POSTER: WLAN Device Fingerprinting using Channel State Information (CSI)

Florian Adamsky
SnT, University of Luxembourg
florian.adamsky@uni.lu

Tatiana Retunskaia
CSC, University of Luxembourg
tatiana.retunskaia.001@student.uni.lu

Stefan Schiffner
SnT, University of Luxembourg
stefan.schiffner@uni.lu

Christian Köbel
Honda R&D Europe
christian_koebel@de.hrdeu.com

Thomas Engel
SnT, University of Luxembourg
thomas.engel@uni.lu

ABSTRACT

As of IEEE 802.11n, a wireless Network Interface Card (NIC) uses Channel State Information (CSI) to optimize the transmission over multiple antennas. CSI contain radio-metrics such as amplitude and phase. Due to scattering during hardware production these metrics exhibit unique properties. Since these information are transmitted unencrypted, they can be captured by a passive observer. We show that these information can be used to create a unique fingerprint of a wireless device, based on as little as 100 CSI packets per device collected with an off-the-shelf Wi-Fi card. For our proof of concept we captured data from seven smartphones including two identical models. We were able to identify more than 90% when using out-of-the-box Random Forrest (RF).

1 INTRODUCTION

Smart devices, such as smartphones or smartwatches, are our constant companion and most of them have wireless LAN (WLAN) integrated. There is an ongoing research effort to collect information from a WLAN device to generate a unique fingerprint. In the security arms race, a unique device fingerprint of a smart device can be used on both sides. On the one hand, it can be used as a security mechanism to authenticate a device or a person. On the other hand, it can be used to track devices and therefore invade user's privacy.

Starting from IEEE 802.11n, WLAN has support for Multiple Input, Multiple Output (MIMO), which allows to receive and to send information over multiple antennas. To optimize the transmission over multiple antennas and to adapt it to current channel conditions, IEEE 802.11n uses physical information about the wireless signal (CSI).

In this work, we show our preliminary results to create a unique fingerprint with RF based on CSI. These CSI can be obtained by a passive observer. There is no need to be associated with the smartphone.

2 EXPERIMENTAL RESULTS

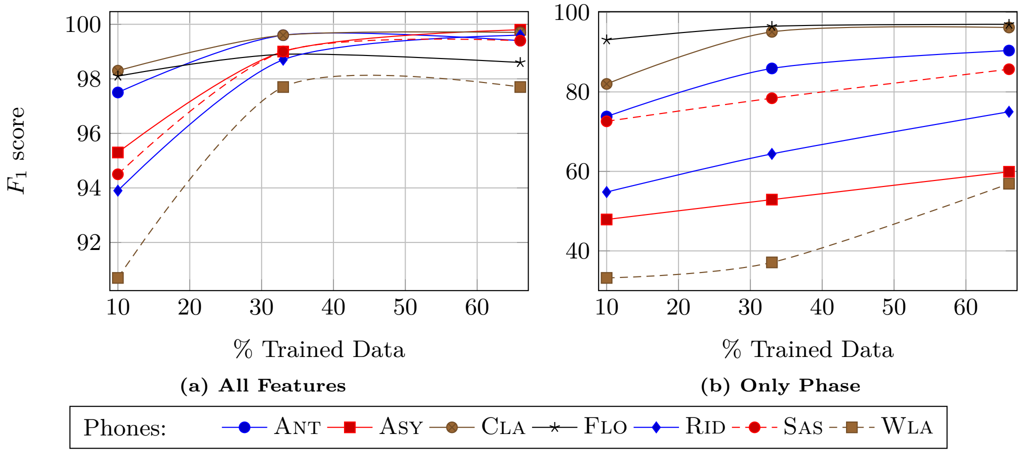
Every wireless NIC that supports IEEE 802.11n measures and receives CSI. Thus our experiments can be translated to any standard hardware. For mere convenience, we used a *Intel 5300* NIC, since there is a modified firmware and driver available to extract the CSI easily, cf. [1]. The CSI contain the hardware timestamp, frame counter, number of receiving antenna, number of sending antennas, Received Signal Strength Indication (RSSI) of each antenna, noise, Automatic Gain Control (AGC), permutation matrix, rate, and the amplitude and phase for the first 30 subcarries in form of complex matrix. We have captured the CSI with 1000 ICMP echo replies from seven smartphones, including two identical models, which are listed in Table 1.

Table 1: List of our tested smartphones.

Abbreviation	Brand of Smartphone	Operation System
ANT	Asus Zenphone	Android 5.0
ASY	Huawei P8 Lite	Android 6.0
CLA	LG G5	Android 7.0
FLO	LG G5	Android 7.0
RID	Samsung S8	Android 7.0
SAS	Nexus 6P	Android 8.1
WLA	Huawei Honor 8	Android 7.0

After we have obtained the data and converted it to format that *Weka* can process, we used the machine learning algorithm RF to distinguish all phones. In our experiment, we trained our model with 10%, 33%, and 66% of the data and validated it with the rest. In the first experiment, we used all features that are available from CSI. In the second one, we only used the phase, to investigate if the phase could be enough to distinguish the devices. Phase-based unique properties are most probably independent from current channel conditions and are hard to forge. Our results can be seen in Figure 1.

As can be seen from the Figure 1, the F_1 score is increasing with the increase of the percentage split. When 10% of the data set is used for training, an average F_1 score is 95,4% (all features) and 65,3% (phase only). With the increase of the split up to 33%, the results become better: 98,9% (all features) and 72,9% (phase only). The best results were achieved at the percentage split of 66%: 99,2% (all features) and 80,2% (phase only). In all the cases, the F_1 score was always higher than 65%.



(a) All Features

(b) Only Phase

Figure 1: Each line represents F_1 score for a separate phone at three experiments different in percentage split of data set (10%, 33% and 66% of data set used for the training phase). (a) All features taken into consideration. (b) Only phase of signal is taken into consideration.

3 RELATED WORK

Most studies [4–6] are using CSI for indoor localisation. A work from H.Liu et al. [2] investigated the use of CSI for constructing device profiles. They proposed a framework consisting of two main components: attack-resilient profile builder and profile matching authenticator. The latter employs machine learning techniques to perform per-packet user authentication using CSI. In their work, they showed that it is feasible to perform user authentication by utilizing CSI from Orthogonal Frequency-Division Multiplexing (OFDM). Compared to our work, they only tested two devices. Another study [3] has used information from the data link layer such as the information elements in probe requests to create a unique device fingerprint.

4 FUTURE WORK & CONCLUSION

In this preliminary qualitative study, we demonstrated CSI fingerprints are likely unique. With only 100 data points per device, we were able to distinguish seven phones including two identical models with an F_1 score above 91%. This indicates that we might leverage these fingerprints for attacks on privacy and to implement new security features. For future work we plan to investigate if we can confirm our findings for a larger number of devices, and which features of the CSI are contributing to the disambiguation.

Moreover, we want to investigate if our findings can by applied in two scenarios, namely to perform privacy attacks and to leverage these fingerprint as secondary security feature. Particularly for the privacy attack, it would be interesting to know if fingerprints can be generalized from the observation environment and observation equipment. For the security feature, we would need to know in addition if these features are intrinsic to the production process and hard to duplicate and if these features can be used in cryptographic protocols for proof of possession.

ACKNOWLEDGEMENT

This work was funded by the Honda Initiation Grant Europe 2018.

REFERENCES

[1] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool Release: Gathering 802.11n Traces with Channel State Information. *ACM SIGCOMM Computer Communication Review* 41, 1 (01 2011), 53.

[2] H.Liu, Y.Wang, J.Liu, J.Yang, and Y.Cheng. 2014. Practical User Authentication Leveraging Channel State Information (CSI). In *Proceedings of the 9th ACM symposium on Information, computer and communications security*. 389–400. https://doi.org/10.1145/2590296.2590321

[3] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. 2016. Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS '16)*. 413–424. https://doi.org/10.1145/2897845.2897883

[4] Deepak Vasisht, Swarun Kumar, and Dina Katabi. 2016. Decimeter-Level Localization with a Single WiFi Access Point. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX Association, Santa Clara, CA, 165–178. https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/vasisht

[5] X. Wang, L. Gao, S. Mao, and S. Pandey. 2015. DeepFi: Deep learning for indoor fingerprinting using channel state information. *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*. https://doi.org/10.1109/WCNC.2015.7127718

[6] J. Xiao, K. Wu, Y. Yi, L. Wang, and L. M. Ni. 2013. Pilot: Passive Device-Free Indoor Localization Using Channel State Information. *2013 IEEE 33rd International Conference on Distributed Computing Systems*. https://doi.org/10.1109/ICDCS.2013.49