THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

COMP RESEARCH STUDENT SEMINAR

Date : 22 February 2023 (Wed)
Time : 11:00 am - 12:00 pm
Venue : PQ304 (Face-to-face)

Security Threats and Countermeasures of LoRa

Abstract

For IoT applications, security is more important than ever. This talk presents some security threats and countermeasures of LoRa physical layer. LoRa is a popular Low-Power Wide Area Network (LPWAN) technology that is expected to boost the next generation of IoT for its capability to provide ubiquitous long-range connectivity for everyday objects with an AA battery. Despite the popularity, there exists a growing concern about the security of LoRa communication. Current LoRaWAN systems are susceptible to security attacks due to the inherent features of LoRa communications. This talk will explore possible security attacks at both the transmitter (covert channel) and receiver (jamming attack). Corresponding countermeasures against such attacks will also be described.

Dr Ningning HOU
Postdoctoral Fellow
Department of Computing

About the Speaker

Ningning Hou is a postdoctoral fellow at the Hong Kong Polytechnic University. She obtained her bachelor's degree in telecommunication from the Beijing University of Posts and Telecommunications and her Ph.D. degree in computing from the Hong Kong Polytechnic University. Her research interests include Internet-of-Things, low-power wide-area networks, physical layer security, and wireless sensing. Her research has been published in well-recognized conferences and journals, including INFOCOM, MobiCom, ICNP, SenSys, TON, and TOSN.

RF-DNA: Large-Scale Physical-layer Identifications of RFIDs via Dual Natural Attributes

Ms Qingrui PAN
PhD student
Department of Computing

About the Speaker

Qingrui Pan received the B.E. degree from the School of Electronic and Engineering at the City University of Hong Kong in 2017. She is now a Ph.D. student at the Department of Computing at The Hong Kong Polytechnic University. Her research interest includes artificial intelligence of things (AIoT), indoor localization, backscatter communication, and physical-layer identification.

Abstract

Physical-layer identification aims to identify wireless devices during RF communication by exploiting the imperfections of their radio circuitry, i.e., hardware fingerprint. Previous work proposed several hardware fingerprints for RFIDs (e.g., TIE, ABD, PSD, etc). However, these proposed fingerprints suffer from either unscalability or acquisition inefficiency. This work presents RF-DNA, a new hardware fingerprint composed of millions of Dual Natural Attributes (DNA) organized in a helical structure, where a pair of DNA represents a tag's intrinsic response at some frequency. We take advantage of the frequency agnostic phenomenon that a commercial RFID tag can respond within a wider band than the regulated, to acquire 10× more features than previous fingerprints. At the heart of this work are the context-free acquisition approach to extracting DNA from backscatter signals; and the accurate DNA matching algorithm for verifying a tag's identity. A total of 160,000 RF-DNA instances were collected from 16,000 tags using a customized automatic acquisition system. We subsequently carried out large-scale experiments to test the identification accuracy of RF-DNA and previously proposed fingerprints. Our comprehensive evaluation reveals that RF-DNA can achieve a mean accuracy of 95.98%. In contrast, those of previous fingerprints fall to 60% below in the face of thousands of tags.