Cross-Layer Device Fingerprinting System and Methods

Tech ID: 33340 / UC Case 2023-927-0

BACKGROUND

Networks of connectivity-enabled devices, known as internet of things or IoT, involve interrelated devices that connect and exchange data with other IoT devices and the cloud. As the number of IoT devices and their applications continue to significantly increase, managing and administering edge and access networks have become increasingly more challenging. Currently, there are approximately 31 billion ‘‘things’’ connected to the internet, with a projected rise to 75 billion devices by 2025. Because of IoT interconnectivity and ubiquitous device use, assessing the risks, designing/specifying what’s reasonable, and implementing controls can be overwhelming to conventional frameworks. Any approach to better IoT network security, for example by improved detection and denial or restriction of access by unauthorized devices, must consider its impact on performance such as speed, power use, interoperability, and scalability. The IoT network’s physical and MAC layers are not impenetrable and have many known threats, especially identity-based attacks such as MAC spoofing events. Common network infrastructure uses WPA2 or IEEE 802.11i to help protect users and their devices and connected infrastructure. However, the risk of MAC spoofing remains, as bad actors leverage public tools on 802.11 commodity hardware, or intercept sensitive data packets at scale, to access users physical layer data, and can lead to wider tampering and manipulation of hardware-level parameters.

TECHNOLOGY DESCRIPTION

To help improve wireless network security with a focus on identity-based attacks, e.g., MAC address spoofing, investigators at UC Santa Cruz (UCSC) have proposed a new framework, named Cross-Layer Device Fingerprinting, or CL-DF for short, that uses certain intrinsic device features, or fingerprints, at the physical layer as a way to uniquely identify devices. In combination with physical layer features, UCSC’s end-to-end framework also uses device fingerprints (DF) across other network protocol layers (CL) to enhance conventional network authentication. In the case of MAC spoofing attacks, the proposed CL-DF architecture would use certain physical layer features together with information from the MAC layer, e.g., the MAC address. Determining the most relevant physical layer features that contribute effectively to identify devices in a provably unique fashion (thus contributing to network security enhancement and QoS management) in a computationally efficient way is a challenge. In the MAC address spoofing detection use case, CL-FP uses the Error Vector Magnitude (EVM) as the physical layer fingerprint because it can effectively represent a transmitter’s unique features while being computationally lightweight. In addition to extracting the device's EVM (which represents the device’s unique I/Q gain imbalance), CL-DF generates and maintains a whitelist database that properly stores information from all authenticated devices. Results from preliminary experiments using a software-based testbed resulted in >90% accuracy for MAC spoofing detection with relatively low computation overhead. Future work by UCSC aims to identify additional physical layer features that do not depend on the transmission scheme (e.g., modulation type, coding rate, coding type, etc.) used by wireless devices.

APPLICATIONS

- Network security software
- IoT device software

ADVANTAGES

- preliminary testbed resulted in >90% accuracy
- low computation overhead, taking only seconds
- easier-to-extract FP features as harder-to-extract intrinsic features

INTELLECTUAL PROPERTY INFORMATION

CONTACT

Marc Oettinger
marc.oettinger@ucsc.edu
tel: 831-502-0253.

INVENTORS

- Obraczka, Katia
- Rezki, Zouheir
- Xue, Li

OTHER INFORMATION

KEYWORDS

device fingerprinting, IoT, networks, networking, security, cybersecurity, cross-layer, MAC spoofing, 802.11, network security, wireless, attack, cyber attack, identity-based attack

CATEGORIZED AS

- **Communications**
  - Internet
  - Networking
  - Wireless
- **Computer**
  - Security
  - Software
- **Security and Defense**
  - Cyber security

RELATED CASES

2023-927-0

Patent Pending

RELATED MATERIALS

- "Cross-Layer Device Fingerprinting and Its Applications to Network Security." IEEE ICC 2023. 28 May - 01 June 2023.

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Decoder-Only Transformer Methods for Indoor Localization
- A Novel Iot Protocol Architecture; Efficiency Through Data And Functionality Sharing Across Layers
- Robust Adversarial Attack Detection
- Patient Pressure Injury Prevention Methods and Software
- Platooning System and Methods
- Smart Deployment of Nodes in a Network

University of California, Santa Cruz
Industry Alliances & Technology Commercialization
Kerr 413 / IATC,
Santa Cruz,CA 95064

Tel: 831.459.5415
innovation@ucsc.edu
https://officeofresearch.ucsc.edu/
Fax: 831.459.1658