# Sniffing IEEE 802.11 Mobility

Thomas Claveirole, Marcelo Dias de Amorim, and Serge Fdida

Université Pierre et Marie Curie – Paris 6
{claveiro,amorim,fdida}@rp.lip6.fr

**Abstract.** Portable computing devices have transformed mobility into a serious concern to network researchers. Existing mobility measurement data have been very useful to the community, but achieve their limitations because they apply only to specific contexts (*e.g.* university campuses and conference venues). This paper advocates using Wi-Fi sniffing to study mobility in other environments. This approach is interesting because of its non-intrusiveness: it does not require access to any networking infrastructure nor active participation from users. This is a realistic approach due to the recent proliferation of Wi-Fi devices. This paper also suggests techniques to extract mobility data from raw sniffer traces.

## 1 Introduction

There is a current trend in the proliferation of wireless-capable portable devices. Among the different low-level protocols that enable mobile communications, IEEE 802.11 plays a major role: it is now available on PDA's, smart phones, portable music players, even some digital cameras!

This mean mobility is both a *legitimate* and *increasing* concern in networking. This strengthen the need for a better understanding of users' mobility patterns. There is currently serious issues regarding the validity of existing mobility models. It is also unclear what characteristics a mobility model should depict.

That has yield a prolific amount of research [1, 2]. But measurements have always been done in specific environments so far (that is, in a university campus or during conferences). It would be interesting to validate the existing results in other environments. Yet, doing this is difficult. One cannot always access the network infrastructure, especially when the area to study is covered by several independent networks. And giving mobility measurement devices to many users appears unrealistic in some contexts.

In order to measure mobility in a wider range of settings, this article suggests to use wireless sniffing. Taking advantage of Wi-Fi devices proliferation, one can passively record mobility data without equipping users with special devices or modifying existing networks. This forms a seducing characteristic which previous measurement methods lack in order to be easily generalizable. Using wireless sniffing, a set of monitors (or sniffers) listens to the radio medium, recording every frame exchange at the MAC level. This operation is completely passive and does not interfere in any way with the network's normal operation. Then it is possible to infer mobility data from the recorded traces.

## 2 Background

Two techniques have been used so far to study mobility: querying the network infrastructure and equipping a set of volunteers with special devices.

**Querying the network infrastructure.** This straightforward method consists of extracting data from logs provided by access points or other devices located inside the network (Syslog, SNMP, etc.). With minimum efforts, one can extract data from large geographic area (*e.g.* a campus) for long periods of time (*e.g.* months). On the other hand, this provides generally limited information (*e.g.* access point association sequences) and focus only on one network in the studied area. This is an issue when the area to study is covered by several independent networks, or when it is not possible to access the network infrastructure.

**Equipping a set of volunteers with special devices.** This method consists of giving to volunteers dedicated devices that will measure mobility. This method is interesting because each device works continuously and does not rely on users switching their laptops or PDA's on. It is unlikely however such experiments are tractable for long periods of time or at large scales. Typically, experiments concern a few dozen protagonists for a few days.

## 3 Wireless sniffing and mobility

Using wireless sniffing would provide interesting features the two previous techniques do not offer. This technique being completely passive it becomes possible to study environments where accessing the network infrastructure is not feasible. Also, this is a global technique: inside the coverage area, it records mobility from every users among all networks. To the extent of our knowledge, nobody ever used wireless sniffing to study mobility.

Basically wireless sniffing consists of spreading several wireless monitors across a coverage area. Each monitor *passively* sniffs the radio medium [3, 4]. It records raw IEEE 802.11 frames as reported by network interfaces. Each recorded frame is also augmented with a physical header containing information such as signal strength, data rate, etc. Usually each individual monitor is equipped with at least three radios (*i.e.* network interfaces) in order to scan all available IEEE 802.11 channels. Each radio produces a trace. Therefore each monitor produces several traces, each one being a sequence of frames (PHY + IEEE 802.11). Since each monitor only has a local view of the network, traces from monitors are then merged into a unique global trace.

As traces just include raw frame sequences, one must analyzes them in order to reconstruct mobility. As an example, such processing may consist of computing some virtual coordinates from traces. Such an analysis may rely solely on the content of MAC frames, or it may benefit from the geographic spreading of monitors. Here are some suggestions on how to perform such analyses.

**Access point association sequences.** Previous works almost always use access point association sequences as IEEE 802.11 mobility data [1]. It is indeed possible to extract this information from passive listening.

**Signal strength.** Some positioning systems use IEEE 802.11 signal strength in order to localize users [5]. This article suggest doing a similar operation: compute user locations from their received signal strength at monitors.

**IEEE 802.11 probes analysis.** Another technique might be to extract mobility data from sniffer traces by analyzing IEEE 802.11 probe traffic. This has the advantage of detecting movements despite clients not switching their access points (or even not associating).

One may also envision other techniques to analyze mobility from wireless sniffing. As an example, one might try to model and infer inter-contact times from traces. This may provide a relevant metric for mobility.

## 4 Conclusion

Finding relevant parameters to provide accurate simulations and realistic mobility models is an open issue. This article suggest using wireless sniffing as a powerful technique to extract such parameters. One of its principal advantage is its non-intrusiveness: it allows studying settings where relying on users or network infrastructures is not possible. This paper advocates on using wireless sniffing in open environments to study user mobility. It suggests several techniques to extract mobility data from traces.

Wireless sniffing may also have other usages with regard to network measurements than just mobility. Many other parameters could be measured in order to validate simulation models: frame sizes, inter-arrival times, etc. The main interest of having this completely passive technique is the ability to study any network, not just research labs, conference venues or university campuses.

## References


[1] Kim, M., Kotz, D., Kim, S.: Extracting a mobility model from real user traces. In: INFOCOM'06, Barcelona, Spain (April 2006)

[2] Chaintreau, A., Hui, P., Crowcroft, J., Diot, C., Gass, R., Scott, J.: Impact of human mobility on the design of opportunistic forwarding algorithms. In: INFOCOM'06, Barcelona, Spain (April 2006)

[3] Mahajan, R., Rodrig, M., Wetherall, D., Zahorjan, J.: Analyzing the mac-level behavior of wireless networks in the wild. In: SIGCOMM'06, Pisa, Italy (September 2006) 75–86

[4] Cheng, Y.C., Bellardo, J., Benkö, P., Snoeren, A.C., Voelker, G.M., Savage, S.: Jigsaw: solving the puzzle of enterprise 802.11 analysis. In: SIGCOMM'06, Pisa, Italy (September 2006) 39–50

[5] King, T., Kopf, S., Haenselmann, T., Lubberger, C., Effelsberg, W.: COMPASS: A probabilistic indoor positioning system based on 802.11 and digital compasses. In: WiNTECH'06, Los Angeles, CA, USA (September 2006)