On detecting WLAN users communication attempts

Fatemeh Ganji, Anatolij Zubow, Łukasz Budzisz, Adam Wolisz
Telecommunication Networks Group, Technical University Berlin, Germany
{ganji,zubow, budzisz,wolisz}@tkn.tu-berlin.de

Abstract—Power wastage in dense WLANs is a challenging problem. In order to reduce the power wastage, AP switching on/off strategies have been developed, aiming at decreasing the number of active APs (according to the traffic conditions). The efficiency of such strategies is strongly dependent on the efficiency of detecting WLAN users communication attempts, as a trigger for switching on the inactive APs. We demonstrate that such a communication attempts can be efficiently identified even for SNR values far below thresholds needed for frame reception. We present a signal-detection-based approach and verify its efficiency experimentally.

I. INTRODUCTION AND MOTIVATION

Dense WLANs, i.e., with thousands of APs per square kilometer [1], are typical scenarios for campus and enterprise networks. Such a high density of APs is provided to meet the peak of user demand but is unnecessary during the periods of low activity (e.g., at nights), leading to a considerable power wastage. In order to reduce the number of APs operating during low activity periods, we proposed to aggressively switch off the redundant APs [2]. We have analytically demonstrated that the power consumption might be significantly reduced, if APs remaining in operation provide just sufficient coverage to discover users attempting to connect, with the APs density far below what is needed to support their communication needs. After the detection of a user, an additional inactive AP may be powered on to provide the required connectivity. In [2], we have assumed that the communication attempts can be discovered by just decoding at least one of $R_{PRB-REQ}$ association attempts, transmitted by the user’s station with the most robust modulation and at full power.

In this paper we investigate another approach to discover communication attempts, using signals with SNR even lower than the level needed for successful decoding of the association requests. We demonstrate that it is possible to identify an association attempt by just observing patterns of changes in the energy level of a WLAN channel can indicate the user communication attempts. To this end, we propose a detector whose task is to detect a user attempting to connect to the WLAN by sending a train of Probe Request frames (i.e., known number of frame transmissions and time interval between two consecutive frames), with a given probability of detection and within a given delay of detection.

The main goal of this work is to experimentally verify if patterns of changes in the energy level of a WLAN channel can indicate the user communication attempts. To this end, we propose a detector whose task is to detect a user attempting to connect to the WLAN by sending a train of Probe Request frames (i.e., known number of frame transmissions and time interval between two consecutive frames), with a given probability of detection and within a given delay of detection.

II. SYSTEM MODEL

Our system consists of an IEEE 802.11b/g station attempting to connect to an Access Point (AP). We assume that the user initiates the communication by sending a train of PRB-REQs, characterized by the frame length ($< 301$ Bytes [4], including SSID, supported rate, and vendor specific fields), the time interval between two consecutive frames ($t_{int}$), in case of missing acknowledgement, and the number of PRB-REQ transmissions ($R_{PRB-REQ}$).

According to the active scanning mechanism, defined in the standard [4], PRB-REQs are broadcasted on the channel (no RTS/CTS mechanism) and, thus, the Contention Window (CW) is always set to the initial minimum size, i.e., even in case of a collision, the size of CW is not increased. The PRB-REQs sent by the user may be either successfully decoded, not decoded correctly due to the channel fading and/or an excessive path loss, or lost due to a collision [5]. It is well known that short frames are less prone to the bit-errors and collisions. Therefore, the length of the PRB-REQ is rather limited. In addition, these frames are transmitted always with the most robust modulation.

The number of re-transmissions and the time interval are vendor-specific characteristics. For stations, e.g., using Linux 802.11 configuration API [6], it is recommended that the maximum number of PRB-REQ transmission attempts should
be 5 and the time interval between the two consecutive PRB-REQs is 500 ms. These values have been obtained experimentally [6], and are system default settings that can be easily modified. Hence the active scanning mechanism generates a train of PRB-REQs, sent with an adjustable period. The active AP(s) provide the coverage required to detect the user communication attempts (Fig.1), with a given probability of detection within the maximum tolerable delay of detection \( \Delta t_{\text{det}} \). This detection can be performed by applying the following approaches:

1. Successful decoding of at least one PRB-REQ out of \( n_{\text{PRB-REQ}} \), as discussed in [2].
2. Successful partial decoding of at least one PRB-REQ (i.e., decoding of the header only).
3. Observation of patterns of changes in the energy level on the WLAN channel in the low SNR regime, when neither complete nor partial decoding of the PRB-REQs is possible. In this case, the characteristics of the train of PRB-REQs (known \( n_{\text{PRB-REQ}} \) and \( t_{\text{int}} \)) can be used in order to detect the user communication attempts.

In this paper we focus on the third approach, but the first two cases will be discussed briefly (see Sec.VI) as well.

### III. BASIC CONCEPTS FOR THE DETECTION OF THE USER COMMUNICATION ATTEMPTS

In the following section, we provide brief descriptions of Clear Channel Assessment (CCA) mechanism defined in 802.11b/g standard [4] and its theory background, which are relevant to our framework. 802.11b/g physical layer consists of two sub-layers: PLCP (Physical layer convergence procedure) and PMD (Physical medium dependent).

When the PMD sub-layer receives the energy of the transmitted frames, an indication primitive(s) is issued to report a significant received signal level or PN-code correlation strength to the PLCP. PLCP features the CCA function to determine the state of the channel. Three different methods can be adopted to perform the CCA: (1) energy-detection-based: comparison of the observed energy with a predefined threshold, e.g., the threshold is equal to \(-70 \, \text{dBm} \) for TX power \( \leq 50 \, \text{mW} \) (for more information see [4], Sec. 16.4.8.5 and Sec. 18.3.10.6), (2) carrier-sensing-based (CS-based): detection of DSSS (direct sequence spread spectrum) signal, and (3) hybrid, using combination of both (1) and (2). Whereas only the first method is used in IEEE 802.11g, the CCA mechanism can be chosen from these three methods for IEEE 802.11b transceivers.

The above-mentioned CCA mechanisms stem from principles of the Signal Detection theory, enabling us to quantify the ability of a detector to distinguish between a desired signal (e.g., transmission of the train of PRB-REQs in our case), and noise as well as the background interference, i.e., any other signal transmission. A good signal detector should distinguish a weak signal with a very small probability of false negatives \( P_{\text{FN}} \), i.e., the desired signal is present but it is not detected) and false positives \( P_{\text{FP}} \), i.e., misinterpretation of the background interference and noise), within a limited listening time period (i.e., the time period within that the samples are collected). The threshold of detection can be defined to meet these requirements, although there is a trade-off between acceptable levels of \( P_{\text{FN}} \) and \( P_{\text{FP}} \) [7]. Applying the energy-detection-based method, the desired signal can be detected if the output of the energy detector is above a pre-defined threshold. Although this approach has less computational and implementation complexity, it has been shown that they have shortcomings: (1) higher \( P_{\text{FP}} \) and \( P_{\text{FN}} \) in the low SNR regime, and (2) inefficient detection of DSSS signals [7].

On the other hand, CS-based detectors discover the similarities between the received signal and known patterns, e.g., PN-code of the DSSS signal, preamble of the frames and the periodicity in a desired signal. The latest characteristic of the signal introduces the cyclo-stationary feature. In fact, the cyclo-stationary feature is the result of periodicity of either the signal or its statistics (e.g., mean), which facilitates the detection of the signal with lower \( P_{\text{FP}} \) and \( P_{\text{FN}} \) within a limited listening time. CS-based detectors have higher performance, in terms of low \( P_{\text{FP}} \) and \( P_{\text{FN}} \), at the price of higher complexity.

The design of Atheros WLAN IEEE 802.11b/g chipsets, which are one of the most commonly used chipsets, reveals that indeed the energy- detection- and the CS-detection-based mechanisms are both applied to improve the performance of the detection method in terms of \( P_{\text{FN}} \) and \( P_{\text{FP}} \) [8]. The task of these detectors is to make decision about the transmission of a WLAN signal on the channel.

### IV. PROPOSED METHOD FOR DETECTION OF THE USER COMMUNICATION ATTEMPTS

The approach proposed here is based on the idea of cyclo-stationary-based detection, where the cyclo-stationary feature is caused by the periodic transmission of the PRB-REQs (see Sec.II). This essential feature of the PRB-REQs transmission distinguishes it from the other transmissions. In fact, two periodic WLAN-frame transmissions can be identified: (1) transmission of beacon frames, which happens every 100ms, and (2) PRB-REQ transmission during the active scanning phase. Comparing the period of the beacon and PRB-REQ transmissions, we claim that the transmission of the PRB-REQ is distinguishable from the beacon frame transmission.

Note also that the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism [4] can indeed prevent the periodic transmission due to the transmission of other WLAN devices (e.g., beacons of APs deployed in neighboring WLANs, frame transmission of other stations etc.). In other words, each PRB-REQ can be transmitted with a
delay, depending on the number of co-existing WLAN devices, and the traffic on the channel. The question is therefore, how the known pattern of transmission of the PRB-REQs can be used to detect the user. We will address this issue in the next sections.

A. Problem formulation

Detection of the transmission of a train of PRB-REQs is a binary hypothesis testing problem with the following hypotheses [9]:

\[ H_0: Y[n] = W[n] \]

\[ H_1: Y[n] = H(X[n - \Delta(K, T_K)]) + W[n] \]  

where \( Y[n], W[n], X[n] \) are the samples of the received signal, white Gaussian noise and the train of the sent PRB-REQs, respectively. \( H(.) \) is the channel transfer function, which represents the impact of fading (both small-scale and large-scale fading) and free space path-loss on the signal. \( \Delta(K, T_K) \) shows the medium access delay (in function of number of co-existing WLAN devices and generated traffic, respectively), which can occur when each PRB-REQ is transmitted on the channel.

We further assume that the transmission of a train of the sent PRB-REQs is independent of both noise and fading processes. However, the known pattern of transmission of the PRB-REQs can be negligible in comparison to design of these chipsets, the proposed PRB-REQ detector can make a decision in favor of transmission of a train of the PRB-REQs. However, similar to design of these chipsets, the proposed PRB-REQ transmission detector consists of two main functions. The scheme shown in Fig. 2 can help understand the algorithm of proposed PRB-REQ detector. The first function is a MAP (maximum a posteriori) detector, whose task is to detect the similarity between the received signal and a known pattern of transmission of a train of PRB-REQs.

1) Design of the MAP detector

Consider \( N \) samples of the received signal that are collected during the listening time period (\( T \)), when \( M \) PRB-REQs are sent on the channel. Under the assumption that the airtime of a single PRB-REQ is significantly less than \( t_{air} \) (e.g., the length of a transmission is 100 Bytes, sent every 500ms, with the lowest possible data rate, 1 Mbps), the train of the PRB-REQs can be denoted by a train of delta functions:

\[ x[n] = \sum_{k=1}^{N} \delta[n - \frac{NK}{M}] \]  

(2)

It has been shown that the optimal detection in white Gaussian noise is the MAP (maximum a posteriori) [12]. Using the MAP rule results in the following inequality:

\[ H_0: r_{xy} < \sum_{\Delta(K, T_K)} H(X[n])^2 = \frac{1}{2} \epsilon \]

\[ H_1: r_{xy} \geq \frac{1}{2} \epsilon \]

(3)

where \( \frac{1}{2} \epsilon \) is the threshold of detection, corresponding to the energy of received samples, \( r_{xy} \) is the cross correlation between the received signal and the train of the sent PRB-REQs:

\[ r_{xy} = \sum_{n=0}^{N-\Delta} Y[n]X[n] = \sum_{n=0}^{N-\Delta} Y[n]\delta[n - \frac{NK}{M}] = \sum_{n=0}^{N-\Delta} Y[n - \frac{NK}{M}] \]  

(4)

Regarding the central limit theorem, the \( P_{FA} \) and \( P_{FP} \) can be calculated as follows [12]:

\[ P_{FA} = \text{Prob}(r_{\text{xy, max}} > \gamma | H_0) = Q \left( \frac{\gamma}{\sqrt{\sigma^2}} \right) \]

\[ P_{FP} = \text{Prob}(r_{\text{xy, max}} < \gamma | H_1) = 1 - Q \left( \frac{\gamma}{\sqrt{\sigma^2}} \right) \]

(5)

where \( \gamma = \frac{\epsilon}{2} \), \( \sigma^2 \) is the noise variance and \( Q(.) \) is the standard Gaussian complementary CDF. Let \( \text{SNR}_{\text{wall}} \) be the minimum theoretical SNR, at which the MAP detector can distinguish between the white Gaussian noise and the transmission of a signal on the channel within a limited listening time period.

Due to the fact that \( \text{SNR}_{\text{wall}} = \frac{\epsilon}{2\sigma^2} \), hence \( \gamma = \frac{\text{SNR}_{\text{wall}} \sigma^2}{2} \) and Eq. (5) can be re-written as:

\[ P_{FA} = \text{Prob}(r_{\text{xy, max}} > \gamma | H_0) = Q \left( \sqrt{\frac{\text{SNR}_{\text{wall}}}{2}} \right) \]

\[ P_{FP} = \text{Prob}(r_{\text{xy, max}} < \gamma | H_1) = 1 - Q \left( \sqrt{\frac{\text{SNR}_{\text{wall}}}{2}} \right) \]

(6)

2) Design of the cyclo-stationary-based detector
As it can be seen in Fig. 2, \( H_1 \) can be declared, if both outputs of the MAP and a cyclo-stationary-based detectors are “True”. The cyclo-stationary-based detector calculates the correlation coefficient between the received signal and the train of the sent PRB-REQs. The correlation coefficient shows the strength of linear relation between these signals:

\[
\rho_{xy} = \frac{\text{E}(x[n]-\text{E}(x[n]))(y[n]-\text{E}(y[n]))}{\sigma_x^2 \sigma_y^2}
\]

where \( \text{E}(.) \) returns the mean value. Let us calculate (7) for the case of \( H_0 \): \( \text{E}(y[n] = W[n]) \):

\[
\rho_{xy} = \frac{\text{E}(x[n]-\text{E}(x[n]))W[n]}{\sigma_x^2 \sigma_w^2} = 0
\]

Eq.(8) is valid if there is no medium access delay \( (\Delta t < K\Delta t) \), which is not always the case in practice. As mentioned previously, we can define the 95 % confidence interval for significance of the correlation coefficient \( (\alpha) \). The detector compares \( \rho_{xy} \) and \( \alpha \) to confirm the correlation between these signals and the transmission of the PRB-REQs, consequently.

V. EXPERIMENT DESCRIPTION

We aim to experimentally evaluate the performance of the proposed detector in terms of metrics that are defined in this section. Here we also introduce the setup and explain the design of the experiment.

A. Metrics

We define two comprehensive sets of metrics used for (1) designing the PRB-REQ transmission detector, and (2) evaluating the performance of the designed detector in practice.

1) Metrics used to design the PRB-REQ transmission detector

1. Probability of false positives (\( P_{FP} \)) and probability of false negatives (\( P_{FN} \)) for MAP detector as well as SNR_\text{wall}: as defined in Sec. III and Sec.IV.A, respectively.

2. Delay of detection of the PRB-REQ transmission: the time, which the user spends to send PRB-REQs to be detected. This delay is indicated by \( \Delta t_{\text{Det}} \).

3. Listening time period: the time period within that the samples are collected. The listening time period can be equal to, or greater than, \( \Delta t_{\text{Det}} \).

In order to design the proposed detector of the PRB-REQ transmission, we adopt the values recommended in the literature (e.g., [9]): \( P_{FP} = P_{FN} = 0.1, \text{SNR}_\text{wall} = -10 \text{dB} \).

We assume that the user can tolerate a 10 s delay of the detection (\( \Delta t_{\text{Det}} = 10 \text{ s} \)).

1) Metrics used for evaluating the performance of the PRB-REQ transmission detector

1. The range of the average SNR, at which the PRB-REQ transmission detector can detect the transmission of the train of the PRB-REQs, whose characteristics, i.e., \( n_{\text{PRB-REQ}} \) and \( f_{\text{inter}} \), are known.

2. Probability of false negatives (\( P_{FN_{\text{det}}} \)): the number of train of PRB-REQs, received with a given level of the average SNR and not detected correctly, out of the total number of trains sent with the same average SNR.

3. Probability of false positives (\( P_{FP_{\text{det}}} \)): the number of listening time periods, in which the transmission of other signals on the channel is misinterpreted as transmission of a train of PRB-REQs, out of total number of listening time periods.

B. Setup of the experiment

To conduct experiments, we use a laptop (station), an off-the-shelf IEEE 802.11 AP and a spectrum analyzer.

The off-the-shelf WLAN AP consists of a Wistron Neweb CM9 card using Atheros 5004 chipset, operating in License-Exempt (ISM) 2.4 GHz band [13]. The receiver sensitivity of the AP is -95 dBm at 1 Mbps.

R&S-FSV spectrum analyzer [14] is a fast (5 times faster than other comparable spectrum analyzers) and reliable instrument whose frequency range is up to 7 GHz. It features an analysis bandwidth of up to 28 MHz that exceeds the channel width of IEEE 802.11b/g signals. Measuring power spectral density (PSD), it has a measurement uncertainty of 0.4 dB up to 7 GHz. SMUTS (Spectrum Measurement ToolS) [15] is run on a laptop connected to this instrument to collect the PSD data about every 6 ms during the period of the experiment. The collected data is further fed to the PRB-REQ transmission detector (a Matlab code) and the processing is done offline in Matlab.

C. Experiment design

To conduct the experiment, we should first deal with the interference that may lead to a loss of a PRB-REQ. To reduce the impact of interference on our experiment, we conducted it on weekends with all unnecessary IEEE 802.11b/g APs and Bluetooth equipment being powered off. Furthermore, by running tcpdump and sniffing frames transmitted on all the channels, we try to find the channel, on which the minimum number of APs is operating. The AP is set to sniff all frames sent by all users and APs in its vicinity on this channel.

The AP is placed in one laboratory room and the station (transmission power of which, \( P_{TX} \), is set to 0.1 and 2 dBm for different experiments) is placed in a location, chosen based on
an observation: we alternately run tcpdump (sniffing full frames) and Kismet (capturing the headers of frames) to examine if the PRB-REQs, or the header of them can be decoded correctly, when the station is placed at different distances from the AP. According to this observation, when the station is placed at D~40 m distance from the AP, neither the PRB-REQs nor the header of them can be decoded. Therefore, it may be possible to examine the idea of detection of the communication attempts by using the proposed detector, when the station is placed at this location.

R&S-FSV spectrum analyzer is placed near the AP (see Fig. 3). In order to receive approximately the same level of the signal, the distance between the antenna connected to the R&S FSV spectrum analyzer and the antenna connected to the off-the-shelf AP should be equal to the signal wavelength at 2.4 GHz (\(\lambda=12.5\) cm) or multiples of that. Therefore, the distance between the two antennas is set to 25 cm (\(2\times\lambda\)), chosen due to the size of the AP and R&S-FSV spectrum analyzer.

In this work we use the default value of \(t_{int}=500\,\text{ms}\). It is worth mentioning that the propagation and the transmission delay of the PRB-REQs are in order of \(\mu\)s and are thus negligible in comparison to \(t_{int}\). Regarding the assumed maximum delay of detection, we can calculate the number of PRB-REQ transmissions: \(n_{\text{PRB-REQ}} = \frac{2t_{int}}{\lambda f_{TX}} = 20\).

VI. RESULTS AND DISCUSSION

Although in this work we focus on detection of the user communication attempts by using the proposed detector, it is helpful to briefly consider the other two possible approaches mentioned in Sec.II. Furthermore, we discuss how the noise variance is measured in our experimental framework. Afterwards, we present the results of the performance evaluation of the designed PRB-REQ-transmission detector.

1) Note on the relation of probability of decoding and SNR of the PRB-REQ

In addition to theoretical approaches, e.g., [2], the relation between the probability of decoding \(P_{\text{Dec}}\) and the SNR of the frames for a given receiver has been experimentally studied in the literature. The experiment conducted in [16] reveals that for Prism2.5 chipset [17], when \(P_{\text{Dec}}\) for 1Mbps data rate varies between 10\% and 90\%, the SNR of the correctly decoded frames differs between about -2 dB and 1 dB. In [18], the experiment performed on an Atheros chipset [19] shows that if the SNR is above a certain threshold (received signal strength, RSS, is equal to, or greater than, about -100 dBm), \(P_{\text{Dec}}\) is almost 100\% [18].

In an attempt to address this relation, we apply the model recommended and verified in [18] (Fig. 4, dashed-line curve) and try to measure the threshold of the SNR, where the \(P_{\text{Dec}}\) is virtually 100\%. In order to measure the threshold, the transmission power of the station is set to 0 dBm (minimum \(P_{TX}\) of the station), with which we send 300 PRB-REQs (103 Bytes each). For this experiment, the station is placed in about 30m distance from the AP, where \(\sim75\%\) of the total number of sent PRB-REQs can be sniffed by running tcpdump (correctly decoding the frame). According to the applied model, SNR of the frames, which are not sniffed, is below the threshold.

The result of the measurement is depicted in Fig. 4. In this figure, each point (cross markers) represents a set of frames, decoded successfully with a given SNR. The SNR is calculated based on the information (the RSS and the noise variance at the antenna of the AP), available in the radiotap header of the decoded PRB-REQs. As it can be seen, the threshold of the SNR, observed in our experiment is 0 dB (noise variance is equal to -96 dBm and RSS = -96 dBm) for the tested AP [13].

Moreover, one can have an intuition that the threshold of the SNR, at which only the header of the PRB-REQ is decoded with probability of \(\sim100\%\), is lower than the threshold of decoding the whole PRB-REQ. This can be explained by the fact that for a given bit error rate (BER), the frame error rate (FER) of the header of the frame is less than the FER of the whole frame due to the shorter length of the header (26 Bytes versus 103 Bytes for the full frame). In other words, we may expect that the dashed-line curve, shown in Fig. 4, would be shifted to the left in this case. To examine this, we repeat the experiment under the condition that the station is placed in 32m distance from the AP, where the number of PRB-REQs sniffed by tcpdump is dramatically decreased to \(\sim10\%\) of the total number of sent frames (300 frames).

Based on the fact that Kismet can decode only the header of the frames, we can obtain the information about the PRB-REQs, whose headers are correctly decoded and the SNR of them, by running Kismet on the AP. We observe that however, the number of correctly decoded headers of PRB-REQs is increased in comparison to the number of correctly decoded PRB-REQs, the threshold of decoding the header of the PRB-REQ is 0 dB as well (square markers in Fig. 4). This can be related to the fact that although the header is shorter than the whole PRB-REQ, they are both sent with the lowest possible data rate (1Mbps in our case).

To sum all up, no difference in terms of threshold of the SNR, where the \(P_{\text{Dec}}\) is almost 100\%, is observed between the successful decoding of a PRB-REQ and its header. And the threshold of the SNR, observed in our experiment is 0 dB (noise variance is equal to -96 dBm and RSS = -96 dBm) in both cases.

2) Note on the measurement of the noise variance

In order to measure the average SNR of a train of the PRB-REQs, we have to first measure the noise variance, when the PSD values are collected by FSV spectrum analyzer. As stated in [9], the variance of the white Gaussian noise can differ from
In order to provide an example of how the noise variance changes over time, we record the PSD values measured by the FSV spectrum analyzer for 270s. The noise variance for the data collected every 10s (equal to the listening time period) is calculated in offline fashion by using autoregressive model, AR(p=3) [20] and shown in Fig. 5. It can be seen that the variance of the noise varies for different listening time periods. Hence in our experiment, instead of assuming a constant value for noise variance, we measure the noise variance for each listening time period.

3) Verification of the performance of the proposed detector in terms of $P_{FN-det}$

In this experiment, the station is placed in 40 m distance (see Sec.V.C.) and 100 trains are sent with $P_{TX} = 0$ dBm, then we increase $P_{TX}$ to 1 dBm and send another 100 trains. Afterwards, $P_{TX}$ is set to 2 dBm and additional 100 trains are sent (making it 300 trains). Each train contains 20 PRB-REQs sent every 500 ms. We can calculate the average SNR of the train of the PRB-REQs as $\bar{SNR} = \frac{1}{N_{train}}\sum |h(n)|^2$, where $\sigma^2$ is the noise variance, measured as explained in Sec.VI.2. We observe that the average SNR of the trains varies between -7.8 dB and 1.13 dB, corresponding to $\sim$ -103.3 dBm $\leq$ avg. RSS $\leq$ $\sim$ -97.12 dBm. The histogram plotted in Fig. 6 shows how the average SNR of the trains of the PRB-REQs varies.

In Fig. 7, the vertical axis on the left-side indicates the number of correctly detected trains. The bar chart reveals how this number varies for the different intervals of the average SNR. The vertical axis on the right-side corresponds to the curve showing the percentage of the correctly detected PRB-REQ trains (equal to the ratio of the number of correctly detected PRB-REQ trains and the total number of PRB-REQ trains, whose SNR is in the given range), with 95% confidence intervals. To have statistically meaningful analysis, we consider intervals of the average SNR, where the number of PRB-REQ trains (see Fig. 6) is equal to, or greater than, 30 (10% of the total number of sent trains): -6 dB $\leq$ avg. SNR $\leq$ 0 dB.

It can be seen that if the average SNR of the train of PRB-REQs is between -6 dB and 0 dB, the probability of correct detection is at least 84.6% (mean value is $\sim$ 91% and standard deviation is 5.56%). Thus, $P_{FN-det}$ is less than 15.4%.

4) Verification of the performance of the proposed detector in terms of $P_{FP-det}$

We perform a measurement in order to evaluate the performance of the proposed detector in terms of $P_{FP-det}$, i.e., no PRB-REQ train is transmitted but the detector makes decision in favor of transmission of a train of PRB-REQs. The PSD values measured by the FSV spectrum analyzer for 1000 s (equal to 100 listening time periods) are collected and fed to the proposed detector. The average of the SNR of signals transmitted by other co-existing radios working on the channel is between -1.5 dB and +0.5 dB (the average of the noise variance is $-96.6$ dBm) in this case. In 10 listening time periods (out of 100), the detector makes decision in favor of transmission of a train of PRB-REQs. Hence $P_{FP-det}$ = 10%. Note that $P_{FP-det}$ is not as critical as $P_{FN-det}$ in our scenario. An increase in $P_{FP-det}$ results in switching on an additional inactive AP(s) that can be switched off afterwards, if no user attempts to connect to it (e.g., no PRB-REQ is decoded correctly after one listening time period).

5) Power saving potential in dense WLANs
Here we analytically assess the potential power saving of our proposed approach for detecting the user communication attempts. We perform numerical analysis in Matlab according to the procedure described in [2]. Similar to [2], in order to calculate the power saving, we compare the power consumption of a reference WLAN, with density of 2960 APs/km² [1] with the power consumption of the APs [21] providing only the detection coverage over the target area (1 km²). According to WLAN AP power consumption data available in, e.g., [22], power consumption of each AP can be approximated as 10 W.

Let σ²= -96 dBm, P_TX be 20 dBm, path-loss exponent and standard deviation of the slow fading be equal to 2.5 and 6.8 dB, respectively (similar to indoor scenario defined in [2]). The results of the analytical assessment presented in [2], as well as the numerical analysis for the AP used in our experiment [13] are shown in the figure (star and square markers, respectively). The difference between these two results is due to the different receiver sensitivities of the APs. We further calculate the number of APs required for decoding either the header or the full PRB-REQs (SNR= 0 dB). For the considered scenario, the number of APs providing the coverage with 1Mbps data rate is equal to the number of APs required to decode either full frame or only the header of PRB-REQ. And when the target area is covered by the APs [13] providing the detection coverage, instead of providing the full capacity at the highest data rate (e.g., 11 Mbps following IEEE 802.11b), the power saving potential is in the range of 99% of the total consumed power in the reference WLAN.

More importantly, we calculate the number of APs using proposed PRB-REQ transmission detector to discover the user communication attempts. Let the average RSS be equal to -97.5 dBm (SNR= -0.5 dB), similar to what has been verified in our experiments. From Fig. 8, it can be understood that the number of APs detecting a user by observing the pattern of changes in the energy on the WLAN channel is less than the number of the APs required to detect the user by decoding the PRB-REQ. And the corresponding power-saving improvement is 36%.

Although this power saving potential is significant, it is achieved at the expense of an increase in the number of false negatives, representing an increase in delay of user detection. Nevertheless, we show that this delay does not exceed a tolerable level.

6) Limitations

The performance of the detector can be influenced by how the confidence interval for significance of the correlation coefficient is chosen.

Moreover, the performance of the detector is verified under a certain condition, where there are no ongoing transmissions between the AP and the other users. Otherwise, the detector may misinterpret the ongoing transmissions as being the transmission of the train of the PRB-REQs. However, the considered condition can be easily met during low activity periods (e.g., at nights).

Last but not least, regarding the feasibility of applying the proposed approach in practice, please note that the implementation of our approach requires minor software modifications from user side (e.g., adjustment of n_{PRB-REQ} and t_{int}). On the other hand, from WLAN side, the proposed PRB-REQ-transmission detector should be implemented on the APs. We suggest that the PRB-REQ-transmission detector can be implemented in parallel to energy- and the CS-based detectors used in WLAN IEEE 802.11b/g chipsets. This may require software modifications. Nevertheless, the discussion of possibly necessary modifications is beyond the scope of this study.

VII. CONCLUSION

In this paper we propose a detector, which can be used to discover the transmission of the train of PRB-REQs, with sufficiently low probabilities of false negatives and false positives in the low SNR regime. We verify experimentally that the cyclo-stationary feature of the train of PRB-REQs enables us to detect that, when the average SNR of the train of PRB-REQs varies between -6 dB and 0 dB (less than the SNR required to decode the PRB-REQs successfully).

The importance of such a detection lies in the fact that the power saving in WLAN is directly related to the minimum SNR, sufficient for detecting the train of PRB-REQs sent by the user in order to connect to the WLAN. Therefore, by performing numerical analyses, we have shown that the power-saving improvement can be 36%, which may be achieved at the expense of an increase in the number of false negatives.

ACKNOWLEDGMENT

The work has been funded from the EU 7th Framework Program (FP7/2007-2013) under grant agreement n. 257740 (Network of Excellence “TREND”).

REFERENCES


