Poster Abstract: Practical Limits of WiFi Time-of-Flight Echo Techniques

Theodoros Bourchas
ETH Zürich
Switzerland
bourchat@student.ethz.ch

Maciej Bednarek
ETH Zürich
Switzerland
maciejb@student.ethz.ch

Domenico Giustiniano
Institute IMDEA Networks
Madrid, Spain
domenico.giustiniano@imdea.org

Vincent Lenders
Armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

***Abstract*—Time-of-flight echo techniques have been proposed to estimate the distance between a local and a target station over regular WiFi radio devices. Their current main shortcoming is that they are affected by severe noise components at both stations. Our aim in this work is to quantify the noise level introduced by the target in order to derive practical limits of the ranging accuracy achievable using off-the-shelf devices. For this purpose, we develop a low-noise experimental platform which allows us to measure the echo-reply delay with very high accuracy. Our preliminary results with two popular chipsets from different manufacturers show that the median echo-reply delay at the target is never equal to the nominal SIFS value, and it deviates by approximately $10-20$ ns over time, suggesting a practical ranging accuracy limit of 3 m.**

***Index Terms*—WiFi, Time-of-Flight, Localization, Measurements**

I. Introduction

WiFi-based positioning systems have achieved wide commercial success to complement GPS, despite being proved to be error-prone and offering limited performance figures [1], [2]. In order to alleviate this problem, solutions such as [3], [4] have proposed to use the time-of-flight (ToF) principle to devise echo techniques that leverage the existing 802.11 protocol. While previous studies have shown that WiFi-based echo techniques can provide meter accuracy localization despite this noise, the impact of different sources of noise have not yet been investigated in detail. In this work, we aim at quantifying the noise that the target station introduces while responding to echo requests. For this purpose we have developed a low-noise high-precision experimental setup which allows us to isolate the target's noise and hence derive practical limits of WiFi-based ToF echo techniques.

II. WiFi ToF Localization

While traditional echo techniques like radar systems are based on uncoded RF signals and their reflections, WiFi echo techniques use regular frames of communication. The most recent and promising approaches in the field rely on regular 802.11 DATA frames for the echo requests and on ACK control frames for the echo replies [3], [5]. Generally speaking, these techniques work as visualized in Fig. 1. A local station measures the time $t_{MEAS}(d)$ elapsing from the instant that the DATA frame has been transmitted to the instant that the ACK has been received:

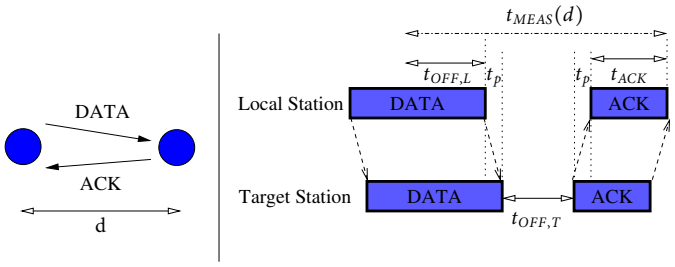

Fig. 1. WiFi ToF echo technique using regular communication frames. $t_{OFF,T}$ is originated at the target station, and it depends on the 802.11 SIFS.

$$t_{MEAS}(d) = 2 * t_P(d) + t_{ACK} + t_{OFF,L} + t_{OFF,T},$$

where $t_P(d)$ is the signal propagation time between the local and target stations, t_{ACK} indicates the duration of the ACK frame, $t_{OFF,L}$ is an offset caused by H/W and S/W processing delays at the local station, and $t_{OFF,T}$ an offset caused by the H/W delay at the target station. The focus of this work is to investigate the noise introduced by the target offset $t_{OFF,T}$. The 802.11b/g standards mandate the time between DATA and ACK frames to be fixed (MAC SIFS - Short InterFrame Space - interval) and equal to 10 μs. However a relatively high tolerance of 1 μs is specified which would result in a distance estimation error of 300 meters if the target would fully exploit this tolerance level.

III. Experimental Platform

We present the measurement system that we have developed to measure $t_{OFF,T}$ with high precision in Fig. 2. This setup allows us to measure the channel occupancy caused by DATA and ACK traffic over-the-air at below nanosecond precision. Our traffic monitoring is based on an Infiniium 90000A Oscilloscope with a fast sampling rate of 10 GS/s. A horn antenna is connected to the oscilloscope which serves as a passband filter for the 2.4 GHz band. The target station is in close proximity of the horn antenna, so that its radio signals are immediately captured by the oscilloscope, and effects of signal reflections are minimized. We place the local station and the target station at one meter of distance and send ICMP ping from the local to the target station. Simultaneously, the oscilloscope, through a python script, captures traces at a fixed time interval and

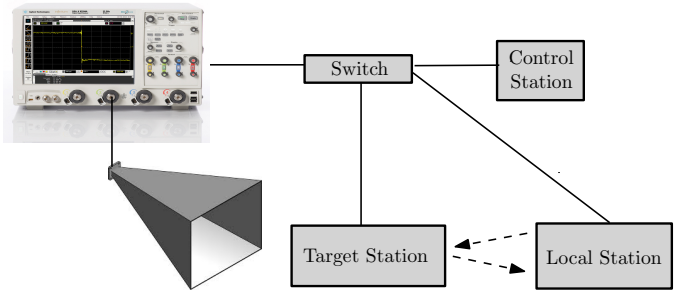

Fig. 2. Experimental setup to investigate the offset of WiFi ToF generated at the target station ($t_{OFF,T}$).

stores them in the control station's hard disk. The probability of capturing traces with the corresponding SIFS intervals increases with the buffer size of the oscilloscope. However an increased buffer size implies bigger files to store and longer time for the conversion into raw data. We reach a good trade-off collecting traces of 5 ms (50 MB buffersize). Once the traces are collected, we downsample them by a factor of five to 2 GS/s in order to reduce the computational burden of the processing. 2 GS/s corresponds to one sample every 0.5 ns which still allows us to quantify $t_{OFF,T}$ at below nanosecond precision. An example trace is shown in Fig. 3, where we use 802.11g Atheros Soekris as target station.

A. *Inferring the remote offset.*

The target offset analysis is conducted based on the raw samples from the oscilloscope. We discriminate traffic sent by the target station from the one at the local station by monitoring the power level of our traces. In this way, we only process the idle time when ACKs are generated by the target station (see Fig. 3). We then convert the raw samples into busy and idle channel states. The conversion should be robust against any false detection of state change, due to spikes of noise, which would affect our results. We apply a Schmitt trigger filter over smoothed samples with exponential weighted moving average and forgetting factor equal to 0.9. In order to have a common baseline, we apply the same high threshold for the Schmitt trigger, 1.5 dB over the noise (low) threshold,

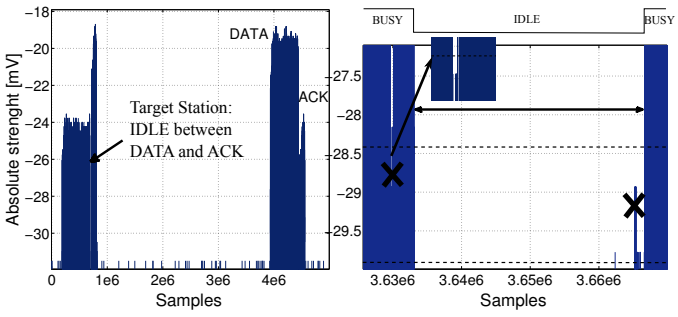

Fig. 3. Two traces gathered with the oscilloscope. Figure on the left: the local station sends ping echo request. Figure on the right: Schmitt trigger's performance, which avoids false detections of busy and idle state (indicated with crosses in the figure).

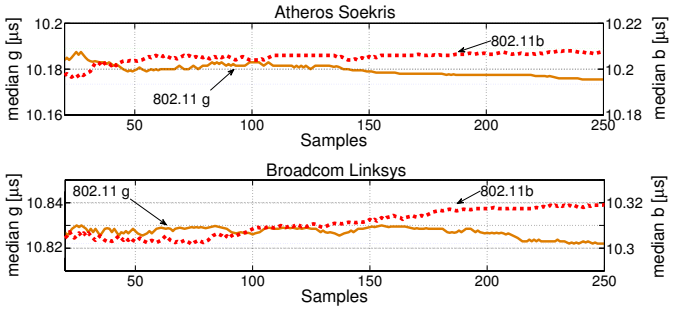

Fig. 4. Evolution of the median of $t_{OFF,T}$ for two different target stations. Median b (median g) indicates the median for 802.11b (802.11g). The values reported are never equal to the nominal 10 μs. The median deviates by 10−20 ns with respect to the initial estimation.

for all the tests. We then derive the delimiters of the busy-to-idle and idle-to-busy transitions. We subtract a value of 6 μs (called signal extension) to our 802.11g traces to convert idle time over-the-air into MAC SIFS. We finally derive the remote offset $t_{OFF,T}$.

IV. Preliminary Results and Conclusions

Figure 4 displays the evolution of the median target offset $t_{OFF,T}$ for two different types of stations, a device from Soekris with an AR9220 Atheros WiFi chipset and a device from Linksys with a BCM4318 Broadcom chipset, both operating in 802.11b and 802.11g modes. The values reported are never equal to 10 μs. In addition, the value reported after a few samples for the four scenarios differs from the one measured over several samples by approximately 10 – 20 ns. These variations would affect by up to 3 meters the median accuracy of the WiFi echo technique, when small number of samples are collected. This can be regarded as a practical limit of WiFi ToF echo techniques that rely on the SIFS interval.

Acknowledgments

We thank Prof. Dr. Srdjan Capkun and Mr. Aanjhan Ranganathan from ETH Zurich for letting us accessing their lab and have access to the Infiniium 90000A oscilloscope.

References

[1] M. Youssef and A. Agrawala, "The Horus WLAN location determination system," in *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '05. New York, NY, USA: ACM, 2005, pp. 205–218.

[2] A. Rai, K. K. Chintalapudi, V. N. Padmanabhan, and R. Sen, "Zee: Zero-effort crowdsourcing for indoor localization," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, ser. Mobicom '12. New York, NY, USA: ACM, 2012, pp. 293–304.

[3] D. Giustiniano and S. Mangold, "CAESAR: carrier sense-based ranging in off-the-shelf 802.11 wireless LAN," in *Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies*. ACM, 2011, p. 10.

[4] M. Ciurana, F. Barcelo-Arroyo, and F. Izquierdo, "A ranging system with ieee 802.11 data frames," in *Radio and Wireless Symposium, 2007 IEEE*, 2007, pp. 133–136.

[5] P. Gallo, D. Garlisi, F. Giuliano, F. Gringoli, and I. Tinnirello, "WMPS: A positioning system for localizing legacy 802.11 devices," in *Transactions on Smart Processing and Computing,*, October 2012.