Reviewer: Li-Chen Cheng May 2023

Article Review

Non-Cooperative Wi-Fi Localization & its Privacy Implications

Summary

The paper presents a new method for revealing the physical location of private devices within a targeted Wi-Fi network without requiring cooperation from any access point or device. Firstly, attackers dispatch false beacon frames to identify the MAC addresses of each device. Then, the attackers repeatedly send fake Wi-Fi packets to each device, locating them through time-of-flight measurement. The experiments demonstrate that the proposed approach can accurately locate Wi-Fi devices in various indoor locations with reasonable errors.

Strength and Weakness

Strength:

1. The paper highlights a significant design flaw in the 802.11 protocol, indicating that devices respond to fake beacon frames and Wi-Fi packets without undergoing proper verifications.

2. The proposed approach is highly practical, as it can be executed in a matter of minutes and doesn't require expensive specialized hardware.

3. The paper presents preliminary experiments that showcase the feasibility of utilizing time-of-flight measurement to locate Wi-Fi devices.

Weakness:

1. The proposed method relies on GPS to determine self-location, which limits its application to environments with GPS availability.

2. The proposed method assumes that the device's position is relatively static, which restricts its potential use cases.

3. The paper should include experimental results demonstrating the ability to locate multiple devices simultaneously. This scenario is common in the real world.

Questions

1. The author proposes using randomized SIFS time to defend against time-of-flight measurement attacks. However, would the suggested defense still be effective if we were to model the SIFS time as a uniform random number?

2. Would the proposed approach remain effective even if the device undergoes significant positional changes, such as moving from one end of a long hallway to the other?

Conclusion

The authors proposed a practical method for revealing the locations of Wi-Fi devices using low-cost hardware and a straightforward technique, thereby bringing attention to a potential security threat in the current 802.11 Wi-Fi protocol.