Abstract

The widespread integration of Internet-of-Things (IoT), observed in 84% of German households by 2022 [Sta22], has given rise to significant security apprehensions. This surge in connected devices amplifies data generation in homes, escalating security and privacy risks. Compromised sensors, e. g., those monitoring doors and windows, create vulnerabilities that adversaries could exploit, potentially leading to undetected intrusions. Passive eavesdropping on IoT systems further intensifies risks by exposing sensitive resident information. Despite cryptographic measures, computational limitations and insecure ciphers render commonly used IoT devices susceptible to various attacks. This thesis aims to enhance residential home security by treating IoT devices as immutable black boxes. The primary objective is to develop a security mechanism overlaying existing systems, utilizing fingerprinting principles and physical features as a protocol-agnostic approach. This aims to detect and respond to changes induced by potential adversaries, addressing inherent vulnerabilities in IoT devices.

The experimental setup involves a Software-defined Radio (SDR), specifically the Ettus Research *USRP B200mini*, and sensor nodes (i. e., Moteiv Cooperation *Tmote Sky sensor*) simulating typical IoT devices. Signal analysis, using *GNURadio* software, focuses on physical signal characteristics, including amplitude, phase, frequency, time-domain, and modulation. The workflow encompasses feature extraction, fingerprint creation, and testing against potential attacks. Assumptions include packet content irrelevance, establishment of a fingerprinting threshold, potential resilience against Generative Adversarial Network (GAN) attacks, non-reliance on secret components, and a non-cryptographic approach by focusing on physical features (PHY-F). Experiment I explores signals captured by SDRs in an uncontrolled office environment, employing advanced signal processing techniques. Experiment II implements a GAN to simulate attacks on IoT devices within a Physical Guard Fingerprinting System (PHY-GF) system. Experiment III focuses on localizing IoT devices using Received Signal Strength Indicator (RSSI) values to obtain a additional positioning feature. In Experiment I, statistical measures like amplitude and phase, along with "I-Q Ratio" and outlier analysis, proved valuable for PHY-GF. Principle Component Analysis (PCA) and Single Value Decomposition (SVD) identified key linear combinations. Auto-correlation and cross-correlation faced challenges in real-time PHY-GF. Periodic patterns and transient components emerged as promising indicators for device identification. Experiment II's GAN showed visually similar signals, but key statistical disparities with real data raised concerns about capturing characteristic features. Trilateration in Experiment III revealed the method's sensitivity to errors, emphasizing the need for improved accuracy. Localization adds a security layer but may not suffice alone; periodic verification is proposed to detect anomalies.

In summary, this research addresses security concerns associated with IoT by employing a multifaceted approach, including physical signal characteristics, GAN simulations, and localization for enhanced security measures. The outcomes aim to establish a practical PHY-GF system, offering insights into securing IoT devices in residential homes.