Influence of Network Load on the Performance of Opportunistic Scanning

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

Abstract—This paper presents a detailed performance evaluation of a novel stochastic network discovery approach denoted as *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 with strict QoS constraints. We apply this concept to 802.11-based networks using power save as one possible signaling protocol to pause the communication between the scanning station and its interlocutor. Within this paper, we present a detailed simulation-based performance analysis of the opportunistic scanning approach showing its effects on real-time services such as VoIP streams. Our results show that opportunistic scanning behaves sturdy against background traffic. This novel approach enables successful network discovery within a 850-milisecond time span while guaranteeing QoS constraints of such a higher layer real-time application.

I. INTRODUCTION

Efficient network discovery is one of the key functional elements for wireless local area networks (WLANs). Hence, its mechanisms and potential improvements have intensively emerged over the last decade. Historically, WLANs simply replaced the wired Ethernet connection for stationary nodes. Communication partners were mostly discovered during the initial power-up phase of the system. Starting with the support of mobile devices, such network discovery occurred more frequently and was even subject to time-constraints if real-time applications, i.e. voice over IP telephone, were to be supported. Still, in the past, such network discovery was a rather seldom occurrence. But this has changed: new application areas as well as the idea of operating unlicensed WLAN devices within licensed frequency bands impose new challenges towards network discovery schemes. The issue on how to scan for new networks at a very high frequency or even how to continuously discover neighboring technologies has to be solved at low cost. Examples for new application areas requiring such frequent network discovery are manifold: 802.11 as the most predominant WLAN technology will move towards the 60GHz frequency bands [1] and discusses on how

to support highly mobile users [2]–[4]. Due to the micro-cellular architecture in the former and the high handover frequency in the latter case, handover is clearly no longer a seldom occurrence. The same applies to nodes having a software-defined radio interface which enables to constantly choose the network for 'best connectivity' and to conduct a handover from one technology to another even during an ongoing communication. Finally, unlicensed devices operating in the 'white space spectrum' have to release the media immediately if primary users appear. To assure this, network discovery / spectrum sensing is mandatory according to the FCC rules [5], [6]. One way to assure such primary user detection is to recurrently scan the spectrum. In summary, all those application scenarios require to *scan for other devices* of the same or different technology *continuously or at a high rate while maintaining QoS constraints of the ongoing communication.*

Opportunistic scanning is one candidate providing continuous network discovery. It periodically scans for alternative access technologies while upholding QoS constraints in terms of assuring maximum interarrival times of user datagrams. The approach behind opportunistic scanning is straightforward: the scanning station leaves its communication channel only for a very short time hence not noticeably affecting the QoS constraints of any higher layer communication. As the dwell time on the scanning channel is very short, opportunistic scanning cannot guarantee to detect an existing technology within a single scanning period. This makes opportunistic scanning a stochastic process with high variability. Also it requires a signaling protocol between the scanning station and its interlocutors in order to pause ongoing data exchange at MAC level. Though the generic concept of opportunistic scanning may be applied to any wireless technology, this paper assumes a 802.11-based system using this novel scanning scheme for network discovery. The rational behind this choice is that 802.11 is the most inexpensive and most widely deployed WLAN technology which we believe will continue to be the predominant technology for WLANs operating in 'white space' as well as in unlicensed, higher frequency bands. Our realization also adheres to the constraints that any system employing opportunistic scanning shall fully comply to the existing 802.11 standard which enables an effortless

integration of this novel scheme in existing WLAN chipsets / deployments.

This paper presents a detailed performance analysis of Opportunistic Scanning using the 802.11 power save to pause any ongoing communication while scanning for other technologies. We hereby extend our previous mathematical analysis of the opportunistic scanning scheme [7] which assessed the smallest achievable service interruption caused by the scanning process and investigated requirements for the choice of scanning intervals. Novelties of this contribution can be summarized as:

- assessing the performance limits while considering implications of the 802.11-architecture and protocol such as delayed beacons and clear channel assessment accounting for random backoff due to a busy media;
- comparing results for an idle communication channel to analytically derived performance limits;
- evaluating the influence of background traffic on the performance of opportunistic scanning; and
- quantifying the cost of opportunistic scanning including a detailed discussion of the introduced protocol overhead.

The remainder of the paper is structured as follows: Section II introduces our system model and is followed by a short description of the opportunistic scanning approach and how it is applied to a 802.11 system using power save as a signaling protocol. Emphasis is set on Section IV which starts paraphrasing the goals and methodology of the performance evaluation. Based on these goals, we derive our simulation scenario and set of applied metrics and conclude the performance evaluation section with a detailed discussion of the results. In the end of the paper, Section V places opportunistic scanning within the context of most recently published work on improved scanning schemes followed by a summary and outlook on our future work.

II. SYSTEM MODEL

We consider a set of 802.11 access points (APs) each having a high capacity connection to the Internet. These APs may be located at user premises (home networks) or in highly populated urban areas (public hot spots). 802.11 devices have a standard compliant implementation of the MAC but are not necessarily limited to operate only on the 2.4 and 5 GHz frequency band defined in the standard. Hereby, our architecture implicitly allows 802.11-based devices to be run in the 'white space' recently opened for unlicensed operation.

No constraints are imposed on the backhaul connection except that we assume that the backhaul's media access is strictly separated from the last hop. This assumption allows a wide range of architectural choices ranging from wired links (e.g., Ethernet), over having heterogeneous (wireless) technologies for the last hop and backhaul (e.g., 802.11 and WiMAX), up to using homogeneous technologies on different frequencies (e.g., 802.11b/g vs. 802.11a). This assumption is feasible as backhaul connectivity is usually set up by a service provider which tries to avoid any effects of end-user-systems on its backhaul technology.

Regarding the last hop, each 802.11 AP forms an infrastructure basic service set (BSS). All considered BSSs belong to the same extended service set (ESS).[1] BSSs may overlap and hence frequently operate on different channels to reduce interference. Also, the coverage area of a BSS may overlap with the one of a secondary technology (e.g. WiMAX or a 3/4G network). We assume that any present technology announces their existence at regular time intervals, e.g. by broadcasting a beacon or frame header (802.11 or WiMAX) or by a recurring energy pattern which can be identified but not necessarily decoded by the scanning STA (footprint-based detection of primary users in white space).

In our system model, users are 802.11-based stations (STA) located within a BSS and are connected to the Internet via their associated AP. Under the 'best-connected network paradigm', STAs may continuously choose among alternative links, i.e. another 802.11 AP or secondary technology. Thus, they continuously scan in order to detect alternative technologies or evaluate the link properties on other frequencies. Such continuous scanning is also used to detect primary users for white-space operation.

III. OPPORTUNISTIC SCANNING APPROACH

The general concept of opportunistic scanning is driven by the paradigm that seamless connectivity (as seen by the end user) does not mean guaranteeing zero-delay, interruption-free communication but limiting the duration and frequency of possible interruptions to an upper bound not affection the QoS constraints of the user application, hence not being noticeable to the user. As a result, our novel scanning approach is driven by two main constraints:

- The approach should enable real-time communication with small packet interarrival times and hard QoS constraints requiring low packet loss and relative small extra delay at MAC. Such applications include, e.g., voice over IP (VoIP) as well as telemetry applications.
- Second, the scanning approach shall only passively scan the scanned channel. This assures that opportunistic scanning does scale with the number of stations employing this approach and does not (unproductively) affect any communication on the scanned channel.

The following subsections highlight the general idea of the opportunistic scanning approach and show how opportunistic scanning can be applied to an IEEE 802.11 based WLAN.

A. General idea of opportunistic scanning

In general, opportunistic scanning aims at periodically leaving the current communication channel only for a very short time to conduct a scanning procedure as indicated by the *scan*-intervals (SI) in Fig. 1. The approach hereby assumes that the the system / technology to be discovered announces its existence at regular time intervals on the scanned channel

---

[1]If a BSS does not belong to the same ESS, clients may not use this BSS for roaming. Hence, detecting such BSSs is conceptually identical to the detection of any other technology (e.g. the presence of a primary user for white space operation) which is not used for communication purposes.
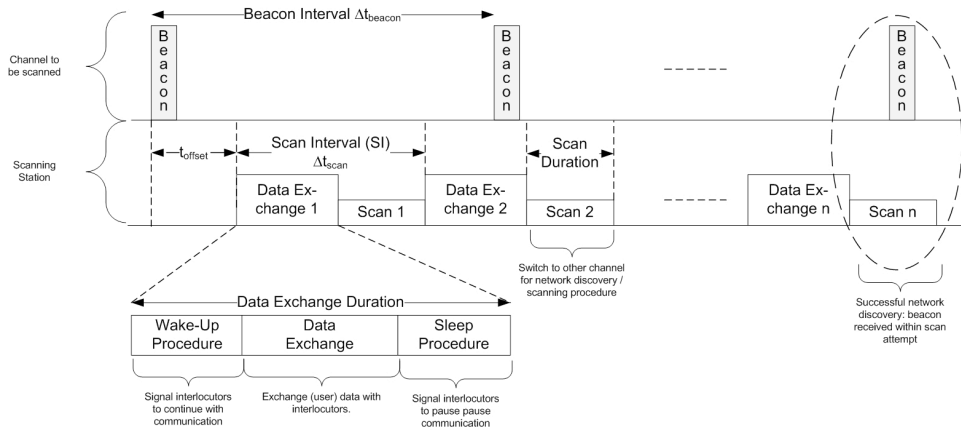
Fig. 1. Generic Opportunistic Scanning approach

(Δt_{beacon}).[2] Thus, two unique phases comprise the scan interval: a *data exchange* and a *scan* phase. In order to avoid packet loss, the former also involves signaling to any interlocutor to pause ongoing transmission (*sleep-procedure*) before it ends, as well as to continue sending data (*wake-up procedure*) in its beginning.

Depending on the implementation, opportunistic scanning allows to prioritize either the scanning or the data exchange process. The former guarantees a minimum scan duration and hence stops the data exchange even if user data packets are pending for transmission. Such priority could be given in a white space environment where the upmost goal is detecting the primary user. The latter would always exchange any pending user data packets even at the cost of reducing the scan duration nearly to zero. Thus, this second mode is suitable if QoS-constrained data exchange is valued higher than network discovery and was hence our choice for this paper.

B. Application of opportunistic scanning to 802.11 WLAN

The power save feature of IEEE 802.11 [8] allows a station to signal its interlocutors to hold (and buffer) any pending traffic. Though, it does not deem the signaling station to actually go into power save mode. Hence we herein use this time for passively scanning another channel.

It should be noted that in most common implementations, the 'sleeping' station only returns from power save after the reception of a 802.11 beacon which would result in unacceptably long sleeping times. Nevertheless, a rarely used sequence of power save signaling messages allows the station to resume communication at any time. This enables us to use the existing, standard compliant power save feature to apply opportunistic scanning to a 802.11 network. Hereby, a STA signals to the AP that it will go into 'sleep mode' for at most n beacon intervals. Nevertheless, the STA may return from its 'sleep mode' any time before this period expires.

[2]Please note that the term beacon includes any kind of *footprint* identifying a technology—ranging from a decodable signaling packet (as known from homogeneous technologies, i.e. 802.11) up to a *unique energy pattern* (whose contents cannot be interpreted but only recognized as known from the primary user detection concept in the white space).
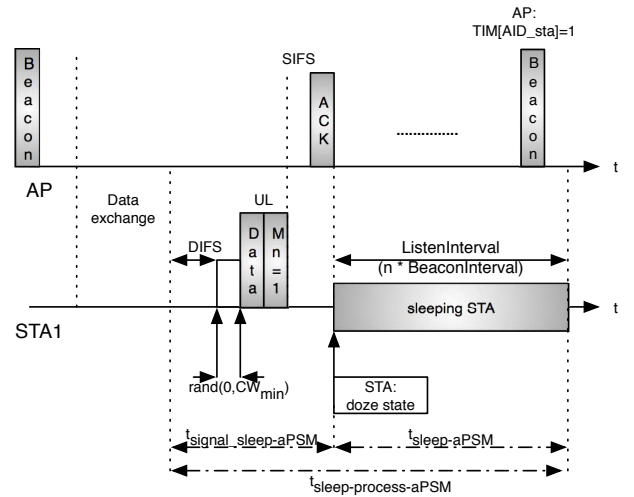

Fig. 2. Sleep procedure of PSM-STA

Figures 2 and 3 illustrate the resulting protocol details for the wake-up and sleep process. Actually, all the signaling information can be piggy-backed in the transmission of pending up-link data packets. The only overhead for this approach comes if no uplink data is pending—at which a null-data packet has to be transmitted. Also the standard requires power save stations to explicitly request all buffered packets in the downlink using a PS-Poll frame [8]. For the sake of briefness, the reader is referred to [7] for a detailed discussion of the signaling procedure. Therein, the theoretical performance limit of the approach is derived and prime numbers as optimal choices for the scan interval are recommended.

IV. PERFORMANCE EVALUATION

A. Goals and methodology

The overall aim of this performance evaluation is to quantify the behavior of opportunistic scanning applied to an IEEE 802.11 WLAN system used for real-time services, i.e. VoIP communication. Hereby, focus is set on three main aspects: Firstly, we consider an idle channel (no other STAs competing
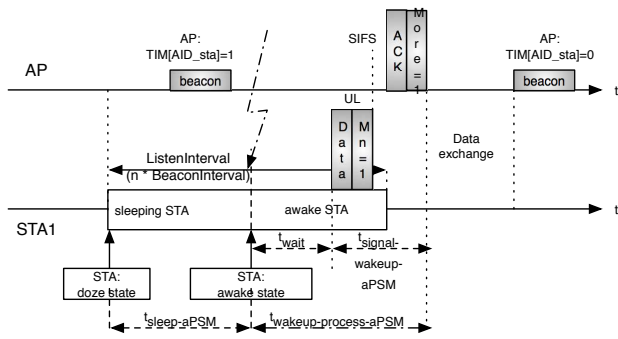
Fig. 3.   STA initiated wake-up procedure

Fig. 4.   Simulation Scenario, static case with background load

for channel access) in order to isolate the effect of the scanning scheme itself on the real-time traffic; secondly, we reveal how background traffic further influences the performance and sturdiness of our novel scanning scheme; and thirdly, we quantify the overhead associated with opportunistic scanning.

The evaluation of the *performance for idle channel conditions* acts as a baseline analysis showing how opportunistic scanning itself influences the inter-arrival time of user data packets. Also, we therein show how long our novel approach needs to discover one existing AP at a given probability. The latter results reveal a 'worst case bound' on the performance of our approach as we consider exactly one existing AP. Obviously, it takes less time to discover at least one AP if several APs independently transmit beacons on the scanned channel. In a second step, we aim at classifying the *influence of background traffic* showing how it affects opportunistic scanning: a potentially busy channel will not only delay the transmission of user data, but also hinder the (piggy-backed) signaling information, and even procrastinate the beacon being transmitted at fixed time-intervals. The final section of this performance evaluation *quantifies the protocol overhead* in terms of additional signaling information imposed by opportunistic scanning. All the former performance aspects are assessed by means of simulation considering all relevant protocol aspects of 802.11 [8] such as clear channel assessment (CCA) functionality and random back-off, delayed beacons due to busy media, and transmit-receive-turnaround time of the RF front-end.

B. Simulation scenario

Our simulation scenario considers two adjacent 802.11 access points (APs) operating on non-interfering channels and having an overlapping coverage area (c.f. Fig. 4). Both APs un-synchronously transmit beacons to announce their basic service set (BSS). Beacon transmissions are scheduled at regular time intervals (target beacon transmission time, TBTT) as defined by the 802.11 standard [8] but may be delayed if the AP's CCA functionality indicates the media to be busy. Both APs are connected via Ethernet to a VoIP server; hereby, the wired connection does not impose any throughput constraints.

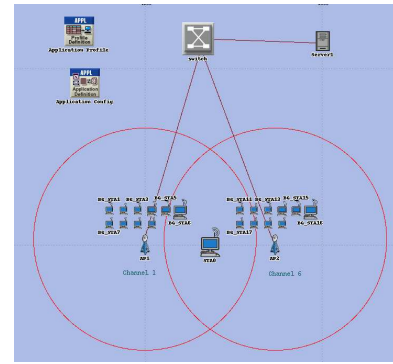The STA employing opportunistic scanning for network discovery is placed in the overlap of the adjacent cells. It is

associated with one of the two APs which is also used to relay an ongoing VoIP call (G711 codec employing 20 ms packetization without silent suppression). Employing opportunistic scanning for network discovery, the STA senses on the neighbor AP's channel for beacon transmissions.

Background traffic is increased by continuously adding additional STAs (BG-STAs) each featuring one ongoing VoIP call. In each step, one background STA is added per AP and is placed within the latter's coverage such that STAs are in communication range of each other. Such placement avoids hidden terminal effects as RTS-CTS is disabled for the considered VoIP service. This approach clearly isolates the opportunistic scanning scheme to be the cause of any observed effects.

All simulations are conducted using OPNET Modeler Wireless Release 14PL2. The 802.11 model of the simulation library is enhanced by power save features compliant to [8] as well as by a network discovery scheme according to the opportunistic scanning approach.

C. Metrics

The following metrics are used throughout the performance evaluation:

- *Beacon reception probability* quantifies the number of scanning attempts / time required to successfully receive a beacon at a given probability.
- *Inter-arrival time (IAT)* of user data is the time between consecutively received user datagrams.
- *Packet loss* accounts for the percentage of lost (user data) packets.
- *Average scan duration* identifies the average time spent on a single scanning attempt on the neighbor AP's channel.
- *Average data exchange duration* quantifies the time required to transmit and receive all buffered (user data) packets after pausing the communication for an opportunistic scanning attempt.
- *Null Data frame rate* quantifies the protocol overhead as null data frames have to be used to carry signaling information incase user data is not pending to piggy-back signal information for the power save procedure.
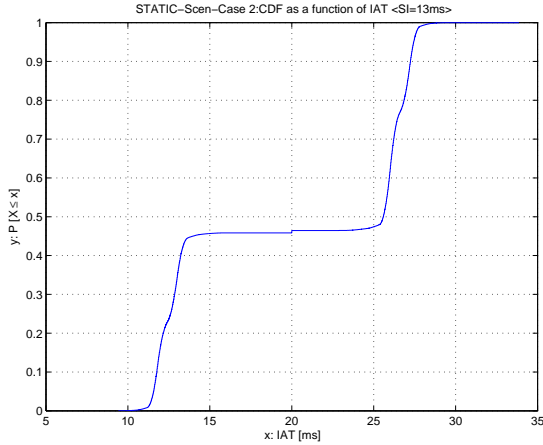
Fig. 5.   Influence of Opportunistic Scanning on IAT of VoIP flow

Fig. 6.   Required time to find a beacon: analysis vs. simulation

- *PS Poll frame rate* quantifies the protocol overhead as, according to the standard, the STA has to poll for buffered downlink data if employing power save mode operations.

D. Results

Previous numerical analysis of the theoretical performance limits for idle channel conditions showed that prime numbers shall be chosen for the scan interval in order to guarantee a successful reception of a beacon after a finite time span [7]. Accordingly, we show results for prime scan intervals in between 13ms and 51ms. The smallest value guarantees a service rate less than the VoIP packetization rate and the largest is in the order close to the 50-milisecond service interruption acceptable for voice communication.

1) Performance for idle channel condition: Opportunistic scanning coarsely divides the time for each STA (independently) into a scanning period and a data exchange period. As this devision is periodically repeated at a fixed rate, we expect VoIP packet to arrive at the STA at multiples of the scan interval. Figure 5 shows the cumulative distribution function (CDF) of the IATs for a scan interval of 13ms. For the 20ms-packetization rate of the VoIP application, the two modes of the IAT's distribution lie expectingly at the two multiples closest to the scan interval (SI), namely 13ms and 26ms. Also, we observe that slightly more packets are transmitted with every second SI. The resulting slight right skewness of the distribution is for the reason of the chosen SI: The 26-millisecond multiple of the SI is simply closer to the expected IAT of 20ms as the 13-millisecond multiple. Choosing a different SI of 17ms would result in a left skewness as transmission would occur at 17ms and 34ms. Also note, that the median being the correct single index of central tendency for such skewed distributions [9] is at 20ms and perfectly corresponds to the typical inter-arrival time of the considered VoIP flow.

Figures 6 illustrates for an idle the probability to successfully detect the neighbor AP's beacon after a given time span. For the chosen SI of 13ms, th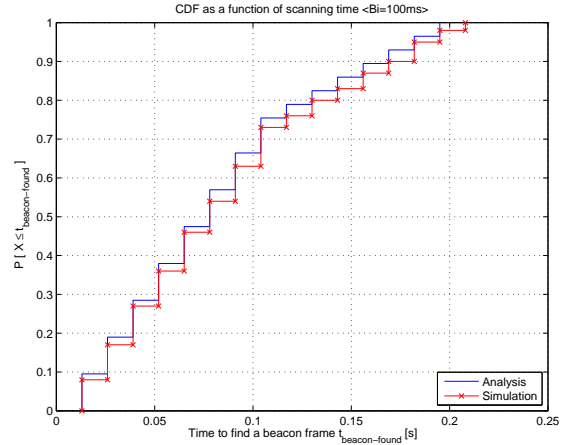e 99%-percentile is found at less than 200ms total scan time which corresponds to receiving the beacon no later than within the 15th scan attempt. The corresponding value for traditional passive scanning would be at 99ms with the implication of causing a service interruption of 100ms as compared to opportunistic scanning continuously guaranteeing the QoS constraints of the real-time application. Also, being for only 200ms within the overlapping area of APs in order to guarantee a beacon reception is an extremely small required dwell time even if the scanning STA were mobile. Finally, comparing the results with the theoretical findings presented in [7], we note that the effects of delayed beacons, random back-off due to busy medium, and rx-tx-turnaround times of the RF front-end impose only a neglectfully small effect on the results hence enabling performance prediction for any chosen target beacon transmission time and scan interval by using the theoretical findings for this special case.

2) Influence of background traffic: Opportunistic scanning by nature is vulnerable to background traffic as an increased network load within a BSS may cause delayed beacons. Also, signaling required to switch from *awake* to *doze* state in order to conduct an opportunistic scan attempt may be delayed due to a busy medium. As our novel scanning scheme primarily aims at providing a data exchange opportunity at every scan interval to guarantee continuous communication at application level, increasing the time spent on signaling any state change automatically reduces the effective time available for scanning another channel for each scanning attempt.

In a first step, we determine the maximum number of STAs simultaneous serviceable by the AP. Figure 7 illustrates the packet loss probability if in addition to the opportunistic scan STA terminals are added to the BSS. We notice no packet loss up to a total of 10 STAs in the system (9 BG-STAs and one OP-Scan-STA). Having $11 (= 10 + 1)$ STAs in the system saturates the WLAN and we notice packet loss due to buffer overflows at MAC level. With an additional simulation, we verified that packet loss does not occur for a total of 10 STAs even if *all* STAs employ opportunistic scanning
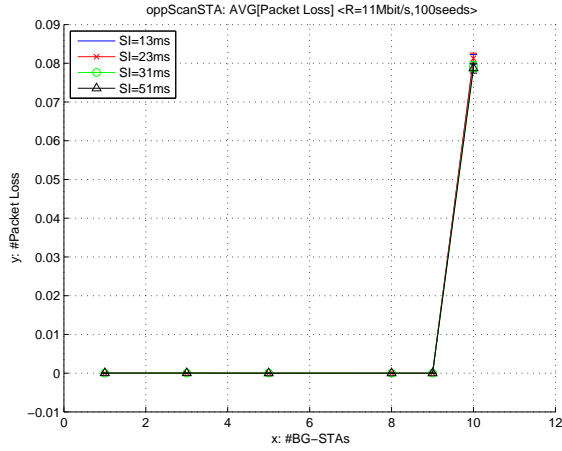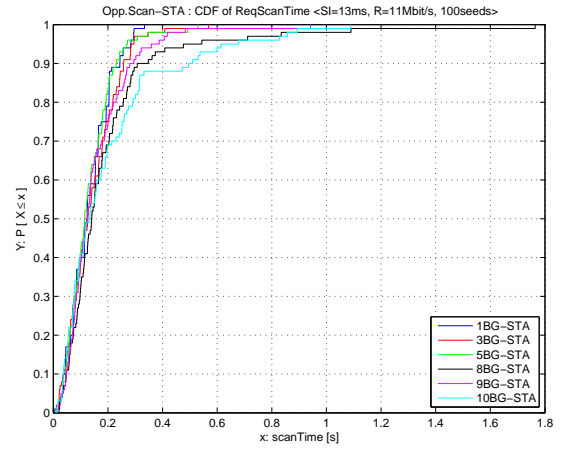
Fig. 7. Packet Loss Probability

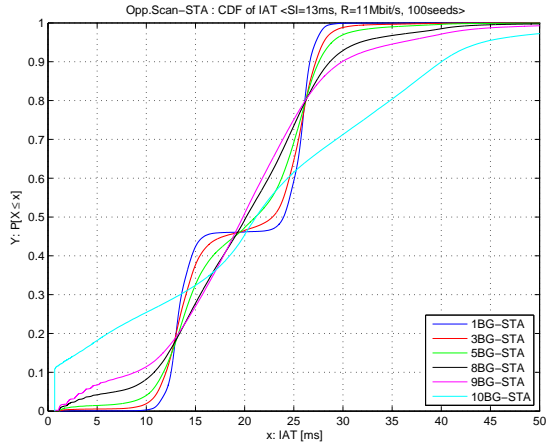Fig. 9. Influence of background traffic on total scan time

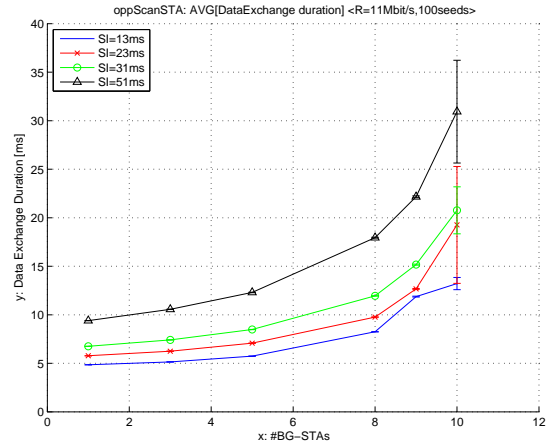Fig. 8. Influence of background traffic on IATs of VoIP data flow

Fig. 10. Static Scenario: Average data exchange duration of opScanSTA

simultaneously. Considering published work by other authors [10], [11], our novel scanning scheme reduces the maximum number of supportable STAs only by one STA at the gain of guaranteeing QoS at application level and conducting a continuous network discovery.

For an increased background load, the channel access delay increases and is more and more dominated by the 802.11 back-off procedure. Hence, the data exchange between the AP and the opportunistic scanning STA is less deterministically bound to multiples of the scanning interval as shown in Fig. 8. The distribution of the IAT of VoIP packets changes from a two-modal to a uni-modal for increased network load. The right skewness reduces at the same time to almost zero for an almost saturated channel. For an unsaturated medium, the median remains at 20ms regardless of the network load. We only notice an increase of the 99%-percentile of the IAT from 28ms to 40ms.

The increased background load results in longer periods spend on exchanging user data per scan interval. Thus, less time is actually spent per scanning attempt reducing the

beacon reception probability. Figure 9 illustrates that the 99%-percentile increased from 300ms for a single VoIP background flow to up to 850ms for highest achievable system load. In spite of this noticeable increase, this time represents the longest possible time required to guarantee detection of the other cell while upholding an ongoing, interruption-free communication on application level.

For completeness, Figures 10 and 11 illustrate the effect of an increased background load on the on effective scan duration and data exchange duration for different scan intervals.

3) Quantification of protocol overhead: In the previous subsection, we already quantified the overhead associated with opportunistic scanning: the maximum number of supportable VoIP STAs within a BSS is reduced by one. In the following, we highlight the cause for this reduction.

If data is pending for uplink transmission, opportunistic scanning does not impose any overhead as all the signaling information is contained in status bits already present in the 802.11 frame header. Only if the STA does not have to transmit data to the AP, it has to send a null data frame signaling its
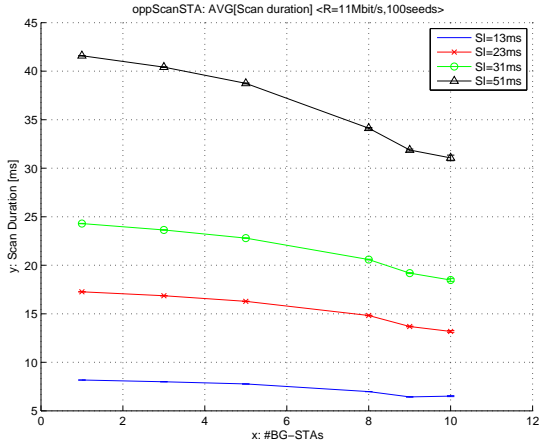
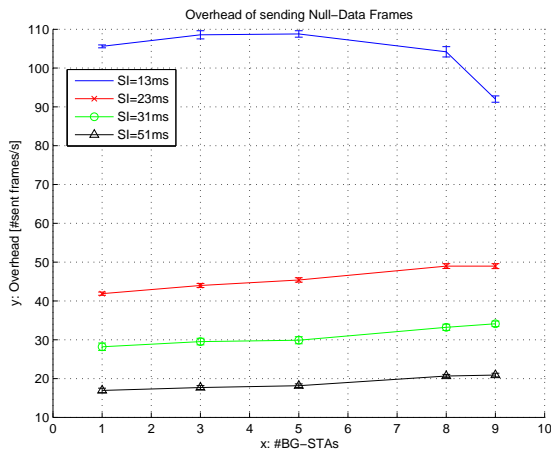Fig. 11.   Static Scenario: Average scan duration of opScanSTA

Fig. 13.   Number of sent Ps-Poll frames per seconds

Fig. 12.   Number of sent Null Data frames per seconds

recorded frame rates: occasional outliers increase the mean from 50fps to approximately 60fps as illustrated in Fig. 13. The increased background load causes more packets to be queued at the AP which are then all polled for transmission in a very short time.

V. 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.

Ramani and Savage [12] developed the SyncScan algorithm which continuously tracks nearby access points using very short listening periods. In contrast to our novel opportunistic scanning scheme, SynScan follows a deterministic approach as it synchronizes the short listening periods with the periodic transmission of the beacons of neighbor APs. This requires knowledge when such beacon transmission occurs which is realized by a centralized approach accumulating such knowledge. In contrast, opportunistic scanning does not require such synchronization nor centralization. Similar to our approach, Ramani and Savage buffer packets at the AP during scan attempts.

Based on SyncScan, Singh, Atwal and Sohi [13] as well as Chui and Yue [14] present an enhanced approach featuring a distributed access point coordination scheme. The latter enables the synchronization of beacon transmissions within a given time period for all APs in a distribution system operating on the same channel. Even though the associated delay is only in the order of 15 ms, the presented scheme is only applicable to single-frequency networks which we consider as a limitation.

The original SyncScan algorithm and its enhancement only know when a beacon of any AP *should* be transmitted. Hence, STAs scan for a particular AP's beacon transmission even if they are not within the latter's coverage. DeuceScan [15], [16] overcomes this drawback including neighborhood graphs in the decision when to scan for beacon transmissions.

state change for a new scanning attempt. Figure 12 illustrated the influence of the background load on the null data frame rate for various scan intervals. The smallest considered scan interval of 13ms result in unproportionally higher overhead as the 20ms-packetization rate of the VoIP flow is larger hence resulting frequently in an empty data queue if signaling information is pending. The influence of the background load is neglectfully small; even for high network loads, we observed that pending user data are transfered 'at a bulk' still causing empty queues if signal information has to be transmitted.

Even though the 802.11 power save feature provides an entirely standard compliant mean of signaling communication pauses used for opportunistic scanning attempts, it has one disadvantage: each packet buffered at the AP for downlink transmission has to be requested by the STA using a PS-Poll frame [8]. Accordingly, we expect a ps-poll frame rate of 50fps caused by the 50 VoIP packets per second imposed by the application. The median of recorded frame rates is constantly near this estimate regardless of the background load. But we observe an increased right-skewness of the distribution of the
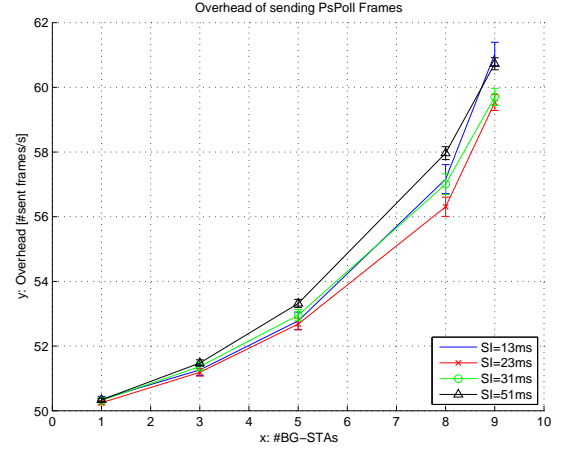
Including the 10 *ms* channel switch delay as observed by [12], DeuceScan can reduce the associated delay to approximately 13.5ms.

As well as our Opportunistic Scanning, all of these best known practices uphold compatibility with legacy 802.11 implementations. Even though their performance qualifies them as well for real-time applications, all of them required more knowledge of the infrastructure in terms of precisely guessing beacon transmissions, requiring strictly synchronized beacon transmissions among neighboring access points, or assume perfect knowledge regarding neighborhood information for all APs.

Instead, Wu et. al. do not impose such constraints on the infrastructure. Their *proactive scan approach* [17] actively scans (a possibly prioritized) list of channels periodically before connectivity is lost and immediately switch to another channel when conducting handover. They utilize a small scan interval of 10ms which is used to *actively* scan for alternative APs using probe-requests and -responses. Such aggressive scanning is known to reduce the network time spend in network discovery to a few milliseconds. In a single-client experiment, the authors show that their scheme is suitable for VoIP communication. Nevertheless, the authors did not evaluate the impact of their scheme on the scanned network and hence do not defeat the concern that active scanning schemes do not scale for a large number of clients.

VI. SUMMARY & FUTURE WORK

This paper applies the novel opportunistic scanning scheme to 802.11 based communication networks. Power save is hereby used as a signaling protocol to pause communication between STA and AP for a very short time while searching for other systems / technologies in the STAs vicinity. Within this context, we presented a comprehensive performance evaluation of the protocol using VoIP as an example for a real-time communication. Results show that opportunistic scanning results in a bi-modal distribution of user packet inter-arrival times (IATs) without affecting the IAT's median corresponding exactly to the 20ms packetization of the considered G711 voice codec. The 99%-percentile of recorded IATs lies at less than 40ms. Featuring a *guaranteed network discovery* within 850ms *without a noticeable service interruption* at application level, opportunistic scanning is fully capable of supporting real-time applications such as VoIP. Cost-wise, the maximum number of simultaneously supportable users in the WLAN cell is only reduced by one.

We conclude that opportunistic scanning is well able of continuously monitoring a STAs environment while upholding QoS constraints for real-time services. Hence, it is suitable as a (network) discovery scheme for various application scenarios such dynamic link selection for load balancing between different APs of the same or different technologies, for fast handover applications, and even for continuously scanning for primary users if a 802.11-based network were to operate in the 'white space'. This universal applicability of opportunistic scanning to the various application scenarios is only achievable as this novel, stochastic scanning approach does not impose any requirements upon the network to be discovered. If applied to an 802.11-based network, this is a clear advantage of opportunistic scanning as compared to state-of-the-art network discovery schemes featuring comparably small service interruptions.

Our next steps focus on the performance evaluation of opportunistic scanning for mobile use cases assessing its suitability for mobility-driven handovers.

REFERENCES

[1] E. Perahia, "Vht 60 ghz par plus 5c's," IEEE 802.11 VHT SG Very High Throughput Study Group, Denver, CO, USA, doc. 11-08/806, July 2008.

[2] *IEEE 802.11p/D6.0 – Wireless Access in Vehicular Environments, Draft Amandment to Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications*, IEEE Std. 802.11p-2009, Rev. D6.0, March 2009.

[3] H. Morioka and H. Mano, "Broadband access for high speed transportation," IEEE 802.11 WNG SC Wireless Next Generation Standing Committee, Dallas, TX, USA, doc. 11-08/1337, November, 10 – 14 2008.

[4] M. Emmelmann, T. Langgärtner, and M. Sonnemann, "Fast handover support for highly mobile users using cots 802.11 cards," IEEE 802.11 WNG SC Wireless Next Generation Standing Committee, Los Angeles, CA, USA, doc. 11-08/1358, January, 19 – 23 2009.

[5] M. Goldhamer, "Tvbd common functions across ieee 802," in *IEEE 802 White Space Tutorial*. IEEE 802 LAN/MAN Standards Committee, March 2009, no. doc.: IEEE sg-whitespace-09/0039r3.

[6] "Fcc part 15.711: Interference avoidance mechanisms for telefision band devices, fcc rules for radio frequency devices," http://www.hallikainen.com/FccRules/2009/15/711/, April 2009.

[7] M. Emmelmann, S. Wiethölter, and H.-T. Lim, "Opportunistic scanning: Interruption-free network topology discovery for wireless mesh networks," in *International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM)*, Kos, Greece, June 15-19 2009.

[8] *IEEE 802.11-2007– Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11-2007, 2007.

[9] R. Jain, *The Art of Computer Systems Performance Analysis: Techniques for experimental design, measurement, simulation, and modeling*. John Wiley and Sons, Inc., 1991.

[10] S. Garg and M. Kappes, "Can i add a voip call?" vol. 2, May 2003, pp. 779–783 vol.2.

[11] S. Wiethölter, "Virtual utilization and voip capacity of wlans supporting a mix of data rates," Telecommunication Networks Group, TU Berlin, TR TKN-05-004, 2005.

[12] 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*, vol. 1, pp. 675–684 vol. 1, March 2005.

[13] 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*. New York, NY, USA: ACM, 2006, p. 14.

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

[15] 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 Transactions on*, vol. 57, no. 2, pp. 1126–1141, March 2008.

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

[17] H. Wu, K. Tan, Y. Zhang, and Q. Zhang, "Proactive scan: Fast handoff with smart triggers for 802.11 wireless lan," *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 749–757, May 2007.