PHY-IDS: A Physical-layer Spoofing Attack Detection System for Wearable Devices

Wenqing Yan
Uppsala University
wenqing.yan@it.uu.se

Sam Hylamia
Uppsala University
Uppsala, Sweden
sam.hylamia@it.uu.se

Thiemo Voigt
Uppsala University, RISE SICS
thiemo@sics.se

Christian Rohner
Uppsala University
christian.rohner@it.uu.se

***Abstract*—In modern connected healthcare applications, wearable devices supporting real-time monitoring and diagnosis have become mainstream. However, wearable systems are exposed to massive cyberattacks that threaten not only data security but also human safety and life. One of the fundamental security threats is device impersonation. We therefore propose PHY-IDS; a lightweight real-time detection system that captures spoofing attacks leveraging on body motions. Our system utilizes time series of physical layer features and builds on the fact that it is non-trivial to inject malicious frames that are indistinguishable with legitimate ones. With the help of statistical learning, our system characterizes the signal behavior and flags deviations as anomalies. We experimentally evaluate PHY-IDS's performance using bodyworn devices in real attack scenarios. For four types of attackers with increasing knowledge of the deployed detection system, the results show that PHY-IDS detects naive attackers with high accuracy above 99.8% and maintains good accuracy for stronger attackers at a range from 81.0% to 98.9%.**

I. Introduction

In Body Area Networks (BANs), wirelessly connected wearable devices play an influential role in the revolution of healthcare applications, such as vital signs monitoring for remote monitoring and diagnostics. Although these systems support critical functionality, a lack of proper security protection is quite common [1]. Most reported security attacks are related to spoofing attacks where a malicious party impersonates another device because it can be exploited to launch many other sophisticated attacks. Spoofing attacks forge higher layer identities, such as MAC and IP addresses, or compromise authentication protocols [2]. Physical layer features in wireless channels are difficult to modify at will because of the spatial separation of sender and receiver and are preferable in security threat prevention. Our system analyses the time series of Received Signal Strength Indicator (RSSI), which is the power level of a received frame measured at the receiver's antenna. It is non-trivial for an attacker to send frames that are received with a signal level indistinguishable from the legitimate data sent over a dynamic wireless channel.

We propose PHY-IDS, a spoofing intrusion detection system specifically for wearable devices leveraging body motion and lightweight statistical algorithms, which can identify a single frame from an impersonating device by analyzing RSSI time series.

This project is financially supported by the Swedish Foundation for Strategic Research

II. Adversary Models

In our adversary models, we do not constrain the attacker's location. However, we assume that in most scenarios, there is a low probability that an adversary is located next to legitimate nodes. We classify attacks into four groups based on their knowledge of our system.

1) *Naive Attacker*: The first attack vector does not know anything about our detection system. It transmits frames with fixed transmit power without any efforts to evade our system inspection. This is the most naive attacker we use as a benchmark to show what is achievable with PHY-IDS.

2) *Model-stealing Attacker*: The second attacker knows the well-trained model that our system uses, but can not get access to any legitimate nodes' real-time RSSI.

3) *Training Data-stealing Attacker*: The third attacker first appears early in initial training data collection. When legitimate nodes are collecting training data, the attacker eavesdrops the same frames and locally records the RSSI. After that, it intercepts the legitimate RSSI trace and trains his own prediction model mapping the relation between attacker data and legitimate data. In the detection period, it is only a passive eavesdropper and can not compromise any nodes.

4) *Mimic Training Attacker*: The final attack vector deploys an emulation attacking setup on another person to collect pseudo training data for legitimate and adversary nodes, which is an imitation of the previous attack.

III. Results

For different levels of spoofing attacks, the experimental results demonstrate that PHY-IDS can detect naive attacks with 99.8% average accuracy and still maintain 81.0% for the strongest attacker with full knowledge and advanced learning capability. It is a promising step towards using wireless-link characteristics for spoofing attack detection in BANs.

References

[1] L. H. Newman. (2019) A model hospital where the devices get hacked on purpose. [Online]. Available: https://www.wired.com/story/defcon-medical-device-village-hacking-hospital/

[2] P. Liu and et al., "Real-time Identification of Rogue WiFi Connections Using Environment-Independent Physical Features," in *IEEE Conference on Computer Communications (INFOCOM)*, 2019.