Opportunistic Scanning: Interruption-Free Network Topology Discovery for Wireless Mesh Networks

Marc Emmelmann, Sven Wiethoelter, and Hyung-Taek Lim *
Technical University Berlin
Telecommunication Networks Group TKN
Berlin, Germany
emmelmann@ieee.org, {wiethoel, lim}@tkn.tu-berlin.de

Abstract

This paper presents the concept and preliminary performance evaluation of a stochastic network discovery approach named opportunistic scanning. *Therein, a station only pauses its communication for an extremely short time interval to scan for other technologies / systems. The selected scanning duration is short enough not to be noticeable by higher layer applications. We place this concept into the 802.11 mesh network context and evaluate 802.11 power saving as one possible signaling protocol used to pause the communication between the scanning station and its interlocutor. We herein derive the theoretical performance limits of opportunistic scanning in combination with 802.11 power save and present first results classifying the time required to find a neighboring technology / system at a given probability.*

1 Introduction

Thousands of cities worldwide have deployed large-scale 802.11 networks employing a multi-level tier including a "mesh backhaul" to extend the networks' coverage. As compared to traditional wireless network architectures, such networks only feature a limited number of high capacity injection points connecting the mesh backhaul to the (wired) internet. In such an architecture, appropriate link selection schemes are required to optimally assign end-users (and their traffic) to access points in their vicinity or even distribute traffic among various links between adjacent mesh points. Additionally, if commercial operators should increasingly favor such architectures, the latter have to guarantee QoS even for mobile users in consequence requiring low handover latencies.

In order to reevaluate the link selection periodically, end-users as well as mesh points forming the wireless backbone have principally two basic options: either they (continuously) check whether alternative access points / links are available or they rely on certain signaling schemes, which update their neighborhood information accordingly. In this work, we apply the first option since we target at minimizing additional load introduced on the wireless links. Thus, this paper presents an opportunistic scanning scheme which periodically scans for alternative access links while upholding QoS constraints in terms of guaranteeing a maximum inter-arrival time between consecutive user datagrams. In our approach, this strong limitation is achieved as the scanning station leaves its communication channel only for an extremely short time period not affecting the QoS constraints of higher applications. As a result, the dwell time within scanning state is shorter than the beacon interval of other nodes hence making this network discovery approach a stochastic process. Additionally, a signaling protocol pausing any communication between a station and its associated interlocutor is necessary to avoid a loss of packets. As we herein apply the opportunistic scanning scheme to a IEEE 802.11-based mesh network, the most natural choice for such signaling is the power saving feature of 802.11 as "power saving stations" are not required to turn off their interface but may instead use the "doze state" to scan for alternative links.

This paper presents the novel opportunistic scanning concept itself including a preliminary performance evaluation of the opportunistic scanning approach in combination with 802.11 power saving signaling. The novel contributions are

- a detailed usability analysis of the 802.11 power saving method evaluating if this feature enables opportunistic

*The authors would like to thank OPNET Technologies Inc. for providing the simulation environment under the university program. This work was partially supported by European Commission through project EU-MESH (Enhanced, Ubiquitous, and Dependable Broadband Access using MESH Networks), FP7 ICT-215320.

978-1-4244-4439-7/09/$25.00

scanning in a strictly standard compliant way;

- the derivation of the theoretical performance limits for opportunistic scanning considering the smallest achievable service interruption caused by scanning process;
- investigations regarding the requirements for the choice of the scanning frequency; and
- a preliminary performance evaluation revealing how much time opportunistic scanning needs to succeed (at a given probability) in detecting another system.

The remainder of the paper is structured as follows: The following section introduces the system model followed by a description of the opportunistic scanning approach. Apart from presenting the general concept of opportunistic scanning, the latter section analyzes the 802.11 power saving feature in detail. It identifies a barely used but entirely standard compliant signaling flow enabling power save as one possible signaling protocol candidate. The final section on the performance evaluation firstly summarizes the goals of the assessment and thereof derives the underlying usage scenario. Following the metric description, we present the theoretical performance limits of our approach. The paper concludes by sketching related work and summarizing the results and future work.

2 System model

A three-tier architecture describes the system under consideration (c.f. Figure 1). [6] Several mesh points (MPs) may communicate with each other via wireless links formed by either omni-directional or highly directive antennas. These MPs form the *mesh backhaul* acting as a capacity pool for end users. Due to channel characteristics as well as employing directive antenna systems, MPs being geographically located next to each other may not necessarily have a direct communication. A subset of MPs, denoted as *mesh portals* connects the mesh backhaul to the Internet. Mesh portals may have a high capacity wired connection (e.g. via dark fiber or high capacity directive wireless links) if deployed by network operators; but also low capacity DSL links are possible for mesh portals deployed at homes or small and medium enterprises. *Mesh access points* (Mesh APs) form the last tire and provide users access to the mesh backhaul. Mesh APs are herein assumed to support legacy IEEE 802.11 operation including power saving; each Mesh AP forms an infrastructure basic service set and hence announces the latter via beacon transmissions. End user systems are assumed to be equipped with a single IEEE 802.11 network interface card. Also, it should be noted that we do not impose any constraints on the technology used within the mesh backhaul allowing a heterogeneous environment formed, e.g., by IEEE 802.11 and WiMAX.

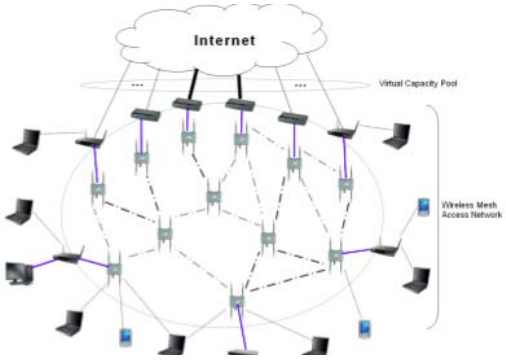


Figure 1. Exemplary System Architecture

3 Opportunistic scanning approach

The design of the scanning approach is driven by three main considerations: Firstly, the scanning procedure should be capable to support even real time traffic with small packet interarrival times and hard QoS constraints which require low packet loss and allow only small extra delay at MAC. VoIP traffic is a typical representative for such pattern (e.g., G.711-coded speech with $10ms$ inter-packet generation time). Secondly, since the opportunistic scanning has to scale with the number of stations applying this approach, we target to introduce no overhead in terms of additional traffic on the target channel being scanned. Finally, a feasible solution in real hardware can be only built upon mechanisms that are standard compliant.

3.1 General Concept

In order to meet hard QoS constraints of real-time traffic, the opportunistic scanning approach only leaves the current communication channel for a very short time to scan other channels for beacons announcing neighboring Mesh APs. Not to affect any ongoing communication, this requires a signaling between the Mesh AP and the associated end system to 'pause' communication. The following sections discuss one possible signaling scheme being entirely compliant to the existing IEEE 802.11 specification employing the power save procedure of the standard. The only difference is that instead of sleeping while in power save mode, the mobile STA discovers the networks topology.

3.2 Signaling of IEEE 802.11 power saving

IEEE 802.11 power saving defines two modes of operation: the 'awake state' (of the station) and the 'doze state'.

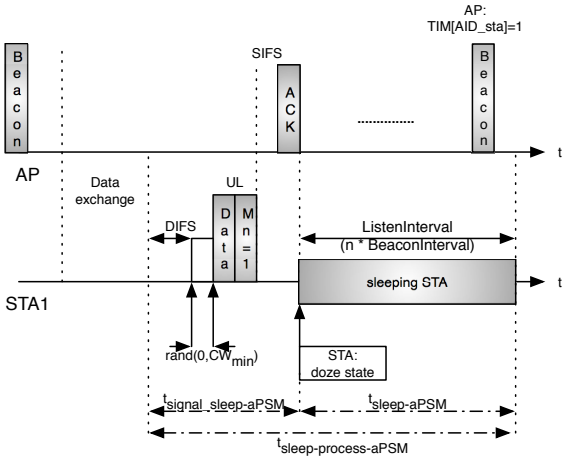


Figure 2. Sleep procedure of PSM-STA

In the former, regular communication between the AP and the station (STA) occurs whereas in the latter, the AP buffers any pending data for the STA–communication is paused.

3.2.1 Sleep procedure

Figure 2 illustrates the frame exchange used by all standard compliant stations to change in 'doze state'. The station has to go through clear channel assessment procedure (CCA) and may then send an uplink data frame in which the power management bit of the frame control field is set to one [1]. The following ACK confirming the reception, the STA may change into 'doze state' and the AP buffers data for the station. Also, the AP indicates pending traffic by setting a corresponding bit in the traffic indication map (TIM) contained in the beacon.

3.2.2 Wake-up procedure

Even though only rarely used, 802.11 power saving stations may change from 'doze' to 'awake' state at any time and signal this state change immediately to the AP. As shown in Fig. 3, the STA has to wait for a given time (t_{wait}) after changing into 'awake state' or has to successfully obtain a current setting for the network allocation vector (NAV). This guarantees that the station does not interfere with any ongoing transmission even physical CCA indicates an idle channel (hidden note problem). Afterwards, the STA competes for channel access and may transmit an uplink data frame indicating its state change in the power management bit of the frame header. The AP in turn indicates if it has any buffered data for the STA using the more data bit in the frame header of the subsequent ACK.[1] Back in 'awake'

[1]Note that the STA may sent a null-data frame if it has no pending uplink data.

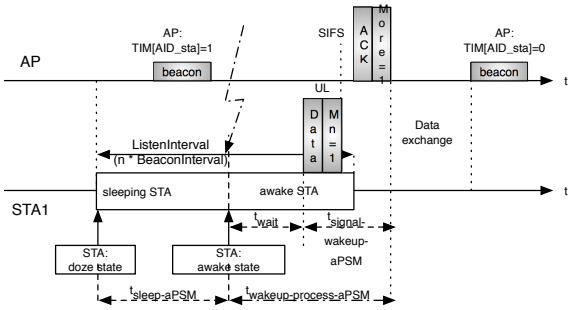


Figure 3. STA initiated wake-up procedure

state, the STA polls buffered data from the AP using the PS-Poll frame [1].

3.3 Employed scanning scheme

As the standard does not require a power saving station to switch off its transceiver chain while in 'doze state', the STA may freely use this time span for network topology discovery. As our goal is to employ only standard compliant protocol approaches, choices are limited to *passive* and *active scanning*. Also, we aim at having minimum assumptions towards the 802.11 infrastructure such as synchronization of beacon transmissions among Mesh APs. Hence a STA employing the opportunistic scanning scheme achieves its superior scanning behavior in any standard compliant 802.11 environment.

The third design consideration targets to avoid additional load at other cells. Though resulting in faster network topology discovery, active scanning would have such an impact. This fact has also been acknowledged by the IEEE 802.11 working group. The most recent amendment for radio resource management (IEEE 802.11k [2]) introduced 'pilot frames': a short version of the beacon which can be frequently transmitted for enhanced passive scanning performance thus supporting passive scanning as the primary topology discovery choice if the impact on the scanned network shall be minimized. Accordingly, the following performance evaluation considers only passive scanning. It is therefore a conservative performance assessment in terms of the time required to discover the mesh network topology.

4 Performance evaluation

4.1 Goals and methodology

We herein aim at classifying the theoretical performance limits of the opportunistic scanning approach. In particular, we intent to answer the following questions:

- How large is the minimum duration just for the whole power save signaling?

- How long does it take to find an existing station at a given probability?

Answering the former quantifies the smallest possible turnaround time from data exchange to scanning and back to data exchange if 802.11 power save is used as the underlying signaling protocol. Hence it is a measure for the *smallest supportable service interval* for user data. The latter in turn assess the *time required* in the overlap of adjacent cells *to successfully complete the topology discovery* under the optimistic assumption that the station scans only one channel on which an alternative Mesh AP is known to be found. Also, these results may also be used to quantify an upper limit after which the opportunistic scanning process should start its topology discovery on a new channel if no station has been found. In the following, we employ analysis to assess these theoretical limits.

4.2 Scenario

We consider two adjacent mesh nodes having an overlapping coverage area. Both mesh nodes un-synchronously transmit beacons to announce their existence at regular time intervals as defined by the 802.11 standard. The analysis considers the opportunistic scanning station being stationary located within the overlap. It is associated with one of the mesh nodes. Apart from the beacon transmissions and communication between the opportunistic scan station with its associated mesh node, the channel is assumed idle.

4.3 Metrics

Our analysis makes use of the following two metrics: power save mode duration and beacon reception probability. The *power save mode duration* defines the time from the beginning of the signaling involved to transition from the 'awake' into the 'doze' and back into the 'awake state'. It quantifies the service interruption imposed on the application due to the opportunistic scanning approach. The *beacon reception probability* quantifies the number of scanning attempts / time required to successfully receive a beacon at a given probability.

4.4 Analytical results for idle channel

4.4.1 Minimum power save duration

Figure 4 illustrates the signaling sequence involved in going from 'awake' into 'doze' and immediately back into 'awake state'. As we do not spend any time in the 'doze state', we are actually not conducting any opportunistic scanning at all. This quantifies the smallest possible duration to switch back and forth between channels. In order to hold a specific

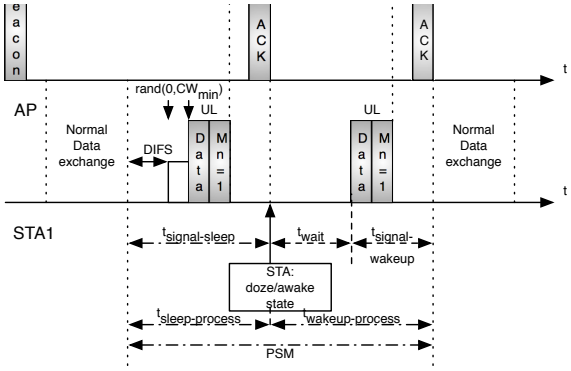


Figure 4. Signaling sequence for minimum PSM duration

QoS constraint, the minimum power save duration represents the lower bound for the inter-arrival time of application data at MAC level.

The minimum time spent in power save mode (t_{minPSM}) is given by

$$t_{minPSM} = t_{signal-sleep} + t_{wait} + \\ + t_{signal-wakeup} \quad (1)$$

where

$$t_{signal-sleep} = t_{DIFS} + rand_{uniform}(0, cw) + \\ + t_{DATA-UL} + t_{SIFS} + t_{ACK}$$

$$t_{wait} = \begin{cases} t_{probeD}, & \text{if channel is idle} \\ t_{busy} + t_{DIFS} + \\ \quad + t_{rand(0,cw)}, & \text{if channel is busy} \end{cases}$$

$$t_{signal-wakeup} = t_{DATA-UL} + t_{SIFS} + t_{ACK}$$

Assuming an idle channel, Equation (1) can be directly simplified into

$$t_{minPSM} = t_{DIFS} + 2 \cdot t_{SIFS} + 2 \cdot t_{DATA-UL} + \\ + 2 \cdot t_{ACK} + t_{probeD} \quad (2)$$

Apart from PHY specific parameters (t_{DIFS}, t_{SIFS}, and t_{probeD}), t_{minPSM} depends on the employed modulation and coding scheme (MCS) for the Data and Acknowledge frame [1]. Figure 5 shows the minimal achievable PSM duration for parameterization and defined MCS for two situations: first assuming that the signaling is transmitted in a Null Data frame, and second, if it is piggy backed in a VoIP data stream packet assuming an underlying G.711 codec and 10 ms packetization without silent suppression. Obviously, the smallest achievable interruption of roughly 1.3 ms occurs for the lowest packet size (Null Data frame) at the highest data rate. But also a 2.6 ms-long interruption at the most robust MCS schemes is acceptable even for

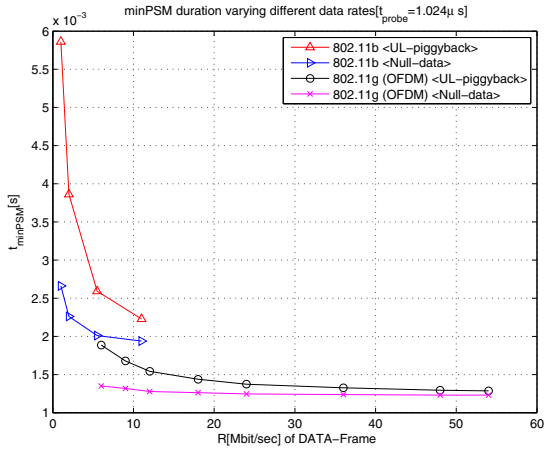


Figure 5. Minimum PSM duration

hard real time services [9]. Also, the theoretical limits show that opportunistic scanning should be a feasible approach not noticeably affecting VoIP applications as service interruption for piggy backed signaling may be reduced to less than 6 ms for the most robust MCS.

4.4.2 Required scan duration

In order to detect a neighboring mesh AP during the $n\text{th}+1$ opportunistic scanning attempt, the beginning of the scanning t_{SS} has to be before the beginning of the beacon reception / start t_{BS} and the end of the scan t_{SE} has to lie after the beacon's end t_{BE} (c.f. Fig. 6):

$$t_{SS} \leq t_{BS} \ \wedge \ t_{BE} \leq t_{SE} \tag{3}$$

Therein,

$$\begin{aligned} t_{SS} &= t_{offset} + n_{scan} \cdot \Delta t_{scan} \\ t_{BS} &= n_{beacon} \cdot \Delta t_{beacon} \\ t_{BE} &= t_{BS} + t_{beacon} \\ t_{SE} &= t_{SS} + t_{scan} \end{aligned}$$

where t_{offset} is a random variable uniformly distributed over $[0, \Delta t_{beacon})$, Δt_{beacon} the target beacon transmission time, Δt_{scan} the scan interval, and t_{scan} the (effective) scan duration remaining after the involved signaling is deducted from the time span given by Δt_{scan}. Equation 3 can accordingly be rewritten into

$$\begin{aligned} & \frac{n_{beacon} \cdot \Delta t_{beacon} - t_{offset}}{\Delta t_{scan}} - \left(\frac{t_{scan} - t_{beacon}}{\Delta t_{scan}} \right) \leq n_{scan} \\ \wedge \quad & n_{scan} \leq \frac{n_{beacon} \cdot \Delta t_{beacon} - t_{offset}}{\Delta t_{scan}} \end{aligned} \tag{4}$$

which gives the condition if beacon number n_{beacon} is successfully received within scan attempt n_{scan}. Solving the latter equation numerically and due to the stochastic nature

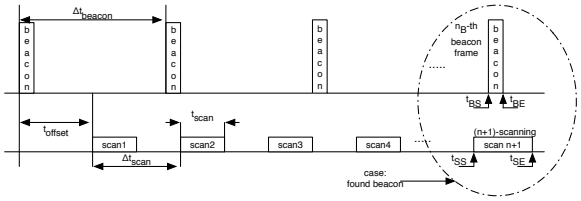


Figure 6. Calculation of the number of scanning attempts (signaling not shown)

of t_{offset} , we obtain the probability functions of detecting a beacon at a given scan attempt / after a given time (c.f. Fig. 7). Obviously, t_{offset} and Δt_{beacon} may not have a common divider to guarantee beacon detection. As we assume that a provider will employ common values with multiples of $10\ ms$ for the target beacon transmission time (e.g., $100\ ms$) we choose prime numbers for Δt_{scan}.

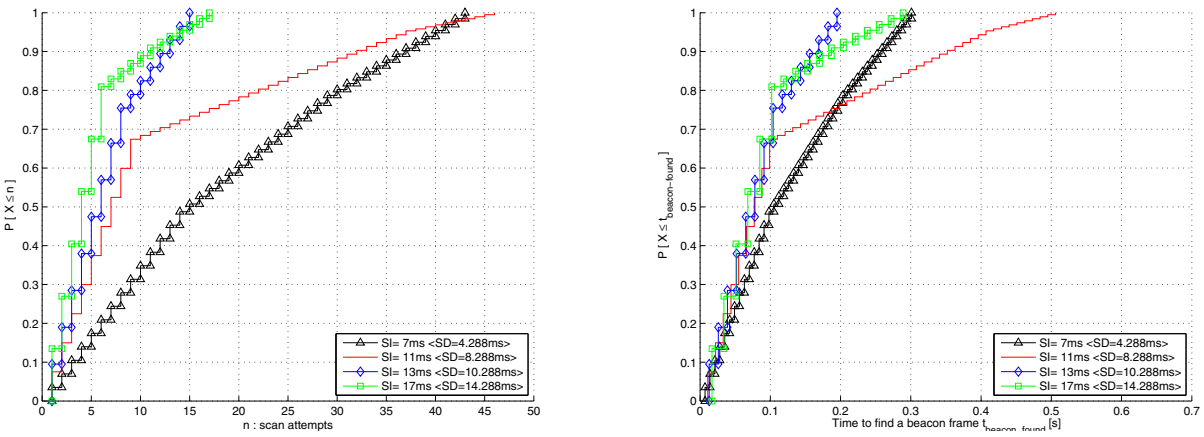
As expected, longer scan intervals yield to better results but interestingly, the effect is less noticeable if one considers the time required to find a beacon as compared to the number of scanning attempt. A topology discovery in two target beacon transmission times (TBTT) is possible. This is only twice the time needed as compared to traditional passive scanning resulting in long service interruptions. But even unsuitable scan intervals resulting in a high duration can accomplish a successful discovery within five TBTTs.

5 Related work

Regarding network discovery (probing) being the most intensively studied handover phase, we only summarize most novel research resulting in the best known, published reduction of its duration.

The SyncScan algorithm presented by Ramani and Savage [7] continuously tracks nearby access points by synchronizing short listening periods at the client with the periodic transmission of beacons of neighboring APs. Hereby, knowledge when a neighboring AP should transmits its beacon is required for scheduling the synchronized scan attempts. To avoid packet loss during these scan attempts, the AP and STA buffer user data in the meantime; hence experiencing a very frequently occurring delay which the authors quantify in the order of 15 ms.

Singh, Atwal and Sohi [8] as well as Chui and Yue [5] extend the SyncScan approach and present access point coordination and signaling schemes providing a (distributed) approach to synchronize beacon transmissions within a given time period for all APs in the distribution system operating on the same channel. Their work, however, does not affect the delay associated with the handover process. While the original SyncScan algorithm only knows when a



(a) CDF over number of scanning attemps

(b) CDF over time

Figure 7. Probability of receiving a beacon

beacon of any AP *should* be transmitted, STAs still attempt to scan for beacons of APs even if they are not within the latter's coverage. DeuceScan presented by Chen et al. [3, 4] combines neighborhood graphs with SyncScan hence reducing the scan attempts to channels where the probability to receive a beacon is high. Additionally, they use (geographic) position information of APs to estimate mobile's movement based on the radio signal strength indicator (RSSI) received from APs. Based on simulation results, DeuceScan can reduce the associated service interruption down to 3.5 ms which corresponds to the transmission time of an IEEE 802.11 probe request presumably not considering the channel switching time adding an additional delay of 10 *ms* as observed by [7].

Even though these best known practices may be realized upholding legacy compatibility, they required more knowledge of the infrastructure in terms of precisely guessing beacon transmissions or even requiring strictly synchronized beacon transmissions among neighboring access points.

6 Conclusion

This paper presented a preliminary performance evaluation of the novel opportunistic scanning approach employing 802.11 power saving as a underlying signaling protocol. We showed that depending on the employed MCS scheme, service interruption may be reduced to values in between 1.5 and 5.8 ms. This makes opportunistic scanning attractive for real-time communication with tight QoS constraints while being entirely compliant with the 802.11 standard. Our preliminary performance evaluation showed for an idle channel that a beacon reception can be guaranteed in less than 200 ms which is only twice as long as traditional passive scanning assuming a common TBTT of 100ms. Our future work will further evaluate the performance of the opportunistic scanning approach revealing the effects of channel load caused by other stations as well as a detailed evaluation of approach's cost in terms of quantifying the overhead of the signaling protocol.

References

[1] Ieee 802.11-2007– wireless lan medium access control (mac) and physical layer (phy) specifications, 2007.

[2] Ieee 802.11k/d7.0 – radio resource measurement, draft amandment. (802.11k), January 2007.

[3] Y.-S. Chen, C.-K. Chen, and M.-C. Chuang. Deucescan: Deuce-based fast handoff scheme in ieee 802.11 wireless networks. *VTC-2006 Fall. 2006 IEEE 64th*, 1:1–5, Sept. 2006.

[4] Y.-S. Chen, M.-C. Chuang, and C.-K. Chen. Deucescan: Deuce-based fast handoff scheme in ieee 802.11 wireless networks. *Vehicular Technology, IEEE Trans. on*, 57(2):1126–1141, March 2008.

[5] S. K. Chui and O.-C. Yue. An access point coordination system for improved voip/wlan handover performance. *VTC 2006-Spring. IEEE 63rd*, 1:501–505, May 2006.

[6] E.-M. Consortium. Eu-mesh system architecture. Technical Report D2.2, July 2008.

[7] I. Ramani and S. Savage. Syncscan: practical fast handoff for 802.11 infrastructure networks. *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, 1:675–684 vol. 1, March 2005.

[8] G. Singh, A. P. S. Atwal, and B. S. Sohi. An efficient neighbor information signaling method for handoff assistance in 802.11 wireless. In *Mobility '06: Proceedings of the 3rd international conference on Mobile technology, applications & systems*, page 14, New York, NY, USA, 2006. ACM.

[9] Virtual Automation Networks Consortium. Real time for embedded automation systems including status and analysis and closed loop real time control. Deliverable D04.1-1, EC Information Society Technology, July 2006.