legitimate transmissions, etc. This paper proposes a new integrated radioprint framework (IRID) that has two main components. First, we propose a machine learning-based radio identification solution that relies on hardware variabilities of internal components of the transmitter caused during manufacturing, allowing us to achieve passive device identification. Second, we introduce a new kind of covert channel, based on variations in the emitted signal strength, which allows us to implement unique active device identification. We evaluate our proposed framework on an experimental test-bed of 20 identical WiFi devices. Although our experiments deal only with IEEE 802.11b, the approach can easily be extended to any wireless protocol. The experimental results show that our proposed solution can differentiate between network devices with accuracy in excess of 99% on the basis of a standard-compliant implementation.

INDEX TERMS Radioprint, machine learning, covert channel, PUF, WiFi, 802.11, wireless security, neural network, emerging technologies.

I. INTRODUCTION

The rapid development of wireless technologies has allow wireless communications to play increasingly important roles in the way we communicate. However the "over the air" nature of wireless communications creates privacy and security concerns, such as eavesdropping for data interception and jamming for disrupting legitimate communications [1].

Several authentication methods exist to distinguish devices from each other when connected to a network. Traditional identification techniques, for instance, provide the ability to recognize a device connected to the network using a unique identifier (IP or MAC address). The procedure can be used to track a device's activity, enabling the network administrator to verify and, if needed, suspend any suspicious device. However, this procedure does not guarantee the true physical identity of the device connected to a network [2].

In the case of WiFi, for example, we can mention at least two different types of attacks: rogue access point (rogue AP), and MAC spoofing. A rogue AP is a device set up by a malicious attacker to fool the client stations. This rogue AP mimics an AP by using the same identification credentials as the legitimate AP [3]. MAC address spoofing is a technique of switching a factory-assigned MAC address with a legitimate MAC address, thus creating uncertainty about the validity of the data shared on the network [4].

One way to ensure the authenticity of a device is to rely on its physical properties. Physical Unclonable Functions (PUF) are partly a physical distortion embodied in a physical structure of a system that can serve as a unique identifier, namely, a digital fingerprint [5]. These physical variations are often due to involuntary introduction of physical micro-structure variations, which occur naturally during semiconductor manufacturing and assembling of the device. These factors are random and uncontrollable, making it practically impossible to reproduce them at a reasonable cost [6].

Instead of relying on digital identification, PUF advocates for a new kind of challenge-response authentication method. This new method provides the ability to confirm the identity of a device by testing the response of the device's

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenhui Yuan.

micro-structure using a specific challenge. To validate the challenge-response authentication, the verification of the device's response must be simple to evaluate in terms of computational complexity. In addition to that, the micro-structure response must be mathematically unpredictable, to avoid the ability to copy. However, the same challenge must remain repeatable under different conditions. The device identification and authentication are established only when the unique response matches the expected response [7].

Another way to ensure the authenticity of a device is to conceal the transmission of a unique identifier through the use of a covert communication. Recent research has demonstrated that it is possible to transmit a message through a covert channel without being detected reliably by a malicious attacker [8], [9].

In this paper, we will investigate whether the imperfections and variations introduced during the manufacturing process of radio transmitters could be used as an identification method and of a covert communication technique could be used to increase unique device identification accuracy. Our contributions are the following:

- We propose the use of a passive low-complexity machine learning method to uniquely identify devices connected to a network.
- We analyze the most relevant features needed for identification and show that a low-cost solution is achievable.
- We propose the use of an active covert channel method based on the signal strength (power) to identify network devices.
- We propose a new framework that combines machine learning and covert channel techniques to enhance the real-time identification accuracy.
- We evaluate the accuracy of the identification of a network device based on our proposed framework.

The remainder of this paper is organized as follows: In Section II, we describe the relevant related work. Section III presents an overview of the proposed solution. Based on the proposed model, our implementation is then described in Section IV. In section V we analyse the simulation results. Finally, Section VI presents our conclusions.

II. RELATED WORK

In the past decade, identification of devices has gained more and more attention due to the need to certify the authenticity of the data shared on a wireless network. Physical Unclonable Functions, for instance, can help to mitigate this problem. As manufacturing imperfections get embedded in the micro-structure of a device, multiple opportunities are available. The PUF technique has successfully demonstrated its usefulness in terms of improving network security and privacy [10]–[12].

The PUF approach can be implemented in the design of a basic circuit to generate distinctive unique responses. This can be used as an alternative low-cost authentication method able to generate a secret key for cryptographic operations [13].

Radio Frequency (RF) identification can also rely on the hardware variations embedded in a device during the manufacturing process. In this scenario, each device will exhibit a unique behavior, which can be used as a wireless identifier [14], [15]. For instance, RF identification can be used to identify and stop cloning and avoid frauds in cellular networks [16].

The authors of [17] developed a method that measures the electromagnetic field and identifies devices with an accuracy of 98.9%. However, this method works only when devices are in very close proximity to the target.

In [18] the authors proposed a method based on the imperfections of the digital-to-analog converter, the power amplifier and the RF oscillator. However, the main drawback is that the RF oscillators were not analyzed as part of a transmitter but in isolation.

Another interesting approach was studied in [19], where the use of machine learning for device identification was proposed. The authors of [19] claim that some initial layers of a neural network can be trained using data from only a few devices, showing remarkable potential for scalability to large device populations.

In [20] the error signal between the received signal and the ideal signal is used as a feature, and then a deep learning network is proposed to identify cognitive radio devices, Tested on seven IEEE 802.15.4 devices, an accuracy better than 92% is reported. However the authors of [20] show not only that changing the central carrier frequency could be a problem but also that this approach requires high-end hardware.

Wireless device identification with low-end hardware was analyzed in [21]. The reported performance shows that using low-end hardware causes identification to become specific to the receiver used and has a noticeable negative impact on the identification accuracy.

The work of [22] proposes a radioprint identification based on dimensional reduction and machine learning. It uses the Hilbert transform to extract the necessary features. This method was tested with 10 devices, and has reported an accuracy of 90%. We should mention that to reach this accuracy at least 76 features need to be extracted, which adds to the computational complexity of the solution.

Some wireless technologies make physical layer information available. For example, the IEEE 802.11 standard makes channel state information readily available. This information can be used to extract the carrier frequency offset [23] or the phase error in subcarriers [24]. In LTE it is possible to estimate the I/Q offset with low complexity [25].

Another technique that can be used to enhance wireless device identification is the use of a covert channel. A covert channel is a communication path that is neither designed nor intended to carry information [26]. This method is generally described by using the prisoners' scenario. By modifying the transmission protocol, the covert channel can be created and used as a way of achieving confidentiality and maintaining the user's anonymity. These types of channels are habitually used for leaking sensitive information such as secret

messages and commands. They can be designed at any layer, including the physical layer [27].

We distinguish two different types of covert channels: storage and timing channels [28]. a storage channel directly embeds the information in the covert media, while the timing channel transmits the secret message by modulating and altering the resources over time. Here, we explore the latter

Most covert channel schemes are designed for the data link layer or higher, using, for example reserved fields, time delays, packet corruptions, etc. [29]–[31].

Manipulating quadrature amplitude modulation (QAM) constellations or creating errors can also be a technique to hide information. In [32]–[34], the carrier signal is modulated with a secret message. Before transmitting the signal, the quality of the constellation is slightly altered so that the original message can be transmitted without a standard receiver being able to detect the embedded hidden message.

Varying the transmitter's power and phase as a means to create a covert channel was studied in [35]. In this approach, the covert transmission happens only when the channel quality is high. To the best of our knowledge, there is no previous work that combines PUF and a covert channel to authenticate wireless devices.

III. DEVICE IDENTIFICATION

In this section we describe our radioprint identification framework. First we describe the machine learning method, and then we explain the covert channel method followed by the integrated proposed framework.

A. MACHINE LEARNING IDENTIFICATION (MLID)

MLID identifies a wireless device on a per-frame basis by finding the unique characteristics of the received signal in the modulation domain. In the modulation domain, signals are represented at the most basic level, and interpretation requires knowledge of the modulation scheme.

1) MLID OVERVIEW

Figure 1 provides a basic structure of MLID.

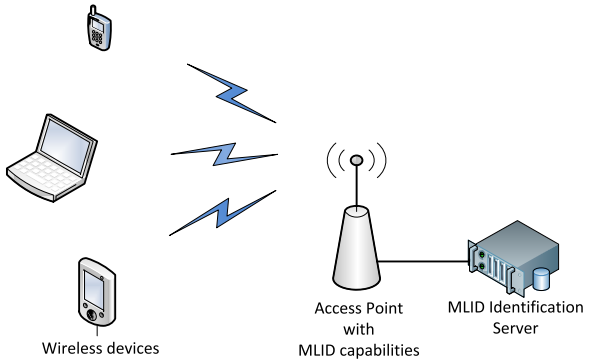


FIGURE 1. High-level overview of MLID. Devices connected to WiFi AP 802.11b, AP with MLID capabilities connects to the MLID identification server via Ethernet.

An MLID system consists of an access point, enabled with capabilities to measure the radiometric fingerprint (radioprint) connected to the identification server containing the authorized radioprints. The identification server keeps a database with the authorized radioprints. It obtains the radioprints by measuring them through the access point, or they can be provided by the wireless device manufacturer. If a wireless device wants to gain access to the network, the access point measures its radioprint and sends it to the identification server. If the radioprint matches an authorized device, access is granted; otherwise access is denied and an alert is sent to the network administrator.

2) FEATURE ANALYSIS

The metrics that are most frequently used as machine learning features for radiometric identification are the normalized magnitudes of the following parameters:

- Frequency error: the difference between the ideal and the received carrier frequency.
- SYNC correlation: the correlation of I/Q values between the ideal and received SYNC, which is a signal used for synchronization.
- I/Q origin offset: the distance between the origin of the ideal I/Q plane and the origin of the received symbols.
- Magnitude error: the difference in magnitudes of the ideal and received signals.
- Phase error: the angle between the ideal and received signals.

Note that the above mentioned metrics are general and can be defined for any digital communication standard.

To understand which metrics are more effective in identifying a device, we use the Pearson's correlation matrix (correlation coefficients lie between -1 and $+1$) presented in Fig. 2.

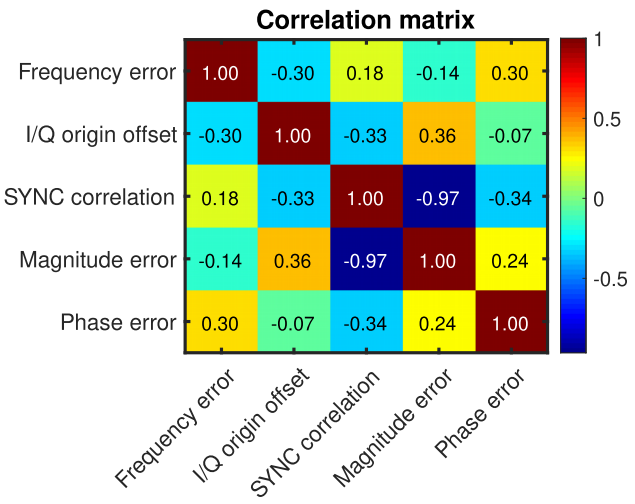


FIGURE 2. Pearson's correlation matrix with Heatmap including five features.

As we can see in Fig. 2 the best discrimination features are frequency error, I/Q origin offset, and phase error.

Although we can use all the features depicted in Fig. 2 (and many others), a very important factor in choosing these three features is that they must be readily deployable in current systems without requiring any expensive hardware changes to the APs. In [23], the authors describe a practical implementation to measure the frequency error by using channel state information measurements, which can be easily obtained by higher-layer applications without the need for any additional hardware. [25] describes an approximate estimation approach to find the I/Q origin offset based on the maximum likelihood criterion by using only one pilot symbol. This interactive approach can be implemented at the AP with low computational complexity due to its ability to use possible precomputations.

B. COVERT CHANNEL IDENTIFICATION (CCID)

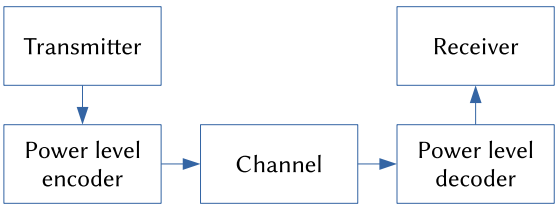
CCID identifies a wireless device by finding the unique bits hidden in the received signal by means of varying the transmitted power. We describe the overall architecture of the Covert Channel Identification method as follows:

1) CCID OVERVIEW

Covert channel identification is based on an important observation that additional useful information bits (at a very slow rate) can be transmitted together with the standard traffic by varying the power level of the transmitted signal.

Fig. 3b depicts the architecture of our proposed wireless communication system, including the covert channel. Compared with the standard communication system shown in Fig. 3a, CCID includes a power level module and a power level decoder.

(a) Standard communication system.



(b) CCID communication system.

FIGURE 3. Architecture with and without a covert channel. The power level module is in charge of varying the power level in order to send covert data at a very low rate.

Covert channel identification works in a pairwise mode between two entities; without loss of generality, we assume that the access point performs the identification process while the user initiates the request. This process includes five stages: radioprint extraction, signature, covert channel transmission, verification, and radioprint and public key retrieval and identification.

a: RADIOPRINT EXTRACTION

A radioprint corresponding to the sending device is extracted using MLID and stored in both the sending and receiving devices.

b: SIGNATURE

The transmitter gets the current date and time. A part of the message sent over the main channel could (optionally) be hashed and appended to the date and time. It first sends this clear text message over the covert channel and then hashes this message and encrypts it using its own private key (corresponding to a public key cryptographic algorithm such as RSA) before sending this signed hash over the covert channel.

c: COVERT CHANNEL TRANSMISSION

On the transmitter side, after modulation of the WiFi signal, we encode the hidden data S by varying the power level at a very low rate, and then the signal is sent to the antenna. On the receiver side, before demodulation, the received signal contains the covert channel bits that are decoded by reading power level variations. Note that the original WiFi signal continues its normal process.

d: VERIFICATION

The receiver extracts the sender's MAC address and looks up the corresponding public key. It extracts the date and time (and optionally the hash of a part of the message sent over the main channel) sent over the covert channel, hashes it, and extracts the signed hash sent over the covert channel. It then decrypts the signed hash using the sender's public key and ensures that this hash matches the hash previously computed by the receiver.

e: RADIOPRINT AND PUBLIC KEY RETRIEVAL AND IDENTIFICATION

The receiver looks up the radioprint and the public key associated with the MAC address of the sender. It then ensures that it matches both the radioprint sensed from the sender's transmission characteristics and the public key used for signing the timestamp (and optionally a hash of a part of the main message) transmitted through the covert channel.

In the following section, we discuss the effective use of the above-mentioned techniques for device identification.

C. INTEGRATED RADIO IDENTIFICATION FRAMEWORK (IRID)

As discussed above, MLID and CCID can be used for passive and active identification, respectively. To ensure a reliable system, we integrate both techniques in IRID. Both identification methods offer good advantages for IoT. First, both methods exhibit low computational complexity as all the expensive computation is done only during training. Second, MLID and CCID take advantage of the hardware variabilities inherent

in the manufacturing process. The hardware variabilities are difficult to predict.

Since the channel quality is generally very good for IoT applications, it is possible to introduce a covert channel exploited by CCID to enhance authentication. After the private key used for encryption is obtained, the access point will use the trained model (MLID) and the private key (CCID) to confirm the legitimacy of the device. This dual and complementary identification framework ensures a more accurate system.

D. TYPICAL USE CASES

MLID is for the most part aimed at ensuring that a wireless radio device, such as WiFi, really is the device it claims to be. An application example is an industrial site (or smart home) exploiting IoT sensors such as structural conditions or environmental sensors. MLID could be used during periodic audits to assess whether the sensor's actual radioprints match the expected radioprints or not. In this scenario, we can assume that the non-matching sensors might have been tampered with or even replaced by rogue sensors. MLID can also be implemented directly within a receiver station (access point), continuously checking whether the sensors' radioprints match the expected one or not. In such a configuration, the system could easily detect whether a legitimate IoT was replaced by a rogue one or a rogue device installed beside a legitimate sensor.

CCID can be used in situations where (slightly) stronger device authentication is needed, but the communication itself cannot be altered (or be replaced by a secure, authenticated and/or encrypted communication channel such as TLS or an encrypted VPN). A receiver station could ensure that the hidden signature of the device is present and valid. In the case of sensors broadcasting information that should be immediately processed by lightweight devices that do not support cryptographic authentication or encryption, the CCID-aware receiver station could simply trigger an alarm if some sensors were no longer sending valid hidden signatures. In this scenario, CCID could be advantageously replaced by IRID in order to combine the hidden authentication mechanism with hardware fingerprint authentication.

IV. IMPLEMENTATION

In this section we explain the design and implementation choices of our proposed radioprint framework.

A. MLID IMPLEMENTATION

Let $x \subseteq \Re^N$ be the features that constitute the input to the neural network. Let $d \in \{1, \ldots, D\}$ be the wireless device to be classified. We then model the neural network as a function $f : x \rightarrow d$, where x and d, respectively, represent the spaces of the input (i.e., features) and output (i.e., probability distribution). Figure 4 shows the neural network structure of MLID.

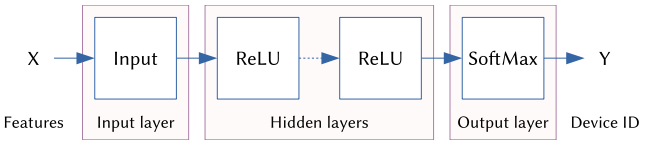


FIGURE 4. Neural network structure of MLID. Input dense layer, two hidden dense layers with ReLU activation, and output dense layer with Softmax activation, Dropout 0.5 between layers.

In some sense, we can imagine that the mapping of the function f will approximate the mapping of the system.

$$f(x; w) = arg \max_{d} \hat{P}(d|x; w), \tag{1}$$

where $\hat{P}(d|x; w)$ denotes the conditional probability density function and w are the network parameters. Without loss of generality, we now define the loss function as the cross entropy:

$$L(w) = E_{x,d}[-\log \hat{P}(d|x; w)]. \tag{2}$$

If we fix the network structure and size then the parameters w can be estimated as:

$$w^* = arg \min_{w} L(w), \tag{3}$$

where w^* are the estimated parameters. Note that the conditional distribution $\hat{P}(d|x; w)$ tries to approximate the optimal $P(d|x; w)$, i,e,. $\hat{P}(d|x; w) \approx P(d|x; w)$.

We can now define the probability of error as:

$$P_e = P(y \neq f(x; w)). \tag{4}$$

Note that the most common way of selecting the size of a neural network is the trial and error approach. After a network structure is selected, the parameters are trained. Cross-validation is used to decide whether or not the performance of the trained network satisfies the desired requirements.

1) COMPLEXITY ANALYSIS

From our design, we find that the total number of multiplications performed by MLID is:

$$\omega^2(L-3) + \omega(8N + D), \tag{5}$$

and the total number of additions is:

$$\omega^2(L-3) + \omega(8N + D), \tag{6}$$

where ω is the neural network width (maximal number of nodes in each hidden layer) and N is the number of features. Assuming $N < D < \omega$, the complexity of the proposed MLID is of the order of $\mathcal{O}(\omega^2 L)$, i.e., the algorithm has linear complexity in the number of layers L and quadratic complexity in the network width ω. N and D are given parameters, L and ω are network parameters to be tuned when designing the neural network; in practice, we have found that the network is sensitive to big changes in L but not so sensitive to big changes in ω.

B. CCID IMPLEMENTATION

1) POWER LEVEL MODULE

As mentioned in the previous section, a power level module must be utilized. We propose to use a simple solution, which is to modulate slowly (at a very low rate of 1 bit per second) the amplitude of the power level of the signal ready to be sent. This allows us to minimize interference.

2) POWER LEVEL DECODER

On the receiver side, a power level decoder needs to be implemented. Here we propose to measure the $RSSI_{REF}$ (Received Signal Strength Indicator) and use it as the reference. A sample transmitted signal plot can be seen in Figure 5.

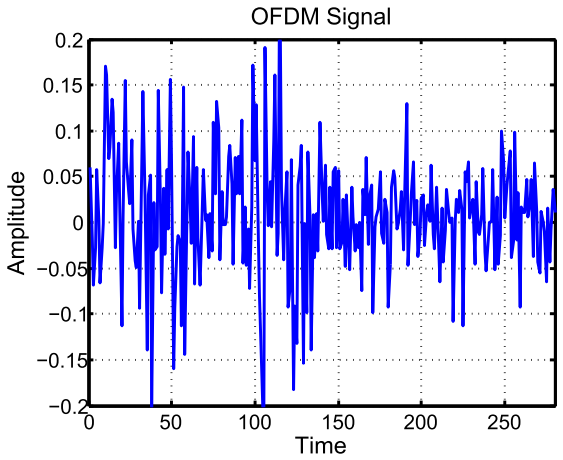


FIGURE 5. Sample transmitted signal, first half average power P, second half average power $P/2$.

Then at every frame we measure the $RSSI$ and compare it with $RSSI_{REF}$. We can determine if a bit is transmitted as:

$$\text{side channel bit} = \begin{cases} 0, & \text{if } RSSI < \alpha RSSI_{REF} \\ 1, & \text{otherwise,} \end{cases} \quad (7)$$

where $0 < \alpha < 1$ is a design parameter that ensures that the BER is acceptable. The power level decoder algorithm is described in Algorithm 1.

Algorithm 1 Power Level Decoder

1: at the beginning of the side channel transmission
2: measure $RSSI_{REF}$
3: **for** every frame **do**
4: measure $RSSI$
5: find side channel bit according to (7)
6: **end for**

Fig. 6 shows the physical layer architecture according to the 802.11b standard. The RSSI is processed by the Physical Layer Convergence Procedure (PLCP) and measured in the preamble of the PLCP frame, between the Start Frame Delimiter and the PLCP Header Error Check.

A sample RSSI plot over a few minutes in an indoor environment is illustrated in Fig. 7. The RSSI amplitude

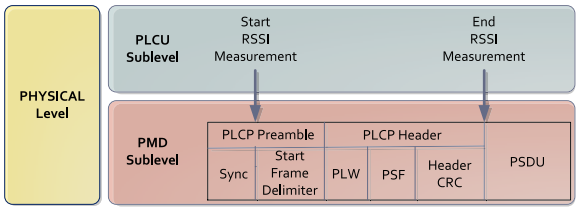


FIGURE 6. RSSI measurement process as described in the 802.11b standard.

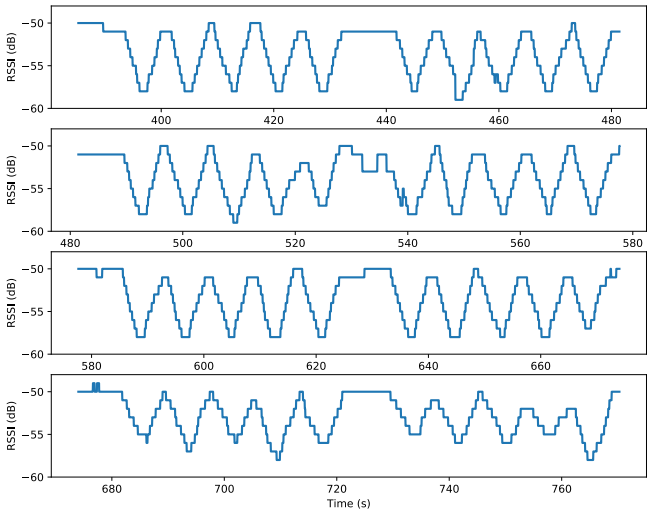


FIGURE 7. Sample RSSI measurement over time.

modulation is clearly visible, even though we notice some variations of around 1 to 3dB, mainly due to interference caused by people walking around.

V. EVALUATION

In this section, we evaluate the performance of our proposed framework. First, we present the performance of MLID and justify the parameter choices. Then we evaluate the covert channel method, and finally we discuss the overall performance.

A. SIMULATION SETTINGS

The proposed framework is implemented using Tensorflow in Python; the performance evaluation dataset of MLID consist of data from 20 IoT devices. Table 1 summarizes the simulation parameters.

TABLE 1. Simulation parameters.

Parameter	value
Number of IoT devices	20
device location	indoor
device speed	< 3m/s
device transmit power	max 100 mW
WiFi standard	802.11b
Maximum number of samples per device	100

B. SIMULATION RESULTS

Fig. 8 shows the impact of the number of frames on MLID performance. As the number of frames increases, the error rate is seen to fall until it reaches its lowest value when 10 frames are utilized as features. This tells us than in order to have the best performance our method needs data of 10 frames. Remember that one frame provides one sample.

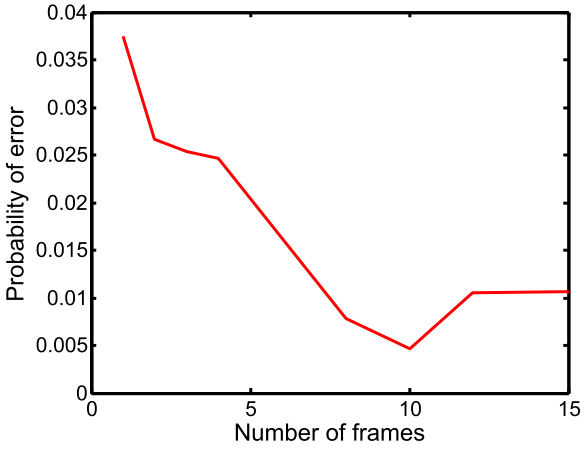


FIGURE 8. Effect of number of frames on accuracy.

Fig. 9 illustrates the error rate with respect to the number of epochs used by MLID. In this figure we can see that as the number of epochs increases, the performance also increases, and the performance no longes increases after 150 epochs. To avoid over-fitting we used the Dropout method.

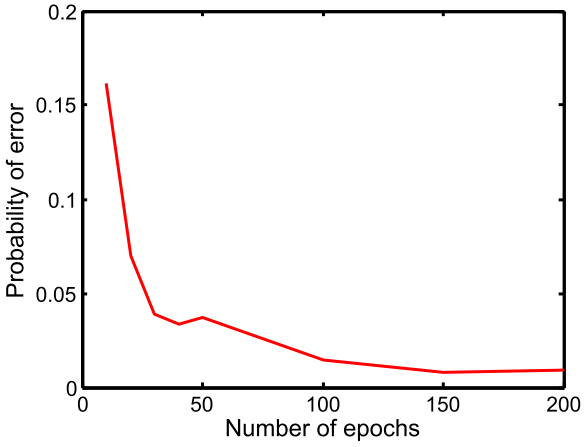


FIGURE 9. Effect of number of epochs on accuracy.

We also show the accuracy of MLID when varying the number of hidden layers (Fig. 10). As one can see the performance seems to deteriorate after two layers, mainly due to the fact that neural networks benefit the most by having big datasets.

Fig. 11 shows the accuracy with respect to the number of neurons in a hidden layer (width). As the figure demonstrates, twice the size of the output layer is enough to obtain the best performance.

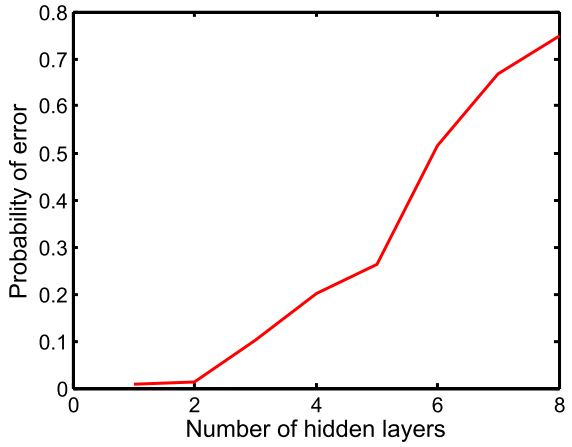


FIGURE 10. Effect of number of hidden layers on accuracy.

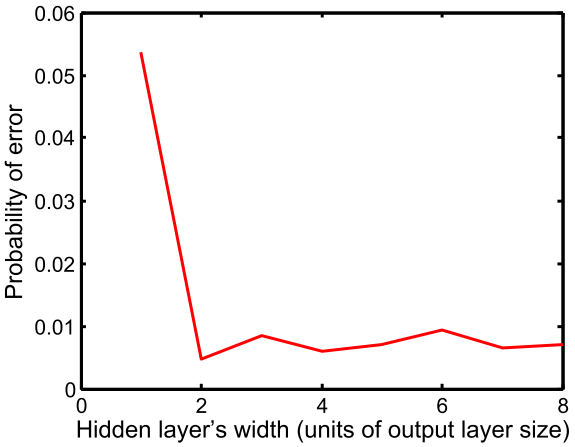


FIGURE 11. Effect of width of hidden layers on accuracy.

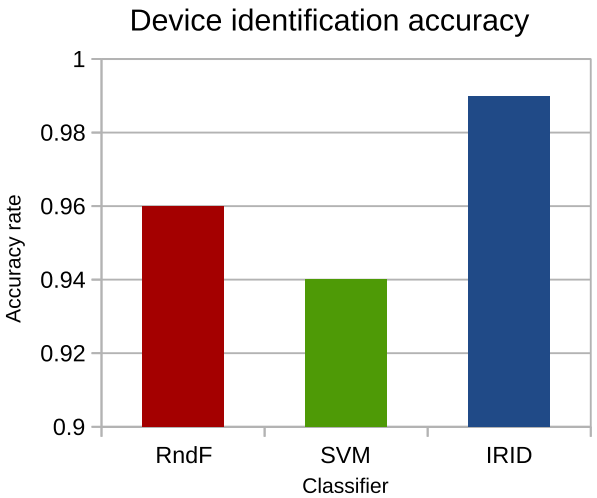


FIGURE 12. Device identification accuracy. Random forest (RdnF), support vector machine (SVM) and integrated radio identification (IRID).

To evaluate the covert channel method, we used low-cost IoT devices that did not allow us to manage the internal parameters directly. Nevertheless, we were able to have a raw control over the power level and to transmit at a very

low rate of <1 bps with a bit error rate better than 10^{-3} without interfering with the normal communication, thereby verifying that it was possible to introduce a covert channel that enhanced the accuracy of our authentication method.

Initial evaluation results involving 20 identical IoT devices at a high signal-to-noise ratio (20dB) show promising results. To validate our results, we include a comparison of some of the techniques found in the literature, such as Random forest (RdnF) and Support vector machine (SVM).

As shown in Fig. 12. IRID has an overall accuracy rate of over 99% which suggests that a low-cost radio authentication method is possible.

VI. CONCLUSION

In this paper, we propose a machine learning (passive) and covert channel (active) framework to achieve device identification with high accuracy. We show that our IRID framework can distinguish network devices effectively, first by reading the signal variations caused by manufacturing imperfections and applying machine learning techniques. Second, to further improve our method, we use an easily implemented ''power'' covert channel to reinforce the system by offering another alternative to validate the identity of a given device. Utilizing these two techniques, we have designed a framework to identify network devices uniquely.

We implemented our framework using low-cost IoT devices and a VSA analyser. In our experiments with 20 devices, we showed that our framework could detect network devices with 99% accuracy. In future work, we plan to implement our solution on IoT devices fully and expand the test to more devices under different channel conditions. By reducing the implementation complexity and differentiating among multiple network devices, we expect to be able to achieve many new applications, such as identifying network attackers.

ACKNOWLEDGMENT

The authors would like to thank Prof. Fabrice Labeau from McGill University for the constructive discussions in the course of this research.

REFERENCES

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

[2] S. W. Shah and S. S. Kanhere, ''Recent trends in user authentication—A survey,'' *IEEE Access*, vol. 7, pp. 112505–112519, 2019.

[3] N. S. Selvarathinam, A. K. Dhar, and S. Biswas, ''Evil twin attack detection using discrete event systems in IEEE 802.11 Wi-Fi networks,'' in *Proc. 27th Medit. Conf. Control Autom. (MED)*, Jul. 2019, pp. 316–321.

[4] H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri, ''Wireless anomaly detection based on IEEE 802.11 behavior analysis,'' *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2158–2170, Oct. 2015.

[5] M. Bhargava, ''Reliable, secure, efficient physical unclonable functions,'' Ph.D. dissertation, Carnegie Mellon Univ., Dept. Elect. Comput. Eng., Pittsburgh, PA, USA, May 2013.

[6] Z. He, M. Wan, J. Deng, C. Bai, and K. Dai, ''A reliable strong PUF based on switched-capacitor circuit,'' *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 6, pp. 1073–1083, Jun. 2018.

[7] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, ''Implementation and characterization of a physical unclonable function for IoT: A case study with the TERO-PUF,'' *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[8] A. El-Atawy, Q. Duan, and E. Al-Shaer, ''A novel class of robust covert channels using Out-of-Order packets,'' *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 2, pp. 116–129, Mar. 2017.

[9] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, ''Achieving covert wireless communications using a full-duplex receiver,'' *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[10] N. Asokan, J. Ekberg, K. Kostiainen, A. Rajan, C. Rozas, A. Sadeghi, S. Schulz, and C. Wachsmann, ''Mobile Trusted Computing,'' *Proc. IEEE*, vol. 102, no. 8, pp. 1189–1206, Aug. 2014.

[11] M. Potkonjak and V. Goudar, ''Public physical unclonable functions,'' *Proc. IEEE*, vol. 102, no. 8, pp. 1142–1156, Aug. 2014.

[12] Q. Xu, R. Zheng, W. Saad, and Z. Han, ''Device fingerprinting in wireless networks: Challenges and opportunities,'' *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[13] M. A. Usmani, S. Keshavarz, E. Matthews, L. Shannon, R. Tessier, and D. E. Holcomb, ''Efficient PUF-based key generation in FPGAs using per-device configuration,'' *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 2, pp. 364–375, Feb. 2019.

[14] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, ''Wireless physical-layer identification: Modeling and validation,'' *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091–2106, Sep. 2016.

[15] X. Wang, P. Hao, and L. Hanzo, ''Physical-layer authentication for wireless security enhancement: Current challenges and future developments,'' *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[16] R. Waheetha and J. M. M. Vijila, ''Approaches and techniques to prevent cloning in mobiles,'' *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 4, pp. 21791–21795, Dec. 2016.

[17] B. Perez, M. Musolesi, and G. Stringhini, ''Fatal attraction: Identifying mobile devices through electromagnetic emissions,'' in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw. WiSec*, 2019, pp. 163–173.

[18] A. C. Polak and D. L. Goeckel, ''Wireless device identification based on RF oscillator imperfections,'' *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2492–2501, Dec. 2015.

[19] K. Youssef, L. Bouchard, K. Haigh, J. Silovsky, B. Thapa, and C. V. Valk, ''Machine learning approach to RF transmitter identification,'' *IEEE J. Radio Freq. Identificat.*, vol. 2, no. 4, pp. 197–205, Dec. 2018.

[20] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, ''Deep learning for RF device fingerprinting in cognitive communication networks,'' *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.

[21] S. U. Rehman, C. Coghill, and K. W. Sowerby, ''Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios,'' *IET Commun.*, vol. 8, no. 8, pp. 1274–1284, May 2014.

[22] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, ''The individual identification method of wireless device based on dimensionality reduction and machine learning,'' *J. Supercomput.*, vol. 75, no. 6, pp. 3010–3027, Jun. 2019.

[23] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, ''Accurate and efficient wireless device fingerprinting using channel state information,'' in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2018, pp. 1700–1708.

[24] P. Liu, P. Yang, W.-Z. Song, Y. Yan, and X.-Y. Li, ''Real-time identification of rogue WiFi connections using environment-independent physical features,'' in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2019, pp. 190–198.

[25] C. Kuhn, ''IQ offset and imbalance estimation for LTE basestation receivers and measurement devices,'' in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2011, pp. 1–5.

[26] Y. Heda and R. Shah, ''Covert channel design and detection techniques : A survey,'' in *Proc. IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT)*, Jul. 2015, pp. 1–6.

[27] J. Ullrich, T. Zseby, J. Fabini, and E. Weippl, ''Network-based secret communication in clouds: A survey,'' *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1112–1144, 2nd Quart., 2017.

[28] M. Hussain and M. Hussain, ''A high bandwidth covert channel in network protocol,'' in *Proc. Int. Conf. Inf. Commun. Technol.*, Jul. 2011, pp. 1–6.

[29] X. Zhang, L. Guo, Y. Xue, and Q. Zhang, ''A two-way VoLTE covert channel with feedback adaptive to mobile network environment,'' *IEEE Access*, vol. 7, pp. 122214–122223, 2019.

[30] A. Velinov, A. Mileva, S. Wendzel, and W. Mazurczyk, ''Covert channels in the MQTT-based Internet of Things,'' *IEEE Access*, vol. 7, pp. 161899–161915, Nov. 2019.

[31] M. A. Elsadig and Y. A. Fadlalla, "Network protocol covert channels: Countermeasures techniques," in *Proc. 9th IEEE-GCC Conf. Exhib. (GCCCE)*, May 2017, pp. 1–9.
[32] P. Cao, W. Liu, G. Liu, X. Ji, J. Zhai, and Y. Dai, "A wireless covert channel based on constellation shaping modulation," *Secur. Commun. Netw.*, vol. 2018, pp. 1–15, Jan. 2018.
[33] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *Information Hiding*, M. Kirchner and D. Ghosal, Eds. Berlin, Germany: Springer, 2013.
[34] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, Nov. 2018.
[35] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert wireless communications with channel inversion power control in Rayleigh fading," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 12135–12149, Dec. 2019.

OSCAR DELGADO (Member, IEEE) received the M.A.Sc. degree from Concordia University, Montreal, QC, Canada, in 2010, and the Ph.D. degree in electrical engineering from McGill University, Montreal, in 2016. In 2017, he joined the Telecommunications and Signal Processing Laboratory (TSP), Department of Electrical and Computer Engineering, McGill University, where he is a Postdoctoral Researcher. His current research interests are in the applications of 5G wireless mobile communication technologies, including AI/machine learning, software-defined networks, network virtualization, and green wireless systems, and the analysis and design of video traffic management techniques, resource allocation strategies, and energy efficiency algorithms.

LOUAI KECHTBAN received the B.S. degree in mechatronics engineering from Rafik Hariri University, Lebanon, in 2016, and the M.S. degree in electromechanical engineering from the Université Catholique de Louvain (UCLouvain), Belgium, in 2018. As a part of the master's degree thesis work, he explored new aspects to improve 3D monocular SLAM for autonomous drone navigation. From 2018 to 2019, he was a Research Assistant working on Wal-e-Cities Research Project, which aims to develop an innovative solution for the smart city as a part of Prof. B. Macq's Pixels and Interactions LAB (PiLAB), Institute of Information and Communication Technologies, Electronics, and Applied Mathematics (ICTEAM), UCLouvain. He is currently working with the Department of Electromechanical Innovation, Alstom, Belgium. His research interest includes the development of new technical methods for identification and communication security toward the IoT embedded systems.

SÉBASTIEN LUGAN (Member, IEEE) received the master's degree from École Supérieure d'Ingénieurs en électronique et électrotechnique (ESIEE), France, the D.E.A. degree from the Gaspard–Monge Institute of Electronics and Computer Science, Université Paris-Est Marne-la-Vallée (UPEM), France, and the Ph.D. degree in engineering sciences from the École Polytechnique de Louvain, Université Catholique de Louvain (UCLouvain), Belgium. In 2003, he joined the Pixels and Interactions Lab (PiLAB), Institute of Information and Communication Technologies, Electronics, and Applied Mathematics (ICTEAM), UCLouvain, where he is currently a Senior Researcher. His research activities include medical imaging, image compression and mega-image navigation, the LIDAR detection of wake turbulence generated by airliners, and secure communications for embedded devices and sensors such as the IoT for smart cities.

BENOÎT MACQ (Fellow, IEEE) received the Ph.D. degree from the Université Catholique de Louvain (UCLouvain), Belgium, in 1989. He was a Researcher with the Philips Research Laboratory, Belgium, from 1990 to 1991, developing wavelet-based compression algorithms and contributing to the JPEG-2000 Standard. He has been a Professor with the Polytechnic School, UCLouvain, since 1993. He has been a Visiting Professor with the Ecole Polytechnique Fédérale de Lausanne and the Massachusetts Institute of Technology, Boston, and he is currently a Visiting Professor with McGill University, Montreal. His main research interests are image compression, image watermarking, and image analysis for medical and immersive communications. He is a member of the Royal Academy of Science of Belgium. He was the General Chair of the IEEE ICIP 2011 in Brussels. He has been the Chair of several European projects, including a Network of Excellence on Multimodal Interactions (SIMILAR project) and an Integrated Proposal, EDcine, which paved the way for the technology of digital cinema in the European Union. He is the Founder of the *Journal of Multimodal Interfaces* edited by Springer Verlag. He is the co-founder of 11 spin-off companies. He was an Associate Editor of the IEEE TRANSACTIONS ON MULTIMEDIA and the IEEE TRANSACTIONS ON IMAGE PROCESSING, and a Guest Editor of the PROCEEDINGS OF THE IEEE. He is currently a Senior Associate Editor of the IEEE TRANSACTIONS ON IMAGE PROCESSING.