Advancing Device Uniqueness through Physical-Layer Identification: A High-Resolution Strategy

Qingrui Pan[1], Zhenlin An[2], Xiaopeng Zhao[3], Lei Yang[3]

[1] The University of Edinburgh, UK;
[2] Princeton University, US;
[3]The Hong Kong Polytechnic University, HK SAR

Radio Frequency Identification (RFID) tags are becoming essential in the Internet of Things (IoT) ecosystem, serving critical functions in systems like electronic passports and supply chains. With the increasing prominence of RFIDs, security issues have also intensified, leading to the development of various protocols for authentication and privacy. However, industry preference leans towards simpler password-based protocols suited to the limited power and computational capabilities of battery-free tags. At the physical layer, identification leverages inherent manufacturing variations to produce a unique hardware fingerprint, making exact replication nearly impossible due to micro and nanoscale production variances. This method provides an effective security solution for RFIDs without requiring additional hardware or computations, facilitating applications such as anti-counterfeiting and key management.

In this presentation, we will share a novel approach to utilize high-resolution backscatter frequency drift in RFID Identification [1]. This work was published in IEEE SECON 2023, where it received the best paper award, and the extended version was accepted for publication by IEEE TMC [2]. In this study, we re-evaluate the backscatter frequency drift (BFD) as a robust hardware fingerprint for RFID tags, initially introduced a decade ago. BFD stands out for its stability across different RF systems and is not influenced by the tag's orientation, distance, or multipath effects, unlike other RF-related fingerprints such as power spectrum density and minimum activated power. Additionally, BFD's reliability is unaffected by structural imperfections in the tag's antenna, making it an optimal choice for physical-layer RFID identification. Unfortunately, BFD has shown a low level of recognition. In this research, we reassess BFD focusing on improving frequency resolution, which currently can only differentiate up to 225 tags. By utilizing techniques like redundancy, harmonics, and multifrequency, we are able to enhance the frequency resolution from kilohertz to sub-hertz. This enhancement significantly lowers the likelihood of fingerprint collisions to below 10^{-11}.

To evaluate the efficacy of high-resolution BFD, we developed an automated acquisition system that gathered approximately 800,000 BFD instances from 7,135 RFID tags across nine models. Our extensive assessment demonstrates significant improvements: (1) The proportion of unique BFD fingerprints increased from 0.08% to 99.39% with the integration of 5x redundancy, 23rd-order harmonics, and 10 frequency adjustments for better resolution. (2) The identification accuracy of high-resolution BFD improved from 26.8% to 95%, even when analysing thousands of tags, marking a 68% enhancement over low-resolution BFD. (3) High-resolution BFD remained effective across various acquisition conditions, including different encoding schemes, temperatures, transmitting powers, and orientations.

References

[1] Pan, Qingrui, Zhenlin An, Xiaopeng Zhao, and Lei Yang. "Revisiting Backscatter Frequency Drifts for Fingerprinting RFIDs: A Perspective of Frequency Resolution." In 2023 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 124-132. IEEE, 2023.
[2] Pan, Qingrui, Zhenlin An, Xiaopeng Zhao, and Lei Yang. "The Power of Precision: High-Resolution Backscatter Frequency Drift in RFID Identification." IEEE Transactions on Mobile Computing (2023).