Enhanced Channel Scanning Schemes for Next Generation WLAN System

Zheng Chang*, Olli Alanen*, Eng Hwee Ong†, Jarkko Kneckt†

*Magister Solutions Ltd, Hannikaisenkatu 41, FIN-40010 Jyväskylä, Finland
Email: {zheng.chang, olli.alanen}@magister.fi

†Nokia Research Center, Itämerenkatu 13, FIN-00180 Helsinki, Finland
Email: {eng-hwee.ong, jarkko.kneckt}@nokia.com

Abstract—The IEEE 802.11 standard based Wireless Local Area Networks (WLANs) are widely deployed and have gained greater popularity. It is anticipated that WLAN will play an important role in the future wireless communication systems in order to provide several gigabits data rate. However, it has been a challenging problem to support the IEEE 802.11 WLAN devices to fully exploit the high throughput gains offered by the IEEE 802.11 standard whenever possible since the current channel scanning mechanisms in standard may result in unacceptable delay for network discovery. In this work, we review the behavior of passive and active channel scanning schemes of the current IEEE 802.11 specification, and also propose two enhancements for the active scanning mechanism based on the draft of IEEE 802.11ai standard. The proposed schemes can reduce the overhead of transmitted management messages while improving the channel scanning performance. In addition, it can also increase the speed of discovery of APs before associating with one and enable more precise discovery operations. Through simulation study, it is shown that simulation results can explicitly verify our expectations on the superiorities of the proposed schemes.

Index Terms—WLAN, active scanning, passive scanning, IEEE 802.11ai

I. INTRODUCTION

The IEEE 802.11 Wireless Local Area Networks (WLANs) [1] are widely used for its convenience and low costs. It can be anticipated that WLAN will play an important role in the future wireless communication systems in order to provide data rate solutions of multi-gigabits transmission. So far, the current IEEE 802.11n can offer data rate up to 600 Mbps and IEEE 802.11ac is one of the ongoing WLAN standards aiming to support Very High Throughput (VHT) with data rate of up to 6 Gbps below 6 GHz band [2].

As the data rate speed offered by current IEEE 802.11 WLAN increases, the demands for fast and seamless connection are also enlarged. Nowadays, the number of mobile devices being designed to the IEEE 802.11 specifications are increased continuously and dramatically. The majority of electronic devices, including laptops, tablets, cell phones and even vehicles are equipped with IEEE 802.11 interfaces for broadband wireless access. The high data rate offered by the IEEE 802.11 standard is a key driver for dual mode functionality in handsets. Hence, it is essential that these mobile stations (STAs) can fully exploit the throughput gains offered by the IEEE 802.11 WLAN whenever possible. However, the current specification of IEEE 802.11 standard limits this for the devices that only take a short dwell time within the coverage area of an Extended Service Set (ESS); or for a high number of users closely entering the coverage area of an Access Point (AP) within an ESS for the first time. One reason for such limitations is the long time that devices spend on the initial communication link set-up phase, especially when more channels are defined for transmission in the upcoming standard, such as IEEE 802.11ac [2]. Therefore, we expect that the VHT together with a fast initial link setup (FILS) can offer the most efficient tools to provide much faster data speed to the handheld devices. Moreover, these STAs strongly require the Quality of Service (QoS) aware seamless mobility connection for real-time service provisioning (e.g., VoIP and IPTV). In order to provide such real-time services, packet transmission should be continued with low packet loss, limited delay, and guaranteed throughput. Since an AP in the IEEE 802.11 WLAN usually covers a fair small service range, there are frequent handovers among APs if the STAs are moving around. Network discovery with channel scanning is also known as the first phase of handovers [3]. Therefore, we can conclude that channel scanning mechenism is a key factor which mostly affects the STAs’ experiences in the IEEE 802.11 WLAN.

In this work, we focus on the algorithm design of the channel scanning scheme for AP discovery in FILS scenario. First, we review the active and passive scanning scheme in the current IEEE 802.11 standard. In addition, based on the active scanning mechanism, the main contributions of this paper are to propose enhanced active scanning schemes that can reduce the numbers of transmitted management frames. Since channel scanning is a frequent repeating operation in mobile devices, by speeding up the discovery and by reducing the amount of overhead, the power consumption of the channel scanning is reduced and battery lifetime is improved as well. Therefore, STAs in the network can find and associate the proper AP much faster and with less battery consumption. The performances of proposed algorithms, as well as conventional active and passive scanning schemes, are also illustrated with assumptions of IEEE 802.11ai environment.

The remainder of this paper is organized as follows: Section II gives an overview of IEEE 802.11 management functions related to channel scanning. In Section III, we introduce two enhancements for the active scanning scheme. Simulation
results and performance analysis are presented in Section IV and Section V summarizes this paper.

II. PRELIMINARY

A. background

In the IEEE 802.11 standard, a STA becomes aware of the existence of a Basic Service Set (BSS) through channel scanning. Channel scanning schemes contain two groups of methods: 1) STA passively seeks beacon transmissions from AP, and 2) STA actively probe for the existence of an AP through a probe request/response exchange [1]. In this section, we introduce background information related to channel scanning methods in the IEEE 802.11 standard based WLAN, including beacon transmission, passive and active scanning schemes.

1) Beacon: In an infrastructure BSS, AP periodically broadcasts beacon frames through available channels. The beacon period defines a fixed schedule of Target Beacon Transmission Time (TBTT) and the beacon frame itself is transmitted on or as close to the TBTT as possible subject to the medium being idle. Beacon frames include the information of AP, e.g., maximum transmit power, and the channels to be used for the regulatory domain. The beacon transmission is presented in Fig. 1.

2) Passive Scanning: Passive scanning is a receive only operation that is compatible with all regulatory domains. With passive scanning, the STA listens to the channels for \( T_{\text{listen}} \) duration and looks for beacon transmissions. Once the STA has discovered the APs through beacon transmission and has APs’ information, it may then selects the strongest AP from whom it has received a beacon.

3) Active Scanning: The procedure of active scanning with 1 STA and 2 APs is illustrated in Fig. 2. In active scanning scheme, when STA starts to perform AP discovery operation, it first listens to the channels. If it receives a packet or probe delay duration elapses, it will send a broadcast probe request packet. All the APs receiving the probe request replies with probe response directed to the requested STA. If there are multiple APs receiving probe request, they may respond with a probe response using channel access procedures to avoid collisions. All the STAs that receive probe responses and beacons can get the information of APs. When selection time \( T_{\text{selected}} \) has passed after sending the probe request, the best known AP is selected by the request sender.

Comparing with passive scanning method, active scanning scheme is much faster since it can actively probe the candidate APs instead of only waiting for beacons passively. However, active scanning scheme can produce more transmission overhead comparing to passive scanning due to its active probing feature. Moreover, since probe requests are broadcasted and acknowledgments for them are not compulsory, e.g., for the broadcasted frames, errors in probe request due to collision or bad channel may result in scanning failures in active scanning mode.

B. Related work

Some channel scanning approaches have been proposed to reduce handover time, such as [3], [4] and [5]. One class of work proposes schemes aiming to reduce the number of channels to be scanned, e.g., in [3] and [4]. The major improvement of such scanning schemes in these proposals is that the scanning STA can selectively obtain the information of the active channels and thus, can scan only active channels. Another class of methods is to reduce the time spent on scanning each channel. For example, in [5], the proposed scheme reduces the passive scanning time by making all APs synchronize their beacon transmission time.

However, none of the above mentioned prior work meets our target since they need non-trivial modifications to current functions of AP or require additional hardware implementation to STAs. In addition, none of them can fulfill the requirements for FILS, i.e., the one presented in [6]. Therefore, we are going to propose enhancements for current used active scanning method, which can decrease the number of management frame exchange while highly improving the scanning performance and also meet the requirement for FILS phase in an ESS with high STA arriving density.
III. ENHANCED SCANNING SCHEMES

In this section, we are going to propose two enhancements for the active scanning scheme, which can improve the effectiveness and reliability of the current active scanning method in the FILS environment.

1) Enhanced Active Scanning Scheme 1: This method works as the normal active scanning but contains several enhancements to reduce the number of transmitted management messages, i.e., probe request/response frames. These enhancements are from both AP and scanning STA sides. When AP receives a probe request, it does not send response if:

a) there is already a probe response in the transmission buffer waiting for transmission opportunity. Transmission of beacon is scheduled to happen within next scheduling time $T_{schedule}$.

b) AP is included in the filter list of the probe request. The filter list is defined as: If STA receives a beacon or probe response from AP, it will put a filter list to the probe request. This filter list contains the address of the AP from whom STA already has a probe response.

2) Enhanced Active Scanning Scheme 2: This scheme works as the previous proposed enhanced active scanning scheme but also contains one further additional enhancement. When AP receives a probe request, it will reply with a probe response containing information on all the neighbor APs. When AP receives a probe response from another AP, it will flush the probe response messages from its own buffer.

Both of these two schemes are aiming at decreasing the number of probe request/response exchange frames while improving the scanning performance. Therefore, the time spending on searching proper AP can be reduced and power consumption for that can be reduced. In the following section, we will present our simulation results based on our IEEE 802.11ai WLAN simulator.

IV. SIMULATION STUDIES

The parameters that are used in the simulation are presented in Table I. In order to verify the performance of our proposed schemes for FILS, an ESS scenario is assumed. A simple $30m \times 30m$ indoor scenario is considered with 4 APs and 4 STAs with fixed positions. The STAs are deployed for testing the performance of channel scanning schemes in presence of other data transmissions. We refer these 4 STAs as background STAs and the transmission between background STA and AP as background transmission. Each background STA associates with one AP and transmits 0/2Mbps data flow to AP. AP also transmits with same data rate to associated background STA. The distance between transmission pair is 3m, and each AP is 10m far from the scenario boundary. The scenario is illustrated in Fig. 3. IEEE TGac propagation model [7] is considered in this simulation. 10000 STAs are assumed to be created in the random positions in this scenario with random intervals. All of these STAs use channel scanning methods to discover the best AP based on the received power level, then connect to it and transmit single packet in both uplink (UL) and downLink (DL) (200 bytes/packet). Some realistic examples of this scenario can be a large number of pedestrians entering/leaving a train station during rush hour, entering for the first time (or passing through) the coverage area of an AP within an existing ESS which is a typical deployment of cafeteria. We denote the current used active scanning method as "Active", the first proposed enhanced active scanning scheme as "EnhancedActive", and the second enhanced active scanning scheme as "EnhancedActive2". The current used passive scanning method is marked as "Passive" in the followings as well. In addition, two assumptions are made.

A. Assumptions

a) The STAs were created with mean of 1 ms, 10 ms and 100 ms intervals;

b) The above assumption results in 3 different real time simulation lengths (10s, 100s and 1000s).

<table>
<thead>
<tr>
<th>Table I</th>
<th>SIMULATION PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>Slot time</td>
<td>8 μs</td>
</tr>
<tr>
<td>Data rate</td>
<td>270 Mbps</td>
</tr>
<tr>
<td>Management message rates</td>
<td>6 Mbps</td>
</tr>
<tr>
<td>SIFS duration</td>
<td>16 μs</td>
</tr>
<tr>
<td>DIFS duration</td>
<td>32 μs</td>
</tr>
<tr>
<td>Packet size of background transmission</td>
<td>1000 bytes</td>
</tr>
<tr>
<td>Packet transmission interval</td>
<td>150 ms</td>
</tr>
<tr>
<td>Beacon size</td>
<td>145 bytes</td>
</tr>
<tr>
<td>Probe Request size</td>
<td>101 bytes</td>
</tr>
<tr>
<td>Probe Response size</td>
<td>165 bytes</td>
</tr>
<tr>
<td>Enhanced Probe Response size</td>
<td>165 bytes + 15 bytes/AP</td>
</tr>
<tr>
<td>$T_{beacon}$</td>
<td>100ms</td>
</tr>
<tr>
<td>$T_{schedule}$</td>
<td>10ms</td>
</tr>
<tr>
<td>$T_{listen}$</td>
<td>100ms</td>
</tr>
<tr>
<td>$T_{schedule}$</td>
<td>10ms</td>
</tr>
<tr>
<td>Probe delay duration</td>
<td>6ms</td>
</tr>
</tbody>
</table>

B. Simulation Results, Passive vs. Active Scanning

In Figs. 4 and 5, the Cumulative Distribution Functions (CDFs) of delays from the creation of the STA to the first time that STAs receive the information of operation parameters of AP are illustrated. In this part, we only consider passive and active scanning scheme to present the performance of
current used scheme. When CDF=1, it means that all STAs are counted. In general, we can see that the Passive scheme requires much longer time to receive operation parameters of AP than the Active scheme. That is mainly because STA has to wait for message from AP passively instead of actively probe for AP. For Passive scheme, it can be noticed that the background transmission does not have any impact on the performance as well. The delay performances appear almost the same in Figs. 4 and 5. The Active scheme, however, suffers from the background transmission. If there is no background transmission, the delay of using Active scheme is quit short, while the delay can be up to 70ms when there is total 4Mbps (2Mbps UL and 2Mbps DL) background transmission. Figs. 6 and 7 present the same delay CDF respect to the fourth time that STAs receive same information. We can observe same situation as previous two figures, e.g., the background transmission can make delay longer for the Active scheme when STA arrives at mean of 100ms. The difference is that the background transmission makes delay up to 80ms longer than the one without background transmission when the Passive method is used (Passive, creatInt:1ms). For all the cases, we can see that Passive scanning scheme results in much longer delay than Active Scanning, which can be viewed as one of the major drawbacks of using passive scanning scheme.

![Figure 4. CDF of time needed to receive the first frame containing operation parameters, 0 Mbps background transmission](image)

![Figure 5. CDF of time needed to receive the first frame containing operation parameters, 4 Mbps background transmission](image)

![Figure 6. CDF of time needed to receive the last frame containing operation parameters, 0 Mbps background transmission](image)

![Figure 7. CDF of time needed to receive the last frame containing operation parameters, 4 Mbps background transmission](image)

However, Active scheme also has its disadvantage. In Fig. 8, channel idle percentage is presented as one performance metric to see the impact of the scanning schemes on the channel occupation. We can observe that the Active scheme can decrease the channel idle time, especially when STAs enter into the scenario with high intensity (1ms interval). This is due to the exchange of probe request/response frames. Therefore, the use of Active scheme can result in longer occupation of the medium, which may lead to negative impact on system performance, e.g., APs’ capability of hosting more STAs.

![Figure 8. Channel idle time percentage, Active vs. Passive](image)
C. Simulation Results, Enhanced Active Schemes vs. Active Scheme

As we can see from previous subsection, active scanning can outperform passive scanning scheme when considering STA can receive information from AP much faster. However, Active scheme also has its inherent drawbacks. In this part, we present the performance of our proposed enhanced active scanning methods in order to show that our proposed schemes can overcome those limitations.

In Figs. 9 and 10, performance is measured by the number of probe responses that have been sent by AP. The number of transmitted probe responses indicates the amount of overhead created by the active scanning mechanism. We can see that the number of sent probe responses decreases significantly with the proposed enhancements, which means that more radio resource can be released and power consumption for transmitting them can be reduced. The reason for that is the filter list we define in the enhancement. It also indicates that STA can find proper AP with less management frame exchange. For instance, in Fig 10, we can find the EnhancedActive2 can reduce the number of probe responses up to around 23% when mean creation interval for STA is 1ms with 4Mbps background transmission.

![Figure 9. Number of sent probe responses, no background transmission](image9.png)

Channel idle percentages are also presented to see the impact of proposed algorithms on the channel occupation. From Figs. 11(a) and 11(b), we can observe that our proposed schemes help to increase the channel idle time when STAs enter into the scenario with high intensity (1ms interval). In such cases, both of the proposed schemes can reduce the cost of radio resource and thus increase the system capability of hosting more transmissions.

![Figure 11. Channel idle percentage](image11.png)

Another performance gain comes from the ability of decreasing of probe response collision time as shown in Figs. 12(a) and 12(b). As we expected, our proposed schemes can significantly decrease the collision time of probe responses, especially when there are background transmissions and STAs are created with short time intervals. In Fig. 12(b), we can observe that when creation interval is 1ms, EnhancedActive2 can reduce collision time of probe responses 3 times comparing to the one of Active scheme. However, the improvement is not such visible when low background traffic loads are considered. This is mainly because if low background traffic loads are considered, the channel idle time is already rather high without any improvements so that less collision would happen.

![Figure 12. Probe responses collision time](image12.png)

We also analyze STAs’ ability of discovering APs before associating with one of them. An AP is assumed to be discovered by a STA if the STA has received operating parameters from this AP. Fig. 13 plots how many STAs can discover...
all the APs (4 APs) in the scenario by using different active scanning schemes without background transmission. From Fig. 13, we find that if there is no background transmission, the EnhancedActive2 only achieve up to 10% better performance than the one of Active scheme. For example, when the STAs are created with mean of 100ms interval, nearly all the STAs can discover all APs in the scenario if they are using EnhancedActive2, where only less than 90% STAs know all APs using Active scheme. However, we can also observe that if the STA creation interval is 1 ms, using Active method can help more STAs to get the information of all APs. In such case, EnhancedActive scheme could be the worst choice since only more than 60% STAs can discover all APs when using it. This is mainly due to that we have defined the new rule of transmitting probe response in EnhancedActive. Therefore, STA may obtain less information from AP due to less probe request/responses exchange. However, EnhancedActive2 can mitigate this since probe response can carry other APs’ information in EnhancedActive2 scheme. Fig. 14 shows the same performance respect to with 4 Mbps background transmission as well. We can notice that EnhancedActive2 scheme outperform active scanning scheme in all cases. Especially when 1ms creation interval is considered, the performance gain is up to 5 times. We can also notice that although using EnhancedActive method can get slight better performance with two larger creation interval, only 10% STAs know all APs while 20% STAs can discover all APs by using Active scheme when creation interval is 1ms. Therefore, we can observe that the ability of STA for discovering AP is enhanced by using EnhancedActive2.

Figure 13. 4 APs are discovered, 0Mbps transmission

Figure 14. 4 APs are discovered, 4Mbps transmission

V. CONCLUSION AND FUTURE

In this paper, we have proposed two enhanced active scanning algorithms based on the current channel scanning scheme in the IEEE 802.11 standard. Aiming to reduce the number of probe request/response frames while improving scanning performance, some enhancements are made to the probe request/response exchange rules at both STA and AP sides. In the first proposed scheme, a new rule of when to send probe response is defined. In addition, extra information on neighbor APs are added into probe response in the second proposed enhancement. We have implemented our proposed scanning schemes and our simulation studies demonstrate that the algorithms are generally more efficient than existing scanning schemes. It also can be found that our proposed schemes can significantly decrease the number of probe request/response exchange frames and obtain remarkable performance gain. For the future work, we plan to investigate an effective multi-channel scanning scheme that can fully support multi-channel features and preserve handover mechanism in the upcoming IEEE 802.11 standards.

REFERENCES