LoRa-PUF: A Two-Step Security Solution for LoRaWAN

Mohammed Bello Aliyu
School of Computing and Engineering
University of Huddersfield
Huddersfield, United Kingdom
Email: Mohammed.Aliyu@hud.ac.uk

Maryam Hafeez
School of Computing and Engineering
University of Huddersfield
Huddersfield, United Kingdom
Email: M.Hafeez@hud.ac.uk

Anju Johnson
School of Computing and Engineering
University of Huddersfield
Huddersfield, United Kingdom
Email: A.Johnson@hud.ac.uk

2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) | 979-8-3503-1114-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/VTC2023-Spring57618.2023.10199591

***Abstract*—The ever-increasing penetration of Internet of Things (IoT) applications across all sectors require better information and communication security for IoT devices. Physical Unclonable Function (PUF) circuits are a low-cost method used for generating unique responses, ideal for key generation and device authentication in high-performance microprocessors. PUFs are extracted from manufacturing variations embedded in the hardware of accessible devices, thereby requiring no additional computation or modification. Static Random Access Memory (SRAM) PUFs are widely used with keys generated from power-up values for authentication. This work is based on improving device authentication in the context of LoRa, which is a low-power wide-area network (LPWAN) technology. This paper exploits the integration of Carrier Frequency Offsets (CFOs) and SRAM PUF to create a two-step authentication security solution for LoRaWAN called LoRa-PUF. The power-up state value of three SRAM chips from the same off-the-shelf manufacturer are analyzed for SRAM PUF properties and 36000 packets of CFOs of four LoRa device types have been analyzed for LoRa-PUF. Our results indicate that LoRa SRAMs serve as sources of reliable challenge-response pairs for PUFs and the CFOs of the LoRa device type can be classified during communication with more than 70% accuracy which can be implemented on resource-constrained LoRa microcontrollers.**

***Index Terms*—Internet of Things (IoT) security, Physical Unclonable Function (PUF), RF fingerprinting, Machine learning, SRAM, Microcontrollers, LoRaWAN**

I. Introduction

The advancement of low-cost communication, computing, and embedded wearable technologies has resulted in a disrupting rise in the number of IoT devices. A vast number of these devices operate continuously in an un-trusted environment, vulnerable to malicious attacks. In the context of LoRaWAN, identifying and authenticating a huge number of complex heterogeneous devices imposes problems specifically for the receiving LoRa gateways. Traditional techniques for authentication like symmetric-key cryptography require storing secret keys in non-volatile memory (NVM) to create hash-based encryption which is ; (i) vulnerable to hacking and (ii) requires significant power overhead which is not suitable for low-cost and low-powered IoT solutions. Hence, PUFs which exploit manufacturing process variations to generate device-specific identity are increasingly popular and are resource efficient for LoRaWAN implementation [1]–[5]. PUFs are classified as strong and weak based on the number of challenge-response pairs (CRPs) they can validate. Weak PUFs generally accept a smaller number of CRPs which are proportional to the complexity of the hardware. Strong PUFs support large CRPs and prevent polynomial-time attacks. Hence, it is ideal for device authentication applications [6].

An easy implementation of a PUF-based authentication protocol secures and authenticates devices in an IoT environment. Exploiting SRAM non-idealities as PUFs is one method for implementing hardware-based security in IoT devices [1]. Additionally, when a LoRa transmitter transmits modulated digital data, RF properties containing specific device features such as frequency offset and I-Q imbalance can also serve as PUF. These features are usually irrelevant at the receiving gateway in terms of the information required. However, if the non-idealities are analyzed and exploited on the gateway, random unique information can be used to create a framework to identify and authenticate the transmitter for a low-cost security solution. This is termed RF fingerprinting. Existing methods rely on either an SRAM PUF or RF fingerprinting. However, SRAM PUFs are prone to modeling attacks [7] while RF-PUF is susceptible to jamming attacks and effects of device aging and mobility [8]. In this paper, we present a unified security scheme called LoRa-PUF that combines SRAM PUF for unique device identification and CFO-based RF Fingerprinting for device type identification to suit the low power requirements of IoT devices and provide enhanced security. Fig. 1 presents a framework for our proposed LoRa-PUF and goes further to secure communication by incorporating a two-stage authentication process.

The process starts with an SRAM PUF authenticating the

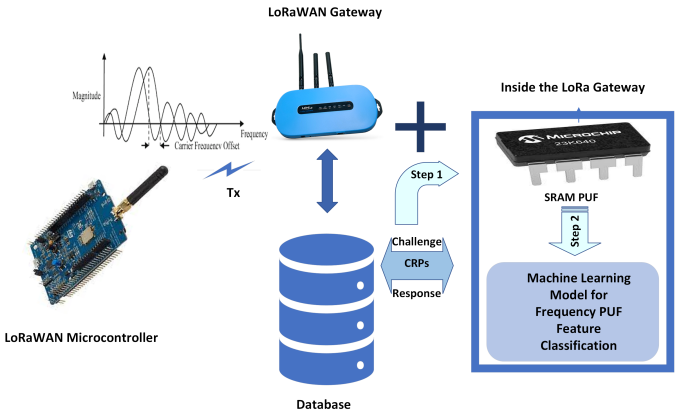

Fig. 1. Two-step PUF Authentication system

device using CRPs stored in a database. The latter stage uses CFOs of trusted devices stored in the database that have been modeled using machine learning tools to further authenticate the device type for robust security authentication. The resulting two-step solution offers a novel framework that requires no extra hardware on the transmitter while exploiting existing computational and storage capability at a typical receiving LoRa gateway. Such a framework can be applied in multiple environments for intrusion detection, preventing attacks like man-in-the-middle and replay attacks as a low-power low-cost solution. To our knowledge, the proposed LoRa-PUF is a novel framework for IoT device authentication. Technical analysis of the two PUF schemes using unique CFOs as PUF frequency features and SRAMs of commercial LoRa devices has been carried out as the main contribution of this paper.

II. Background and Preliminaries

A. SRAM-PUF

Several microcontrollers in the IoT environment have an onboard SRAM chip. PUFs can be gotten from existing SRAM as well as external SRAM connected to a microcontroller. The phases involved are enrollment and reconstruction of an SRAM PUF shown in figure 2 and 3

1) Enrollment: During enrolment, the power-up values, static IDs, and addresses are stored in the database.

2) Reconstruction : During reconstruction, the static ID is sent to the database which issues a challenge and gets a response to compare.

There are various ways to quantify the performance of SRAM PUF. The main metrics used during enrollment where power-up values become CRPs are the stability of the cells which requires the output of the chip to be the same also known as the Bit Error Rate (BER). Also, different PUF chips should have no correlation of power-up values to maintain uniqueness. The reconstruction phase which entails the decryption of the CRPs must not be predictable and remain identical during decryption [9]. These are the metrics used to evaluate the SRAM PUF in this paper.

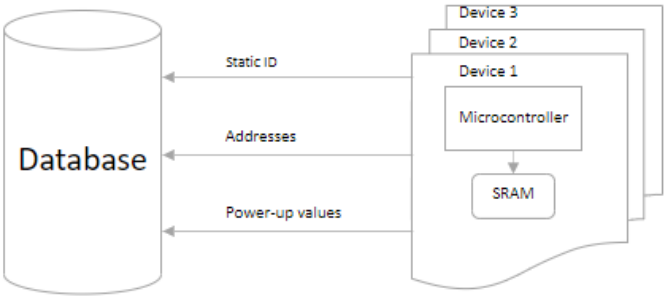

Fig. 2. SRAM PUF Enrollment

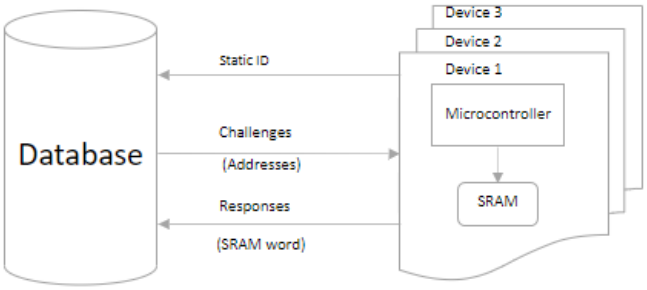

Fig. 3. SRAM PUF Reconstruction

The initial power-up state of SRAM as a digital signature was introduced by [10]. Out of 256 bytes, 128 bits of random CMOS SRAM-generated numbers were used to generate a cryptography key. Several researchers have used different methods to generate keys for SRAM PUF security. [9] used Error Correction Code (ECC) to reduce the error rate on microcontroller SRAMS and achieved a $7 * 10^{-7} bit/cell$ Temporal Majority Voting (TMV) proposed by [11] proved more reliable with an error rate of $10^{-6} BER$ for a 128-bit key. However, both of these methods require extensive computations. The data remanence method by [12] generated 100% stable keys by writing 0s and 1s to the SRAM cells and powering them down to check the strongest 0s or 1s. [13] proposed a proof of concept authentication technique that uses an ML model to authenticate devices by storing corrupted images of PUF fed into a CNN model and predicting the challenge given by the server. However, as explained earlier, modeling attacks have been successful in compromising SRAM PUF-only identification and authentication approaches [7]. .

B. RF-PUF

A popular technique for device identification in the transmission is Radio-Frequency Fingerprint Identification (RFFI) which is a proven method for authenticating and identifying wireless devices based on their hardware features [14], [15], [16]. Radio Frequency Fingerprint (RFF) is extracted from inherent hardware impairments during the manufacturing of these device chips. The features of the devices change slightly from their original values. These changes are small enough not to affect normal communication function but will show slight differences in the waveform. These differences are isolated and

used as device signatures. Similar to biometric fingerprints, RFF uniqueness is efficient and requires a huge effort to break. These make them suitable for low-powered IoT, made from low-cost components containing hardware imperfections. These imperfections are the fingerprint employed for the RFFI technique. Moreover, the low power consumption required to implement RFFI on device authentication makes it desirable due to the large number of end nodes in IoT with constrained energy resources and computation. [14]. Identification of wireless devices at the physical layer prevents several security attacks such as authentication, detection monitoring, forensic data collection, and intrusion detection, [17]. CFOs are used as a frequency feature for RFF and RF-PUF implementation which is inherent in the fixed carrier frequency of non-FDM device oscillators allowing for each Tx to have its unique frequency offset. Authors [18] and [19] used offsets as a primary for device identification. The different standard for frequency offset allows several limits, an example is the IEEE 802.11b standard requires a frequency offset with a 25 ppm range from the frequency center at 2.412 GHz), which corresponds to the normal standard deviation (σ) of 20.1 kHz. A reference clock with enough efficiency at the Rx can calculate offsets accurately for multiple transmitters. Also, a carrier synchronizer module existing in standard Rx is used for Low Oscillator (LO) offset compensation and can be employed to find and compensate for frequency offsets. [6] proposed using a sub-system of machine learning to use ppm offset as a primary feature that identifies Tx devices. A practical study by [20] resulted in over 97.44% to 99.78 % in signal-to-noise (SNR) range of 10 dB to 30 dB for 12 Zigbee devices under various conditions. This proves the practical implementation of CFOs as a reliable PUF feature for the proposed system.

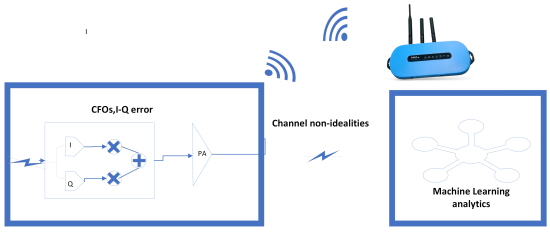

Fig. 4. RF-PUF Features Extraction
[6]

RFFI has also been considered a classification problem, which has recently been solved using deep learning methods [21]. Figure 4 [6], provides an overview of the exploitation of the RF signature embedded in devices during manufacturing, and the features that can be used to train the neural network-based deep learning model for authentication at the receiver. The recent work by [22] demonstrates a framework using an RFF extractor trained using deep learning. This approach yields an accuracy of 88.67% for other LoRa types for the classification of devices and rogue detection accompanied by effective channel mitigation.
The methods shown in figure5 by [22] used a channel-

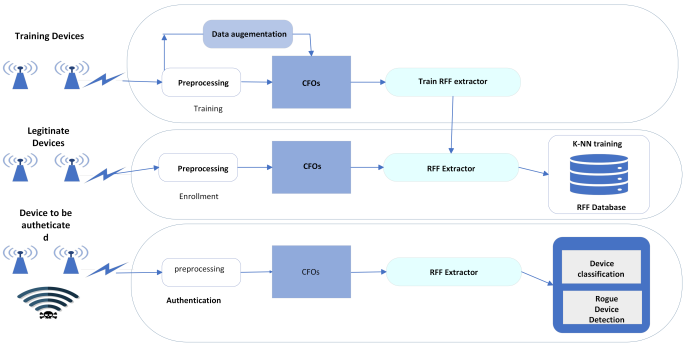

Fig. 5. Radio Frequency Fingerprinting Identification
[22]

independent spectrogram to train an RFF extractor and substituted it with the proposed CFO feature. The process was based on a deep learning-powered RFF extractor.

1) Training: The training stage uses the efficient capability of the RFF features extracted using deep learning rather than the classification of neural networks. Precisely, a large number of packets are stored from different devices for training with data augmentation used to increase channel diversity. The input to the extractor will be the CFOs and the training will only be done once.

2) Evaluation: Different channel conditions are to be used for evaluation on the same number of transmitters. The frequency features are analyzed with various metrics and environmental effects to check suitability.

3) Enrollment: The enrollment will acquire CFO as the RFFs of legitimate devices using the extractor. Legitimate working Lora devices in the IoT space from different manufacturers will be sent several packets to the RFFI system where the CFOs will be extracted using the trained RFF extractor and stored in a database. RFFs of new devices that fit the CFOs estimation will be enrolled and the previous devices will be deleted to allow the system to efficiently update. This enrollment should be executed in a controlled environment to prevent rogue devices from enrolling.

4) Authentication: Total authentication will consist of two parts with rogue detection to ensure the transmitted device belongs to the legitimate group and the latter being the classification to confirm its label. Both are implemented by the ML algorithm specifically K-Nearest Neighbour (KNN).

While RFFI techniques discussed above are useful, however, relying solely on these techniques for device authentication is limited as they are prone to adverse effects of device aging and attacks such as jamming as explained above. Hence there is a need to carefully design an authentication scheme that can ensure low-power secure authentication of LoRa devices.

III. Methodology

In this paper, we use stable cells as the proposed SRAM PUF method for key generation in combination with the CFO as a novel two-step authentication security for LoRaWAN devices. The first step of the process requires a challenge to

be sent to the database housing responses. When the SRAM response is received, it then verifies the CFO expected range with a classifier model using machine learning uploaded on the microcontroller to further verify the authentication of devices.

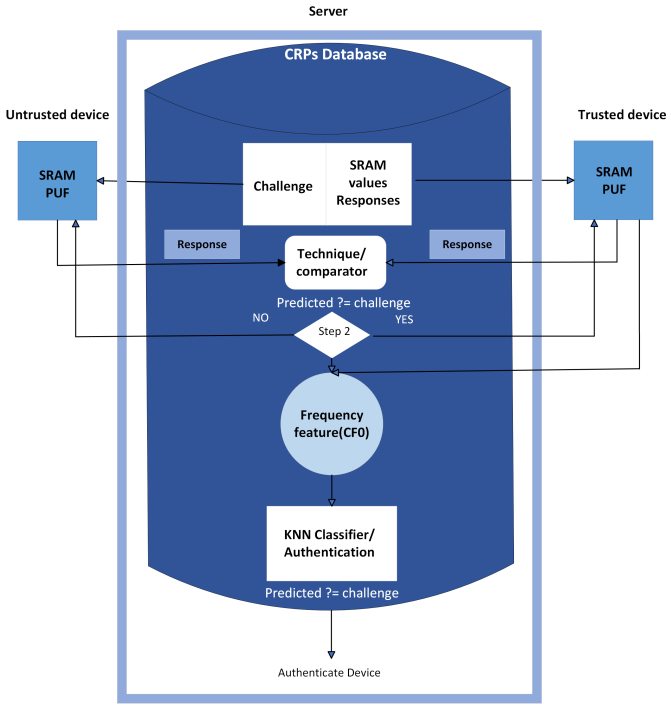

Fig. 6. Proposed Two-Step LoRa authentication

The methodology is shown in figure 6 details the approach in this paper.

1) CFO-based LoRa device classification: In our work, a public dataset of signals collected from 60 LoRa devices by [22] is used to simulate the expected CFO of LoRa devices as an identification and classification technique. The data set contains 36000 packets from 4 different LoRa commercial off-the-shelf chipsets detailed below and was captured using USRP N210 software-defined radio (SDR). Google Colab machine learning tool was used to analyze the data set and generate graphs of CFOs, device labels, and packets which was sufficient to generate results and predictions. The graph in figure 7 shows the unique range of CFOs for different devices and can be used to enroll a particular chipset type for identification.

2) SRAM PUF Implementation: The SRAM PUF implementation is done on a 23k640 SRAM chip interfaced with an Adafruit RFM95 LoRa module microcontroller using Arduino IDE to read out the power-up values. The pin function shown in the table I is used to interface the microcontroller to the SRAM shown in figure 8 using the SPI interface on the Arduino platform. The connection gives read/write access to the RAM allowing for the power-up values to be read multiple times.

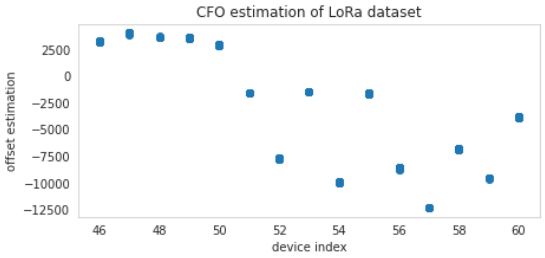

Fig. 7. CFO ranges for devices of three types. Devices 46-50 belong to type 1 chipset (SX1261), devices 51-55 belong to type 2 chipset (SX1272) and 56-60 belong to type 3 chipset (SX1276)

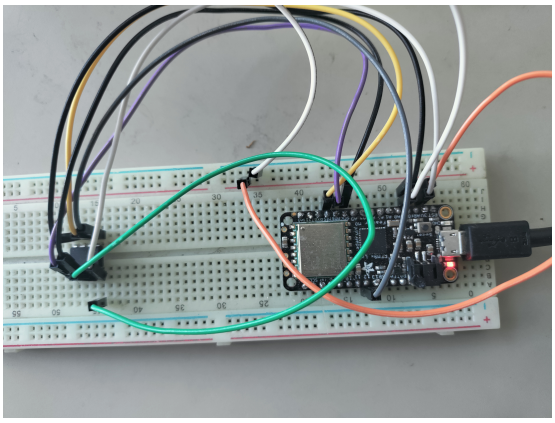

Fig. 8. LoRa Microcontroller wiring to 23k640 SRAM chip

A. Analysis/Result

Figure 9 shows the power-up value of three different chips of the same manufacturer. Ideally, there should be no correlation between chips and the hamming distance HD_{inter} which shows the correlation between different chips calculated from a stable cell is 50% validates the uniqueness of the chip used in this research.

Figure 10 shows the error rate of the stable region used in this research and the error rate HD_{intra} is 4.6% which is very close to the expected HD_{intra} of the 5-20% region. The mean value without temperature variation is 0.5.

Figure 11 shows the challenge and response from an 8-bit stable cell and validates what happens if the challenge entered is the wrong one, acceptable due to human error, and allows for re-entry with the second step making sure the authentication is trusted. Table II shows the results of the parameters evaluated

Name	Function
$\overline{CS}$	Chip Select Input
SO	Serial Data Output
VsS	Ground
SI	Serial Data Input
SCK	Serial Clock Input
$\overline{HOLD}$	Hold Input
VCC	Supply Voltage

TABLE I
23K640 PIN FUNCTION

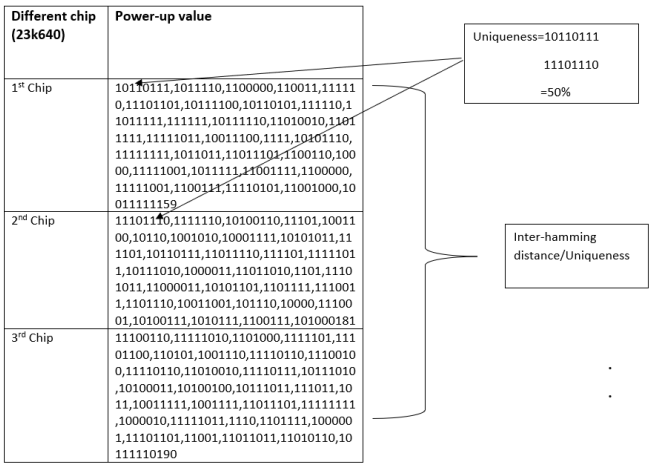

Fig. 9. Inter-distance/Uniqueness

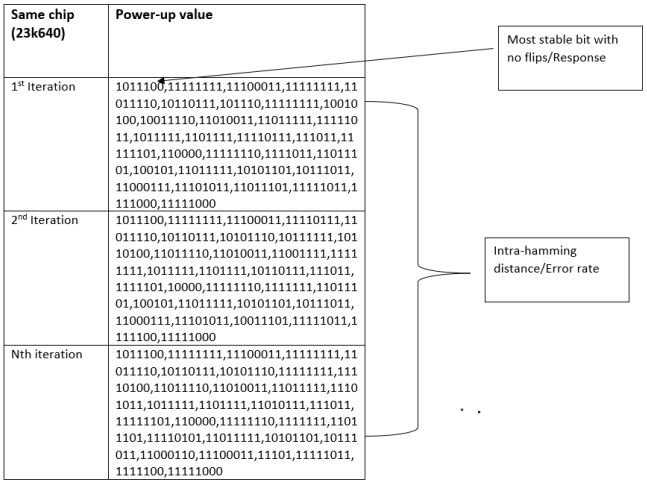

Fig. 10. Intra-distance/ Error rate

for SRAM PUF.

1) Identification of devices using LoRa CFOs: KNN classification model is used to predict the labels and confusion matrix to prove its accuracy is displayed in figure 12. The parameter used for identification is a comprehensive database by [22]. The CFO captured by the data set was data framed. The matrix generated is the identification of the device based on the CFO. A confusion matrix is generated to map the prediction of the true CFO labels to the predicted ones. The diagonal values show the accuracy of the prediction in

Property	Parameter	Region Result
Correlation between chips/Uniqueness	HD_{inter}	50%
Error Rate	HD_{intra}	4.6875%
Mean value/symmetry	u	0.48

TABLE II
PROPERTIES OF PUF VALIDATED

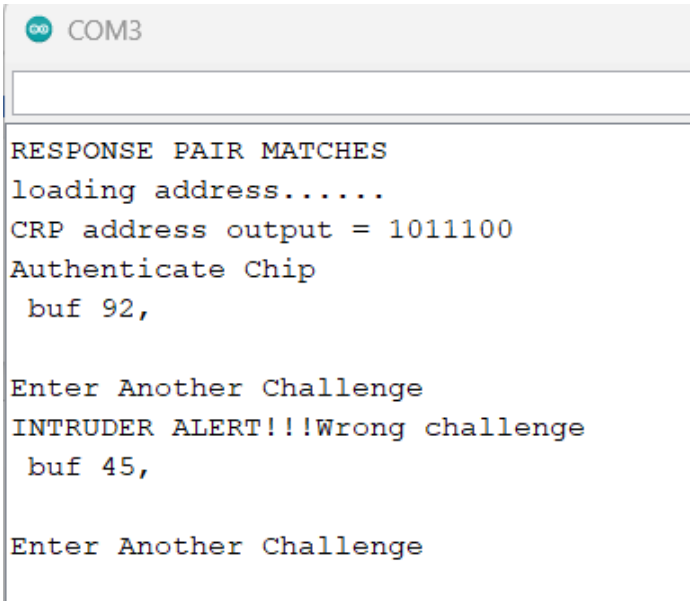

Fig. 11. CRP generation from a stable cell

percentage shown in III.

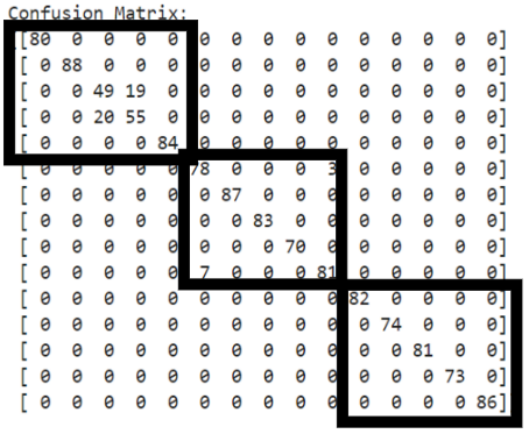

Fig. 12. Confusion matrix for the predicted label using KNN-classifier

Figure 13 is a plot showing the true label vs the predicted one. The produced shows identification is possible for an acceptable percentage of accuracy above 70% prediction.

Device index	Model	Chipset	CFO Accuracy
46-50	mbed SX1261 shield	SX1261	71.2%
51-55	Pycom FiPy	SX1272	79.8%
56-60	Dragino SX1276 shield	SX1276	79.2%

TABLE III
CLASSIFICATION ACCURACY BASED ON DIFFERENT LORA DEVICE CFOS

From table III shows that the classification of LoRa device type can be identified with an average of 76.7% accuracy for different device type classification.

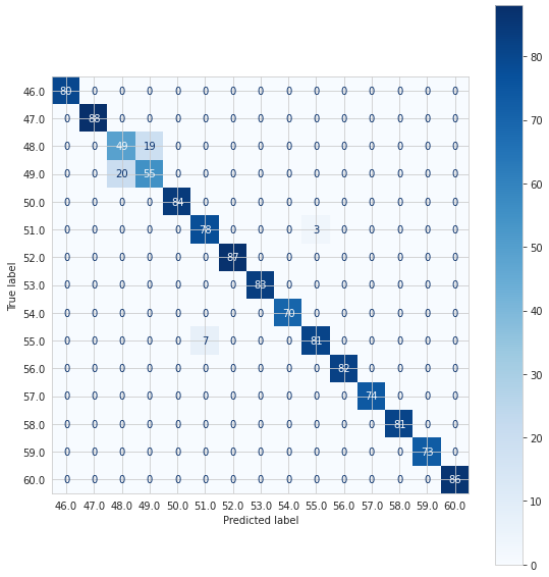

Fig. 13. Confusion matrix for true vs predicted label using KNN-classifier with device labels

IV. Conclusion/Future Work

In this paper, a novel technique that integrates SRAM PUF and LoRa CFOs as a two-step authentication for LoRaWAN security is proposed. Power-up values from 23k640 SRAM chips were used to generate PUF features. Stable cells were identified and validated for key generation and a further step to identify LoRaWAN devices by their CFO which is PUF frequency feature to create a robust two-step authentication system. Future work will detail stable key generation subjected to environmental factors such as the degree of mismatch and ambient condition variation which is mitigated by the second authentication. The CFO identification was limited to three device types and will require more devices to validate the robustness. The implementation of the CFO classifier will be done on an ultra-low-powered microcontroller using TensorFlow-lite for Tiny machine learning.

Acknowledgment

This research was partially supported by EPSRC Connected Everything (CE) Network Plus under grant RIS6543528 complemented by the support of Nick McCloud at Handy Little Modules Ltd and EU Horizon MSCA EVOLVE grant agreement No 101086218 and EP/X039161/1 from UKRI.

References

[1] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[2] M.-D. Yu, R. Sowell, A. Singh, D. M'Raïhi, and S. Devadas, "Performance metrics and empirical results of a puf cryptographic key generation asic," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2012, pp. 108–115.

[3] R. Maes, "Physically unclonable functions: Constructions, properties and applications (fysisch onkloonbare functies: constructies, eigenschappen en toepassingen)," 2012.

[4] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of sram-puf," in *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE, 2014, pp. 101–106.

[5] G. Kömürcü and G. Dündar, "Determining the quality metrics for pufs and performance evaluation of two ro-pufs," in *10th IEEE international NEWCAS conference*. IEEE, 2012, pp. 73–76.

[6] 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 of Things Journal*, vol. 6, no. 1, pp. 388–398, 2018.

[7] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges," *Computer Networks*, p. 109455, 2022.

[8] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Radio frequency fingerprinting and its challenges," in *2014 IEEE conference on communications and network security*. IEEE, 2014, pp. 496–497.

[9] C. Böhm, M. Hofer, and W. Pribyl, "A microcontroller sram-puf," in *2011 5th International Conference on Network and System Security*. IEEE, 2011, pp. 269–273.

[10] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2008.

[11] A. Vijayakumar, V. C. Patil, and S. Kundu, "On improving reliability of sram-based physically unclonable functions," *Journal of Low Power Electronics and Applications*, vol. 7, no. 1, p. 2, 2017.

[12] M. Liu, C. Zhou, Q. Tang, K. K. Parhi, and C. H. Kim, "A data remanence based approach to generate 100% stable keys from an sram physical unclonable function," in *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. IEEE, 2017, pp. 1–6.

[13] R. Suragani, E. Nazarenko, N. A. Anagnostopoulos, N. Mexis, and E. B. Kavun, "Identification and classification of corrupted puf responses via machine learning," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2022, pp. 137–140.

[14] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 94–104, 2015.

[15] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146–152, 2018.

[16] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[17] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identification via analog signal fingerprinting: A matched filter approach." in *NDSS*. Citeseer, 2006.

[18] P. Scanlon, I. O. Kennedy, and Y. Liu, "Feature extraction approaches to rf fingerprinting for device identification in femtocells," *Bell Labs Technical Journal*, vol. 15, no. 3, pp. 141–151, 2010.

[19] P. Welch, "The use of fast fourier transform for the estimation of power spectra: a method based on time averaging over short, modified periodograms," *IEEE Transactions on audio and electroacoustics*, vol. 15, no. 2, pp. 70–73, 1967.

[20] Y. Ren, L. Peng, W. Bai, and J. Yu, "A practical study of channel influence on radio frequency fingerprint features," in *2018 IEEE International Conference on Electronics and Communication Engineering (ICECE)*. IEEE, 2018, pp. 1–7.

[21] J. Gong, X. Xu, and Y. Lei, "Unsupervised specific emitter identification method using radio-frequency fingerprint embedded infogan," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2898–2913, 2020.

[22] G. Shen, J. Zhang, A. Marshall, and J. R. Cavallaro, "Towards scalable and channel-robust radio frequency fingerprint identification for lora," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 774–787, 2022.