Poster: LAPWiN: Location-Aided Probing in Wi-Fi Networks

Yu Seung Kim (Student), Yuan Tian (Student), Le T. Nguyen (Student), and Patrick Tague (Faculty)
Carnegie Mellon University

***Abstract*—Reckless Wi-Fi probing is becoming a serious threat as diverse Wi-Fi based services emerge for mobile devices. An attacker, for instance, can observe the list of previously associated Wi-Fi access points (APs) in the user's Wi-Fi device without efforts, and exploit the information for launching fake AP attack, revealing hidden APs, or profiling users. In this work, we propose a novel Wi-Fi probing mechanism (*LAPWiN*), which is based on the current location of device and show how it can mitigate the possible threats.**

I. Introduction

Recently diverse services over widely deployed Wi-Fi networks are rapidly emerging. Wi-Fi users, for instance, can easily locate themselves even indoor without GPS by using the position stored by a location service provider [1]. Even the Wi-Fi network infrastructure is now able to track users' locations by checking the Wi-Fi signal from their devices observed at the nearby access points (APs) in real time, and this can be used for providing location-based target marketing to resale business or surveillance system to building managers [2]. Most of these services rely on the traces leaked from Wi-Fi devices, which are supposed to be exchanged with other devices for initiating connections. Although varying with each vendor's implementation, many modern Wi-Fi enabled mobile devices emit these traces even in the sleep mode, not recognized by users. Most of these traces are categorized as management frames in Wi-Fi protocol standard [3] and they are exchanged in plain text over the air. Because these traces are used in very initial stage of association, they are not encrypted by the management frame protection [4].

In this work, we found that the information easily collected from any Wi-Fi devices without efforts can be significantly harmful when used by malicious parties. We focus on the scanning procedure of Wi-Fi device for searching the accessible APs nearby. The Wi-Fi scan procedure is largely divided into passive scan and active scan. In passive scan, a Wi-Fi device waits and listens to the channel until it hears any beacon frames sent by nearby APs during a specified period. This procedure continues by changing the listening channel and finishes when the device scans all channels in the given frequency range. In each channel, the scanning Wi-Fi device waits for at least the beacon interval of APs, thus usually taking a long time to finish the scan procedure. Many commodity Wi-Fi devices accordingly implement the faster scanning method, which is known as active scan. A Wi-Fi device broadcasts probe request frames over the wireless channel and expects a response from the surrounding APs. Due to the transmitting operation, active scan requires more energy to be spent, but it reduces the connection time in return. The sent probe request frames include the service set identification (SSID) of previously associated APs in order to automate the association process with the APs.

The SSID of APs previously associated with the user's Wi-Fi device, however, is critical information, which can be exploited by an attacker. Many Wi-Fi connection management software check only the SSIDs of AP to connect with, and an attacker can therefore easily set up a fake AP using the identical SSID with which the user's device has ever associated, impersonating the legitimate APs [5]. Observing this SSID information in the probe request frames can also be one of easy methods for an attacker to reveal hidden APs which are intended to not publicize its SSID. In addition, many SSIDs of public APs contain the identifiable location names, enabling an attacker to infer the user's visited places in the past as shown in Fig. 1. An attacker will be able to correlate other information with user's visited places for user profiling, thus resulting in a serious privacy breach.

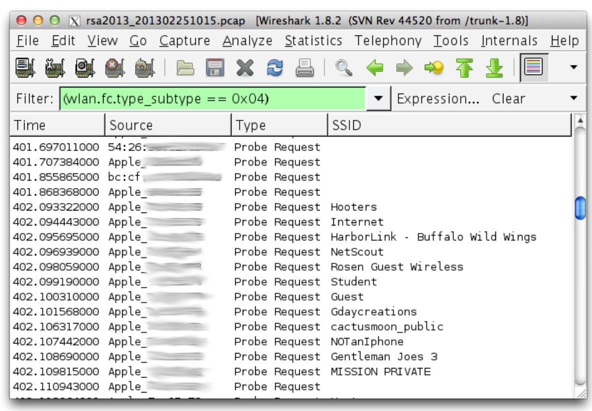


Fig. 1: Frames captured at RSAConference 2013 show anonymous user's previously connected APs, implicitly enabling an attacker to infer user's visited places.

In this work, we propose the *location-aided probing in Wi-Fi networks (LAPWiN)* to prevent the reckless probing which causes the aforementioned privacy issues. LAPWiN sends the probe request frames of only nearby APs, hence it minimizes the exposure of information about the previously connected APs with the user's device. Moreover, LAPWiN broadcasts the smaller number of probe requests at each channel, and thus it is even faster than the original active scanning method. Namely, both **privacy** and **efficiency** are leveraged by LAPWiN. We summarize the advantages of LAPWiN as follows.

- LAPWiN provides both improved privacy and faster scanning performance by minimizing the exposure of AP list in user's Wi-Fi device.
- LAPWiN requires modification only in the Wi-Fi client side, thus making the deployment of our method practical.
- LAPWiN supports Wi-Fi clients with and without positioning auxiliary such as GPS.

We implement LAPWiN with *wpa_supplicant* [6], which is an open source network connection manager used in Linux-based platforms and evaluate its performance by comparing to the original scanning methods.

II. Defenses against Reckless Wi-Fi Probing

A. Legacy approach

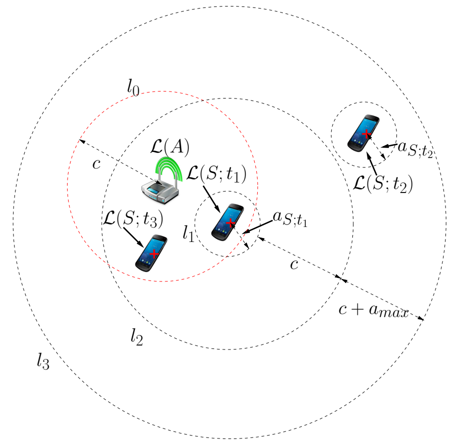
The user's privacy may be protected by using a temporal pseudonym instead of the real MAC address of the user's device during the scanning procedure, although this cannot help the user prevent the fake AP attack or reveal the SSID of hidden APs. The scanning procedure, however, also happens even after the connection is established to find back-up APs used in case of failure in current network, and thus the user's device will be eventually identified. Lindqvist *et al.* [7] proposed the idea of encrypting the frames during AP discovery and association, but it requires a significant amount of modification in the current protocol at both Wi-Fi clients and Wi-Fi APs and fundamentally premises that the encryption key is securely managed.

B. Location-aided probing in Wi-Fi Networks: LAPWiN

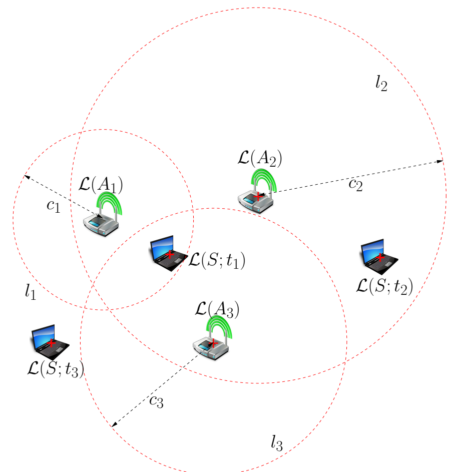
Instead of probing with all associated APs stored in the local storage, Wi-Fi devices supported by LAPWiN check the proximity of each associated AP with the current location. Since LAPWiN broadcasts only probe requests which are relevant to the current location, it reduces the attacker's chance to exploit the user's SSID information. Fig. 2 depicts how LAPWiN devices detect the proximity of AP and probe with only SSID of relevant APs. The two versions of LAPWiN support GPS-enabled devices and non-GPS devices, respectively.

As shown in Fig. 2(a), if the Wi-Fi client S is able to get the GPS coordinate, it stores the information of the associated AP A with its current location $\mathcal{L}(S;t_1)$ and the accuracy $a_{S;t_1}$ at the time t_1 in the device's local storage. Since S does not know the location $\mathcal{L}(A)$ of A, the possible location of A is estimated by using the maximum hearing distance c between A and S, which is generally a few hundreds meters. When S visits this area again and tries to connect to A at the time t_3, it probes with the SSID of A if the condition $d\big(\mathcal{L}(S;t_1),\mathcal{L}(S;t_3)\big) < a_{S;t_1} + 2c + a_{max}$ is satisfied, where $d(x,y)$ is the Euclidean distance between x and y, a_{max} is the maximum accuracy. If S locates at $\mathcal{L}(S;t_2)$, S will try to probe A although it is beyond the wireless coverage l_0 of A. This unnecessary probe will happen in the area between the boundaries of l_0 and l_3. However, the size of this area can be reduced by fine tuning the parameters such as c and a_{max}.

If GPS is not available in S, it uses the Wi-Fi signature of neighboring APs as in Fig. 2(b). At $\mathcal{L}(S;t_1)$, S connects to A_2 and also hears the beacons of neighbor AP A_1 and A_3. The SSIDs of these neighbors are stored together with A_2 in the local storage, and used as references of proximity testing. For example, when S locates at $\mathcal{L}(S;t_2)$, it probes with A_1, A_2, and A_3. In contrast, S does not probe with any of these APs at $\mathcal{L}(S;t_3)$ since it cannot hear any beacons of these APs.



(a) GPS-based probing: a Wi-Fi station is capable of getting GPS coordinate.



(b) Wi-Fi signature based probing: a Wi-Fi station cannot determine its current location without an Internet connection.

Fig. 2: We illustrate the operation of the two different location-aided probing mechanisms.

References

[1] Skyhook. [Online]. Available: http://www.skyhookwireless.com

[2] Cisco mobility service engine. [Online]. Available: http://www.cisco.com/en/US/products/ps9742/index.html

[3] *IEEE Std 802.11-2012, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society Std.

[4] *IEEE Std 802.11w-2009, Amendment 4: Protected Management Frames*, IEEE Computer Society Std.

[5] WLAN Karma Attack. [Online]. Available: https://www.hacking-lab.com/cases/5034-wlan-karma-attack/index.html

[6] Linux WPA/WPA2/IEEE 802.1X Supplicant. [Online]. Available: http://hostap.epitest.fi/wpa_supplicant/

[7] J. Lindqvist, T. Aura, G. Danezis, T. Koponen, A. Myllyniemi, J. Mäki, and M. Roe, "Privacy-preserving 802.11 access-point discovery," in *Proceedings of the second ACM conference on Wireless network security*, ser. WiSec '09. New York, NY, USA: ACM, 2009, pp. 123–130. [Online]. Available: http://doi.acm.org/10.1145/1514274.1514293