Physical Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY 4.0

SUBMISSION DATE / POSTED DATE

09-08-2021 / 13-08-2021

CITATION

Khadka, Grishma; Ray, Biplob; Choi, Jinho; Karmakar, Nemai (2021): Physical Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications. TechRxiv. Preprint.
<https://doi.org/10.36227/techrxiv.15138711.v1>

DOI

[10.36227/techrxiv.15138711.v1](https://doi.org/10.36227/techrxiv.15138711.v1)

Physical Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications

Grishma Khadka, *Member, IEEE*, Biplob Ray, *Member, IEEE*,
Jinho Choi, *Senior Member, IEEE*, and Nemai Chandra Karmakar, *Senior Member, IEEE*

Abstract—This paper has proposed detection and physical layer security provision for printed sensory tag systems for internet of things (IoT) applications. The printed sensory tags can be a very cost-effective way to speed up the proliferation of the intelligent world of IoT. The printed Radio Frequency Identification (RFID) of a sensory tag is chipless with the fully printable feature, non-line-of-sight reading, low cost, and robustness to the environment. The detection and adoption of security features for such tags in a robust environment are still challenging. This paper initially presents a robust technology for detecting tags using both the amplitude and phase information of the frequency signature. After successfully identifying tag IDs, the paper presents novel physical layer security using a deep learning model to prevent the cloning of tags. Our experiment shows that the proposed system can detect and identify the unique physical attributes of the tag and isolate the clone tag from the genuine tag. It is believed that such real-time and precise detection and security features bring this technology closer to commercialisation for IoT applications.

Index Terms—Backscatter Communication, Chipless RFID System, physical security, Deep Learning, Long short term memory (LSTM)

I. INTRODUCTION

THE importance of the chipless tags system for low-cost item tagging is growing due to its various important features compared to the chipped tag system and Barcodes. Most of the current research on printed chipless tags are focusing mainly on tag and reader technology developments [1]. However, it is still challenging to detect and protect authentication of a chipless tag within the reader interrogation zone in a cluttered environment.

During the detection, the backscattered interfering signal from static and moving objects along with the interference waves from nearby radio degrades the quality of the tag signal information [2]. The main difficulties lie in the identification of electromagnetic (EM) response of the chipless tag, which is severely affected by conductivity, permittivity, and permeability of the material [3] where the tag is attached. A low

permittivity item has a high speed of signal propagation [4] in comparison to an item with high permittivity. The high permittivity items result in a noticeable fading of the microwave signal [5] which affects the performance of the backscattered signal of the tag and would be a source of amplitude variation, bandwidth broadening, and shifting of the resonant frequency. Variations in the amplitude level of the tag response cause the misreading of the tag information. Also, the bandwidth broadening and frequency shifting overlap the resonant frequency with the nearby resonances, affecting the detection of the tag ID [6]. Various tag detection techniques have been developed to overcome the detection issue in the chipless RFID domain. However, most techniques face limitations to decode the tag signature due to the non-stationary behaviour of the signal.

Physical layer security is also essential beside detection, to advance chipless RFID tag for IoT application. The tags need to ensure their authenticity by protecting them from cloning and counterfeit. For a more sensitive system with high-security requirements, the tag information, during transmission and at rest, needs to be protected from malicious use such as tempering and reply attack. A malicious adversary may try to control and mislead the entire communication system to an unsafe state [7] by tempering transmitted signals or inserting malicious signals, or introducing a counterfeit tag with malicious code [8] in the system. For example, in supply chain or retail, an unauthorised eavesdropper may attempt to obtain the information of different tagged shopping items, which includes product ID and price without the concern of the item holders [9] [10]. In literature, studies focused on the security of the chipped, tagged system with very few attempts to address the need for printed chipless tags IoT system's security. For a practical security solution of chipless RFID tags, it is essential to consider innovative and lightweight security mechanisms [11] by exploring and leveraging existing features of the system so that it will be feasible and easily adaptable in the industry. In IoT enabled retail marketplace, cloning or counterfeit of a tag may lead to various security violations such as losing ownership of the object, privacy invasion and counterfeiting of expensive products. Therefore, it is essential to identify and isolate cloned or counterfeit smart objects from original objects immediately to prevent further damage.

This paper has looked into designing and developing physical layer detection and security techniques for identifying clone and counterfeit tagged objects in IoT systems. Initially,

Grishma Khadka and Jinho Choi is currently with the School of Information Technology, Deakin University, Burwood, VIC 3125, Australia (e-mail: g.khadka@deakin.edu.au; jinho.choi@deakin.edu.au).

Corresponding author: Grishma Khadka.

Biplob Ray is with the School of Engineering and Technology, CQ University, Melbourne VIC 3000 (e-mail: b.ray@cqu.edu.au).

Nemai Karmakar is with the Department of Electrical and Computer System Engineering, Monash University, Clayton, VIC, 3800, Australia (e-mail: nemai.karmakar@monash.edu.au).

the paper proposed a detection technique to detect the chipless RFID tag IDs, which then used a machine learning model to identify an original, clone or counterfeit tags. More importantly, there is no requirement of a hardware modification to implement the proposed techniques in printed tags based IoT systems. The contributions of this study are as follows.

- A novel tag detection technique that avoids false detection in a cluttered environment.
- A clone or counterfeit tag identification using a machine learning model.
- Verification and validation of the detection technique and machine learning model.

The organisation of this paper is as follows. Section II present the background and related work in the development of physical layer tag detection and security. The details of the IoT system model is presented in section III. Section IV and V present the proposed detection technique followed by the physical security model. Discussion and Comparative Study is presented in Section VI. Finally, Section VII concludes the study.

II. BACKGROUND AND RELATED WORKS

The remarkable progress in microelectronics and semiconductor technologies have moved the conventional chipped RFID technology into mainstream application. It is a contactless, non-line-of-sight(NLoS) wireless communication technology that uses radio frequency (RF) waves to read electronics tags from a distance and reduce the human intervention interaction and manual scanning of tagged items [12]. Although, conventional chipped RFID tags have moved into mainstream applications. The design and assembling of the application-specific integrated circuits (ASIC) increase the fabrication cost in an integrated circuit (IC)-based tag. Due to the bulky structure of the tag, the printing of the tag on commercial paper or polymer substrate is impossible. Also, the IC-based tag cannot withstand the cold temperature below zero and a high temperature above 40°C [13].

The recent development of the sensory tag (chipless RFID tag) opens up new possibilities to tackle these issues [14], [15]. A chipless RFID consists of passive resonators on a single-layer structure [16] without a silicon chip. Each resonator of a chipless tag forms a peak or null in the frequency response of the tag based on its property. The absence of a silicon chip significantly reduces the implementation cost in comparison to the chipped tag. Besides being fully printable, it is a favourable solution to overcome the limitation of chipped tags for next-generation RFID technology. Due to the growing interest in an RFID system, various detection techniques and security model has been proposed for the chipless tags. The following section provides a brief discussion of recent works on detection techniques and security models.

A. Related works on detection technique

In the past various chipless RFID tag detection techniques have been developed to overcome the challenges as mentioned above in section I. However, most of the techniques face limitations to decode the tag signature due to the variations

in the amplitude level and shifting of frequency [6]. For example, Short Time Fourier Transform (STFT) [17] needs a more extended window width to obtain a good frequency resolution. Optimisation between frequency and time causes frequency shift, which results in missing bits for high data capacity tags within limited bandwidth [18]. Wavelet-based technique [6] that uses the mother wavelet and confident band for detection does not meet the non-stationary behaviour of the signal and is challenging to adapt for high data capacity tag. The threshold-based detection technique [19] detects the tag signature by comparing the magnitude of tag response against a fixed threshold level which shows minimal flexibility in tag detection in the presence of noise, clutter, and interference. Likewise, the moving average filtering technique [20], which uses a fixed threshold level, faces a similar challenge. The signal space representation (SSR) technique [21] finds the minimum distance between the received frequency signature points with other fixed points. Moreover, the techniques mentioned above are difficult to implement to analyse the tag information in real IoT applications.

B. Related works on physical layer security

Due to the growing interest in the RFID system, various security protocols based on software and hardware have been proposed for the conventional chipped RFID to prevent cloning and counterfeiting of the RFID tags. The work in [22] use an electronic fingerprint of a tag based on the minimum power response at multiple frequencies. [23] proposed a BASE, DeClone, and DeClone+ protocols suitable for faster deterministic clone detection for small to large anonymous RFID systems. The authors in [24] study the cloning detection of passive UHF RFID tags. The literature shows numerous research on physical layer security for chipped RFID tags, using physical layer fingerprinting [25] [22] and physically unclonable function [26] [27] to prevent cloning, but are limited and not applicable for chipless RFID tags.

The author in [28] presented the unclonable chipless RFID tag (UCR) and analysed its system to the potential attacks. Its results show the uniqueness and unclonable identifier of the proposed UCR tags. The paper in [29] proposed the authentication of chipless tags by using natural randomness to generate a unique electromagnetic signature in the RF field for authentication during the fabrication process. The main limitation lies during the fabrication process, as the design values of the tag shift with the change in slot parameter. It results in the variation of trace width, air gap, substrate thickness and material dielectric of each resonator, making it difficult to prevent an attack. The different authentication technique in [30] [31] [32] [33] have a limitation in terms of 3D structures, printing and imaging procedure as discussed in [29].

III. SYSTEM MODEL

The paper has used an IoT network model, illustrated in Fig. 1 designed for the detection of smart objects tagged using chipless tags. The network model in Fig. 1 has a master reader with Low-Power Wide Area Network (LPWAN). The master

Fig. 1. IoT network model for smart objects

reader communicates to the backend system in the cloud using wireless, like Wi-Fi, or wired backhaul communication. As illustrated in Fig. 1, the master reader communicates to client readers to collect information of tagged smart objects. The client readers have both LPWAN and ultra-wideband communication modules to work as an intermediary between the master reader and smart objects. The client reader also stores the client module of our physical layer security model to identify a clone or counterfeit smart objects.

Using network model presented in Fig. 1, the system model in Fig. 2, smart shop, is designed. The shop has tagged smart objects for sale as presented in Fig. 2. In addition to individual tags to identify smart objects, some of these tags are networked [34] or grouped [35] to represent grouped objects to the system. The smart shop in Fig. 2 has an auto checkout that identifies the customer in the system by reading membership card using IoT enabled master reader. The client reader captures the backscatter chipless RFID tag signal attached to the item. It then processes the signal in real-time using the appropriate detection algorithm and sends the product information to the master reader. The client readers are responsible for identifying all the objects placed in the shopping cart during checkout.

Fig. 2. System model used in the experiment - Smart shop

As illustrated in Fig. 2, an attacker may use secretly clone/counterfeit an expensive items tag to evade paying the item as the system knows that a specific item or group of items are already sold. It can create various dispute scenarios; for example, the attacker pretends to be the customer's representative and return the item to get a refund. Furthermore, large scale tag cloning can also be used to jam the entire system by confusing client readers.

For the practical implementation of the chipless RFID system for smart shopping, we need to consider developing the proper detection technique and security model. Thus, this paper presents the detection technique to collect backscatter tag signal information and a security model to identify tag authenticity to increase usability and system performance.

IV. DETECTION TECHNIQUE FOR CHIPLESS RFID TAG

In this section, the paper proposed detection steps in detecting tag data bits from a high level of noise and interference [36]. The proposed technique is based on the analysis of both amplitude and phase spectral to separate the tag IDs from environment reflection even the tag radar cross section (RCS) undergo a change in amplitude variation and frequency shifting. The different steps of the proposed technique are explained as follows:

A. Reader Setting and Background Subtraction

Initially, the reader [37] was configured for reading the tag placed in front of it. The tag was illuminated with the reader operating within the frequency range of 3.3-10 GHz by transmitting radio signal at different frequencies to the passive chipless tag using its array of antenna elements [38]. The transmitted signal excites the resonant elements encoded within the chipless tag and starts resonating within their predefined frequency. The exciting signal is re-radiated as a backscattered signal to the reader. This signal consists of both the desired tag signature as well as unwanted signal components in the form of interference and noise [39]. The received signal by the reader is defined by

$$r(t) = \sum_{m=1}^M A_m \cos(2\pi f_m(t-\tau) + \frac{k(t-\tau)^2}{2} + \phi_m) + n(t) \quad (1)$$

where m is the number of the reflected signal from the tag RCS and echoes from static and moving objects. A_m , ϕ and τ are the amplitude, phase and time delay of the reflected signal, and k , $n(t)$ are the slopes of the frequency domain signal and the additive white Gaussian random noise. The round trip time t_1 is the time excitation signal travels from the transmitting antenna to the stationary chipless tag plus the time backscattered signal travels from the chipless tag to the receiving antenna, t_1 is denoted as:

$$t_1 = 2r/c \quad (2)$$

where r is the distance between the chipless RFID tag and the UWB reader, and c is the speed of the light. The received signal consists of tag signal and interfering signals such as cable loss, the coupling between the antennas, free space path loss,

and echoes from static and moving objects. The background measurement, which is the transmission coefficient between the transmitting and receiving antennas without the presence of a tag, also called as empty-room response [40] is performed to remove the effect of the static noise from the environment. Therefore, to eliminate the static interference components, the measured complex RCS of the tag is subtracted from the measured background response without the presence of tag and divided by the known RCS of the reference object. The calibrated measured tag RCS of the frequency coded tag is given by [41]

$$\sigma_{tag} = \left[\frac{S_{21}^{Tag} - S_{21}^{BG}}{S_{21}^{Ref} - S_{21}^{BG}} \right]^2 \times \sigma_{Ref} \quad (3)$$

where S_{21}^{tag} is the measured RCS of the tag, S_{21}^{Ref} is the known RCS of the reference object, S_{21}^{BG} is the measured background response without the presence of the tag, and σ_{Ref} is the RCS of the reference object. After background subtraction, the second step is to find the power level and selection of antenna pair. The detail is explained in next section.

B. Finding Power Level and Antenna Pair Selection

The power received when the tag is within the interrogation zone of the reader is given by

$$P_r[dB] = P_t[dB] + G_t[dB] + G_r[dB] + 10\log_{10} \frac{G_{tag}^2}{2\pi} \quad (4)$$

$$+ 10\log_{10} \frac{\lambda^2}{4\pi} - 20\log_{10} \frac{\lambda}{4\pi} - 40\log_{10} r$$

where P_t is the transmitter output power level, G_t is the gain of the transmitting antenna, G_r is the gain of the receiving antenna, and σ is the tag RCS. This paper used a reader [37] which consists of $N_{Tx} = 4$ transmitting and $N_{Rx} = 14$ receiving antenna elements. Each of the transmitter out of 4, operates sequentially within the frequency range from 3.3-10 GHz band. If i and j represents the transmitter and receiver index, then the measurement vector at k cycle index for N number of sample per measurement is given by

$$f_{k,i,j} = [f_{k,i,j}(0) f_{k,i,j}(1) f_{k,i,j}(2) \dots f_{k,i,j}(N-1)] \quad (5)$$

Using equation 5, we can form the data matrix of size $56 \times N$ as given by

$$S_k = [f_{k,1,1}; f_{k,1,2}; f_{k,1,3}; \dots f_{k,4,12}; f_{k,4,13}; f_{k,4,14};] \quad (6)$$

However, in this research, a few antenna pairs are selected by setting the elevation angle θ from -60° to 60° and azimuths angle φ from -60° to 60° as the scanned area. It helps to increase the reading speed and avoids the computation complexity of the system while detecting the backscattered tag signal.

C. Detection of Tag IDs

After selecting the antenna pairs, the communication is established between the reader and the tag to extract the backscattered raw signal information. The raw information

consists of both signal magnitude and phase. The signal magnitude has a high dependency on environmental reflection, orientation and geometry of the surface where the tag is attached, resulting in difficulty finding the peak at particular resonance frequency points. Similarly, the phase of the signal depends on the propagation channel and modulating properties of the tag. Thus, to increase the reliability of the detection technique, instead of using only amplitude or phase information, we exploit both information of the received signal for optimum detection efficiency of the tag data. In the frequency domain, the transfer function response $H(f)$ of the chipless tag amplitude A and phase ϕ for M number of resonators resonating at different frequencies is defined [42] as

$$A(f) = \prod_{m=1}^M |H_n(f)| \quad (7)$$

and

$$\phi(f) = \sum_{m=1}^M \angle H_n(f) \quad (8)$$

The validation of the detection technique with experiment is discussed in section IV-D.

D. Performance Analysis of the detection technique

Fig. 3. Illustration of RFID system using transceiver and chipless tag.

In this section, we analyse the detection of the chipless RFID tag ID in a real environment. For the experiment, as shown in Fig. 3, orientation insensitive circular patch resonators tags and an ultra-wideband (UWB) reader are selected. The encoding of the tag data is based on the resonant elements [43] resonating at different frequency points. The presence of a peak resembles logic '1', whereas its absence resembles logic '0' for frequency-domain based chipless tags. The reader used in the experiment operates over a frequency range of 3.3-10 GHz with a predefined number of antenna pairs for reading the raw signal information of the chipless tag. Multiple reading is recorded to calculate the detection throughput rate of the proposed technique. The throughput is defined as

$$Throughput = \frac{N_{s-r}}{N_{t-r}} \quad (9)$$

where N_{s-r} is the number of successful readings of the tag and N_{t-r} is the total number of readings during each measurement.

Fig. 4 shows the 4-bit tag backscatter signal response when placed within the reader interrogation zone. The response in Fig. 4 (i) and (ii) show the distinct peaks which frequently occur at particular frequency points in both amplitude and phase response. Similarly, Fig. 4 (iii) and (iv) shows the more clear response in normalised amplitude and phase response which justify the detection of tag IDs information. The individual analysis of tag response in multiple readings demonstrates the throughput of 99% for a chipless RFID tag.

Fig. 4. Measured single response using proposed technique. A single response is selected randomly out of multiple reading. (i) Measured amplitude response. (ii) Measured phase response. (iii) Measured normalized amplitude response. (iv) Measured normalized phase response.

Fig. 5. Measured single response using proposed technique when chipless tag is attached to items with low permittivity, highly conductive and high permittivity items. A single response is selected randomly out of multiple readings. (a) Measured amplitude response. (b) Measured phase response. (c) Measured normalized amplitude response. (d) Measured normalized phase response.

The experiment is further extended when the tag is attached to items with different permittivity and conductivity. The EM response of the items with different permittivity can be stronger and much bigger than the tag response, which affects the backscatter tag signal [44]. To mitigate this problem and validate our proposed technique's effectiveness, we select a 4-

bit one-quarter ring chipless tag with good co-polar and cross-polar response. Fig 5 shows the tag response when attached to low and highly scattering items (high permittivity item) and items with metallic structure with higher conductivity. Fig. 5 (i) and (ii) shows the amplitude and phase response along with normalized amplitude and phase response in Fig. 5 (iii) and (iv). The overall results show that the detection technique can reduce the interfering signals when the chipless tag attached to different smart items. The proposed algorithm easily compensate the loss of information in amplitude response by phase response or vice-versa.

The comparisons of the result using the proposed technique with the existing techniques are shown in TABLE II. From TABLE II we observed that the existing techniques such as Maximum Likelihood (ML) and signal Space Representation technique (SSR) need higher computation capacity with increased computation time in comparison to proposed technique. The proposed technique is computationally feasible and show a better reading performance with computation time of 35 ms. The previous reported works perform the post-processing of data after reading the tag response from the vector network analyser (VNA). The post-processing (PP) of tag signal by the use of expensive device such as VNA is replaced by using the low cost UWB reader for real-time processing (RTP) in practical application. Furthermore, our technique shows reliable detection of tag signatures even when the tag is attached to highly scattering objects, whereas the analysis of previous techniques with tagged item is not available in the literature. The proposed technique meets the goal in developing a low-cost intelligent system model demonstrated in Fig. 2.

V. PHYSICAL SECURITY MODEL

This section details the attack model of chipless tags that underpin our proposed physical security model.

A. Attack Model

Fig. 6 illustrates a clone attack using one client reader over a communication link of a chipless RFID system of the smart shop model in Fig. 2.

Fig. 6. Attack Model used in this paper

TABLE I
COMPARISON OF PROPOSED DETECTION TECHNIQUE WITH OTHER TECHNIQUES

Ref.	Detection Technique	Number of bits	Tag attached to	Reading accuracy	Computational complexity	Reader, cost and processing
[19]	Threshold	4-bit	N/A	50%	Low	VNA, expensive, PP
[6]	Wavelet	4-bit	N/A	90%	Medium,	VNA, expensive, PP
[21]	SSR	3-bit	N/A	90-95%	High	VNA, expensive, PP
[45]	ML	4-bit	N/A	90-99%	High	VNA, expensive, PP
This Paper	Proposed Technique	4-bit	highly scattering items	99%	Low	Walabot, <500 USD, RTP

PP = Post Processing (processing after data captured from VNA) and RTP = Real Time Processing of chipless RFID tag data

The attacker has physically cloned tag T_2 as tag T_2^c and presented it closer to the client reader R_1 for a stronger signal to pose as a genuine owner of the smart object associated with the T_2 . Current readers will read the cloned tag T_2^c as a real tag if the cloned tag has a stronger signal or closer to the reader itself [46]. A client reader must be able to identify genuine and clone tag before passing the signal to the backend via master reader as the clone tag may insert malicious signal to compromise the security of the entire smart shop system [8], [34]. For bulk or expensive objects, the smart shop needs assurance of non-repudiation, which may play a key role in dispute resolution [47].

The preliminary analysis of the attack model is performed based on two physically different tags with the same number of bits. The hypothesis of this experiment is to observe the tag signature when the attacker tries to clone the tag to produce the duplicate tag physically. Two tags with similar binary logic bits 1111 but physically different tags represented by T_2 and T_2^c are selected for the experiment. The third tag has binary logic bits 1101, which is represented as T_1 as illustrated in Fig. 6.

We have recorded physical layer signal characteristics: amplitude and phase, from 4 to 6 GHz frequency range during the execution of novel detection technique developed and discussed in Section IV for the attack model illustrated in Fig. 6. Our analysis of the physical layer is illustrated in 2D and 3D planes in Fig. 7 and Fig. 8 respectively, where we choose amplitude response of the backscatter signal for further analysis due to its challenging behaviour in detecting tag IDs as discussed in [6].

Fig. 7 has plotted amplitude of three different 4-bit tag responses against the 4 to 6 GHz frequency range. It is clear from Fig. 7, each tag has its unique feature set from 4 to 4.4 GHz frequency range and from 5.6 to 6 GHz frequency range but amplitudes of T_2 and T_2^c are travelling closely compare to T_1 . However, during transmission of tag's ID in 4.6 to 5.5 GHz frequency range, T_2 and T_2^c has significantly distinguished patterns from separating them from each other. In Fig. 8, we have plotted the amplitude of the tags in 3D plain against frequency and time to see the state of distinguished patterns over time to identify clone tags. As we can see from the illustration in Fig. 8, the variation in amplitude level and shifting of frequency positions over time shows the existence

of distinguished patterns of clone tags T_2^c . From the security perspective, the results show some initial efforts in identifying the falsified tag based on contextual changes of tag reading distance, object it attached, and duration of its existence in the system.

Fig. 7. Measured result of physically different multiple 4-bit tags with tag ID: 1111 and 1101.

A well-planned cloning attack by a group of organised attacked may make the master reader busy using many false interrogations while fooling the client readers for financial gain. Therefore, in this paper, we have proposed a physical layer security model which is lightweight to be resident in client reader to identify a clone or counterfeit tag in real-time. The model also aims to eliminate the possibility of Denial of Service (DoS), signal jamming and malware injection using cloned/counterfeit tags.

B. Physical Security model using Deep Learning

1) *Methodology*: In this study, we adopt the Long short-term memory (LSTM) deep learning technique, a specific type of recurrent neural network (RNN) which was initially designed to capture long-term dependencies [48] [49]. It is widely used in different emerging applications of radio frequency (RF) sensing due to its capability to maintain information in memory for longer periods and outperforms RNN for long dependencies [50]. It solves the problem of vanishing and exploding gradient problems by introducing the gates to control the flow of data [49].

Fig. 8. Measured results of two 4-bit tag of 1111.

Fig. 9. LSTM internal working mechanism

There are four control gates in LSTM: forget (f), cell candidate (g), input (i), and output (o). Fig 9 depicts the general architecture of a LSTM blocks [51]. The working mechanisms of each control gates is mathematically expressed as in equations 10-13 in each time stamp t .

$$i_t = \rho_g(W_i I_t + R_i O_{t-1} + b_i) \quad (10)$$

$$f_t = \rho_g(W_f I_t + R_f O_{t-1} + b_f) \quad (11)$$

$$g_t = \rho_g(W_g I_t + R_g O_{t-1} + b_g) \quad (12)$$

$$O_t = \rho_g(W_o I_t + R_o O_{t-1} + b_o) \quad (13)$$

where ρ_g denotes the gate activation function. W , R , and b are the learnable (adaptable) input weight, the recurrent weights, and the bias. It formed the matrices which are concatenations of the input weights, the recurrent weights, and the bias of each component, respectively. Based on a loss functions these learnable weights are updated at each time step.

The cell and hidden state at timestamp t are expressed by

$$c_t = f_t \odot c_{t-1} + i_t \odot g_t \quad (14)$$

$$h_t = O_t \odot \rho_c(c_t) \quad (15)$$

where $\odot$ denotes the element-wise multiplication of vectors and ρ_c denotes the activation function. However, in MATLAB software, the lstmLayer function uses the hyperbolic tangent function $\tanh$ to compute the state activation function.

2) *Modeling Approach*: For this analysis, a sequence of amplitude and phase information of individual time steps is fed into the LSTM network, obtained at different frequency points. The model is trained within the frequency range between 4-6 GHz, based on the available chipless RFID tag discussed in section III. The input dataset contains the tag information at every frequency interval of 0.025, corresponding to 81 input features within the 2 GHz frequency range. The equation 16 represent the total data collection time t_T with 81 input feature I_f , and two output class O_{class} for real (1) and clone (0) tags.

$$I_f | O_{class} = \begin{bmatrix} I_{f_1 t_1} & I_{f_2 t_1} & \dots & I_{f_{81} t_1} \\ I_{f_1 t_2} & I_{f_2 t_2} & \dots & I_{f_{81} t_2} \\ \dots & \dots & \dots & \dots \\ I_{f_1 t_N} & I_{f_2 t_N} & \dots & I_{f_{81} t_N} \end{bmatrix} \begin{bmatrix} O_1 \\ O_0 \\ \dots \\ O_1 \end{bmatrix} \quad (16)$$

The LSTM network architecture, which is feed with real and clone tag information with 81 input features and two output classes, is defined using one Bidirectional LSTM layer with 100 hidden units to learn the full sequence at each time step. The LSTM network is designed with MiniBatchSize 27 using the 'adam' optimiser algorithm to classify the network either clone or real tag, O_{class} output. The training and test data sets are sorted by sequence length by specifying the sequence length to be 'longest' and mini-batch size to 27. The configuration model [51] of LSTM framework is shown in Fig. 10.

Fig. 10. LSTM deep learning network model

3) *Results*: This section provides a comparative analysis based on the accuracy and loss of the LSTM classification model to identify the real and clone tag. For analysis, the real and clone tag data sets were obtained under two different scenarios: (i) backscatter tag signal obtained after adding additive interference's, (ii) the backscatter tag signal without additive interference in a real time environment. Thus, obtained data sets are splits into training and testing groups. 70% of the dataset are within the training group to optimise the model, and the rest 30% dataset from the whole sequence is used for testing. The performance accuracy of LSTM model with and without additive interference are shown in Fig. 11 and 12 respectively. It shows a higher accuracy of 92.33% with interference and 95.5% without interference for classifying the real and clone tag. Similarly, the model loss of 0.242 is obtained with interference and 0.1512 without interference which is shown in Figs. 13 and 14. Results showed high

accuracy in classifying clone tags from the actual legitimate RFID tag.

Fig. 11. Model accuracy with additive interference using LSTM.

Fig. 12. Model accuracy without additive using LSTM

Fig. 13. Model loss with additive interference using LSTM.

VI. DISCUSSION AND COMPARATIVE STUDY

Table II presents four performance parameters with three-fold cross-validation for the proposed model detailed in sub-

Fig. 14. Model loss without additive interference using LSTM.

section V-B. The three cross validation in Table II is done for two datasets by varying training and testing ratios. For accuracy, the standard deviation value between cross validation results is $\sigma = \pm 0.00140119$ using dataset without interference whereas $\sigma = \pm 0.001634$ with interference. Therefore, the cross-validation variation is minimal in our model between two data sets, with interference and without interference, the accuracy standard deviation is $\sigma = \pm 0.018323$ which is low but higher than the variation within the dataset.

The other three performance parameters, Room Mean Squire Error (RMSE), Room normalised Mean Squire Error (nRMSE) and Mean Absolute Percent Error (MAPE), show similar variation trend of cross-validation result in Table II. While RMSE and nRMSE show errors on the model, the MAPE is a widely used index to determine the forecast accuracy with respect of scale-independency and interpretability. Based on the MAPE value in Table II, we can say the proposed model has a slight error and high scale-independency and interpretability for further adaptation.

The paper has executed the same experiment using several traditional models to compare with our proposed model as illustrated in Fig. 15. Fig. 15 shows Receiver Operating Characteristic (ROC) curve by plotting the True Positive Rate (TPR) in Y-axis against the False Positive Rate (FPR) in X-axis at various threshold settings. It is evident from Fig. 15 that the proposed model using LSTM outperformed other closely performing models, Neural Network (NN) and Support Vector Machine (SVM), by providing the least FPR. As we can see, the proposed model with LSTM has 93.65% accuracy (F_1 score), which is higher than traditional (statistical and machine learning) algorithms. Therefore, the proposed model has high TPR with great scalability and interpretability to detect clone tags in our system model. As the accuracy of the proposed model is higher, the RMSE, nRMSE and MAPE parameters of the traditional (statistical and machine learning) algorithms become irrelevant and unnecessary to compare with our proposed model.

TABLE II
CROSS VALIDATION OF DATASET WITH AND WITHOUT THE PRESENCE OF ADDITIVE INTERFERENCE.

Dataset	Training Data	Accuracy	MSE	PSNR	RMSE	MAPE
Without Additive Interference	90%	0.9518	0.0482	61.3024	0.2195	4.6814
	80%	0.9546	0.0454	61.5594	0.2131	4.0659
	70%	0.9531	0.0469	61.4209	0.2165	4.1340
With Additive Interference	90%	0.9218	0.0782	59.2013	0.2796	7.7514
	80%	0.9199	0.0801	59.0956	0.2830	7.7780
	70%	0.9178	0.0822	58.9841	0.2866	7.8055

MSE: Mean Squared Error; PSNR: Peak signal-to-noise ratio;
RMSE: Root-mean-square error; MAPE: Mean Absolute Percentage Error

Fig. 15. Receiver operating characteristics (ROC) curve for different classification model using the data sets.

VII. CONCLUSION

This paper demonstrates a novel approach to collect backscatter data from a low-cost passive chipless RFID tag. It introduces a novel detection technique to identify the tag IDs and a deep learning model to capture clone or counterfeit tags in commercial applications. Initially, the performance analysis and validation of the proposed detection technique are investigated by measuring the response from the chipless RFID tag placed within a handheld reader. The proposed method showed a throughput of 99%, a positive and convincing outcome which indicates that the proposed technique can be a low-cost solution to address the detection issues. The paper also presents a physical layer security model to develop a systematic and cost-effective approach for different IoT applications such as retail and supply chain management. Using a deep learning-based security model provides a high accuracy above 93%, isolating the clone tag from the legitimate RFID tag even in the presence of additive interference in real-time.

The outcomes of this research open up new possibilities in developing coordinated backscatter communication techniques for cost-effective IoT connectivity using multiple chipless

RFID tags and readers. In the future, we intend to develop a novel approach of detection and security model for a large number of chipless tags and mobile readers to support future IoT applications.

REFERENCES

- [1] C. Herrojo, F. Paredes, J. Mata-Contreras, and F. Martín, "Chipless-rfid: A review and recent developments," *Sensors*, vol. 19, no. 15, p. 3385, 2019.
- [2] M. Forouzandeh and N. Karmakar, "Self-interference cancellation in frequency-domain chipless rfid readers," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 5, pp. 1994–2009, 2019.
- [3] S. Shrestha and N. C. Karmakar, "Analysis of real-world implementation challenges of chipless rfid tag," *IET Microwaves, Antennas & Propagation*, 2019.
- [4] M. T. Sebastian, *Dielectric materials for wireless communication*. Elsevier, 2010.
- [5] G. Hübschen, I. Altpeter, R. Tschuncky, and H.-G. Herrmann, *Materials characterization using Nondestructive Evaluation (NDE) methods*. Woodhead Publishing, 2016.
- [6] G. Khadka, M. A. Bibile, L. M. Arjomandi, and N. Karmakar, "Analysis of artifacts on chipless rfid backscatter tag signals for real world implementation," *IEEE Access*, 2019.
- [7] Y. Lin, B. Ray, D. Jarvis, and J. Wang, "False signal injection attack detection of cyber physical systems by event-triggered distributed filtering over sensor networks," in *Applications and Techniques in Information Security*, L. Batten and G. Li, Eds. Singapore: Springer Singapore, 2016, pp. 142–153.
- [8] B. Ray, S. Huda, and M. U. Chowdhury, "Smart rfid reader protocol for malware detection," in *2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, 2011, pp. 64–69.
- [9] J. Cho, S. Kim, and S. K. Kim, "Hash-based rfid tag mutual authentication scheme with retrieval efficiency," in *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications*, 2011, pp. 324–328.
- [10] P. Jäppinen and H. Hämäläinen, "Enhanced rfid security method with ownership transfer," in *2008 International Conference on Computational Intelligence and Security*, vol. 2, 2008, pp. 382–385.
- [11] V. Sharma, A. Vithalkar, and M. Hashmi, "Lightweight security protocol for chipless rfid in internet of things (iot) applications," in *2018 10th International Conference on Communication Systems Networks (COMSNETS)*, 2018, pp. 468–471.
- [12] L.-S. Huang, J.-Y. Su, and T.-L. Pao, "A context aware smart classroom architecture for smart campuses," *Applied Sciences*, vol. 9, no. 9, p. 1837, 2019.
- [13] Rubayet-E-Azim, "Collision, data recovery and localisation in chipless rfid," Ph.D. dissertation, Monash University, Department of Electrical and Computer System Engineering, 2017. [Online]. Available: https://figshare.com/articles/Collision_Data_Recovery_and_Localisation_in_Chipless_RFID/4669612
- [14] A. Attaran and R. Rashidzadeh, "Chipless radio frequency identification tag for iot applications," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1310–1318, 2016.
- [15] T. Athauda and N. C. Karmakar, "The realisation of chipless rfid resonator for multiple physical parameter sensing," *IEEE Internet of Things Journal*, 2019.
- [16] R. Rezaiesarlak and M. Manteghi, "Radio frequency identification systems," in *Chipless RFID*. Springer, 2015, pp. 1–23.

- [17] Y. Zhang, Z. Guo, W. Wang, S. He, T. Lee, and M. Loew, "A comparison of the wavelet and short-time fourier transforms for doppler spectral analysis," *Medical engineering & physics*, vol. 25, no. 7, pp. 547–557, 2003.
- [18] N. Karmakar, E. Amin, *et al.*, "Short time fourier transform (stft) for collision detection in chipless rfid systems," in *2015 International Symposium on Antennas and Propagation (ISAP)*. IEEE, 2015, pp. 1–4.
- [19] C. Divarathne and N. Karmakar, "An advanced tag detection technique for chipless rfid systems," in *2015 European Microwave Conference (EuMC)*. IEEE, 2015, pp. 251–254.
- [20] R. Koswatta and N. C. Karmakar, "Moving average filtering technique for signal processing in digital section of uwb chipless rfid reader," in *2010 Asia-Pacific Microwave Conference*. IEEE, 2010, pp. 1304–1307.
- [21] P. Kalansuriya, N. Karmakar, and E. Viterbo, "Signal space representation of chipless rfid tag frequency signatures," in *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*. IEEE, 2011, pp. 1–5.
- [22] S. Chinnappa Gounder Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting rfid tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 938–943, 2011.
- [23] K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, "Deterministic detection of cloning attacks for anonymous rfid systems," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1255–1266, 2015.
- [24] D. Zanetti, B. Danev, and S. apkun, "Physical-layer identification of uhf rfid tags," in *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 353–364. [Online]. Available: <https://doi.org/10.1145/1859995.1860035>
- [25] H. P. Romero, K. A. Remley, D. F. Williams, and C.-M. Wang, "Electromagnetic measurements for counterfeit detection of radio frequency identification cards," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 5, pp. 1383–1387, 2009.
- [26] P. Tuyls and L. Batina, "Rfid-tags for anti-counterfeiting," in *Cryptographers' track at the RSA conference*. Springer, 2006, pp. 115–131.
- [27] P. Peng and Y. Zhao, "Anti-cloning and secure rfid mutual authentication protocols," in *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*. IEEE, 2011, pp. 379–384.
- [28] K. Yang, D. Forte, and M. M. Tehranipoor, "Ucr: An unclonable chipless rfid tag," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2016, pp. 7–12.
- [29] Z. Ali, E. Perret, N. Barbot, R. Siragusa, D. Hély, M. Bernier, and F. Garet, "Detection of natural randomness by chipless rfid approach and its application to authentication," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 9, pp. 3867–3881, 2019.
- [30] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. M. Tentzeris, G. R. DeJean, and D. Kirovski, "Rf fingerprinting physical objects for anti-counterfeiting applications," *IEEE Transactions on Microwave Theory and Techniques*, vol. 59, no. 2, pp. 504–514, 2011.
- [31] G. DeJean, V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, and D. Kirovski, "Rfdna: A wireless authentication system on flexible substrates," in *2011 IEEE 61st Electronic Components and Technology Conference (ECTC)*, 2011, pp. 1332–1337.
- [32] Y. Boutant, T. Fournel, and J.-m. Becker, "Method for extracting random signatures from a material element and method for generating a decomposition base to implement the extraction method," Dec. 4 2012, uS Patent 8,325,971.
- [33] D. Christofferson, E. Anderson, J. Geres, and W. Graushar, "Resonator use in the print field," 2009.
- [34] B. Ray, M. Chowdhury, and J. Abawaij, "PUF-based secure checker protocol for networked rfid systems," in *2014 IEEE Conference on Open Systems (ICOS)*, 2014, pp. 78–83.
- [35] G. Al., R. Doss, M. Chowdhury, and B. Ray, "Secure rfid protocol to manage and prevent tag counterfeiting with matryoshka concept," in *Future Network Systems and Security*, R. Doss, S. Piramuthu, and W. Zhou, Eds. Cham: Springer International Publishing, 2016, pp. 126–141.
- [36] A. M. J. Marindra and G. Y. Tian, "Chipless rfid sensor tag for metal crack detection and characterization," *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, no. 5, pp. 2452–2462, 2018.
- [37] V. I. Ltd, "Walabot-technical brief technical specs," [online] accessed on: 14 Nov 2018. [Online]. Available: <https://walabot.com/docs/walabot-tech-brief-416?type=pdf>
- [38] "Walabot-technical brief technical specs." [Online]. Available: <https://walabot.com/docs/walabot-tech-brief-416?type=pdf>
- [39] B. Kubina, "Chipless wireless high-temperature sensing in time-variant environments," Ph.D. dissertation, Technische Universität, 2017.
- [40] Y. Zhu and C. Huang, "An improved median filtering algorithm for image noise reduction," *Physics Procedia*, vol. 25, pp. 609–616, 2012.
- [41] A. Vena, E. Perret, and S. Tedjini, "A depolarizing chipless rfid tag for robust detection and its fcc compliant uwb reading system," *IEEE transactions on microwave theory and techniques*, vol. 61, no. 8, pp. 2982–2994, 2013.
- [42] N. C. Karmakar, R. Koswatta, P. Kalansuriya, E. Rubayet, *et al.*, *Chipless RFID reader architecture*. Artech House, 2013.
- [43] A. Vena, E. Perret, and S. Tedjini, "Chipless rfid tag using hybrid coding technique," *IEEE Transactions on Microwave Theory and Techniques*, vol. 59, no. 12, pp. 3356–3364, 2011.
- [44] F. Costa, M. Borgese, S. Genovesi, L. Buoncristiani, A. Gentile, F. A. Dicandia, A. Monorchio, and G. Manara, "Detection of moving chipless tags by using sar processing," in *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*. IEEE, 2017, pp. 229–232.
- [45] C. Divarathne and N. Karmakar, "A feasible detection technique for chipless rfid systems based on likelihood," in *2014 1st Australian Microwave Symposium (AMS)*. IEEE, 2014, pp. 5–6.
- [46] B. R. Ray, M. U. Chowdhury, and J. H. Abawajj, "Secure object tracking protocol for the internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 544–553, 2016.
- [47] B. R. Ray, M. Chowdhury, and J. Abawajj, "Critical analysis and comparative study of security for networked rfid systems," in *2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, 2013, pp. 197–202.
- [48] J. Pudashine, A. Guyot, F. Petitjean, V. R. Pauwels, R. Uijlenhoet, A. Seed, M. Prakash, and J. P. Walker, "Deep learning for an improved prediction of rainfall retrievals from commercial microwave links," *Water Resources Research*, vol. 56, no. 7, p. e2019WR026255, 2020.
- [49] X. Wang, X. Wang, and S. Mao, "Rf sensing in the internet of things: A general deep learning framework," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 62–67, 2018.
- [50] T. Zheng, Z. Chen, S. Ding, and J. Luo, "Enhancing rf sensing with deep learning: A layered approach," *IEEE Communications Magazine*, vol. 59, no. 2, pp. 70–76, 2021.
- [51] B. Ray, R. Shah, M. R. Islam, and S. Islam, "A new data driven long-term solar yield analysis model of photovoltaic power plants," *IEEE Access*, vol. 8, pp. 136 223–136 233, 2020.