Securing Smart Meter Communication with an Ensemble Fingerprinting Framework

Fahmida Afrin, Venkat Sai Suman Lamba Karanam, Byrav Ramamurthy and Nirnimesh Ghose
School of Computing, University of Nebraska-Lincoln, NE, USA
fafrin2@huskers.unl.edu, saisuman@huskers.unl.edu, ramamurthy@unl.edu and nghose@unl.edu

***Abstract*—Advanced Metering Infrastructure (AMI) comprises several smart meters (SM) that use wireless technologies such as ZigBee to exchange data and commands between each other and the backend systems. The wireless broadcast nature and smart meters' physical vulnerability make them prone to cyberattacks like spoofing, masquerading, and man-in-the-middle. This paper addresses the secret-free smart meter identification challenge in AMI systems, focusing on the widely used Zigbee communication standard. Specifically, we introduce an ensemble device fingerprinting framework, integrating the physical and the medium access control (MAC) layer with multiple machine learning models (Convolutional Neural Network, Logistic Regression, and Decision Tree). Our analysis shows that the ensemble framework outperforms individual fingerprinting models, with a mean accuracy of 83.33%.**

***Index Terms*—Authentication, multiple network layer fingerprinting framework, advanced metering infrastructure.**

I. Introduction

The advanced metering infrastructure (AMI) automates essential functions like sensor readings, billing, and customer data collection. AMI consists of numerous smart meter nodes that collect and transmit data to a central collector and utility base station using a mix of communication technologies, such as wireless LAN, ZigBee, WiMAX, GSM, DASH7, and Power Line Communication (PLC) [1]. Security breaches in smart power grids can lead to anything from minor inconveniences to significant disruptions, causing adverse customer effects and severe economic losses [2]. Smart meters in Advanced Metering Infrastructure (AMI) systems are vulnerable to unauthorized data injection, damaging communication networks, and compromising system security [3]. This vulnerability emphasizes the need for stronger security solutions to comprehensively improve AMI system protection. Our approach can be summarized as:

- We propose an ensemble framework for device fingerprinting combining multiple network layers (physical and MAC).
- We propose combining the physical and MAC layers with an ensemble fingerprinting approach on the individual layer machine learning models of Convolutional Neural Network (CNN), Logistic Regression, and Decision Tree, which combines the strengths of each layer and enhances the overall resilience of our device identification methodology.
- We generate an emulated smart meter dataset by transmitting actual smart meter data on a mesh network of six ZigBee nodes. We collect the physical layer and MAC layer data during transmission.
- We show that Weighted Average Ensemble-based fingerprinting can authenticate a smart meter with 83.33% accuracy.

II. System Overview

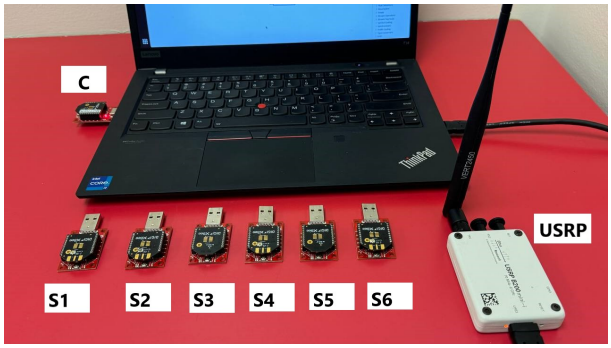

Fig. 1. The testbed setup includes six ZigBee transmitters (which act as smart meters) and a ZigBee receiver (collector) using a USRP.

1) Testbed: As illustrated in Fig. 1, we replicated the AMI using smart meters $(S_1, S_2, S_3, S_4, S_5, S_6)$ implemented as ZigBee transmitters and a collector (coordinator C) linked to the laptop. A single USRP B200 collects the dataset with a VERT2450 antenna installed. We implemented the ZigBee transmission on 2.4 GHz using the XCTU software on the laptop. We used actual smart meter data from [4] for transmission. From this dataset, we used six different files: HomeA-meter3_2016, HomeB-meter1_2016, HomeC-meter1_2016, HomeD-meter2_2016, HomeF-meter3_2016, and HomeG-meter1_2016. Each file has different features, such as LivingRoomOutlets, Barn, Well, Microwave, WasherDrier, Solar, etc., measured in kW. For our experiment, we considered 20 rows from each file, each row transmitted for 10 seconds during data transmissions through ZigBee with 30-second intervals between each transmission.

2) Dataset and Pre-processing: The physical layer dataset was captured as a binary file (.bin), while the MAC layer dataset was captured as a packet capture file (.pcap). We captured the MAC layer dataset's time, source address, destination address, frame length, and acknowledgment information. Before feeding the gathered .pcap and .bin files to models, we pre-processed them by converting them to text files.

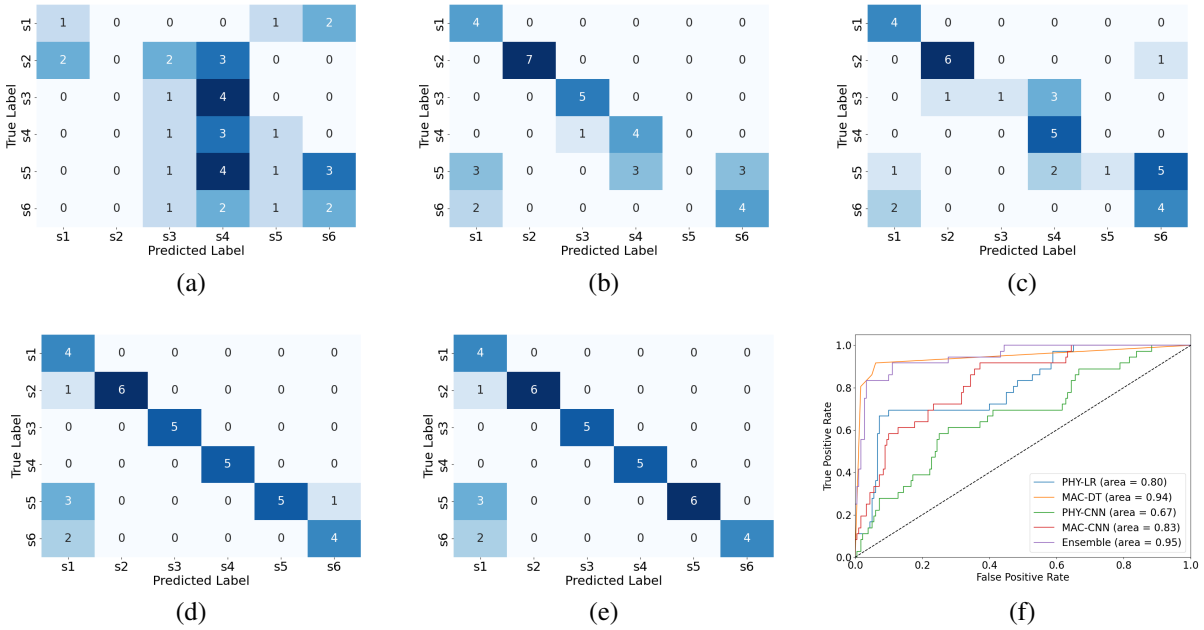

Fig. 2. Confusion Matrix for (a) physical layer-CNN (PHY-CNN), (b) physical layer-logistic regression (PHY-LR), (c) MAC layer-CNN (MAC-CNN), (d) MAC layer-decision tree (MAC-DT), and (e) Weighted Average Ensemble framework. (f) ROC-AUC Curve for all the models.

3) Experimental Setup: We used TensorFlow as the backend to implement our models in Keras for fingerprinting the smart meters. Our system, which was running Ubuntu 22.04.4 LTS, has an 11th-generation Intel(R) Core(TM) i7-1165G7 CPU operating at 2.80GHz. We evaluated the models by splitting the data into 60% for training, 20% for validation, and 20% for testing.

III. Results

We assessed the following performance metrics: accuracy, precision, recall, F1 score, ROC-AUC curve, and confusion matrix. We can see from Fig. 2(a) that physical layer fingerprinting using CNN is associated with higher misclassifications. On the other hand, Fig. 2(b)–(d) demonstrates that while there are minor errors, the performance of the physical layer with logistic regression, the MAC layer fingerprinting with CNN, and the MAC layer with decision tree has improved. Fig. 2(e) displays the weighted average ensemble framework; the higher values along the diagonal indicate that the model generates accurate predictions.The ensemble framework outperforms the individual models, whose AUC scores vary from 0.67 to 0.94, with the greatest ROC-AUC score of 0.95.

TABLE I
Evaluation metrics for smart meter identification for various models.

Model	Accuracy	Precision	Recall	F1 Score
PHY-CNN	22.22	20.39	24.91	20.25
MAC-CNN	58.33	72.14	63.92	54.74
PHY-LR	66.67	57.01	74.44	63.44
MAC-DT	80.56	86.67	84.66	82.27
Ensemble	**83.33**	**90.00**	**86.51**	**84.91**

The accuracy of the ensemble of four models is 83.33%, as seen in Table I. This is a significant improvement above the accuracy of the individual models, which range from 22.22% to 80.56%. Precision increases from 20.39% to 86.67% to 90.00%, and recall improves to 86.51% from the range of 24.91% to 84.66%. With the ensemble, the F1 score also rises to 84.91%

IV. Conclusion

This research tackles a crucial gap in the security of AMI by offering a practical solution for enhancing smart meter identification in ZigBee-based mesh networks. The paper introduces an innovative weighted average ensemble-based deep-learning framework tailored for smart meter identification. It employs a combination of deep learning models, including CNN, Logistic Regression, and Decision Trees, applied to the physical and MAC layers. The ensemble approach enhances security by adding multiple layers of authentication, making it harder for attackers to compromise the system.

V. Acknowledgement

This work was supported by the Nebraska Public Power District (NPPD) through the Nebraska Center for Energy Sciences Research at the University of Nebraska-Lincoln (Cycle 17) and the by NSF Grant CNS-2225161.

References

[1] A. Usman and S. H. Shami, "Evolution of communication technologies for smart grid applications," *Renewable and Sustainable Energy Reviews*, vol. 19, pp. 191–199, 2013.

[2] G. Bendiab, K.-P. Grammatikakis, I. Koufos, N. Kolokotronis, and S. Shiaeles, "Advanced metering infrastructures: Security risks and mitigation," in *Proc. of the International Conference on Availability, Reliability and Security*, 2020, pp. 1–8.

[3] V. S. S. L. Karanam, F. Afrin, B. Ramamurthy, and N. Ghose, "Cross-layer device identification for smart grid substation networks," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2023, pp. 1–2.

[4] UMassTraceRepository, "Smart data set for sustainability," 2024. [Online]. Available: https://dx.doi.org/10.21227/g91z-hz32