A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification

Amir Ashtari
School of ECE, College of Engineering, University of Tehran, Tehran, Iran
amirashtari.74@ut.ac.ir

Ahmad Shabani
School of ECE, College of Engineering, University of Tehran, Tehran, Iran
ah.shabani@ut.ac.ir

Bijan Alizadeh
School of ECE, College of Engineering, University of Tehran, and School of Computer Science, IPM, Tehran, Iran
b.alizadeh@ut.ac.ir

***Abstract*—This paper presents a novel RF-PUF based authentication framework which exploits the intrinsic non-idealities in physical characteristic of a device/medium to generate a unique identity for wireless nodes. It also takes the advantage of Random Forest classification to securely identify the sender nodes based on their unique features extracting from already-existing modules in the receiver side. In contrast to the neural network-based schemes, our proposed approach incurs lower design complexity and overheads, while it no longer needs a large amount of preparatory and preprocessing works related to the learning process and adjusting the network parameters. Thus, the overall runtime required to preparing and testing of network is drastically lessened. The experimental results show that the proposed scheme can reach to 100% accuracy in the identification of 225 nodes when a forest network with 100 trees and depth of 20 is developed, posing a negligible overhead on the receiver side. This high accuracy can be nearly achieved even in the presence of channel variations as our approach has less sensitivity to environmental conditions.**

Keywords*—IoT, Network Security, Random Forest, Authentication, RF-PUF, RF Fingerprinting

I. Introduction

The recent advancements in ultra-low power sensor devices, low power and wide area communication networks, and emerging computing frameworks (*Cloud computing*, *Edge/Fog computing*) for a large amount of data, have resulted in emerging a concept, commonly referred to as Internet of Thing (IoT). Due to the distributed, unsupervised, and resource-constraint IoT nodes, they are permanently vulnerable and exposed to the variety of potential malicious tampering and attacks. The traditional key-based authentications to securely establishing communication, mainly suffer from vulnerability to key-hacking, information leakage through side channel analysis and hardware Trojan insertion [1], and substantial power and area overheads. To rectify the existing challenges, Physical Unclonable Function (PUF) was firstly introduced by [2] for IC anti-counterfeiting application and key generation in cryptographic operations. The idea behind the PUF concept lies on the fact that the intrinsic non-idealities and inherent variations in physical characteristic of a device/medium can be exploited to generate a unique and device-dependent identity, which practically cannot be replicated [3]. From authentication point of view, this unique identity can be exploited to validate the trustworthiness of an entity based on its own physical characteristics or the communication medium impairments and not based on the content they exchange. Accordingly, many works till date are being dedicated to PUF concept developing more complete and robust structures [4]–[6] as the new attack models, i.e., statistical, mathematical models, and machine learning algorithms, are emerging.

RF fingerprinting is an authentication approach in wireless sensor nodes which securely identifies authorized identities by taking advantage of sender's transient features including time and frequency domain properties. Since the sender's transient features are random and almost constant, they can effectively be classified with high accuracy only when the beginning of the transient are reliably identified [7]–[9]. Despite the prominent features of RF fingerprinting, it requires high oversampling rates and its classification accuracy is mainly affected by environmental conditions and aging issue. These drawbacks impose a substantial power and precision requirements on the receiver side resulting in high cost and power-hungry architecture [10][9].

Authors of [11] proposed a new way of RF fingerprinting, which in addition to the amplitude characteristic, it also makes use of phase characteristic of signals for transient detection purposes. The big step toward RF fingerprinting was taken by [10] in which a Probabilistic Neural Network (PNN) is used to classify sender nodes at the receiver side. Instead, the authors of [12] proposed a new authentication method which utilized a Convolutional Neural Network (CNN) as a classifier engine which improved the classification accuracy at the expense of higher design complexity. Although a CNN benefits from high accuracy and reliability in classification, its implementation on resource-constraint IoT nodes is still challenging, thereby consuming high power and posing high computation complexity. Following that, a novel classification algorithm of RF fingerprinting method was developed by [8] in which a de-noising processing is performed and the authentication accuracy improved thanks to the used wavelet-based feature extraction scheme and SVM classifier. Recently, a new deep neural network-based architecture, called RF-PUF [13][14], was proposed for real-time authentication of IoT nodes, which surpassed RF fingerprinting in different aspects by exploiting the inherent process variations of RF properties of wireless transmitters as well as employing in-situ machine learning at the receiver to identify them. The RF-PUF does not require any additional circuitry for feature extraction, and the circuit overheads are merely imposed on the receiver side since the identification burden is completely shifted to the IoT gateway. Moreover, RF-PUF no longer need high oversampling rate, as opposed to the RF fingerprinting, and it takes advantage of

978-1-7281-4374-3/19/$31.00 ©2019 IEEE

higher dimensionalities feature space, resulting in a strong PUF category. However, realizing in-situ machine learning on existing gateway still occupies a large portion of computational power and this might be a serious problem in *Edge-Computing* IoT platforms as the computing power is being shifting to the location where source of data is collected (e.g., gateways) [15]. This shifting is mainly because of lower latency and higher bandwidth requirements in current IoT applications. On the other hand, the low power requirement for gateways located in outlying regions is becoming more crucial, and this dictates the need for a low complex classification method.

In this paper, a new low overhead and low complex RF-PUF-based authentication protocol for identifying transmitters in a wireless network is proposed by leveraging the *Random Forest (RndF)* classification algorithm. In a digital communication framework, several non-idealities cause some variations and generate imbalanced behaviors in intrinsic properties of transmitters chain or communication medium. As these unique and device-dependent impairments are already present in the wireless network, in this paper, we seize the opportunity to extract those non-idealities without any additional circuitry to generate a strong PUF instance. Then, a low overhead RndF, which is a supervised classification algorithm, is employed in a receiver side without posing any overhead on IoT nodes so as to identify transmitters according to their inherent properties already extracted in the previous phase. Unlike the neural networks, the RndF frameworks can handle data without preprocessing and runs efficiently on large databases. They can be trained with a relative small amount of data, so the training process would be fast. Besides, there is no need for preparatory work, e.g., *Normalization*, to bring the inputs into the required form, in contrast to the neural networks. Accompanied with a RndF classification algorithm, the proposed authentication method is employed in a wireless network based on IEEE 802.15.4 standard [16], which primarily focuses on low-cost, low-speed ubiquitous communication between devices.

The rest of the paper is organized as follows. The fundamental backgrounds are provided in Section II, where we mainly focus on the motivations of the current work. In Section III, the proposed RF-PUF authentication flow is described, and the experimental results related to the classification are presented in Section IV. Finally, a comprehensive conclusion is drawn in the last section.

II. Background and Motivation

The idea of RF-PUF has been taken from the existing mechanism in inherent authenticating of human voice communication. In such human communication, the parties establish a trustworthy network based on unique voice signature and not based on the content of message they exchange. Thus, regardless of the message type and content, the human's brain identifies the parties and decides to whether establish a trust or not. Basis on this fact, the RF-PUF uses a similar mechanism as it exploits the intrinsic process variations in RF properties as well as channel impairments to securely identify the involved parties. In this method, device identification is performed in the receiver's brain, which can be either a machine leaning or any classification algorithm, based on the unique signatures extracted from each of the transmitters. As previously mentioned, the recent work on RF-PUF leveraged a deep Neural Networks-based framework as a decision engine [14]. Our work, on the other hand, uses a classification engine, called *Random Forest* (*RndF*) decision tree, which surpasses the prior work in different aspects. In [14], the training of Neural Networks is very time-consuming and computationally intensive. This higher complexity not only pertains to its learning process, but also to the large amount of preparatory and pre-processing works as the input data must be in a specified format and properly normalized. Furthermore, due to the need for adjusting different hyper parameters, e.g., number of layers, neurons per layer, or the learning rate, different combinations of these parameters should be tested to achieve a best model of network. For doing so, a complete model should be calculated and then evaluated for each of the combinations, resulting in a remarkable time and cost overheads.

Random Forests, on the other hand, requires much less preparation efforts, and can be trained with small amount of data, as opposed to the Neural Networks that need more data to reach the same level of accuracy. In essence, Random Forest algorithm consists of a set of decision trees so that each of the trees makes a distinct decision according to their depth given by the feature classification without any dependency on data type. Then, each tree gives an output which is considered as a 'vote' from that tree to the given output. The output which receives the maximum 'votes' is chosen by the random forest as the final result.

In a typical implementation, two parameters of a forest can be adjusted relying on the trade-off between the accuracy and the complexity: 1) tree count and 2) tree depth, which are shown in Fig. 1. As the name suggests, this algorithm creates the forest with a number of trees. The higher number of tree the forest keeps; the higher accuracy in classification can be reached. Meanwhile, the generated forests can be saved for future use on other data, and the algorithm can also be executed in parallel especially when a high performance computation is needed. In addition, this classification algorithm can handle a large data set without substantially increasing in the complexity so this feature can be particularly beneficial in a star topology in IoT networking, where a large number of transmitters are connected to a central connection point, e.g., hub or gateway. As a result, the implementation of Random Forest in the proposed framework has several distinct advantages over the Neural Networks, and incurs much lower complexity in both computational and hardware terms, which makes it a suitable candidate for the proposed implementation at the receiver side of IoT network.

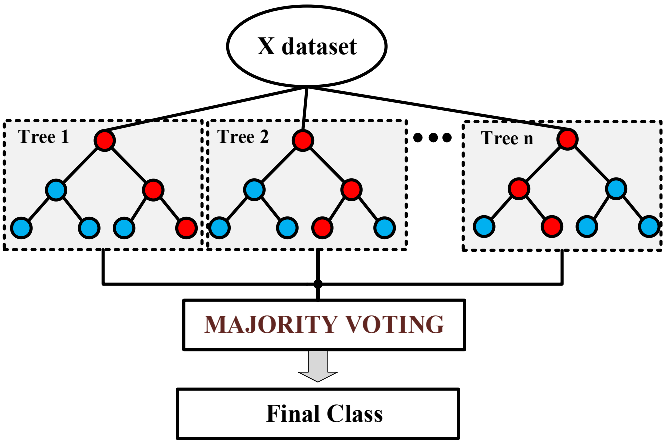

Fig. 1. Random Forest algorithm consisting of a set of decision trees

III. PROPOSED RF-PUF-BASED AUTHENITICATION FLOW

Due to the distributed nature and substantial increase in connected devices, the IoT network is exposed to different attack models originated from inherent network vulnerability or human mistakes. Therefore, presenting a complete framework to securely authenticate parties in network without inspecting content of message is of interest. By developing such framework, it is possible to neutralize different attacks, e.g., key hacking, replay attack, eavesdropping attack, etc., thereby increasing the reliability, the integrity, and the confidentiality in wireless networks. The main goal of this paper is to presenting an effective solution for securely classification of sender's nodes in IoT network by the means of physical characteristic of devices and inherent properties of RF signals. For this reason, we embrace the already-existing non-idealities in the wireless communication signal path as intrinsic features to generate a strong PUF instance by which the necessary features are extracted, and finally the transmitter nodes are securely classified by the Random Forest brain located at the receiver side. Fig. 2 shows the proposed RF-PUF based authentication flow which extracts unique properties from transmitters affected by the process variations for PUF instance and classify transmitters using Random Forest algorithm. To describe the proposed framework, we divide the discussion into three phases: 1) communication framework, 2) feature specification and extraction, and 3) Random Forest classification.

The first step in the proposed methodology, as shown in Fig. 2, is to implement a physical layer communication framework. We select IEEE 802.15.4 as our communication framework since it is one of the preferred standard for IoT networking. One of the important aspects that this standard has taken into account is the low power consideration for wireless nodes, which ensures that they can still be operative even for several years. To generate a strong PUF instance, we need to extract several features related to the process variations in transmitter nodes or channel impairments (e.g., signal attenuation, interference, etc.), which is introduced in the second phase of the implementation. Luckily, this required features to generate PUF instance can be directly extracted from the modules embedded in the receiver side of the communication network without adding additional circuitry. Finally, the transmitter nodes are securely identified for authenticating in IoT network based on Random Forest classification algorithm and features extracted in the previous phase. It should be noted that this algorithm does not need any preprocessing or preparatory work and the classification is quickly performed using the raw data. The detail discussion about every phase will be given in the following subsections.

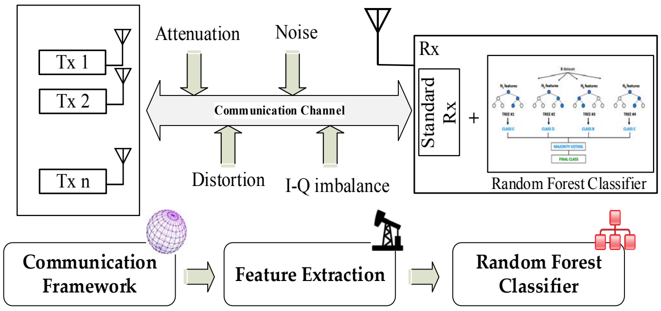

Fig. 2. The proposed RF-PUF authentication framework

A. Communication Framework

The standard IEEE 802.15.4 defines the physical layer (PHY) and medium access control (MAC) sub-layer for low-data-rate wireless connectivity with portable, and moving devices with no battery or very limited battery consumption requirements. The physical layer can be implemented in different ways. Fig. 3(a) shows the block diagram of a typical transmitter in IEEE 802.15.4 standard consisting of four different modules. At first, frames are created according to the standard format and binary data collected from IoT sensor devices. Then, each four-bit binary data is mapped to a symbol, and the generated symbols are mapped to Chip format in subsequent module. For doing so, the O-QPSK PHY employs a 16-ary quasi-orthogonal modulation technique. Finally, the signals are respectively modulated via O-QPSK, filtered and amplified before sending to the receiver.

The block diagram of the receiver side in this standard IEEE 802.15.4 is analogous to its communication counterparts with the difference that it requires additional mapping of Chip to symbol and symbol to binary at the end of flow as shown in Fig. 3(b). At the receiver side, the first block after the antenna and Band Pass Filter (BPF) is DC-blocking which compensates the DC offset of the signal introduced by the noise and the channel interference. Due the inherent variations in local oscillators (LOs), each transmitter has its unique frequency offset in proportion to the ideal carrier frequency. This led to a frequency mismatch between transmitters and the receiver even in the ideal environmental conditions. To compensate for the frequency offset, the synchronizer module is employed in the receiver side so that the frequency offset is calculated respect to the high quality reference clock deployed in the receiver. Another impairment in the communication channel, that should be certainly compensated especially for the long distances, is the attenuation of transmitted signal, which reduces the signal amplitude and lowers SNR value. To amplify the received signal, an Automatic Gain Controller (AGC) unit is utilized which augments the signal power to a reasonable level. The next imbalanced feature in the communication channel is the mismatch of the amplitude and the phase between the in-phase (I) and quadrature (Q) components of the transmitted signal, thus is necessity to extract the above information for all symbols and compensate for them. The I-Q Compensator block in the receiver side is meant for doing so in which the mismatch between the received signal and that of the ideal value is calculated. Finally, the signal is De-modulated in subsequent block and is mapped to the certain symbol and binary formats. Afterwards, the remaining process, e.g., transforming, decoding, can be additionally performed on binary data.

B. Feature Specification and Extraction

As mentioned above, there exist several intrinsic features in RF signal which are unique and device-dependent and mainly differ from one another owing to the presence of process variations and the interference in channel. The idea of RF-PUF concept lies on the fact that these features has the potential to uniquely identify each transmitter in the network. Therefore, one can use such non-idealities and classify them to securely authenticate the IoT nodes in wireless network. In the proposed RF-PUF based authentication framework, four inherent features are extracted from different modules already embedded in the receiver block; thus no additional hardware is needed for the feature extraction phase. Fig. 4 shows the main already-existing modules in the receiver side and four features that can be

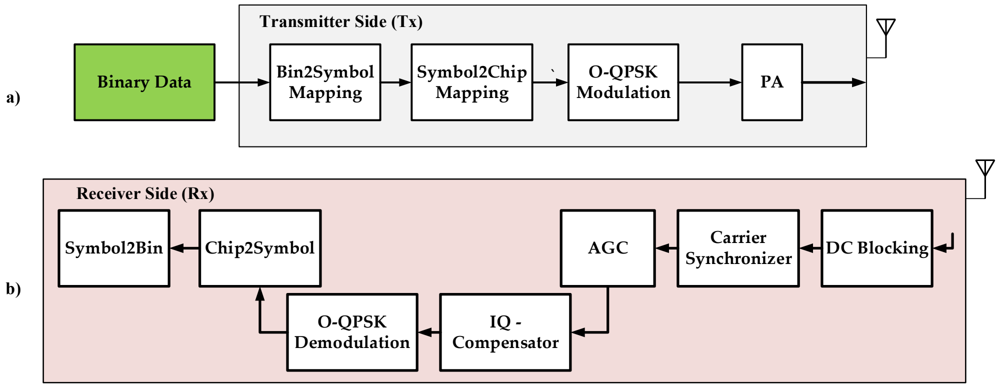

Fig. 3. Block diagram of a) transmitter and b) receiver blocks in IEEE 802.15.4 standard

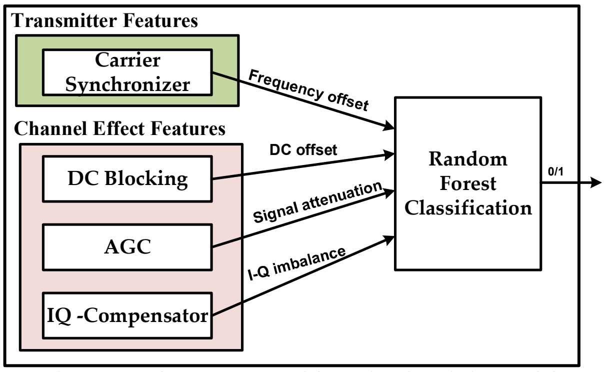

Fig. 4. Four features extracted from already-existing modules

extracted from them. The extracted features can be classified into 1) transmitter features and 2) channel effect features. The former category includes the property related to the frequency offset caused by process variation in LO of transmitter nodes and the latter one consists of DC offset, signal attenuation, and I-Q imbalance introduced by the channel impairments.

C. *Random Forest Classification*

Since the STAR topology has been considered for the network implementation, the proposed authentication scheme is only deployed in the central HUB. Therefore, the hardware overheads are only imposed on a single point and the resource-constraint transmitters can still operate in a low power mode with low hardware overhead. As a result, implementing a classification framework, that in addition to providing a high classification accuracy, also decreases the required overheads, is of interest. In order to identify the transmitter nodes and prevent from malicious tampering in wireless networks, we leverage a framework based on Random Forest classification. The main objective of the proposed framework is to classify the sender nodes based on the unique features extracted from embedded modules in the receiver side so that the senders are authenticated according to their device-dependent features before establishing every mutual connection. This way, a forest consisting of group of trees is created as a network and trained based on the properties of the senders extracted in subsection III(B). Finally, the authentication process is carried out by checking the unique properties of the senders and matching them to a specific sender identity. If the property under evaluation is matched with a known sender identity, the authentication is passed, otherwise, the connection will be aborted.

IV. Exprimental Results

In this section, we implement the entire authentication framework by considering four unique features from both the channel and transmitter nodes effects. The four features, that are considered for identifying sender nodes, are DC offset, frequency offset, signal attenuation, and I-Q imbalance. The allowable limits for the frequency offsets in IEEE 802.15.4 standard is within 40 ppm. The physical layer of this standard has been implemented in Communication Toolbox of Matlab software. We select the following conditions in implementing the physical layer; Frequency=2450 MHz, Modulation: O-QPSK, data rate= 250 kbit/s, 1 MSym/s. Moreover, the Random Forest classifier has been implemented using Scikit library in Python language. Our target is to evaluate the accuracy of authentication of the sender nodes in different situations and select the best candidate for our implementation by adjusting different parameters. In our first try, we select totally 225 sender nodes for network implementation, and generate 25 datasets of four-dimensional features for each individual node, which only 20% of them is chosen for network testing and the rest of them is used in learning process. The environmental condition in the first evaluation is set to Type equation here.Eb/N0=10, where Eb is the signal energy associated with each user data bit, and N0 is the noise spectral density. Fig. 5 shows the effect of tree count and the selected depth for random forest algorithm on identification accuracy. It is concluded from Fig. 5 that as the number of trees and their depths are increased for a forest, the identification accuracy will increase as well. Note that the accuracy will abruptly increase for a depth within 5 to 20, while this increase is nearly saturated for depth larger than 20. On the other hand, the change in the number of trees of forest has a small impact on identification accuracy. More analysis on Fig. 5 reveals that the accuracy of 100% can be achieved for our network in the case of depth larger than 20 and tree count equal

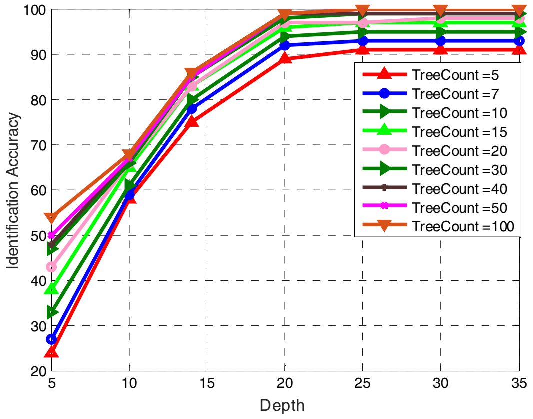

Fig. 5. Identification accuracy versus the number of trees and their depths

to 100. However, this high accuracy comes at the cost of higher design complexity and overhead of classifier module at the receiver side. One can use any of the networks to trade-off between the accuracy and the design complexity. As the accuracy has less sensitivity for depth larger than 20, one of the best candidates in our case in both accuracy and design complexity terms is tree depth of 20 and the tree count of 15, by which the identification accuracy of about 96 % can be reached.

To further analyze, the identification accuracy versus different number of transmitters is shown in Fig. 6. It is evident from Fig. 6 that the more the network grows, the lower accuracy reaches in classification since the matching process gets difficult as the number of choices increases. Moreover, for a forest with high large number of tree and depth, the network growth less affects the accuracy. Results of Fig. 6 signify that the prior choice of forest parameters (i.e., #tree=15, depth=20) almost leads to a sufficient accuracy even for the higher number of transmitters, as the accuracy of blue line in Fig. 6 is almost unchanged (≈96%) when the network constantly grows.

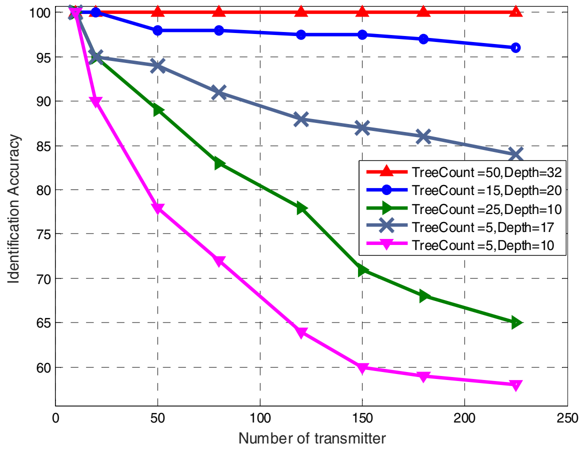

Fig. 6. Identification accuracy versus number of transmitters

One of the fundamental parameters that should be considered and properly adjusted in design time is the number of datasets of features that are used to build a forest. Fig. 7 shows the effect of the number of four-dimensional datasets on the identification accuracy in a network with 20 nodes. As the number of datasets for constructing a forest increases, so does the number of correct identity matching, leading to a substantially increase in identification accuracy. It should be mentioned that the larger datasets, on the other hand, will severely impact both the collecting and processing times of features in a network. There is not much concern about the latter term in Random Forest algorithm as it perfectly handles larger datasets, but the larger datasets of features take quite a while to be extracted and collected in RF-PUF framework. Therefore, it is important to adjust this parameter properly in proportion to the design time so that a rough estimation of initial time of data collection can be measured. It is clear from Fig. 7 that for six datasets of features the accuracy reaches to more than 90% for all cases, and for datasets larger than 14, the accuracy will be 100%. However, the calculated accuracy in this evaluation not only depends on datasets statistic, but also on the environmental conditions (i.e., channel distortion and noise), which in general degrade the accuracy of identification. Thus, it is better to generate datasets more than the required corresponding accuracy in Fig. 7 so as to compensate the channel distortion. In this case, we select 20 four-dimensional datasets for 20 wireless nodes. As mentioned above the environmental conditions and channel distortion can severely affect the identification accuracy. We demonstrate this effect in Fig. 8 which shows the accuracy variations for different forest and channel characteristics. It is apparent from Fig. 8 that the presence of channel distortion has a minor effect (less than 5%) on accuracy degradation, and for different channel conditions the accuracy is still higher than 90 % for 225 wireless nodes. This result is mainly because of the fact that in Random Forest classifier any missing values likely caused by the environmental noise or malicious modification on data can be effectively handle so it can accurately predict even when some of the input values were missing.

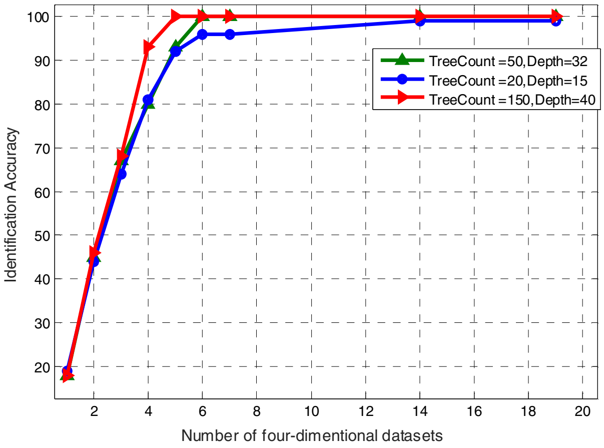

Fig. 7. The effect of number of datasets on identification accuracy

In the next analysis, the total runtime required for preparing and testing the network has been presented as illustrated in Fig. 9. The results of Fig. 9 imply that the required runtime of a network with different forest characteristic and network size in Random Forest algorithm is much less than that of the other neural networks. In final analysis, we investigate the False Positive Rate (FPR), which defines the percentage of malicious nodes that are wrongly identified as the authorized identity. For doing so, different attack scenarios are considered by randomly injecting malicious nodes in network with different number of nodes, then the number of cases that the receiver wrongly identifies a malicious node as an authorized node is calculated as false positive count, as listed in Table I. From the above results, as the network size grows, the FPR decreases so that the proposed framework yields averagely 2% in FPR for different attack scenarios.

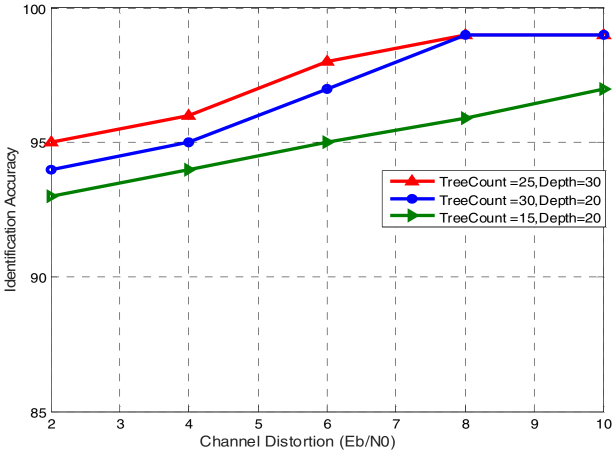

Fig. 8. The effect of channel distortion ($\boldsymbol{E_b/N_0}$) on identification accuracy

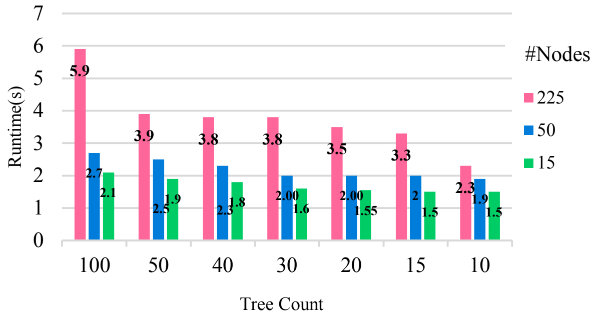

Fig. 9. Runtime required for preparing and testing of a network

The main problem of the exiting authentication based on the inherent properties of the network is its sensitivity to aging effect. However, as Figs. 7 and 9 show, the learning time for preparing the proposed framework is less than 6 seconds and a favorable accuracy can also be reached even with the less amount of data. So, the proposed network can be suspended for a short time of operation to retune the coefficient of the network for mitigating the aging effect. This retuning process is not applicable for the similar method due to its long preparation time. Another interesting feature of the proposed framework is its robustness against replay attacks. The reason behind this claim is that the proposed authentication framework mainly depends upon the transmitter's characteristics which cannot be replicated and modeled even with the advanced equipment. Moreover, the proposed framework leverages the channel properties for the authentication purpose which is hardened the replication process as well.

Table I. False Positive Rate of the proposed authentication framework

# Malicious nodes	# Nodes	# False Positive	FPR (%)
100	50	3	3%
	100	2	2%
	150	1	1%
200	50	7	3.5%
	100	4	2%
	150	2	1%
300	50	10	3.3%
	100	6	2%
	150	3	1%
400	50	13	3.25%
	100	9	2.25%
	150	6	1.5%
Average			2%

V. Conclusion

In this paper, a new RF-PUF based authentication framework was proposed for IoT applications by exploiting the unique and device-dependent features which are extracted from already-existing modules embedded in the receiver side, and leveraging the Random Forest classification for securely identifying the sender nodes. On the basis of implementation results the following conclusions can be drawn: 1) the Random Forest classifier incurs lower design complexity and requires less preparatory work and parameters to be adjusted, as opposed to the neural networks so that the overall runtime required to prepare and test of network is around 6 second, on average. 2) The identification accuracy can be reached to 100% in the proposed framework within a forest with 100 trees and depth of 25, at the expense of minor design overheads imposed to the receiver. 3) The channel distortion has a negligible impact on identification accuracy for the proposed classifier by less than 5%, where the accuracy lessens to 90% in the worst case.

References

[1] A. Shabani and B. Alizadeh, “PMTP: A MAX-SAT Based Approach to Detect Hardware Trojan Using Propagation of Maximum Transition Probability,” *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, 2019.

[2] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, “Silicon physical random functions,” in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 148–160.

[3] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *2007 44th ACM/IEEE Design Automation Conference*, 2007, pp. 9–14.

[4] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, “Reliable and Modeling Attack Resistant Authentication of Arbiter PUF in FPGA Implementation With Trinary Quadruple Response,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 1109–1123, 2019.

[5] J. Delvaux, “Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF--FSMs,” *IEEE Trans. Inf. Forensics Secur.*, 2019.

[6] L. Kusters and F. M. J. Willems, “Secret-Key Capacity Regions for Multiple Enrollments with an SRAM-PUF,” *IEEE Trans. Inf. Forensics Secur.*, 2019.

[7] K. J. Ellis and N. Serinken, “Characteristics of radio transmitter fingerprints,” *Radio Sci.*, vol. 36, no. 4, pp. 585–597, 2001.

[8] F. Xie *et al.*, “Optimized coherent integration-based radio frequency fingerprinting in Internet of Things,” *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3967–3977, 2018.

[9] M. Barbeau, J. Hall, and E. Kranakis, “Detection of rogue devices in bluetooth networks using radio frequency fingerprinting,” in *proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN*, 2006, pp. 4–6.

[10] O. Ureten and N. Serinken, “Wireless security through RF fingerprinting,” *Can. J. Electr. Comput. Eng.*, vol. 32, no. 1, pp. 27–33, 2007.

[11] J. Hall, M. Barbeau, and E. Kranakis, “Detection of transient in radio frequency fingerprinting using signal phase,” *Wirel. Opt. Commun.*, pp. 13–18, 2003.

[12] 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. Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, 2018.

[13] B. Chatterjee, D. Das, and S. Sen, “RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning,” in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2018, pp. 205–208.

[14] B. Chatterjee, D. Das, S. Maity, and S. Sen, “RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-situ Machine Learning,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, 2019.

[15] M. Alrowaily and Z. Lu, “Secure Edge Computing in IoT Systems: Review and Case Studies,” in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, 2018, pp. 440–444.

[16] A. F. Molisch *et al.*, “IEEE 802.15. 4a channel model-final report,” *IEEE P802*, vol. 15, no. 04, p. 662, 2004.