Towards Machine Learning Based Fingerprinting of Ultrasonic Sensors

Marim Elhanafy*, Srivaths Ravva†, Abhijeet Solanki*, Syed Rafay Hasan*
*Department of Electrical and Computer Engineering, Tennessee Technological University, Cookeville, TN 38505, USA
Email: mmelhanafy42@tntech.edu, asolanki42@tntech.edu, shasan@tntech.edu
†Department of Computer Science, Stony Brook University, Stony Brook, NY, USA
Email: srivaths.ravva@stonybrook.edu

***Abstract*—Fingerprinting is now recognized as an approach that identifies or categorizes devices using distinct data characteristics. This paper introduces a sensor fingerprinting model and, through experiments, demonstrates that unique error patterns resulting from manufacturing imperfections can be used to accurately identify sensors. Using various machine learning algorithms such as a random forest classifier, multilayer perceptron, and soft decision tree, accuracies of 87%, 85.5%, and 89.2% respectively were achieved. These results highlight the significant potential for reliable sensor fingerprinting applications.**

***Index Terms*—sensor fingerprinting, sensor detection, machine learning-based sensor detection**

I. Introduction

As Information and Communication Technology (ICT) continues to evolve, particularly in the domains of the Internet of Things (IoT) and Artificial Intelligence of Things (AIoT), it faces significant hardware security challenges [1]–[3]. These technological advances, crucial for improving real-time data analytics, also escalate serious cybersecurity concerns, particularly regarding Hardware Intrinsic Attacks (HIAs) [4], [5]. These attacks can target not only the software, but also the hardware layer of infrastructures. In fact, fortifying hardware systems could provide more robust security compared to software enhancements alone [6]. In response, fingerprinting emerges as an innovative method in which devices are identified or classified based on specific data [7]. This approach is particularly useful for sensors, such as ultrasonic sensors extensively employed in the manufacturing, automotive, and medical sectors [8]. This paper discusses the critical need to integrate an identification matrix into the fingerprints of ultrasonic sensors, emphasizing the identification of sensors through their power consumption data because of their extensive application in various industries.

II. Proposed Model

The proposed model aims to fingerprint sensors using power consumption data to create unique identifiers. It employs a Decision Tree and Multilayer Perceptron to distinguish each sensor within a dataset that includes multiple sensors. The process of generating a sensor fingerprint involves several key steps. Initially, data are collected and segmented into smaller subsets from which power consumption data are extracted. These features are then aggregated and tagged with a specific sensor ID. Finally, we calculate the percentage error between the expected and observed distance for each sensor and apply a machine learning algorithm to classify the sensors based on these fingerprints.

III. Implementation

A. Data Collection

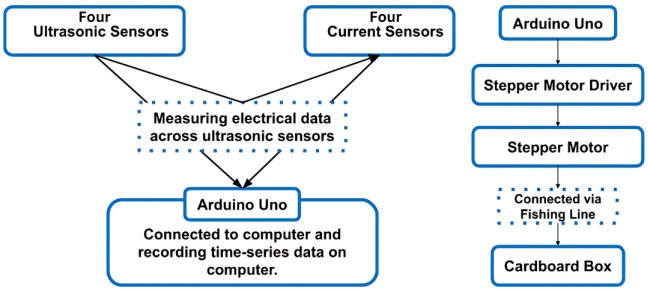

Fig. 1: high-level architecture of the testbed.

The experiment involved four low-cost HC-SR04 ultrasonic level sensors and four INA219 current sensors, managed by two Arduino Uno R3 designated as 'primary' for sensors and another as 'secondary' for controlling a 28BYJ-48 stepper motor via an ULN2003 driver. Data collection was facilitated by the primary Arduino, which connected to the sensors through Inter-Integrated Circuit (I^2C) communication, capturing distance measurements as a cardboard box attached to a fishing line was drawn closer by the stepper motor. This setup, detailed in Figure 1.

The testbed comprised four ultrasonic sensors placed parallel to each other on a breadboard, with the Arduino Uno R3 securely attached to a wall and the breadboard positioned on the floor nearby, as shown in Figure 2. The area within 450 cm of the sensors was cleared to ensure unobstructed measurements. Distances from 400 cm to 2 cm were marked on the floor at 10 cm intervals, representing the working range of the HC-SR04 ultrasonic sensors. The cardboard box served as the target surface for the sensors to measure distance. Initially positioned at the 400 cm mark, the box was aligned perpendicular to the sensors. Measurements from all four sensors were recorded at each 10 cm interval, with the box being incrementally moved closer until reaching the 2 cm mark.

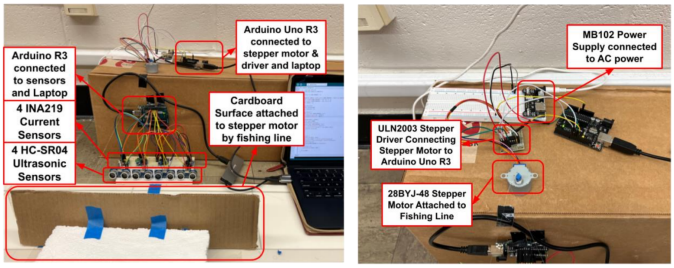

Fig. 2: Four ultrasonic sensors placed on a breadboard, with the Arduino Uno R3 and stepper motor connected to the cardboard box served as the target surface for the sensors to measure distance.

To minimize experimental errors and collect a comprehensive dataset, the data collection process was repeated three times, from 400 to 2 cm. In addition, to evaluate potential effects of sensor placement on readings, the positions of the sensors on the breadboard were changed four times, resulting in four different configurations. Each sensor was assigned an ID from 1 to 4, and when the orientation changed, the wired connections moved with the corresponding sensor, ensuring consistency in Arduino pin assignments.

B. Feature Extraction

In the feature extraction phase, the sensors provide data at a sampling rate of once per second. Data including distance (measured in millimeters), bus voltage, sweep voltage, load voltage (all measured in volts), current (measured in milliamperes) and power (measured in milliwatts) are transmitted from the sensors to the primary Arduino Uno R3. Each dataset captured from the sensors is systematically recorded and then labeled with a unique sensor ID to facilitate subsequent analysis and identification processes. In addition to these data, the features also include Mean, Standard Deviation (Std-Dev), Mean Absolute Deviation, variance, range, skewness, and kurtosis. Another added feature is the percentage error showing the margin of the deviation of the observed distance from the expected distance, for each sensor.

C. Results

Each sensor is assigned a unique ID and subjected to multi-class classification to distinguish it among other sensors. The first classification model used is the Random Forest Classifier, which gave an overall accuracy of 24%. Subsequently, we removed all the percentage error data points within the percentage error feature that are within $\pm 4\%$, approximately 1863 data points out of a total of 2000 data points. After this adjustment, the differences started to appear, as shown in Figure 3, and the accuracy increased to 56%. Another dataset was made after repeating the experiment; using the Random Forest Classifier, Multilayer Perceptron, and Soft Decision Tree, accuracies of 87%, 85.5%, and 89.2% respectively were achieved. Table I provides these results in detail.

TABLE I Performance Metrics of ML Models

Model	Accuracy	Precision	Recall	F1 Score
Random Forest Classifier	0.87	0.86	0.87	0.86
MLP	0.855	0.857	0.855	0.854
DT	0.892	0.899	0.894	0.891

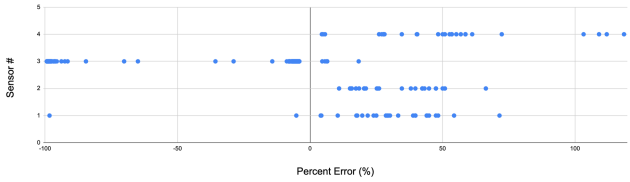

Fig. 3: The percentage error data point after reduction.

IV. Conclusions and Future Work

This work has demonstrated the effective application of percentage error and machine learning models, in sensor identification. The models achieved results with an accuracy as high as 87%, demonstrating the reliability and effectiveness of machine learning in sensor fingerprinting. Future work could explore the integration of additional sensor types and the application of more sophisticated machine learning algorithms to further improve accuracy and robustness.

V. Acknowledgment

This research is partially supported by the Tennessee Tech University's Center for Manufacturing Research, National Science Foundation Grant (NSF-REU 2349104)

References

[1] So-Yeon Park, Sunil Lim, Dahee Jeong, Jungjin Lee, Joon-Sung Yang, and HyungJune Lee. Pufsec: Device fingerprint-based security architecture for internet of things. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pages 1–9, 2017.

[2] Sakthi Vignesh Radhakrishnan, A. Selcuk Uluagac, and Raheem Beyah. Gtid: A technique for physical device and device type fingerprinting. *IEEE Transactions on Dependable and Secure Computing*, 12(5):519–532, 2015.

[3] Hristo Bojinov, Yan Michalevsky, Gabi Nakibly, and Dan Boneh. Mobile device identification via sensor fingerprinting. *arXiv preprint arXiv:1408.1416*, 2014.

[4] Tolulope A. Odetola, Hawzhin Mohammed, and Syed Rafay Hasan. A stealthy hardware trojan exploiting the architectural vulnerability of deep learning architectures: Input interception attack (iia). *ArXiv*, abs/1911.00783, 2019.

[5] Hawzhin Mohammed, Tolulope A Odetola, Syed Rafay Hasan, Sari Stissi, Isaiah Garlin, and Falah Awwad. (hiadiot): Hardware intrinsic attack detection in internet of things; leveraging power profiling. In *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 852–855, 2019.

[6] Abdurrahman Elmaghbub and Bechir Hamdaoui. Domain-agnostic hardware fingerprinting-based device identifier for zero-trust iot security. *IEEE Wireless Communications*, 31:42–48, 2024.

[7] Wenxin Lei, Zhibo Pang, Hong Wen, Wenjing Hou, and Wen Li. Physical layer enhanced zero-trust security for wireless industrial internet of things. *IEEE Transactions on Industrial Informatics*, 20(3):4327–4336, 2024.

[8] Eric Cheek, Dhimant Khuttan, Raghu Changalvala, and Hafiz Malik. Physical fingerprinting of ultrasonic sensors and applications to sensor security. In *2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys)*, pages 65–72, 2020.