Analysis and Evaluation of WiFi Scanning Strategies

German Castignani, Nicolas Montavont and Andrés Arcia-Moret

***Abstract*—Considering the increasing popularity of IEEE 802.11 (WiFi) wireless accesses, users face with the necessity of maintaining a continuous connection to the network while moving. In order to tackle this issue, Mobile Stations (MS) needs to execute scanning processes to discover potential Access Points (AP). This procedure must be fast and reliable to guarantee a continuity on the connection. In this paper, we study the WiFi scanning process and then we propose and evaluate by simulation different scanning strategies focusing on the adaptation of 802.11 scanning timers: MinChannelTime and MaxChannelTime. Then, varying these timers, we obtain notable improvements over the legacy static discovery process.**

***Keywords*—802.11, Handover, Scanning**

I. Introduction

Since the introduction of the IEEE 802.11 wireless access in the market, a vast number of networks have been deployed, creating a heterogeneous scenario. Within this new network communication model, an MS can associate to an AP in infrastructure mode, or spontaneously benefit from local neighborhood to exchange data packets in ad-hoc mode. Then, the topology and resource discovery become critical. These processes must be reliable, efficient and fast. In this paper, we present a first set of simulation results to assess the discovery process in IEEE 802.11 networks, focusing on the influence of the time taken by the resource to respond.

In IEEE 802.11 networks, an MS can operate in infrastructure mode or in ad-hoc mode. In both modes, an MS can probe channels by broadcasting Probe Requests and waiting for Probe Responses from APs or other MSs (see Fig. 1). The IEEE 802.11 standard [1] defines two timers, namely MinChannelTime (MinCT) and MaxChannelTime (MaxCT), to determine the time an MS needs to wait on a channel after having sent a Probe Request. MinCT defines the maximum time to wait for a first Probe Response. If a Probe Response is not received within MinCT, the MS considers that the channel is empty, and starts the process in a different channel. Otherwise, if a Probe Response is received within MinCT, then the MS waits up to MaxCT for further Probe Responses from other nodes on the same channel. The discovery process is mainly characterized by two metrics: the full scanning failure and the full scanning latency. A full scanning failure is defined as the impossibility to discover any of the MSs or APs within all the available scanned channels. The full scanning latency is the time spent to scan all available channels one after the other in whatever order.

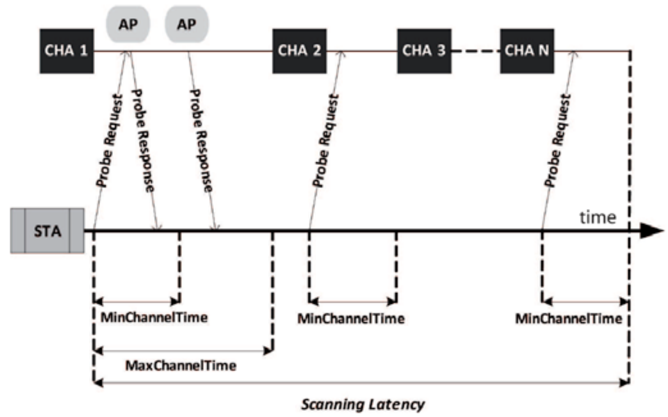

Fig. 1. Standard Active Scanning

As explained in [2] and [3], the discovery phase takes about 90% of the handover latency. We propose a set of simulations on the discovery process and focus on evaluating the impact of MinCT and MaxCT on the scanning latency and the scanning failure. We propose different strategies to set the values for MinCT and MaxCT. The first one consists on using fixed timers while in the last three strategies we propose to dynamically adapt MinCT and MaxCT. We aim at finding a tradeoff between a minimal full scanning latency and a minimal full scanning failure. We have to consider that when decreasing the latency we increase the failure and vice-versa. The principle is thus to lower MinCT and MaxCT values when MS/AP has already been discovered, and on the opposite, to use higher values when no AP has been found.

The rest of the paper is organized as follows. In Section II we survey the related work. In Section III we introduce different strategies to set the timers during a scanning process. In Section IV we evaluate the performance of the proposed strategies by simulation. Finally in Section V, we conclude the paper.

II. Related Work

Most of the related work of the 802.11 discovery process concerns the optimization of the scanning latency during a Layer 2 handover, when a MS roams from one AP to another. One simple way to reduce the full scanning latency is to use Selective Scanning [4] which allows to only scan a subset of channels, instead of probing each of them. Regardless of reducing the scanning latency, this approach is sensible to the

Article received on January 22th, 2010.
G. Castignani. y N. Montavont are with Institut TELECOM / TELECOM Bretagne / Université Européenne de Bretagne, Cesson Sévigné, Francie, Ph: +33 299127000, Fax: +33-299127030, E-mail: german@castignani.com.ar, nicolas@montavont.net. A. Arcia is with Universidad de Los Andes, Sector La Hechicera, Facultad de Ingeniería, Escuela de Ingeniería Eléctrica, Mérida, Estado Mérida, Venezuela, Ph:. +58-274-2402907 / 2824, Fax: +58-274-2402890, E-mail: amoret@ula.ve.

channel subset it assumes with activity. If this assumption is not correct, it falls into a full scanning failure since no AP could be found. Another proposed optimization has focused on reducing the value of the scanning timers (MinCT andMaxCT). Velayos and Karlsson [5] fixed the potential best values for both timers presenting theoretical considerations and simulation results. For MinCT, authors establish the concrete value for the maximum time an AP needs to answer a probe request. They propose 670µs for MinCT. Authors analyze the probe response delay depending on traffic load and the number of stations on each channel. They conclude that MaxCT is not bounded as long as the number of stations can increase. They recommend to set MaxCT to avoid responses from overloaded APs while setting a value of 10240µs. However, providing fixed timers does not guarantee a successful discovery process. These fixed values could effectively work for some scenarios, but in other cases unnecessary delays may be introduced or even worse, the scanning process may fail to find any candidate AP, falling in a link layer disconnection. Standard active scanning algorithmimplicitly defines that the handover process should be performed after detecting weak signal from the current AP. The *Smooth Handover* [6] and the *Periodic Scanning* [7] methods are based on splitting the discovery phase into multiple sub-phases. The objective of this division is to allow an MS to alternate between data packet exchange and the scanning process. An MS builds a list of target APs maintaining some basic information. Authors of [6] propose to scan a group of channels in each sub-phase, while in [7] only one channel is scanned during MinCT. These techniques require that there must be enough overlapping area between neighboring APs; if only small overlapping areas exist, there will not be enough time to distribute the scanning process during the MS movement. The need for overlapping area between neighboring APs strongly constrain the network deployment and require to deploy more APs in a given area.

III. Scanning Strategies

There is still a lack of work in the determination of the most adequate values defining the time to wait for responses on each channel. For every fast handover approach, an MS still needs to scan channels one after the other to discover APs. In order to determine the time needed by an MS to wait for a response on each channel, we study the impact of MinCT and MaxCT on the discovery process. We define in this section four strategies to set the values for these timers: Fixed Timers and Adaptive Timers Scanning (including three variants).

a) *Fixed Timers*: This first strategy consists in fixing predefined values for both MinCT and MaxCT, which determine the time an MS will wait on a channel for AP's responses. Low values will provide low full scanning latency, but will increase the risk of missing AP since the MS does not wait long enough to get a response. While theoretically an MS should expect a response before 1 ms [5], experimental results suggest that the response from an AP varies from 1 ms to 40 ms. Considering the empirical analysis proposed by Mishra et al. [3], and our own experimentation results, we decided to evaluate the following timer configuration <MinCT, MaxCT>: <10ms, 20ms> and <25ms, 50ms>.

b) *Adaptive Timers*: The other possible strategy is to adapt or dynamically change the values for MinCT and MaxCT during a scanning process based on the discovered resource. After scanning each channel, we calculate a quotient between the greatest Received Signal Strength Indicator (RSSI) of all discovered APs and the number of discovered APs on the channel. This quotient is used to rank APs on each channel in order to decide the values for MinCT and MaxCT for the next channel to scan. We reduce timer's values if some AP has been found, otherwise they are increased. This new approach allows an MS to spend less time on channels once candidate APs have been already found. The main goal consist on reducing the timers, channel by channel if while APs are discovered. Remark that the impact of missing APs will be less important as if no AP were found. On the contrary, timers may be increased if no AP has been found, so as to increase the chances of finding an AP on the next channel(s). The selection of the sequence of channels to scan becomes important if we consider timers adaptation. The sooner an AP is found, the faster the timers will be decreased, and thus the importance of scanning first the channels on which AP(s) is (are) operating. In 802.11 networks, only three non-overlapping channels exist. A proper deployment typically uses only these channels [8] [9]. Then, prioritizing those channels [4], candidate APs may be discovered sooner. We randomize the channel switching sequence in two different subsequences. The first subsequence randomly switches between the non-overlapping channels. Then, the rest of the channels are randomly considered. If an AP with relative good signal level is discovered in channels 1, 6 and/or 11, the adaptive system will set lower timers for the next channels to scan. In all cases, the adjustment of both timers is performed between a set of thresholds that have been previously defined by experimentation. MinCT vary between MinLower (6ms) and MinUpper (34ms); then MaxCT is adapted between MaxLower (8ms) and MaxUpper (48ms). In [10] we present a testbed evaluation of an adaptive timers strategy.

We proposed three different adaptive strategies depending on the initial conditions, i.e., the values set for the timers when the scanning phase starts. The objective is to analyze the impact of each strategy on the *full scanning failure* and *full scanning latency* trade-off. The strategies are as follows:

-AAS (Aggressive Adaptive Strategy): In this strategy initial conditions are set to the minimum thresholds values (6ms and 8ms for MinCT and MaxCT respectively).

-FAS (Fair Adaptive Strategy): Using FAS, the MS uses half the maximum thresholds values as initial conditions (17ms and 24ms for MinCT and MaxCT respectively).

-NAAS (Non-AggressiveAdaptive Strategy): Within NAAS, the MS sets the initial conditions to the maximum threshold values (34ms and 48ms for MinCT and MaxCT respectively).

IV. Evaluation by Simulation

We have implemented a lightweight simulator in C to evaluate these strategies. Both fixed and adaptive timers strategies were evaluated in 25 different scenarios. For each scenario, there is either 0 or 1 AP per channel. This is to simplify the simulation, since we are interested only if the channel has activity or not. We have defined 12 optimistic scenarios, where the APs are deployed in the first scanned channels; an ideal scenario where 13 APs are deployed one by one in the 13 available channels and 12 pessimistic scenarios, where Aps are deployed in the last scanned channels. We identified both optimistic and pessimistic channel sequences since the adaptive strategy depends on when APs are discovered in the sequence of scanned channels. For each scenario, we evaluated the impact of probe response delays.

For space reasons, we only present the results for 4, 8 and 12 channels with activity for the optimistic and pessimistic channel sequences using the AAS (Fig. 2), the FAS (Fig. 3) and the NAAS (Fig. 4). These figures show the full scanning latency on the left ordinate and the full scanning failure percentage on the right ordinate according to the probability of receiving a Probe Response before a given time in abscissa. We can appreciate in all cases that the fixed timers strategy using both sets of timers (red and green curves) tends to increase the full scanning latency when the number of probe responses received before 10ms increases. Additionally, the fixed timers strategy always reaches high levels of full scanning failure (red solid curve) for long probe responses delays (e.g., 60% for a 4 AP scenario with long probe responses delay).

In the adaptive strategies (Fig. 2) we can appreciate that for the optimistic scenario (pink curves), AAS gives high priority to full scanning latency. For 4 APs, the full scanning latency decreases while the number of probe responses received before 10ms increases. On the other hand, on the 8 and 12 APs deployments using optimistic sequences, full scanning latency tends to increase for a higher percentage of probe responses received before 10ms. This is due to the fact that since more channels with activity are detected on those scenarios, we wait longer (i.e., for MaxCT to expire). In the optimistic sequences, *full scanning failure* for AAS starts to be lower than the fixed timers strategy using <10ms, 20ms>, only for a high number of channels with activity. In those cases, the probability of missing all channels is lower than the scenario of 4 AP. In fact, using optimistic sequences, since APs are deployed on the first channels on the sequence, we have not the opportunity to increase timers as much as necessary in order to guarantee a lower full scanning failure. In the case of pessimistic sequences (blue curves), it seems that the trade-off between *full scanning latency* and *full scanning failure* is managed better. *Full scanning latency* reaches low values and *full scanning failure* is negligible. This situation is produced when there is no activity on the firsts channels. Then, we have the time to increase timers to guarantee a lower *full scanning failure*. For example, in the 4 AP scenario using the pessimistic sequences we increase the timers nine times before probing the 10th channel on the sequence.

In Fig. 3 we appreciate that *full scanning failure* is not as high as in the case of AAS. For a 4 AP deployment using the optimistic sequences (pink curves), a *full scanning failure* rate of 10% is reached for only a 10% of probe responses received before 10ms. Considering pessimistic sequences (blue curves), *full scanning failure* is negligible, but full scanning latency is still higher than the fixed timers strategy for an 8 AP deployment. There is an intersection between the *full scanning latency* curves for the fixed timers strategy using <10ms, 20ms> and the FAS curves in all the optimistic and some pessimistic scenarios. In the zone where *full scanning latency* of FAS is higher than the fixed timers strategy (from the intersection point to the left), the fixed timers strategy performs worse in terms of *full scanning failure*, reaching very high levels compared to FAS.

Using the NAAS strategy, as illustrated in Fig. 4, *full scanning failure* is negligible independently of the considered scenario, including both optimistic (red curves) and pessimistic (blue curves) sequences. Regarding *full scanning latency*, it is a little higher than the FAS *full scanning latency*, but much higher than the case of fixed timers strategy using <10ms, 20ms>.

V. CONCLUSIONS AND PERSPECTIVES

In this work, we have analyzed and evaluated different strategies for the discovery process on 802.11 devices. Several optimizations were proposed in the literature, and they highlight the importance of the values of MinCT and MaxCT, that condition the *full scanning latency* and *full scanning failure*. To perform this evaluation, we used simulations to study the influence of both timers (MinCT and MaxCT) for different probe response delays on the *full scanning latency* and *full scanning failure* rate. We proposed different strategies for setting timers. Firstly, we proposed fixed timers, and secondly we proposed three other strategies using adaptive timers. We have shown that the fixed timers strategy keeps a high full scanning failure for long probe responses delay, independently of the number of channels with activity and the channel sequence. On the other hand, the proposed adaptive strategies (AAS, FAS and NAAS) help to manage the trade-off between *full scanning failure* and *full scanning latency* depending on the scenario. AAS performs aggressively in terms of latency, providing low *full scanning latency* values and a *full scanning failure* that tends to decrease when the number of channels with activity increases. FAS focus on balancing the trade-off under study, the *full scanning latency* does not overshoot and the full scanning failure is always maintained bellow low limits (9% of full scanning failure on the optimistic 4 AP scenario with only 10% of received probe responses before 10 ms). Finally, NAAS gives priority to the *full scanning failure*, but it tends to decrease the full scanning latency for scenarios with a higher number of channels with activity. This case illustrates the use of adaptive strategies, instead of defining a static fixed timers algorithm which only fits some AP deployment configurations. An MS could potentially use cross-layer information, and it may select a concrete adaptive strategy (AAS, FAS or NAAS) depending

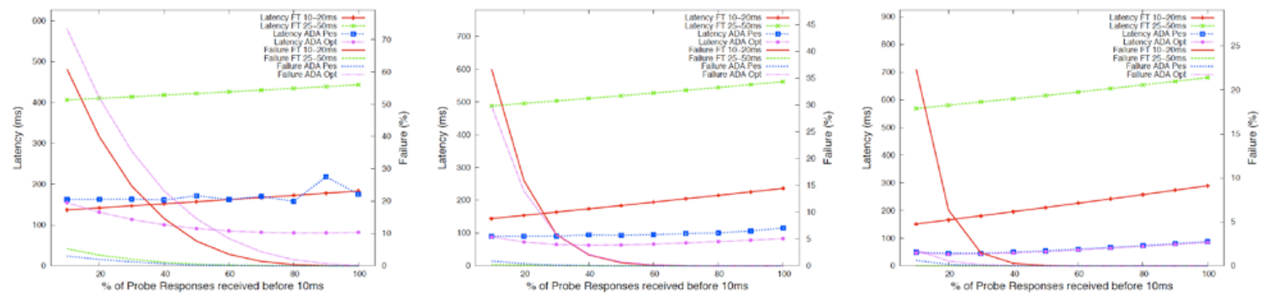

Fig. 2. Results for 4, 8 and 12 APs for the optimistic and pessimistic sequences using AAS

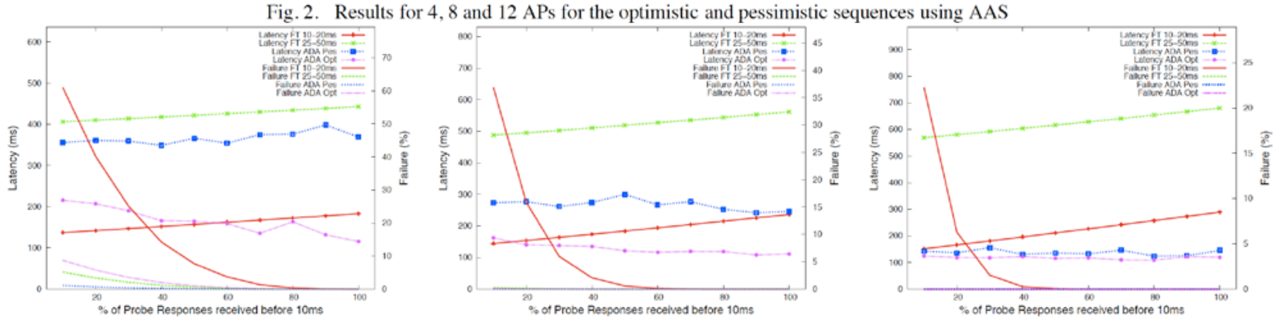

Fig. 3. Results for 4, 8 and 12 APs for the optimistic and pessimistic sequences using FAS

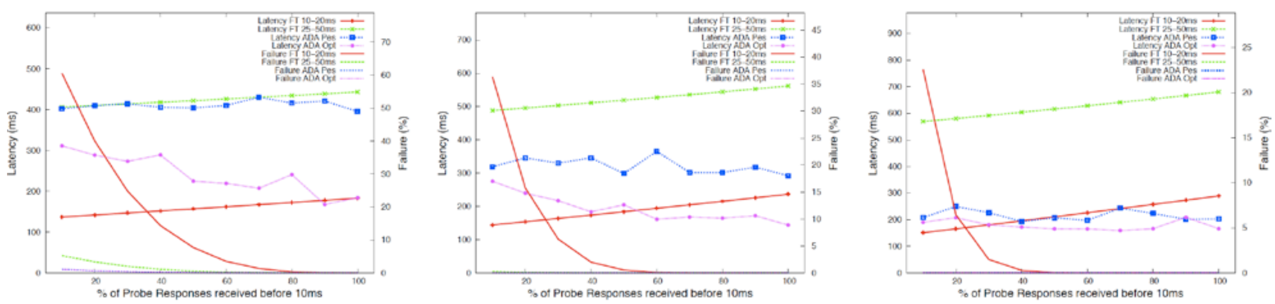

Fig. 4. Results for 4, 8 and 12 APs for the optimistic and pessimistic sequences using NAAS

on the application necessities in terms of QoS. As a future work we plan to further investigate different adaptive functions, scanning policies and candidate AP selection algorithms. A sensibility analysis of the adaptive algorithm parameters is currently being performed in order to obtain a unique set of parameters that optimizes the algorithm. As it was proposed in several optimization techniques, a selective scanning approach not only reduces the full scanning latency, but it also conditions the successfulness of the handover process. Thus, we could apply an optimized channel switching policy, and interrupt the scanning process before all channels have been scanned. Finally, we are working on the implementation of different scanning strategies on the ath5k driver, in order to evaluate them on a real environment.

REFERENCIAS BIBLIOGRÁFICAS

[1] IEEE Std. 802.11-2007,IEEE **Standard for Information technology - Telecommunications and information exchange between systems – Local and metropolitan area networks -Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, IEEE-SA Standards Board, 2007.

[2] Francisco A. Gonzalez, Jesus A. Perez and Victor H. Zarate, **HAMS: Layer 2 Accurate Measurement Strategy in WLANs 802.11**, Int. Workshop on Wireless Network Measurements (WiNMee), 2005

[3] A. Mishra, M. Shin and W. Arbaugh, **An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process**, ACM SIGCOMM Computer Communication Review (Volume 33 - Issue 2), Technical Paper, 2003.

[4] S. Shin, A. Singh and H. Schulzrinne, **Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs**, International Conference on Mobile Computing and Networking, Proceedings of the second international workshop on Mobility management and wireless access protocols, 2004.

[5] H. Velayos and G. Karlsson, **Techniques to reduce the IEEE 802.11b handoff time**, IEEE International IEEE International Conference on Communications, 2004.

[6] Y. Liao and L. Gao, **Practical Schemes for Smooth MAC Layer Handoff in 802.11 Wireless Networks**, Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), IEEE, 2006.

[7] N. Montavont, J. Montavont and T. Noel, **Enhanced schemes for L2 handover in IEEE 802.11 networks and their evaluations**, IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2005.

[8] Cisco Systems, Inc., **Channel Deployment Issues for 2.4-GHz 802.11 WLANs**, Technical Report OL-6270-01, 2004.

[9] Cirond Technologies, Inc., **Channel Overlap Calculations for 802.11b Networks**, White Paper, 2002.

[10] G. Castignani, N. Montavont and A. Arcia, **An Evaluation of the Resource Discovery Process in IEEE 802.11 Networks**, Second Int. Workshop on Mobile Opportunistic Networking (MobiOpp) 2010