Misbehavior Detection in Wi-Fi/LTE Coexistence over Unlicensed Bands

Islam Samy[1], Xiao Han[2], Loukas Lazos[1], Ming Li[1], Yong Xiao[3], and Marwan Krunz[1]
[1] University of Arizona, [2] University of South Florida [3]Huazhong University of Science and Technology

Abstract—We address the problem of detecting misbehavior in the coexistence etiquette between LTE and Wi-Fi systems operating in the 5 GHz U-NII unlicensed bands. We define selfish misbehavior strategies for the LTE that can yield an unfair share of the spectrum resources. Such strategies are based on manipulating the operational parameters of the LTE-LAA standard, namely the backoff mechanism, the traffic class parameters, the clear channel access (CCA) threshold, and others. Prior methods for detecting misbehavior in homogeneous settings are not applicable in a spectrum sharing scenario because the devices of one system cannot decode the transmissions of another. We develop implicit sensing techniques that can accurately estimate the operational parameters of LTE transmissions under various topological scenarios and *without decoding*. These techniques apply correlation-based signal detection to infer the required information. Our techniques are validated through experiments on a USRP testbed. We further apply a statistical inference framework for determining deviations of the LTE behavior from the coexistence etiquette. By characterizing the detection and false alarm probabilities, we show that our framework yields high detection accuracy at a very low false alarm rate. Although our methods focus on detecting misbehavior of the LTE system, they can be generalized to detect Wi-Fi misbehavior and to other coexistence scenarios.

1 Introduction

The high demand for wireless services has fueled a severe shortage in radio spectrum resources. The regulatory approach for meeting this galloping demand is to allow the coexistence of competing wireless technologies in common bands. An example of such coexistence is that of LTE and Wi-Fi in the 5 GHz U-NII band [2]–[4], which has already become a reality. Recent reports have shown that there are 36 cellular operators currently investing in LAA, nine of which have already deployed/launched networks [5]. Furthermore, there are 21 commercially available modems equipped with chipsets that are LAA-compatible, many of which are integrated into smartphones from leading manufacturers [6]. Moreover, a recent measurement campaign performed between January and March 2020 in various locations in the Chicago metropolitan area revealed that all three major US cellular carriers operate dense LTE-LAA deployments [7]. The study reported 557 unique LAA physical cell IDs (PCIs) running Release 13 of LAA where all downlink traffic is over the unlicensed 5 GHz band, whereas the uplink traffic is over licensed bands.

However, shared spectrum introduces novel challenges for the secure, efficient, and fair channel access. Many of these challenges arise from the heterogeneity of the coexisting systems, the system scale, and the lack of explicit coordination mechanisms between them. Such heterogeneity is manifested in different PHY-layer capabilities, channel access dynamics (dynamic vs. fixed), schedule-based vs. random access, interference-avoiding vs. interference-mitigating, etc. Altogether, this creates a complex coexistence scenario without a unified control plane.

Several recent efforts have addressed the problem of fair coexistence of LTE/Wi-Fi and Wi-Fi/Zigbee under benign settings (e.g., [8]–[20]). Recent analytical and experimental studies have shown that an LTE system could cause serious performance degradation to a co-present Wi-Fi system, even if the LTE remains protocol-compliant [21], [22]. The main approach to address unfair channel access is to introduce the Licensed-Assisted Access (LAA) protocol that follows the Listen-Before-Talk (LBT) mechanism [23]. Tao *et al.* showed that dynamically adjusting the contention window (CW) size can be beneficial for fair coexistence [24]. Follow-up works achieved further improvements by controlling other protocol parameters and applying other enhancements, e.g., [25]–[27].

Intentional violations of the coexistence etiquette to gain an unfair spectrum share have not been studied at length. The dangers of ignoring the coexistence etiquette systematically is a serious and realistic threat. The measurement campaign in [7] reported that the authors *never observed LAA, irrespective of the operator, dynamically adapting its unlicensed channel usage in response to Wi-Fi usage of the same channels.* Ying *et al.* were among the first to consider the problem of misbehavior when cycle-based LTE-U and Wi-Fi coexist [28]. The authors recognized that because the LTE duty cycle is unilaterally controlled by the LTE system, it can be abused to increase LTE's spectrum share. They proposed a monitoring mechanism that accurately estimates the duty cycle and allows a spectrum manager to detect any misbehavior. The proposed scheme is not applicable to LTE-LAA, which is embraced by most operators and the standardization bodies [23]. *In this paper, we focus on misbehavior detection mechanisms specific to the prevailing LTE-LAA standard.*

Our methods build upon prior works on misbehavior detection for homogeneous networks, e.g., [29]–[32], with notable differences. First, heterogeneous networks do not share common coordination channels for communicating explicit control information such as the network allocation vector (NAV) field, device IDs, reservation messages (RTS/CTS), etc. Without explicit coordination, detecting the state and monitoring the behavior of stations operating under a different technology is challenging, as the messages exchanged by one system are undecodable at the other. Relevant challenges include determining which system occupies

An abridged version of this paper appeared in the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (Wisec), 2018, [1].

the channel, for how long, at what locality, with what range, and which stations collided, to name a few. Moreover, although the LTE-LAA and Wi-Fi standards follow the same carrier-sense multiple access (CSMA) approach, they adopt different channel contention parameters that affect the overall system behavior. Determining a system's behavior requires accurate estimation of these parameters but using only implicit monitoring. We propose a framework that detects LTE misbehavior when coexisting with Wi-Fi. Our framework relies on implicit sensing mechanisms that provide accurate approximations of the operational parameters. Our contributions are summarized as follows:

- We study the problem of channel access misbehavior of LTE-LAA when coexisting with Wi-Fi. Although possible misbehaving strategies bear resemblance to those in a homogeneous setting, we highlight novel challenges that stem from the technology heterogeneity and lack of explicit coordination.
- We introduce a new suite of monitoring mechanisms that do not rely on signal decoding for estimating relevant LTE-LAA protocol parameters. We develop implicit sensing techniques that go beyond simple LTE transmission detection to determine the presence of hidden stations, identify retransmitted frames, and specify the LTE priority class. These are essential parameters for accurately estimating the overall LTE behavior.
- We validate the effectiveness of the implicit parameter-estimation techniques in a USRP testbed. We show that these techniques are reliable and accurate.
- We introduce additional types of misbehavior such as the CCA threshold manipulation and defer manipulation. For these new misbehavior strategies, we show that they can all be reflected on the estimated backoff counter.
- We investigate the detection performance under different traffic loads and adapt our framework accordingly to guarantee high detection and low false alarm probabilities. We perform extensive simulations to validate the proposed misbehavior detection mechanism and show that our approach yields near-perfect detection probability and a negligible false alarm rate.

Our framework also involves a statistical inference method for identifying misbehavior from a time series of backoff counters. This is a fairly standard technique and similar methods have been applied for homogeneous networks. We further highlight that although we focus on the misbehavior of LTE devices, our framework is general and can be applied for detecting Wi-Fi misbehavior. Furthermore, the implicit parameter estimation techniques can be applied to a homogeneous network, although some observations can be collected via decoding.

The remainder of this paper is organized as follows. We discuss related works in Section 2. The system and misbehavior models are introduced in Section 3. The adopted implicit techniques for monitoring LTE activities are detailed in Section 4. In Section 5, we demonstrate how the LTE channel access behavior can be accurately evaluated. We validate the performance of the proposed implicit techniques in Section 6. We analyze the detection scheme performance in Section 7 and summarize the main contributions of this work in Section 8.

2 Background and Related work

Related Work. LTE/Wi-Fi coexistence in a benign setting has been studied extensively [14]–[20]. Ratasuk *et al.* [22] showed that LTE outperforms Wi-Fi by replacing one of the Wi-Fi deployments with an LTE cell and comparing the respective throughput. In [7], the authors conducted a measurement campaign for the Chicago metropolitan area. The measurements showed that the LTE/Wi-Fi coexistence in dense, urban environments continues to be a challenging problem and that the coexistence ettiquete is not followed. Hirzallah *et al.* [33] showed that different access protocols for Wi-Fi and LTE can cause an increased collision rate and latency for both systems. They suggested a CCA threshold adaptation mechanism to promote fairness. In [17], the authors proposed a framework for adapting the CW sizes based on observed transmissions, to promote fair airtime distribution. Adapting the backoff parameters to achieve fair coexistence was also studied in [24]–[27]. However, these works assumed that all stations are trustful and protocol-compliant.

Misbehavior detection for channel access in homogeneous networks has been extensively studied, especially for IEEE 802.11 protocols (e.g., [29]–[31], [34], [35]). In [29], the authors introduced modifications to the IEEE 802.11 protocol to simplify misbehavior detection and presented a penalty scheme for punishing selfish users. Li *et al.* [31] used multiple backoff counter observations to calculate the probability Y of choosing a small backoff counter. This probability was compared with the expectation $E(Y)$, considering no misbehaving, multiplied by a detection factor μ. If $Y \leq \mu E(Y)$, the terminal was identified as misbehaving. In [36], the authors proposed a framework that detects misbehavior by comparing the average estimated backoff counter across all observations with some threshold.

Tang *et al.* proposed a real-time misbehavior detection mechanism, which relies on the difference between the number of successful transmissions of a given terminal n and other terminals [30]. Toledo *et al.* applied the Kolmogorov-Smirnov test to detect misbehavior from the number of idle slots between two transmissions [34]. As all stations follow the same protocol, misbehavior is detected if the idle slot distribution of a station differs from that of the compliant protocol. Whereas there is a wealth of interest in channel access misbehavior for homogeneous networks, misbehavior between coexisting technologies is relatively new. The work closest to ours is reported in [28]. However, the authors considered the misbehavior in the CSAT-based LTE-U protocol, not LAA. They developed a method for estimating the LTE duty cycle by tracking LTE transmissions. The latter are identified based on the frame length, as LTE frames are typically longer than Wi-Fi frames. Possible LTE misbehavior is detected by a central node called the spectrum manager, which has prior knowledge of the permitted duty cycle for LTE.

The pivotal difference between our work and misbehavior detection in homogeneous networks lies in the monitoring mechanisms for obtaining samples of behavior. All prior works rely on frame decoding to attribute transmissions to their originators. This is not generally possible between different technologies. Moreover, LTE and Wi-Fi systems execute channel access protocols with different parameters. For instance, the LTE-LAA backoff parameters depend on the priority class. Accurate estimation of the LTE behavior requires mechanisms for classifying frames according to their respective classes. Additional challenges stem from the heterogeneity in transmission and interference ranges. A Wi-Fi station may backoff in the presence of an LTE transmission, but the converse may not occur.

Our work is similar to the state-of-the-art for homogeneous networks in the analysis of the time series representing the LTE behavior. Like some prior works, we use statistical inference to identify misbehavior with some differences. Contrary to the work

Fig. 1: Backoff between two consecutive transmissions.

in [31], [36], we use the Jensen-Shannon divergence to detect deviation from the nominal behavior rather than relying on first-order moments of the distributions. This is a reliable metric because the same moments can be satisfied by multiple distributions. Other inference methods could also be used here such as the Kolmogorov-Smirnov test employed in [34]. On the other hand, the work in [30] can be only applied if all competing terminals are assumed to have equal channel access opportunities. However, this assumption does not hold in heterogeneous coexistence where devices use different priority classes and have different airtime per transmission. Fair channel access does not translate to an equal number of transmissions, as it may be the case for homogeneous networks running the same protocol with the same parameters.

LTE-LAA Release 15: We consider an LTE system that follows the LAA Release 15 specification [23]. The standard defines four traffic priority classes. The first two classes are suitable for transmitting control messages and short frames, whereas classes C_3 and C_4 accommodate longer LTE frames.

Downlink channel access: The downlink channel access mechanism of LTE-LAA is shown in Fig. 1 with parameters listed in Table 1. The channel access steps are as follows.

1) Before transmitting a frame, the eNB freezes for an initial time T_{init} consisting of a defer time $T_{def} = 16\mu s$ plus p observation slots, each of length $T_s = 9\mu s$. The parameter p takes larger values for lower priority classes to compensate for the longer frame size. If the channel stays idle during T_{init}, the eNB proceeds to the backoff phase described in Step 2, otherwise it repeats Step 1. The channel state (busy or idle) is determined by sensing the power on a given channel. If the power is less than the CCA threshold ($P_{th} \approx -72$ dBm according to [23]), for at least $4\mu s$, the channel is inferred to be idle and it is busy, otherwise.
2) The eNB initializes the backoff counter to a value b uniformly selected in $\{0, 1, \ldots, q-1\}$, where q is the contention window (CW) size, initially set to a minimum value $q_{\min}$.
3) The eNB decrements its backoff counter by one with every idle slot. If a slot is sensed busy, the eNB freezes its backoff counter until the channel becomes idle. The channel must remain idle for T_{init} before the backoff countdown can be resumed.
4) When the backoff counter becomes zero, the eNB transmits a frame with a maximum duration of T_{MCOP}. The eNB then waits for an ACK/NACK. If it receives an ACK, the transmission round is completed. Otherwise, the process is repeated from Step 1 by doubling the CW size, up to a $q_{\max}$.

Uplink channel access: To make an uplink transmission, a UE must receive an uplink (UL) grant permission from the eNB. The UL grant permission determines the access type that should be used by the UE. The standard specifies two candidate types.

- Type 1: The UE follows the same backoff process as in the downlink, but with slightly different parameters (see Table 1).
- Type 2: The UE waits for the channel to be idle for 25 μs and then accesses the channel without further contention.

From both the DL and the UL procedures, we note that the priority classes differ in both the defer time and allowed CW sizes. As will be shown later, these differences can be exploited by LTE devices to shorten the time between consecutive transmissions.

TABLE 1: LTE parameters for different priority classes.

Class	p (slots)	$q_{\min}$ (slots)	T_{MCOP} (ms)	q (slots)
Downlink channel access				
C_1	1	4	2	$\{4, 8\}$
C_2	1	8	3	$\{8, 16\}$
C_3	3	16	8 or 10	$\{16 - 64\}$
C_4	7	16	8 or 10	$\{16-1024\}$
Uplink channel access				
C_1	2	4	2	$\{4, 8\}$
C_2	2	8	4	$\{8, 16\}$
C_3	3	16	6 or 10	$\{16-1024\}$
C_4	7	16	6 or 10	$\{16-1024\}$

3 Models and Framework Overview

3.1 System Model

We consider N_L LTE devices that coexist with N_W Wi-Fi access points (APs), each serving a set of Wi-Fi devices, over the 5 GHz unlicensed band. The one-hop neighborhood set (other devices inside the interference range) of device X is denoted by $\mathcal{N}_X^{(1)}$. LTE devices and Wi-Fi APs may transmit at different powers, so $Y \in \mathcal{N}_X^{(1)}$ does not imply that $X \in \mathcal{N}_Y^{(1)}$. As an example, in Fig. 2, AP B is in the interference range of LTE A (solid line), but LTE A is not in the interference range of B (dashed line). The transmission powers of the LTE and Wi-Fi are denoted by P_ℓ and P_w, respectively. LTE devices and Wi-Fi terminals are considered to follow the LTE-LAA and IEEE 802.11ac standards, respectively.

We consider the misbehavior of one or more LTE devices which are monitored by any AP in their vicinity. The monitoring APs can perform simple operations on RF signals like sampling and correlation. LTE-related observations are collected by APs and analyzed at a central hub. This could be achieved through a cloud service that allows the uploading of all observations made by the APs to a central repository. Such scenario is relevant in enterprise networks where multiple APs are under a single administrative control or can be offered as an overlay service to which APs subscribe. This assumption also helps us identify if misbehavior is detectable at the system level, given all distributed observations.

We initially focus on detecting the LTE misbehavior in backlogged conditions. Under such conditions, gains in performance due to LTE misbehavior occur at the expense of the Wi-Fi system. We later consider the detection of LTE misbehavior under unsaturated traffic conditions.

3.2 Misbehavior Model

The goal of a misbehaving LTE is to capture the channel more frequently and for a longer time than competing APs. This can be achieved by manipulating the LAA protocol parameters in the uplink or downlink direction.

Misbehavior in the downlink direction. This is the most beneficial type of misbehavior because the downlink direction carries a far higher traffic volume than the uplink one and the eNB nodes transmit to a large number of LTE devices. An eNB node can misbehave in the following ways.

1) Decrease the defer time p: An LTE device can reduce the defer time to initiate the backoff countdown process faster. It can select a defer time that belongs to a high priority class and transmit a frame of low priority class with longer duration. Alternatively,

Fig. 2: Coexistence between LTE and Wi-Fi. Wi-Fi and LTE stations have different interference ranges.

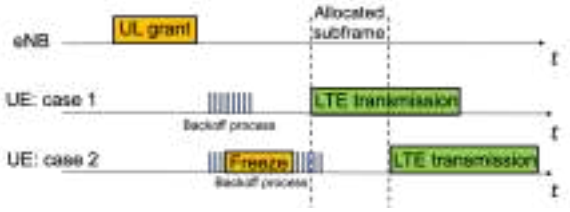


Fig. 3: Uplink channel access procedures.

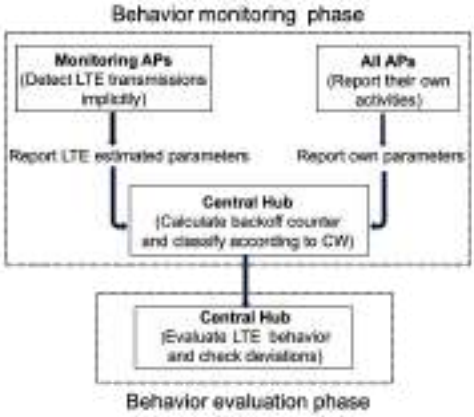


Fig. 4: Overview of the misbehavior detection mechanism.

the LTE can completely ignore the defer time and initiate the backoff countdown immediately within a transmission round.

2) Increase the CCA threshold: Another manipulation strategy is to avoid freezing the backoff counter in the presence of active Wi-Fi APs. This leads to faster acquisition of the medium, which can be beneficial if a high-power eNB transmission overshadows Wi-Fi transmissions. Note that avoiding backoff freezing can occur due to hidden terminals or due to power asymmetry. This is illustrated in Fig. 2. Assume that Wi-Fi AP B acts as a monitor for the behavior of LTE A, which is outside the interference range of AP C (hidden terminal) and therefore does not freeze its backoff counter when AP C transmits. This behavior may be perceived by AP B, which is within the interference range of LTE A, as misbehavior. In another scenario, AP B observes that LTE A does not freeze its backoff window when AP B is active. This could be due to the transmission power asymmetry or due to misbehavior.

3) Reduce the backoff window: An LTE system can manipulate the LAA backoff process by selecting its backoff counter from a smaller window range $b \in \{0, 1, \ldots, q_m - 1\}$, where $q_m < q$. The value of q_m may be selected from a high-priority class so that the LTE appears to be protocol-compliant. Moreover, the LTE can avoid increasing its CW size after a collision, to reduce the delay between two consecutive channel access attempts. Here, we consider a general model in which the LTE remains protocol-compliant for a fraction of time $0 \leq \alpha \leq 1$, while it uses a smaller CW of size q_m for the remaining time. As an example of backoff manipulation, the LTE device can consistently select backoff values in the range $[0 - 3]$, irrespective of the priority class. Essentially, all priority classes are treated as if they were of C_1. We emphasize that there is an inherent difficulty in attributing collisions to a transmitting device because: (a) collisions are receiver-dependent, and (b) in a heterogeneous setting, one system cannot decode the transmissions of other systems. Hence, detecting misbehavior that involves collisions is challenging.

Misbehavior in the uplink direction. Unlike DL transmissions, any UL transmission must be preceded by an UL grant permission from the eNB. This grant specifies the subframe where the UL transmission should start. Once the UL grant is received, the UE starts the backoff process. Here, the misbehavior strategies described for the DL direction are possible. However, they have limited benefit for the UE because a failure to seize the channel for a Type 1 transmission will lead to a much more aggressive channel access strategy for the next subframe (Type 2).

If the UE cannot complete the backoff process before the beginning of the allocated subframe due to contention (case 2 in Fig. 3), the UE is allowed to access the channel in the following subframe by only deferring for an initial time $T_{init} = T_{def} + p \cdot T_s$, where $p = 1$. That is, the UE senses the channel for minimal time and does not follow a backoff process, thus increasing the chances of capturing the channel substantially.

Given the significantly higher volume of DL traffic, the requirement for a DL frame to schedule an UL transmission, and the aggressive channel access strategy of UL Type 2 transmissions, we only focus on detecting LTE misbehavior in the DL direction.

3.3 Misbehavior Detection Framework Overview

To detect misbehaving eNBs, we propose a detection framework which consists of a behavior monitoring phase and a behavior evaluation phase, as shown in Fig. 4. During the behavior monitoring phase, monitoring APs listen to the wireless medium when they do not transmit. Each monitoring AP overhears LTE frames and infers behavior-related parameters such as the start and end times of the LTE frame, the transmitting eNB, the retransmission round, the traffic class, and the topological relation of the AP to the LTE (whether the AP is a hidden terminal to the transmitting LTE or not). *All parameters are implicitly estimated without decoding LTE frames.* Monitoring APs periodically report a time series of observations along with a time series of their own activity to a central hub for further processing.

In the behavior evaluation phase, the hub processes the information reported by the distributed network of APs to derive the channel access pattern of each monitored eNB. If the access pattern is deemed to deviate from the LAA specifications, the LTE system is considered misbehaving.

4 Behavior Monitoring Phase

The key challenge in monitoring the LTE behavior is the system heterogeneity. The monitoring APs cannot decode LTE transmissions as they may not be equipped with LTE receivers. In this section, we present several techniques for the implicit estimation of the LTE operating parameters. Specifically, each monitoring AP listens to the wireless medium when it is not active. Upon detection of channel activity that is not Wi-Fi decodable, it processes the signal without decoding to determine if it belongs to an LTE. For the i^{th} detected LTE transmission, the AP estimates an observation vector $\mathbf{o}(i)$ of six parameters

$$\mathbf{o}(i) := < t_s(i), t_e(i), ID(i), C(i), r(i), h(i) >, \qquad (1)$$

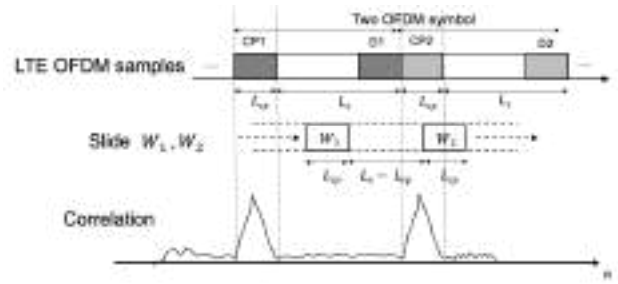


Fig. 5: Detecting LTE transmissions using CP correlation.

where $t_s(i)$ and $t_e(i)$ denote the start and end times of the i^{th} transmission, respectively, $ID(i)$ denotes an eNB identity, $C(i)$ denotes the LTE traffic class, $r(i)$ denotes the retransmission round, and $h(i)$ is a flag that denotes if the monitoring AP belongs to the one-hop neighborhood of the transmitting LTE. In the remainder of the section, we describe this parameter estimation.

4.1 Detecting LTE Transmissions

The first step for estimating the LTE operating parameters is to determine when and for how long eNBs transmit. This allows the estimation of $t_s(i)$ and $t_e(i)$. To detect LTE transmissions, we adopt the cyclic prefix (CP)-based method proposed in [33]. Like any OFDM modulated signal, LTE transmissions utilize the CP concept to mitigate inter-symbol interference. The end of an OFDM symbol is appended at the beginning, forming the CP. In Fig. 5, CP1 is equal to D1, CP2 is equal to D2, etc.

A Wi-Fi AP can attribute a signal to an eNB by verifying that the CP and its copy are $L_S - L_{CP}$ samples away, where L_S and L_{CP} denote the lengths, in samples, of the LTE symbol and the CP, respectively. The duration of the LTE OFDM symbol, and consequently the appended CP, are fixed to unique values in the LTE standard [23]. Based on the fixed duration and the sampling rate, the AP determines the values of L_S and L_{CP}. The main idea of this method is to detect high signal correlation when the CP samples are correlated to the end of the LTE symbol.

Algorithm 1: LTE transmission detection

Step 1: The AP samples the received signal.

Step 2: The AP fixes two time windows W_1 and W_2 of length L_{CP}, separated by $L_S - L_{CP}$ samples. Then, it shifts the two windows simultaneously by one sample at a time while keeping the window separation fixed to $L_S - L_{cp}$.

Step 3: For each shift n, the AP obtains the vectors of signal samples $\mathbf{s}_1(n)$ and $\mathbf{s}_2(n)$ that correspond to windows W_1 and W_2 (each of length L_{CP}) and computes

$$\rho(n) = \frac{|A(n)|^2}{(\max(E_{\mathbf{s}_1}(n), E_{\mathbf{s}_2}(n)))^2}, \quad (2)$$

where $A(n)$ is the correlation between $\mathbf{s}_1(n)$ and $\mathbf{s}_2(n)$,

$$A(n) = \sum_{k=0}^{L_{CP}-1} \mathbf{s}_1(n-k)\mathbf{s}_2^*(n-k-L_S). \quad (3)$$

Here, $\mathbf{s}^*$ is the complex conjugate of $\mathbf{s}$. The energies $E_{\mathbf{s}_1}(n)$ and $E_{s_2}(n)$ are computed as

$$E_{\mathbf{s}_1}(n) = \sum_{k=0}^{L_{CP}-1} \mathbf{s}_1(n-k)\mathbf{s}_1^*(n-k), \quad (4)$$

$$E_{\mathbf{s}_2}(n) = \sum_{k=0}^{L_{CP}-1} \mathbf{s}_2(n-k-L_S)\mathbf{s}_2^*(n-k-L_S). \quad (5)$$

We use the max in the denominator to ensure that $\rho(n)$ always stays within $[0, 1]$ and to help minimize the value of $\rho(n)$ when $\mathbf{s}_1(n)$ and $\mathbf{s}_2(n)$ are different.

Step 4: If $\mathbf{s}_1(n) \approx \mathbf{s}_2(n)$, the correlation spikes indicating that $\mathbf{s}_1(n)$ is the CP of $\mathbf{s}_2(n)$. The correlation spike is recognized if $\rho(n) \geq \gamma_{LTE}$ where γ_{LTE} is a minimum correlation threshold that defines a signal match. We discuss the selection of the threshold γ_{LTE} in Section 6.2.

Step 5: The AP sets $t_s(i)$ to the time of the first local maximum (correlation spike) that exceeds γ_{LTE} and $t_e(i)$ to the time of the last local maximum that exceeds γ_{LTE}.

The required signal processing for implementing the monitoring function at the APs is less computationally- and energy-intensive than the typical receiving and decoding operation for OFDM signals. Only the signal sampling stage is implemented for monitoring purposes (no CP removal, FFT, and demodulation). Once samples are collected, the computation of signal correlation is a fairly efficient operation.

4.2 Differentiating Between eNBs

Attributing transmissions to individual eNBs is necessary for building the behavioral profile of each eNB. However, this requires: (a) to distinguish downlink LTE transmissions from uplink ones and (b) differentiate between eNBs in the downlink.

To perform these two operations, we propose that monitoring APs use two distinct frame fields included only in the DL direction. Those are the primary synchronization signal (PSS) and the secondary synchronization signal (SSS), which are used for synchronization and carry information about the transmitting eNB's identity. As shown in Fig. 6, the PSS and SSS fields are repeated twice at fixed locations in an LTE DL frame. Samples of DL LTE signals at those fixed locations are identical. This gives the opportunity to a monitoring AP to identify DL frames.

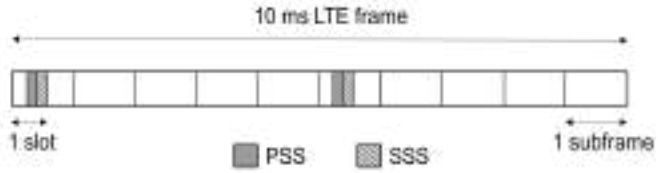


Fig. 6: The PSS and SSS fields in LTE frames.

Moreover, the identity of an eNB is calculated as ID $= ID_1 + 3ID_2$, where ID_1 and ID_2 define the physical-layer cell identity group and physical layer identity of the LTE, respectively. The ID_1 and ID_2 values are part of the PSS and SSS fields. The pair (ID_1, ID_2) is unique for every eNB, however, both can only be obtained by decoding the PSS and SSS fields.

Monitoring APs can exploit the known locations for ID_1 and ID_2 to attribute LTE transmissions to different eNBs. Note that we are not interested in extracting the ID value, but to identify LTE frames with the same ID. We use the "signal signature" of the static PSS and SSS fields for this attribution. The main idea is to detect the unique fields (ID_1, ID_2) by sampling the LTE transmission at the PSS and SSS locations and correlating the signal samples with previously recorded samples. Two transmissions from the same eNB will exhibit a high correlation on the ID fields, if the channel effect is neutralized. A monitoring AP can identify DL frames and differentiate between different eNBs by executing the following LTE frame attribution algorithm.

Algorithm 2: LTE Frame Attribution

Step 1: For the i^{th} LTE frame, the AP applies the CP-based LTE detection algorithm and synchronizes with the frame start time $t_s(i)$.

Step 2: The AP collects two sets of samples $\mathbf{s}_{ID}^{(i)}$ and $\tilde{\mathbf{s}}_{ID}^{(i)}$ of length L_{ID}, at the two locations of the PSS and SSS fields.

Step 3: The AP computes the signal correlation $\rho_{DL}(i)$ between these two sets of samples as follows

$$\rho_{DL}(i) = \frac{|\sum_{k=1}^{L_{ID}} \mathbf{s}^{*(i)}_{ID}(k)\, \tilde{\mathbf{s}}^{(i)}_{ID}(k)|^2}{(\max(E_{\mathbf{s}^{(i)}_{ID}}, E_{\tilde{\mathbf{s}}^{(i)}_{ID}}))^2}, \tag{6}$$

where $E_{\mathbf{s}^{(i)}_{ID}}$ and $E_{\tilde{\mathbf{s}}^{(i)}_{ID}}$ are the energies of $\mathbf{s}^{(i)}_{ID}$ and $\tilde{\mathbf{s}}^{(i)}_{ID}$, respectively, calculated in a similar way to (4). A downlink transmission is inferred if the correlation exceeds a threshold value that defines a signal match (see Section 6.3). If the correlation is below the threshold, the current LTE frame is ignored (uplink transmission). Otherwise, the AP proceeds to the following steps.

Step 4: The AP maintains a signature database that includes the observed LTE signatures up to the current observation. The signature $\mathbf{s}_{ID_j}$ of the j^{th} LTE represents the samples carrying ID_1 and ID_2, collected from previous transmissions. The database is assumed to be initially empty and is updated gradually according to the collected observations.

Step 5: Due to the change in the channel impulse response over time, the AP adjusts the samples $\mathbf{s}^{(i)}_{ID}$ by a fixed phase to compensate for the channel effect. The AP observes the phases of the complex samples $s^{(i)}_{ID}$ collected over the i^{th} frame, denoted by vector $\theta^{(\mathbf{i})}_{\mathbf{ID}}$. The AP recovers the phases $\theta_{\mathbf{ID_j}}$ of the complex samples $\mathbf{s}_{ID_j}$ stored in the signature database, for each ID_j. The AP computes the average phase shift between the two sample vectors $s^{(i)}_{ID}$ and $\mathbf{s}_{ID_j}$ as,

$$\bar{\theta}(i,j) = \frac{1}{L_{ID}} \sum_{k=1}^{L_{ID}} |\theta^{(\mathbf{i})}_{\mathbf{ID}}(k) - \theta_{\mathbf{ID_j}}(k)|. \tag{7}$$

The AP updates the phase part of $\mathbf{s}^{(i)}_{ID}$ as $\theta^{(\mathbf{i})}_{\mathbf{ID}} = \left(\theta^{(\mathbf{i})}_{\mathbf{ID}} + \bar{\theta}(i,j)\right) \mod \pi$. The phase compensation method is explained in detail in the experimental validation section (Section 6.3).

Step 6: The AP computes the signal correlation between $\mathbf{s}^{(i)}_{ID}$ and every signature in the database,

$$\rho_{ID}(i,j) = \frac{|\sum_{k=1}^{L_{ID}} \mathbf{s}^{*}_{ID_j}(k)\, \mathbf{s}^{(i)}_{ID}(k)|^2}{(\max(E_{\mathbf{s}_{ID_j}}, E_{\mathbf{s}^{(i)}_{ID}}))^2}, \forall j, \tag{8}$$

where $E_{\mathbf{s}_{ID_j}}$ and $E_{\mathbf{s}^{(i)}_{ID}}$ are the energies of $\mathbf{s}_{ID_j}$ and $\mathbf{s}^{(i)}_{ID}$, respectively, calculated in a similar way to (4).

Step 7: The AP attributes the i^{th} LTE transmission to LTE ID_j that yields the maximum $\rho_{ID}(i,j)$,

$$\text{ID} = \arg\max_{ID_j} \{\, \rho_{ID}(i,j) |\, \rho_{ID}(i,j) \geq \gamma_{ID}\}. \tag{9}$$

Here γ_{ID} is a minimum correlation threshold that defines a signal match. If a match is found, the AP also replaces $\mathbf{s}_{ID_j}$, the current signature of LTE ID_j, with $\mathbf{s}^{(i)}_{ID}$.

Step 8: If no correlation value exceeds γ_{ID}, the AP adds $\mathbf{s}^{(i)}_{ID}$ to the database as a new eNB signature.

A challenge for this method is the attribution of an LTE transmission when it collides with another transmission. Although performing such classification via signal correlation in the presence of collisions is possible [37], we leverage the distributed nature of the monitoring operation to resolve colliding transmissions. As collisions are receiver-dependent, not all monitoring APs experience collisions. Those APs that do not experience a collision correctly classify the LTE transmission. As an example, AP A in Fig. 2 is in the interference range of LTE A and LTE B thus being unable to classify frames of A and B that collide. Such frames are correctly monitored by AP B and D. Finally, even if colliding frames fail to be correctly classified, they only represent a small fraction of the transmitted frames.

4.3 Priority Class Estimation

The channel access parameters of LTE transmissions depend on the priority class. Lower priority classes utilize longer frames and thus are designed to access the channel less frequently, whereas higher classes accommodate shorter frames, shorter defer times, and smaller contention windows.

To evaluate the compliance of an eNB with the class parameters, the APs classify frames to one of the four classes of Table 1 using the transmission duration. By measuring the length of the i^{th} frame as $T_{\text{MCOP}} = t_e(i) - t_s(i)$, the AP can classify the frame to classes C_1, C_2, and C_3/C_4. Note that the T_{MCOP} values for C_3 and C_4 are equal. However, C_3 has shorter defer time allowing for faster medium access and a better choice for misbehavior. Thus, for all practical purposes, we air on the conservative side and assume that any frame of length 8ms or 10ms belongs to class C_3.

4.4 Contention Window Size Estimation

Another important behavior parameter is the CW used at every LTE transmission. Maintaining a small CW improves the channel access opportunities for the LTE. Monitoring APs can estimate the CW size of an eNB by tracking the retransmission round $r(i)$ of a frame. The CW size $q(i)$ at the i^{th} transmission is given by

$$q(i) = \min\{2^{r(i)} q_{\min}, q_{\max}\}, \tag{10}$$

where $q_{\min}$ and $q_{\max}$ are the minimum and maximum allowed CW sizes, as listed in Table 1. Following the LTE protocol specifications, the monitoring AP sets $r(i)$ to zero after a successful transmission by the eNB and increments it by one with every retransmission attempt. Note that the AP needs to keep track of $r(i)$ individually for each eNB.

Parameter $r(i)$ is difficult to infer in practice via overhearing because collisions are receiver-dependent. Rather than attempting to directly infer collisions, APs rely on identifying retransmissions to estimate $r(i)$. Specifically, a monitoring AP utilizes the signal correlation method to detect if the same frame is retransmitted by an LTE. The AP exploits the fact that the payload and most fields in the header of a retransmitted frame remain identical to the original transmission. Therefore, the sampled signal of two identical transmissions should exhibit high signal correlation, even if one is corrupted by a colliding signal. The main challenge in performing signal correlation is identifying the start and end times of the LTE frame, along with the ID field of the collided eNB in the presence of a collision.

Collision between Wi-Fi and LTE: We first consider the case of an LTE colliding with an AP. This is the most common case, as eNBs are typically deployed to minimize collisions and are usually assigned different operating frequencies. A monitoring AP can estimate $r(i)$ through the following steps.

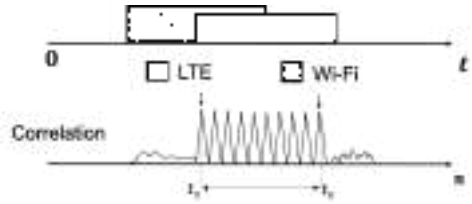


Fig. 7: Example of applying the CP-based LTE detection method in case of collisions with a Wi-Fi frame.

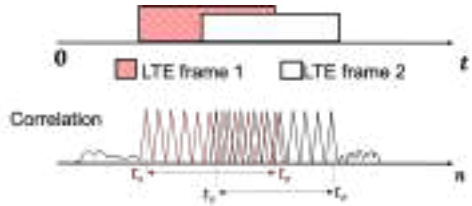


Fig. 8: Example of applying the CP-based LTE detection method in case of collisions between LTE frames.

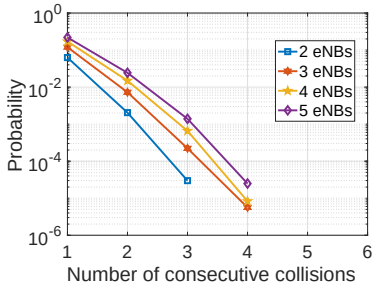


Fig. 9: Probability of r consecutive collisions when the LTE uses class C_4 for different contending eNBs.

Algorithm 3: Transmission Round Estimation

Step 1: The AP applies the CP-based LTE detection method described in Algorithm 1 to determine the start time $t_s(i)$ and end time $t_e(i)$ of the i^{th} LTE frame. These times are identified by the first and last correlation peaks of the CP with the end of the symbols, respectively, as shown in Fig. 7.

Step 2: Using the start time $t_s(i)$ as a time reference, the AP extracts the samples carrying the LTE ID. As the collision does not necessarily corrupt all samples (e.g., only half of the samples are involved in the collision in Fig. 7), the samples carrying the LTE ID may be clean or corrupted. If the samples are clean, the AP identifies the LTE ID field by performing Algorithm 2 and it proceeds to the following step. Otherwise, if the samples are corrupted, it proceeds to Step 5.

Step 3: The AP buffers the samples of the i^{th} and $(i+1)^{st}$ eNB transmission denoted by $\mathbf{s}(i)$ and $\mathbf{s}(i+1)$, respectively.

Step 4: The AP correlates $\mathbf{s}(i)$ with $\mathbf{s}(i+1)$ using the correlation function in (8) and computes the correlation value $\rho(i, i+1)$. If $\rho(i, i+1) \geq \gamma_{rt}$, where γ_{rt} is a correlation threshold that defines a signal match, the AP identifies the $(i+1)^{st}$ frame as a retransmission and sets $r(i+1) = r(i) + 1$.

Step 5: If the samples carrying the ID field are corrupted (no match in Step 4), the AP determines the length of the i^{th} LTE frame as the difference between the start and end times identified in Step 1. The AP buffers the samples $\mathbf{s}(i)$ of the i^{th} LTE transmission.

Step 6: The AP tracks subsequent frames transmitted by the eNB that have the same length as the i^{th} frame. For each of these frames, the AP buffers the related samples.

Step 7: Let $\mathbf{s}(j)$ be the buffered samples of a subsequent eNB transmission. The AP correlates $\mathbf{s}(i)$ with $\mathbf{s}(j)$ using the correlation function in (8) and computes the correlation value $\rho(i, j)$. If $\rho(i, j) \geq \gamma_{rt}$, the AP identifies the frame j as a retransmission of the i^{th} frame, sets $r(j) = r(i) + 1$. It further identifies the ID of the i^{th} frame to be the same as the ID carried in the j^{th} frame.

Step 8: If no frame is found to exceed γ_{rt}, the AP ignores the particular transmission. As our behavior estimation depends on many observations, we can tolerate ignoring a small percentage of collisions that remain unidentifiable.

Collision between two eNBs: If the eNB transmissions collide, Algorithm 3 can be applied to each of the colliding frames separately, with a modification to Step 1. In this case, symbols in both frames cause a peak in signal correlation. The AP observes two groups of peaks as shown in Fig. 8. The peaks in each group are separated by a period equal to the duration of an LTE OFDM symbol. Each group of peaks identifies the start and end times of the related LTE frame. The start time t_s of the first frame (group) is identified with the first peak. The end time t_e of the first frame is identified with the last peak that is multiple symbol periods away from the first peak (last peak in the group). The start of the second frame is identified as the first peak that is not periodic to the OFDM symbol length. The end of the second LTE frame is identified as the last peak that is multiple symbol periods away from the first peak of the second frame. From parameter $r(i)$ and the class priority $C(i)$, the hub can infer $q(i)$ using (10). The class $C(i)$ is used to determine both $q_{\min}$ and $q_{\max}$. For instance, the $q(i)$ of a Class 3 frame with $r(i) = 1$ should be equal to 32 according to Table 1.

Impact of the priority class on the estimation of the CW. In the priority class estimation method, we have stated that all C_4 traffic is classified as C_3. This can impact the CW size estimation as follows. The transmission round estimation algorithm (Algorithm 3) still provides the correct estimation of $r(i)$, as this is solely based on detecting retransmissions. Using C_3 instead of C_4 impacts the estimated CW size given the correct $r(i)$ because the maximum contention window is capped at 64 when C_3 is assumed. However, this error in CW estimation only occurs when the retransmission round exceeds two. The first three contention window sizes are the same for C_3 and C_4. We highlight that observing three or more consecutive collisions is a rare event.

To demonstrate this, we measured the probability of consecutive collisions as a function of the number of competing stations when class C_4 is adopted. Figure 9 shows the results of the simulation under saturation condition (worst contention scenario). We observe that three or more consecutive collisions occur with negligible probability (less than 2×10^{-3}), indicating that classifying all traffic as C_3 has a negligible impact on the CW size estimation. An alternative approach is to ignore any observations for which the transmission round exceeds two. Given the rarity of such events, ignoring two every 1,000 observations does not affect the detection accuracy.

4.5 Discovering APs in the LTE Collision Domain

The final parameter to be estimated is the value of the flag $h(i)$ that defines if a monitoring AP belongs to the one-hop neighborhood of a transmitting LTE. Although $h(i)$ may be fixed over all i's for static topologies, we update it with every transmission to reflect channel fluctuations. The importance of $h(i)$ is shown in Fig. 10. AP K can overhear LTE A when A is active. Contrary,

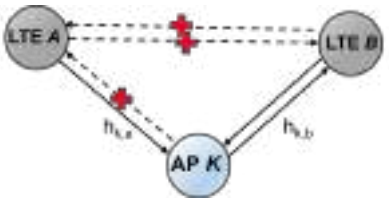


Fig. 10: AP K is a hidden terminal to A but not B. eNBs A and B are hidden terminals.

the received power at A falls below A's CCA threshold when K is transmitting because K transmits at lower power than A. Moreover, although A and B are both overheard at K, they are hidden terminals to each other. These topological configurations impact how K estimates the freeze time of a monitored LTE. Let LTE A be monitored by AP K. To determine if K is overheard by A, i.e., $K \in \mathcal{N}_A^{(1)}$, the AP executes the following algorithm.

Algorithm 4: Discovering APs in the LTE Collision Domain

Step 1: A monitoring AP K keeps track of the average received power over the last z transmissions by eNB A. Let this series be represented by a $z \times 1$ vector $\mathbf{P}_r^{(K)}$. The j^{th} element $P_r^{(K)}(j)$ of $\mathbf{P}_r^{(K)}$ is equal to

$$P_r^{(K)}(j) = P_\ell |h_{A,K}(j)|^2 + \sigma^2, \tag{11}$$

where $h_{A,K}(j)$ denotes the channel impulse response, P_ℓ is the transmission power of the eNB, and σ^2 is the noise power.

Step 2: AP K exploits the channel reciprocity principle $(h_{K,A}(j) = h_{A,K}(j))$ to estimate the received power at A when K transmits. AP K generates a $z \times 1$ vector $\mathbf{P}_r^{(A)}$ that represents the received power at A, if K were to transmit using power P_w over the same channel. The j^{th} average received power value at eNB A is computed as

$$P_r^{(A)}(j) = P_w |h_{K,A}(j)|^2 + \sigma^2 = \frac{P_w (P_r^{(K)}(j) - \sigma^2)}{P_\ell} + \sigma^2. \tag{12}$$

The number of observations z is chosen based on the channel fading conditions. For slow fading channels, z should take small values, whereas longer observation times are needed if the AP experiences a fast fading channel.

Step 3: If the majority of the power samples in $\mathbf{P}_r^{(A)}$ exceed the CCA threshold, AP K considers itself a member of the one-hop neighborhood $\mathcal{N}_A^{(1)}$ of A and sets $h(i)$ to zero. Otherwise, K is a hidden terminal to A, and sets flag $h(i)$ to one.

We note that channel reciprocity is a well-established principle in communications that holds due to the symmetry in the space geometry (multipath).

Monitoring Wi-Fi activity: Although we have our framework on implicit estimation of LTE activity, the main principles are general and can be applied to implicitly estimate the related parameters of Wi-Fi activity. The main necessary changes to adjust the framework to Wi-Fi are: (a) adjust the parameters in Section 4 to observe Wi-Fi activity and (b) update the channel access parameters (defer time, transmission duration, classes, etc.) for defining compliant Wi-Fi behavior. For instance, Wi-Fi transmissions can be detected using the CP-based technique presented in Section 4.1 by adjusting the length and location of the CP. The ID of a Wi-Fi can be extracted by looking at fields in Wi-Fi frame headers that carry information similar to PSS and SSS (e.g., MAC addresses).

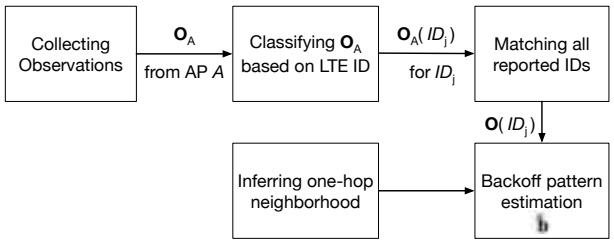


Fig. 11: Overview of the behavior evaluation phase.

5 Behavior Evaluation Phase

The behavior monitoring phase is followed by the behavior evaluation phase where the central hub models and analyzes the behavior of each eNB based on the collected observations. An overview of the behavior evaluation phase is shown in Fig. 11. The hub first integrates the data from the different APs into a single observation set. Subsequently, the observation set is analyzed to detect any LTE misbehavior.

5.1 Integration of the AP Observations

The first task in the evaluation phase is to attribute the reported observations by the multiple APs to eNBs. Each AP independently associates the observations with unique ID fields. Recall that no LTE frame decoding takes place, so the real LTE ID is not recorded in the observation sets reported by the APs. To match the unique IDs, the central hub exploits the timing reported with each observation. The intuition here is that LTE transmissions recorded by multiple APs will share common start and end times. The hub matches the different LTE ID versions using the following steps.

Algorithm 5: Matching the Reported LTE ID Fields

Step 1: Let $\mathbf{O}_A$ be the set of observations reported by a monitoring AP A to the hub. The hub partitions $\mathbf{O}_A$ based on the reported ID field, such that the observations tagged with ID_j are included in subset $\mathbf{O}_A(ID_j) \subset \mathbf{O}_A$.

Step 2: The hub utilizes the start and end times within observation subsets from different APs to match the LTE IDs. These times are almost synchronous when the reported observations from different APs represent the same eNB. For any two LTE IDs ID_j and ID_k reported by monitoring APs A and B, respectively, if the start and end times of most observations within subsets $\mathbf{O}_A(ID_j)$ and $\mathbf{O}_B(ID_k)$ are identical, then ID_j (reported by AP A) and ID_k (reported by AP B) represent the same eNB. The i^{th} observation from A and ℓ^{th} observation from B shall satisfy the following conditions:

$$|t_s(i) - t_s(\ell)| \leq \epsilon, \quad t_e(i) - t_s(i) = t_e(\ell) - t_s(\ell). \tag{13}$$

That is, the frame start times recorded by the two monitoring APs should not differ by more than ϵ and the frame length should be the same. Parameter ϵ represents the synchronization error due to differences in propagation delay, and clock offsets. As the two APs do not necessarily collect the same number of observations, the previous relation should be true for some fraction of observations in $\mathbf{O}_A(ID_j)$ and $\mathbf{O}_B(ID_k)$.

Step 3: The hub merges the observation sets that correspond to the same LTE ID. Specifically, if subsets $\mathbf{O}_A(ID_j)$ and $\mathbf{O}_B(ID_k)$ are attributed to the same ID based on Step 2, the two sets are merged into a single one as follows: (a) any unique observation is retained intact and (b) for a duplicate observation $\mathbf{o}(i)$ only one copy is retained, except for the hidden terminal flag

TABLE 2: Observations reported by AP 1 and AP 2.

i	Observations reported by AP A ($\mathbf{O}_A$)
1	$< 10, 150, ID_1, C_1(1), r_1(1), h_1(1) >$
2	$< 160, 300, ID_2, C_1(2), r_1(2), h_1(2) >$
3	$< 320, 500, ID_2, C_1(3), r_1(3), h_1(3) >$
4	$< 510, 650, ID_1, C_1(4), r_1(4), h_1(4) >$
ℓ	Observations reported by AP B ($\mathbf{O}_B$)
1	$< 160.1, 300.1, ID_3, C_2(1), r_2(1), h_2(1) >$
2	$< 320.1, 500.1, ID_3, C_2(2), r_2(2), h_2(2) >$
3	$< 550.1, 700.2, ID_4, C_2(3), r_2(3), h_2(3) >$
4	$< 720.1, 820.1, ID_4, C_2(4), r_2(4), h_2(4) >$

$h(i)$. The flag $h(i)$ is extended to a vector $\mathbf{h}(i)$ that includes the different $h(i)$'s reported by APs.

To illustrate Algorithm 5, let AP A and AP B report the observation sets shown in Table 2. First, the hub separates the observations of each AP into subsets based on the ID field. This creates subsets $\mathbf{O}_A(ID_1) = \{\mathbf{o}_A(1), \mathbf{o}_A(4)\}$ and $\mathbf{O}_A(ID_2) = \{\mathbf{o}_A(2), \mathbf{o}_A(3)\}$ for AP A and subsets $\mathbf{O}_B(ID_3) = \{\mathbf{o}_B(1), \mathbf{o}_B(2)\}$ and $\mathbf{O}_B(ID_4) = \{\mathbf{o}_B(3), \mathbf{o}_B(4)\}$ for AP B. Next, the hub checks if there is any matching between the four reported ID fields by applying the checks in (13) on the observations of each subset. Based on the reported timings, the hub matches subset $\mathbf{O}_A(ID_2)$ with $\mathbf{O}_B(ID_3)$. This is because the respective observations have almost identical start and end times. Also, we observe no matching for $\mathbf{O}_A(ID_1)$ and $\mathbf{O}_B(ID_4)$. The hub concludes that there are three different ID fields reported by the two APs, namely ID_1, ID_2, and ID_4. The last step is to merge the observations within $\mathbf{O}_A(ID_2)$ and $\mathbf{O}_B(ID_3)$ in a new observation set. This is done by keeping only one copy for each repeated observation and expanding the hidden terminal flag to a vector. For example, $\mathbf{o}_A(2)$ and $\mathbf{o}_B(1)$ are merged into following observation:

$$< 160T_s, 300T_s, ID_2, C_1(2), r_1(2), \mathbf{h}(i) = \{h_1(2), h_2(1)\} >$$

We emphasize that $C_1(2)$ and $r_1(2)$ should be the same as $C_2(1)$ and $r_2(1)$, respectively. Once the hub matches all reported IDs, it analyzes the behavior of each eNB individually. Without loss of generality, we focus on the behavior evaluation of a single eNB. The same process is repeated for other eNBs. For notation simplicity, we reduce the observation set to $\mathbf{O} = \{\mathbf{o}(1), \mathbf{o}(2), \ldots, \mathbf{o}(n)\}$.

One vital step in evaluating the LTE behavior is the identification of the one-hop neighborhood for each eNB. This is important to estimate when a given eNB should freeze its contention process relative to other active eNBs and APs. The topological information is inferred at the central hub using the following process.

Algorithm 6: Inferring the One-hop Neighborhood of an eNB

Step 1: For the i^{th} observation, the hub uses the reported vector $\mathbf{h}(i)$ to identify the APs that belong to the one-hop neighborhood of the eNB. Let $\mathbf{h}(i, w)$ be the flag reported by AP W. The hub places W to the one-hop neighborhood of the eNB if $\mathbf{h}(i, w) = 0$.

Step 2: For eNBs, the hub utilizes the reported start and end times for each monitored eNB to identify the airtime intervals. If the fraction of overlapping transmissions between two eNBs exceeds a threshold γ_{int}, the hub concludes that the involved eNBs are not in separate collision domains.

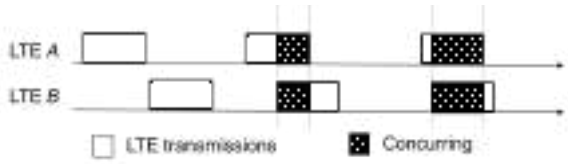


Fig. 12: Transmissions of two eNBs which are hidden terminals.

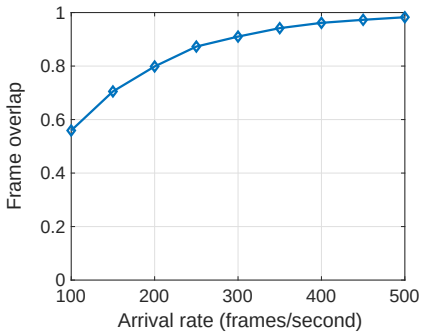


Fig. 13: Fraction of overlap vs. arrival rate for two competing out-of-range eNBs.

Step 3: If the fraction of overlapping transmissions is below γ_{int}, the eNBs are placed in the same one-hop neighborhood.

To demonstrate Algorithm 6, consider the transmission timeline shown in Fig. 12. The two transmitting eNBs are not within range and therefore several frames overlap in time, indicating that one is not aware of the other's transmissions.

Setting γ_{int}. The threshold γ_{int} has to be greater than the expected fraction of colliding frames between two eNBs in the same collision domain, but smaller than the expected number of frame overlaps between two eNBs at separate collision domains. From Fig. 9, we observe that the probability of two eNBs colliding is below 6% when both eNBs are backlogged. We further simulated two eNBs that are located in separate collision domains at different saturation conditions controlled by a Poisson arrival process. Figure 13 shows the fraction of the frame overlap per 1,000 transmission rounds. The fraction approaches one with the increase in the level of saturation (the medium saturates at 500 frames/second), controlled by the arrival rate. From Fig. 9 and Fig. 13, we can select γ_{int} to be a safe margin between the probability of collision and the probability of overlap. A typical value would be in the order of 15% of the reported frames.

5.2 Number of Required Monitoring APs

For monitoring one eNB, the minimum number of required monitoring APs is one. The monitoring AP has to be within the same collision domain as the eNB to perform the monitoring function. Note that the AP will be able to overhear all the eNB transmissions because, according to the coexistence etiquette, the AP would have to defer from transmission when the eNB transmits. Thus, a single AP has the ability to monitor the behavior of the eNB. Multiple monitoring APs add redundancy in the monitoring process, as multiple APs observe the same transmissions. Because of this redundancy, the observations have to be consolidated when they are fused at the central hub (using Algorithm 5). The multiple APs enhance the monitoring process in two ways. First, they can observe collisions between the eNB and other monitoring APs. Second, they provide a better estimation of the eNB's one-hop neighborhood, which is used to accurately estimate the eNB's freeze time. In practice, three APs that surround the eNB would be more than sufficient for accurate monitoring.

5.3 Backoff Pattern Estimation

Consider the behavior analysis of an eNB A. After the observation set $\mathbf{O}$ and the one-hop neighborhood $\mathcal{N}_A^{(1)}$ of A have been determined, the hub performs the following steps to estimate the backoff pattern $\widehat{\mathbf{b}}$ of the eNB.

Algorithm 7: Backoff Pattern Estimation

Step 1: The hub computes the inter-transmission time between two successive transmissions $\mathbf{o}(i-1)$ and $\mathbf{o}(i)$ as:

$$T(i) = t_s(i) - t_e(i-1), \tag{14}$$

where $t_e(i-1)$ and $t_s(i)$ are the end and start times reported during the $\mathbf{o}(i-1)$ and $\mathbf{o}(i)$ observations, respectively.

Step 2: Let v_i denote the number of all intermediate transmissions that occur between $\mathbf{o}(i-1)$ and $\mathbf{o}(i)$, from stations in the one-hop neighborhood $\mathcal{N}_A^{(1)}$. The hub computes v_i by tracking all observations that have a starting time t_s such that $t_e(i-1) < t_s < t_s(i)$ and belong to $\mathcal{N}_A^{(1)}$.

Step 3: According to the LAA-LTE backoff process, the time $T(i)$ between two successive transmissions consists of defer, freeze, and backoff times and can be expressed as:

$$T(i) = \underbrace{\sum_{j=1}^{v_i+1} (T_{def} + p_j \cdot T_s)}_{\text{defer time}} + \underbrace{\sum_{j=1}^{v_i} L_j(i)}_{\text{freeze time}} + \underbrace{b(i) \cdot T_s}_{\text{backoff time}}. \tag{15}$$

In eq. (15), T_{def} is the default defer time followed after every transmission, p_j is the number of defer slots before the j^{th} intermediate transmission and $L_j(i)$ is the length of the j^{th} intermediate transmission. Recall that v_i is the number of intermediate transmissions and T_s is the slot duration. We emphasize that the collision of more than one transmissions is registered as only one intermediate transmission whose length is the combined interval of the colliding transmissions.

Step 4: Let $p(i)$ be the number of observation slots related to the class $C(i)$ (see Table 1) reported within the observation $\mathbf{o}(i)$. The hub computes the defer slots p_j as

$$p_j = \min\{p(i), \frac{T_j - T_{def}}{T_s}\}, \tag{16}$$

where T_j is the idle time before the j^{th} intermediate transmission. This means that p_j is calculated based on one of the following two scenarios

- If the channel stays idle until the $p(i)$ observation slots have passed $\left(\frac{T_j - T_{def}}{T_s} \geq p(i)\right)$, then $p_j = p(i)$.
- When another device starts transmitting before $p(i)$ slots are observed $\left(\frac{T_j - T_{def}}{T_s} < p(i)\right)$, then $p_j = \frac{T_j - T_{def}}{T_s} < p(i)$.

Step 5: The hub estimates the backoff counter $b(i)$ from (15):

$$b(i) = \frac{T(i) - (v_i+1)T_{def} - \sum_{j=1}^{v_i+1} p_j \cdot T_s - \sum_{j=1}^{v_i} L_j(i)}{T_s}. \tag{17}$$

Intuitively, eq. (17) states that the backoff counter selected by an eNB is equal to the time between two successive transmissions from that eNB minus all the defer time, and minus all the freeze time (normalized over the slot duration to convert it to slots). The correct estimation of $b(i)$ requires the knowledge of $p(i)$, which is determined according to the reported priority class $C(i)$ during the observation $\mathbf{o}(i)$.

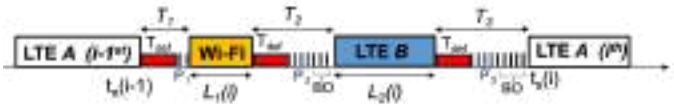


Fig. 14: Estimation of the i^{th} backoff counter between two successive transmissions from LTE A.

An example of all the timings involved in the estimation of $b(i)$ is shown in Fig. 14. The time between two successive transmissions from LTE A is $T(i) = t_s(i) - t_e(i-1)$. Two intermediate transmissions occurred during $T(i)$ from devices in the one-hop neighborhood of A. The first transmission was from a Wi-Fi station and the second from another LTE, so v_i is set to two. The backoff is computed by reducing $T(i)$ by the duration of the two intermediate transmissions (freeze time) and the defer time before each transmission (T_{def}+observation slots). The Wi-Fi transmission duration $L_1(i)$ is known because Wi-Fi APs report their own activity to the hub (see Fig. 3), whereas the duration $L_2(i)$ for LTE B is implicitly sensed and reported by APs. Finally, p_j is inferred using Step 4.

Unsaturated LTE Traffic: It is worth noting that the backoff counter in (17) is accurate under saturation conditions where idle slots only exist due to the backoff and channel sensing processes. However, if traffic is not saturated, idle slots can inflate the backoff estimation. To avoid misdetection due to backoff inflation, the hub excludes all observations that definitively include idle slots outside those related to the backoff process. To identify these observations, we rely on the estimated backoff counter values from (17). Let $q(i)$ and $b(i)$ be the estimated CW size and backoff counter for the i^{th} observation. The hub excludes $\mathbf{o}(i)$ if the estimated backoff exceeds the contention window (i.e., $b(i) > q(i) - 1$.) This is because it is expected that the idle slots due to an empty transmission queue will far exceed the small values taken by the backoff counter.

This process will filter most of the unwanted observations where a correct backoff estimate cannot be made, especially for low levels of saturation. We emphasize that eliminating the observations that belong to unsaturated conditions provides a misbehavior opportunity to the LTE, which can reduce its defer and backoff time, once a frame arrives at its transmission queue. However, as we show through simulations, this misbehavior has a limited impact on the Wi-Fi performance due to low contention.

5.4 LTE Misbehavior detection

By processing each observation in set $\mathbf{O}$ using Algorithm 7, the hub recovers the estimated backoff pattern $\widehat{\mathbf{b}}$ for a monitored eNB. This pattern is used to evaluate the LTE behavior as follows. The hub creates two distributions $\mathbf{M}$ and $\mathbf{W}$ representing the observed and the expected backoff counter distributions, respectively. Distribution $\mathbf{M}$ is the empirical distribution obtained from the appearance frequency of each backoff counter value in $\widehat{\mathbf{b}}$. The density function of $\mathbf{M}$ is expressed as:

$$P_{\mathbf{M}}(x) = \frac{\sum_{i=1}^{n} I(b(i) = x)}{n}, \quad x \in \{b_{\min}, \ldots, b_{\max}\}, \tag{18}$$

where $I(\cdot)$ is the indicator function, and $b_{\min}$ and $b_{\max}$ are the minimum and maximum backoff counters found in $\widehat{\mathbf{b}}$.

The expected backoff counter distribution for a protocol-compliant node is then calculated from the contention window values used in every transmission. Those can be extracted from

observation set $\mathbf{O}$, which contains the retransmission round $r(i)$ and class $C(i)$ for each of the n observations. The contention window for the i^{th} transmission is:

$$q(i) = \min\{2^{r(i)} q_{\min}, q_{\max}\}, \tag{19}$$

where $q_{\min}$ and $q_{\max}$ are the minimum and maximum allowed CW sizes for the reported class $C(i)$. Using (19), the hub estimates vector $\widehat{\mathbf{q}}$ of all contention windows. A protocol-compliant eNB should choose each backoff counter at random within each contention window, leading to a density function for the following backoff counter distribution.

$$P_{\mathbf{W}}(x) = \sum_{k \in \mathcal{N}_{cw}} \Pr(q = k) \cdot \Pr(x | q = k), \tag{20}$$

where $\mathcal{N}_{cw} = \{4, 8, \ldots, 1024\}$ is the set of all possible contention window sizes and $\Pr(q = k)$ is the probability that the LTE uses a CW of size k. Taking into account that the backoff counter selection is uniform regardless of the CW size, we get,

$$P_{\mathbf{W}}(x) = \sum_{k \in \mathcal{N}_{cw}} \Pr(q = k) \cdot \frac{1}{k}. \tag{21}$$

To determine the probability $\Pr(q = k)$, the hub relies on the frequency of appearance of value k in vector $\widehat{\mathbf{q}}$, which can be written as:

$$\Pr(q = k) = \frac{\sum_{i=1}^{n} I(q(i) = k)}{n}. \tag{22}$$

To detect a deviation from the expected behavior, the hub measures the distance between the observed backoff counter distribution $\mathbf{M}$ and the expected distribution based on the CW sizes $\mathbf{W}$. The distance is measured through the Jensen-Shannon divergence defined as

$$D_{JS}(\mathbf{M}||\mathbf{W}) \triangleq \frac{1}{2} D(\mathbf{M}||\mathbf{C}) + \frac{1}{2} D(\mathbf{W}||\mathbf{C}), \tag{23}$$

where $D(\cdot||\cdot)$ is the Kullback-Leibler divergence, and $\mathbf{C} = 1/2(\mathbf{M} + \mathbf{W})$. An eNB is suspected of misbehavior if $D_{JS}(\mathbf{W}||\mathbf{M}) > \delta$, where δ is a threshold specified by the hub.

Effect of multi-channel Operation: Through this work, we have been primarily concentrated on misbehavior over a single channel. A salient feature of operating in the unlicensed bands is that multiple channels can be combined via channel aggregation (CA) for LTE or channel bonding for Wi-Fi. Extending misbehavior to multiple channels can have a more severe impact on the performance of Wi-Fi.

Release 15 [23] includes two models for multi-channel access of unlicensed bands. In LBT Type A, an independent backoff process is followed on each of the aggregated 20 MHz channels. The Wi-Fi APs residing on each of those channels can perform misbehavior detection independently on each channel. In LBT Type B, the backoff process is followed only on the primary channel and simultaneous access on all channels is granted, once the primary channel is seized. A short sensing period on the secondary channels is meant to avoid interference. For LBT Type B, our misbehavior detection framework can be applied on the primary channel.

Some new challenges emerge when the LTE is allowed to operate on multiple channels. As the LTE may switch between the channels, the required time to collect enough observations to detect misbehavior through each channel could be longer. Moreover, matching the reported LTE ID across monitored channels is required. Algorithm 5 can be used for this purpose in the case when the LTE uses multiple channels simultaneously. Algorithm 2 can still be used by correlating LTE signatures reported through different channels. We leave the treatment of multi-channel misbehavior detection as future work.

6 Validation of Implicit Techniques

To evaluate the performance of our proposed misbehavior detection framework, we first evaluate the accuracy of the implicit LTE monitoring techniques proposed in Section 4. For this part, we performed experimentation using the USRP platform and measured the efficacy of extracting various LTE operation parameters without decoding using signal correlation.

6.1 Experimental Setup

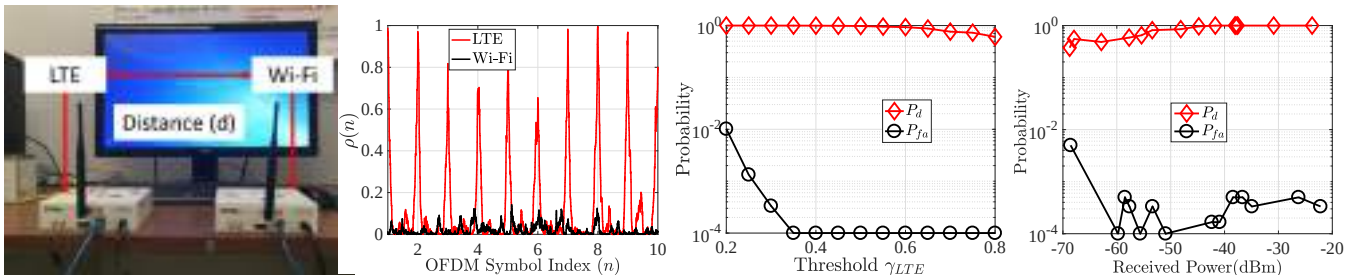
For the experimental part, relied on the LabVIEW NI software to program NI-USRP 2921 radios. To implement LTE transmissions, we employed the LabVIEW Modulation Toolkit to create OFDM signals and tuned the parameters (CP length, frequency, BW, etc) to match the LTE specifications, respectively. A similar approach was followed to implement Wi-Fi OFDM signals, but with parameters that matched the Wi-Fi specifications. To implement the monitoring mechanisms at the AP, we used the available sampling function at LabVIEW, without incorporating any further functions on the receiving chain such as FFT and demodulation. The samples were then used on custom-made modules within LabVIEW to compute the signal correlation functions.

The devices were tuned to the 5 GHz U-NII band. The physical layer of the LTE device was programmed in LabVIEW to operate according to the LTE standard. The transmission bandwidth was set to 20MHz (limit of the 2921 USRP devices), whereas the IQ rate was set to 1.92MHz. The LTE frame duration was set to 10ms. Each frame consisted of 10 subframes occupying 2 slots. Each slot had a duration of 0.5ms and allowed for the transmission of 6 OFDM symbols. The duration of each OFDM symbol was set to 83.4μs of which 16.7μs corresponded to the extended CP. The AP sampled the LTE signal on the same band, without implementing any further decoding. The experiment setup is shown in Fig. 15(a).

6.2 Detecting LTE Transmissions

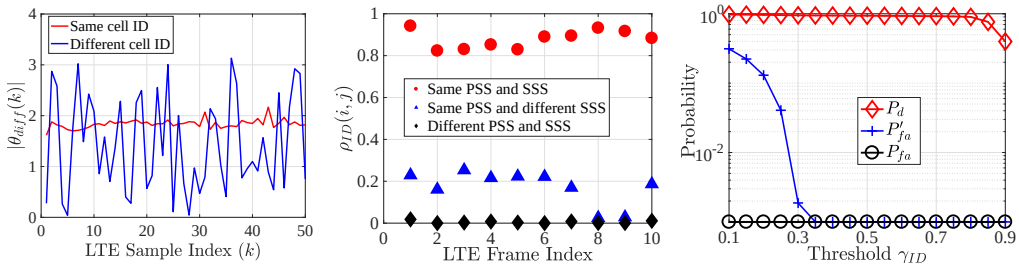
In the first set of experiments, we evaluated the Wi-Fi's ability in identifying the LTE signals using the CP detection method proposed in Section 4.1. For LTE signals, the number of samples per data symbol was set to $L_S = 256$ and for the CP to $L_{CP} = 64$. The eNB continuously transmitted 6,000 OFDM symbols, repeating the sequence $\{0, 1, 1, 0\}$. To further ensure that other signals are not misclassified as LTE, we repeated the experiments but configured the transmitting USRP device to send Wi-Fi OFDM symbols. Each Wi-Fi OFDM symbol had a duration of 4μs (3.2μs for the data symbol and 0.8μs for the CP).

The AP sampled the LTE signal and applied Algorithm 1 to compute the correlation $\rho(n)$ as a function of the shift n. Figure 15(b) shows sample values of $\rho(n)$ for the duration of ten LTE and Wi-Fi symbols. We observe that when an LTE transmits and the correlation windows W_1 and W_2 align with the CP and its copy, the correlation $\rho(n)$ peaks to values higher than 0.6. The peaks also denote the start time of OFDM symbols. Using the LTE CP detection parameters on Wi-Fi transmissions yields correlation values of almost zero. This is due to the different OFDM symbol length and CP length in Wi-Fi transmissions.



(a) (b) (c) (d)

Fig. 15: (a) Experimental setup, (b) ρ(n) vs. OFDM symbol index, (c) detection and false alarm probabilities as a function of the threshold γ_{LTE}, and (d) detection and false alarm probabilities as a function of the input power at the Wi-Fi AP.



(a) (b) (c)

Fig. 16: (a) The absolute phase difference as a function of the LTE sample index, (b) correlation $\rho(i,j)$ as a function of the LTE frame index, and (c) detection and false alarm probabilities vs. the threshold γ_{ID}.

In Fig. 15(c), we show the detection probability P_d and false alarm probability P_{fa} for the CP-based approach, computed over 6,000 OFDM symbols, as a function of the correlation threshold γ_{LTE}. The P_d was computed as the fraction of LTE symbols that were correctly classified, whereas P_{fa} was calculated as the fraction of Wi-Fi OFDM symbols falsely classified. Intuitively, a greater threshold would lower the false alarm rate but will decrease the detection probability. We observe that for thresholds in the 0.4-0.6 range, $P_d \approx 1$, whereas $P_{fa} = 0$. Following these experiments, we set the detection threshold to 0.4.

In the next experiment, we investigated the effect of the received signal strength (RSS) on the detection probability. We repeated the LTE signal detection experiment while moving the eNB away from the AP. In Fig. 15(d), we show P_d and P_{fa} as a function of the RSS at the AP. The signal correlation threshold was set to 0.4. Even at low power levels, P_d remains high whereas P_{fa} remains quite low with the exception of -70dBm, which is close to the CCA threshold for detecting any activity.

6.3 Differentiating between eNBs

In this set of experiments, we evaluated the LTE frame attribution algorithm for classifying LTE frames to different eNBs. In the first part of the experiments, one USRP transmitted LTE frames with the same primary and secondary synchronization signal (SSS/PSS) while the second USRP sampled the signal. The signal correlation $\rho_{ID}(i,j)$ was calculated over a total of 640 samples per frame, which is equal to the combined length of the two OFDM symbols carrying the SSS and PSS fields.

One practical issue in correlating the sampled PSS and SSS fields over different frames is the fact that the channel changes over time. Whereas the channel attenuation could remain relatively constant for a static LTE-AP distance, the phase of the impulse response could vary more rapidly. Indeed during our experiment, we noted an almost constant phase difference between samples of the same fields that belong to different frames of the same LTE ID. Figure 16(a) shows the absolute phase difference $|\theta_{diff}(k)|$ between the samples carrying the PSS and SSS fields in two consecutive frames as a function of the OFDM sample index k,

$$|\theta_{diff}(k)| = |\theta_{ID}^{(i)}(k) - \theta_{ID}^{(i-1)}(k)|, \quad \forall k \in [1 : L_{ID}], \quad (24)$$

where $\theta_{ID}^{(i-1)}(k)$ and $\theta_{ID}^{(i)}(k)$ are the phases of the k^{th} sample in the L_{ID} samples carrying both SSS and PSS fields in the $i-1^{st}$ and i^{th} LTE frames, respectively. We observe a fixed shift when both frames belong to the same LTE ID. This fixed shift is due to the coherence time of the channel. The channel remains relatively constant over the transmission of one frame, but changes over multiple frames. On the other hand, when two frames carry different PSS and SSS fields, the phase difference is random. To improve the eNB identification method, we apply a compensation technique for the channel response phase in Step 4 of the frame attribution algorithm, which operates as follows.

- The AP extracts $L_{ID} = 640$ samples representing $\mathbf{s}_{ID}^{(i)}$, i.e., the SSS and PSS fields of the i^{th} LTE frame. Denote the phases of the L_{ID} samples in $\mathbf{s}_{ID}^{(i)}$ by vector $\theta_{ID}^{(i)}$.
- For each signature $\mathbf{s}_{ID_j}$ stored in its database, the AP calculates the mean difference $\bar{\theta}(i,j)$ between $\theta_{ID}^{(i)}$ and θ_{ID_j} denoting the phases of the corresponding samples in $\mathbf{s}_{ID_j}$,

$$\bar{\theta}(i,j) = \frac{1}{L_{ID}} \sum_{k=1}^{L_{ID}} |\theta_{ID}^{(i)}(k) - \theta_{ID_j}(k)|. \quad (25)$$

- The phase part of $\mathbf{s}_{ID}^{(i)}$ is compensated by $\bar{\theta}(i,j)$ as follows

$$\theta_{ID}^{(i)} = \left(\theta_{ID}^{(i)} + \bar{\theta}(i,j)\right) \mod \pi. \quad (26)$$

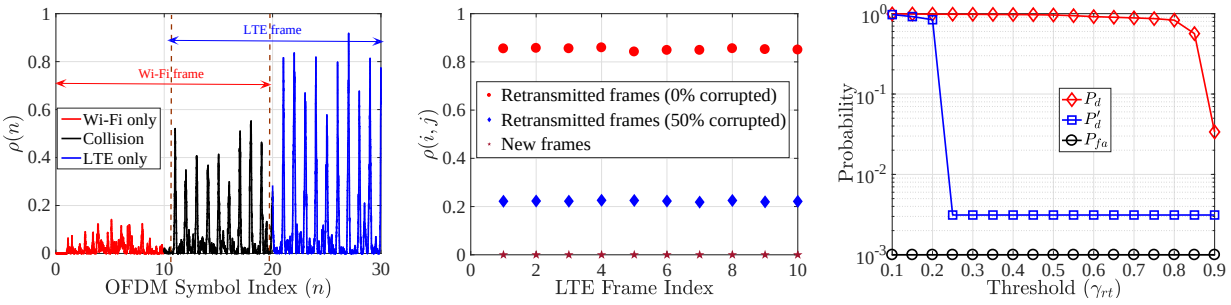


Fig. 17: (a) $\rho(n)$ for a collision between LTE and Wi-Fi frames, (b) correlation $\rho(i,j)$ as a function of the LTE frame index and (c) detection and false alarm probabilities as a function of the threshold γ_{rt}.

- The AP computes the correlation $\rho_{ID}(i,j)$ between $\mathbf{s}_{ID}^{(i)}$ and $\mathbf{s}_{ID_j}$ after the former has been phase-compensated, using equation (26).

We emphasize that the proposed phase compensation method does not require decoding LTE transmissions at the AP, as all operations occur on signal samples. Fig. 16(b) shows $\rho_{ID}(i,j)$ for 10 LTE frames in the following cases: (1) frames from the same eNB, (2) frames with the same PSS (cell ID) but different SSS (eNB ID), and (3) frames with different PSS and SSS fields. For the first case, we always have a high correlation as all frames belong to the same LTE. For the second and third cases, frames belong to different eNBs, thus the correlation is much lower. In Fig. 16(c), we plot the detection and false alarm probabilities as a function of the detection threshold, we vary the threshold from 0.1 to 0.9. The false alarm P'_{fa} represents the case of the same cell ID but different SSS, whereas P_{fa} represents the case of the different PSS and SSS. The value of P_{fa} is almost zero even for very low thresholds. For the second case, P'_{fa} becomes almost zero when the detection threshold is selected to be higher than 0.35, whereas P_d remains close to 1. The experiments confirm that applying the correlation technique on the PSS and SSS fields can successfully attribute LTE signals to the transmitting eNB.

6.4 Transmission Round Estimation

In the final set of experiments, we evaluated the transmission round estimation algorithm discussed in Section 4.4. First, we evaluated Step 1 in Algorithm 3 by implementing a collision between LTE and Wi-Fi frames and applying the CP-based correlation method. Figure 17(a) shows the correlation $\rho(n)$ as a function of the OFDM symbol index for a sample LTE collision with Wi-Fi. We observe that once the LTE frame starts, correlation peaks start to appear. Although the correlation is not as high as the case when the samples are interference-free, it is still sufficiently high to indicate the start of the LTE frame.

Furthermore, we implemented retransmissions of the same LTE frame and computed the signal correlation over a window of 38,400 samples, which is the length of one LTE frame. The phase compensation mechanism was also used here to account for the variations in the CIR. The phase difference was computed over the entire frame. Figure 17(b) shows the correlation between 10 pairs of frames when the frames in each pair are identical (retransmission due to channel impairments), identical but one is corrupted by another transmission (collision), and when they differ (not a retransmission). In the collision case, half of the samples representing the initial LTE frame are corrupted. We observe that the signal correlation between two identical transmissions is substantial enough to distinguish it from two different transmissions, even if some of the samples are corrupted.

In Fig. 17(c), we show the probability P_d of detecting a retransmission when both the original frame and the retransmission do not collide with other frames. Moreover, we show the detection probability P'_d of a retransmission when the original frame collided with another frame and the false alarm probability P_{fa} as a function of the threshold γ_{rt}. The false alarm P_{fa} is evaluated by changing the payload of consecutively transmitted LTE frames. We observe that the correlation technique yields a nearly perfect detection for any threshold less than 0.8 when the frames are not corrupted and 0.2 when the frames are corrupted. The false alarm, on the other hand, is close to zero for any threshold greater than 0.1. Setting $\gamma rt = 0.2$ allows the identification of retransmissions for both clean and corrupted frames. The high accuracy is attributed to the large number of samples used in the computation of the correlation.

7 Performance Evaluation

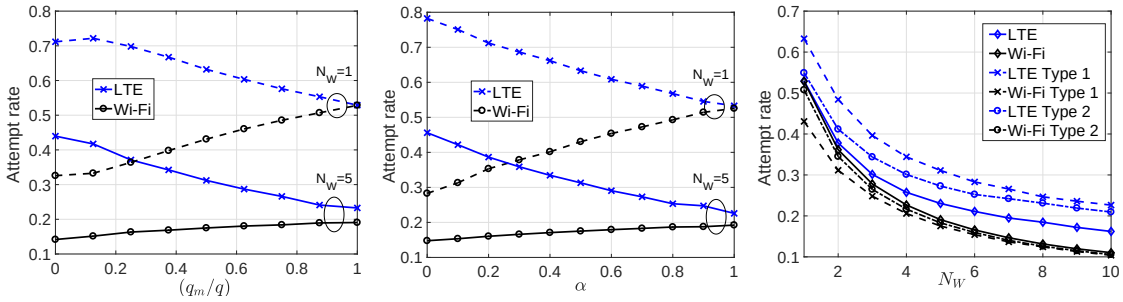
In this section, we validate the proposed misbehavior detection framework using simulations.

7.1 Simulation Setup

We implemented an event-based MATLAB simulator for the LTE/Wi-Fi coexistence. Specifically, we deployed a set of LTE and Wi-Fi devices within the same collision domain so that activity from every device affects the behavior of others. The eNBs followed the LTE-LAA standard whereas the APs implemented the IEEE 802.11ac protocol. No actual transmissions took place and the channel was assumed to be ideal. The simulator implemented the respective channel access protocols dictated by the two standards. Each experiment was run for 100,000 events, where each event corresponds to a transmission round. For each device, we evaluated the transmission attempt rate defined as the number of times a device tried to transmit (backoff reached zero) including collisions, over the total number of attempts by any device. This metric indicates the success rate in seizing the common medium. We further evaluated the detection and false alarm probabilities, P_d and P_{fa}, under different misbehavior scenarios.

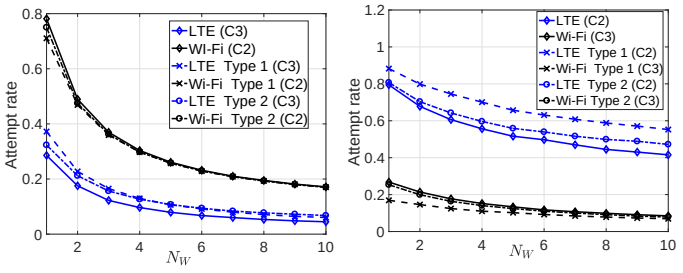
7.2 Effect of LTE Misbehavior on Wi-Fi

In the first set of experiments, we evaluated the effect of LTE misbehavior on the Wi-Fi channel access opportunities.



(a) (b) (c)

Fig. 18: Attempt rate for LTE and Wi-Fi systems: (a) vs. q_m/q, with $N_W = 1, 5$, and $\alpha = 0.5$, (b) vs. α, with $N_W = 1, 5$, and $q_m = 0.5q$, and (c) vs. number of Wi-Fi terminals, for class 3 LTE and class 3 Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.5$.



(a) (b)

Fig. 19: Attempt rate for LTE and Wi-Fi systems vs. number of Wi-Fi terminals for: (a) class 3 LTE and class 2 Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.5$, and (b) class 2 LTE and class 3 Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.5$.

LTE misbehavior was implemented by adopting smaller values for the default CW. The LTE chose its backoff uniformly in $\{0, 1, \ldots, q_m - 1\}$, where q_m is the modified CW that is chosen independently of the frame class and transmission round. In Fig. 18(a), we show the transmission attempt rate as a function of the normalized reduction in the CW size, denoted by q_m/q, where q is the compliant CW ($q_m/q = 1$ indicates no misbehavior). We set α, the fraction of time that the LTE remains compliant, to 0.5. We considered the coexistence of one LTE with $N_w = 1$ and $N_w = 5$ Wi-Fi APs, respectively. Wi-Fi APs are assumed to use class 3. The Wi-Fi channel access opportunities are shown to degrade when the LTE adopts smaller q_m values whereas the opportunities equalize when q_m approaches q. In addition, the LTE maintains its channel access advantage even when a larger number of Wi-Fi stations compete (note that for $N_W = 5$, the Wi-Fi attempt rate is normalized per AP). The degradation in the Wi-Fi attempt rate goes up to 50%. Figure 18(b) gives similar intuition when the fraction of time that the LTE misbehaves is varied and $q_m = 0.5q$.

Next, we studied the relation between the number of APs competing with the LTE and the attempt rate. We evaluated the effect of two misbehavior types. In Type 1 misbehavior, the LTE always decreases the CW to $q_m = 0.5q$, whereas in Type 2 it used the compliant CW ($q_m = q$), but disregarded the CW exponential growth after collisions. We compared the attempt rate under the two misbehavior types with the attempt rate when there is no LTE misbehavior, represented by the labels LTE and Wi-Fi with no type. In Fig. 18(c), we show the attempt rate as a function of N_W. An interesting point here is that the effect of Type 1 misbehavior is more prominent at small N_W's, whereas Type 2 misbehavior has a higher impact at high N_W. Overall, Type 1 misbehavior has higher impact than Type 2, as it affects all retransmission rounds.

In the previous set of experiments, the LTE and all Wi-Fi APs used the same priority class, i.e., almost similar backoff parameters. In the next set of experiments, we varied the priority class and measured the achieved attempt rate. In Fig. 19(a), the APs employed a lower priority class that utilizes a smaller CW. We observe that the Wi-Fi performance is almost the same as that of the LTE because reducing the CW for the LTE to $q_m = 0.5q$ equalizes the channel access opportunities for all devices. As expected, the LTE gains are significant when the LTE uses a lower class than Wi-Fi and the LTE also misbehaves. These results are shown in Fig. 19(b) where we see a larger difference in performance relative to Fig. 18(c), where the LTE and the APs operate the same class.

7.3 Receiver Operating Characteristic Curves

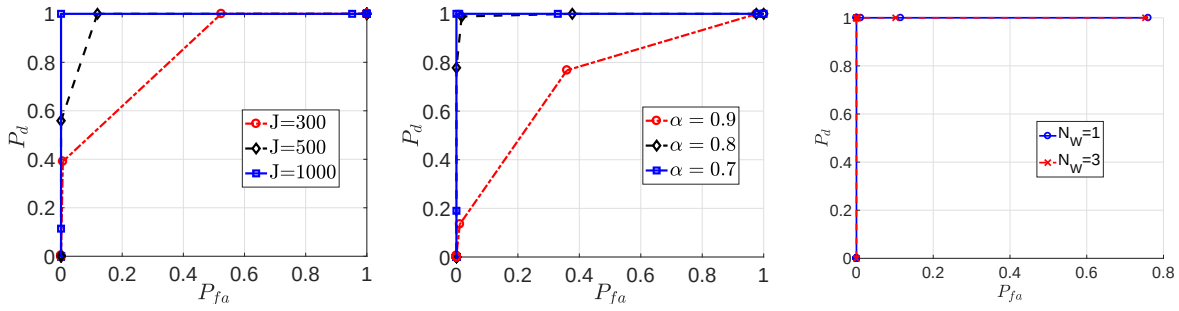
To investigate the efficacy of our misbehavior detection framework, we studied the tradeoff between P_{fa} and P_d, for different values of the misbehavior detection threshold δ, through receiver operating characteristic (ROC) curves.

7.3.1 Manipulation of the CW q

To measure P_d, we implemented a Type 1 misbehavior strategy with $q_m = 0.5q$ when the LTE misbehaved 50% of the simulation time. To measure P_{fa}, we applied our detection framework when the LTE did not misbehave. Figure 20(a) shows the ROC curve for different lengths of observation set (sizes of set $\mathbf{O}$) denoted by J. Indeed, with the increase in the length of the observation set, the ROC approaches the optimal curve indicating that our system can operate with almost sure detection and almost zero false alarm probability. Figure 20(a) also shows that 1,000 observations are sufficient to drive the detection probability to one with a negligible false alarm rate. As the duration of a single transmission is at most 8 ms, the required airtime for these 1,000 transmissions does not exceed 8 seconds. Considering different channel access delays before each of these transmissions, the 8 ms may be extended in the order of seconds to minutes. Generally, this time depends on the used parameters and how severe the misbehavior is. In Fig. 20(b), we see the effect of the fraction of time the LTE misbehaves. Even at low levels of misbehavior (e.g. $\alpha = 0.9$), the misbehavior is detectable.

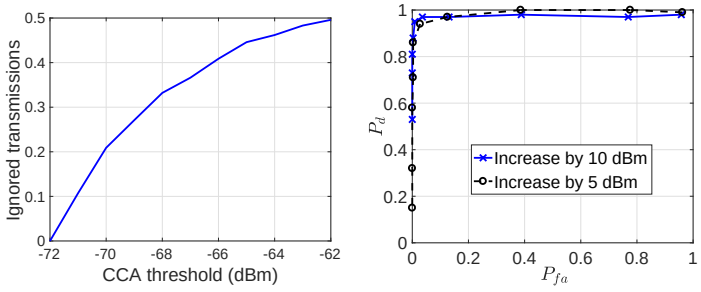
7.3.2 Manipulation of the defer time p

We further evaluated the performance of the proposed detection framework when the LTE manipulates the defer time p. To simulate this misbehavior, we implemented an LTE that uses the



(a) (b) (c)

Fig. 20: ROC curves: (a) $q_m = 0.5q$, and $\alpha = 0.5$, (b) $J = 1000$, and $q_m = 0.5q$, and (c) $q = 16$, and defer ($p = 1$).



(a) (b)

Fig. 21: (a) Average number of ignored Wi-Fi transmissions per channel access attempt, (b) ROC curve: $q = 16$, and $N_W = 200$.

defer time from traffic class C_1 (i.e., $p = 1$) while transmitting frames that belong to class C_3 ($p = 3$). Our simulations in Fig. 20(c) show an almost perfect ROC curve for any non-zero false alarm probability, when $N_w = 1$ and $N_w = 3$. The results are justified by the fact that the consistent selection of a smaller defer time skews the estimated distribution of backoff values in a detectable manner. This is a detectable phenomenon for any δ that fixes the false alarm probability to a given value.

7.3.3 CCA threshold manipulation

We further performed another set of experiments to evaluate the manipulation of the CCA threshold. A selection of a higher CCA threshold increases the number of APs that are ignored by the LTE. To simulate the CCA threshold manipulation scenario, we uniformly deployed multiple APs and one LTE in a square area of 200 × 200 meters. We set the transmission power of each Wi-Fi AP to 20dBm and modeled the channels between terminals using the free path-loss model (the channel model is not really important here). We set the carrier frequency to 5 GHz.

We evaluated the performance of our detector when the CCA threshold is increased by 5, and 10 dBm. To highlight the effect of CCA threshold manipulation, we implemented a deployment of $N_W = 200$ APs. Here, we increased the number of APs to ensure that we have a non-negligible number of ignored Wi-Fi transmissions. This is shown in Fig. 21(a) where we plot the average number of ignored Wi-Fi transmissions, normalized over the LTE channel access attempts. For instance, when the CCA threshold is set to -70 dBm, the LTE ignores on average one Wi-Fi transmission every five channel access attempts. On the other hand, the LTE ignores on average one Wi-Fi transmission every other channel access attempt when the threshold is set to -62 dBm. The high number of APs is a relevant scenario in urban areas where there are dense deployments of APs. In Fig. 21(b), we show the ROC for increasing the CCA threshold by 5 or 10 dBm. We observe that when the CCA is increased by more than 5dBm, the ROC approaches the optimal one.

7.4 Comparison of Statistical Framework with Methods from Homogeneous Networks

To demonstrate the adequacy of our statistical inference method presented in Section 5.4, we compared it to representative methods that were developed for homogeneous networks. Such methods are comparable because they all analyze a time series of backoff counter observations. Specifically, we selected the methods in [36] that compares the average backoff counter to a threshold derived from the nominal behavior. First, we simulated an LTE eNB that reduces the CW size from 16 (typical value in class C_3) to 8, but still selects the backoff randomly from the reduced range. A total of 1,000 observations were collected. Figure 23(a) shows the ROC curve for both frameworks. We observe that both methods have similar performance and are able to detect misbehavior with perfect detection probability and a near-zero false alarm rate.

We further repeated our simulations under a different misbehavior model. In this set of simulations, the LTE manipulated the backoff counter b based on the following non-uniform distribution.

$$\Pr(b = i) = \begin{cases} 0.8, & i = 0, \\ 0.2, & i = 38, \\ 0, & \text{otherwise.} \end{cases} \quad (27)$$

This particular distribution was selected in the following way. First, we fixed the probability of selecting a zero backoff counter to 0.8. That is, the majority of the time the LTE does not back off. Then, we assigned the remaining probability mass to a backoff value that would make the average backoff equal to that of the uniform distribution $U[0, 15]$. Figure 23(b) shows the ROC curve for the non-uniform distribution strategy. In this case, we can see that the framework in [36] fails to provide a reliable detection without having a high false alarm rate. On the other hand, our proposed framework can still guarantee a very high detection probability with a near-zero false alarm rate (We were not able to observe any false alarm in our experiments).

7.5 Unsaturated traffic

In the last set of experiments, we studied misbehavior under unsaturated traffic conditions. We implemented a Poisson frame arrival process with an average rate λ for each device. We measured the saturation level by the percentage of time a device's

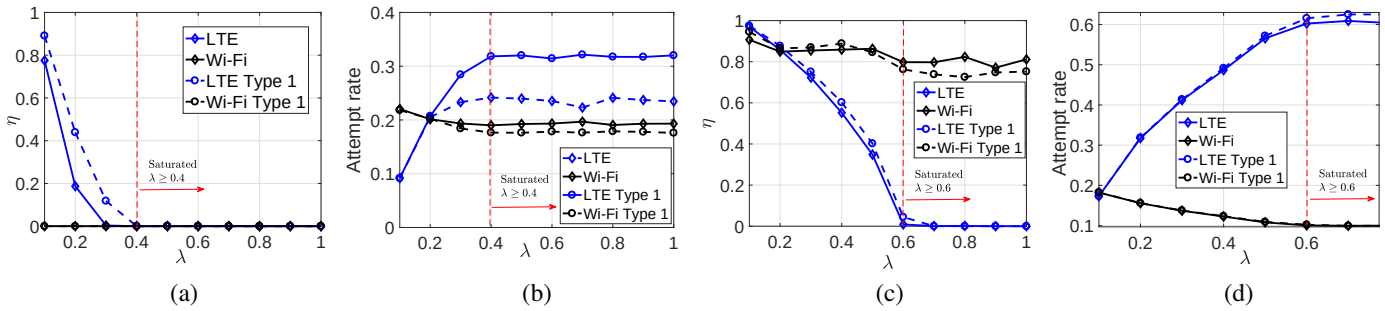


Fig. 22: (a) Attempt rate vs. λ, and (b) η vs. λ when Wi-Fi traffic is saturated. (c) Attempt rate vs. λ, and (d) η vs. λ when Wi-Fi traffic is unsaturated.

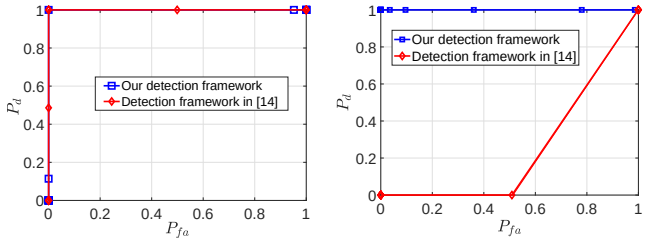


Fig. 23: (a) ROC curve for a backoff manipulation strategy when C_3 class is transmitted and the CW is reduced from $q = 16$ to $q_m = 8$. (a) uniform selection, and (b) non-uniform selection with the same backoff average.

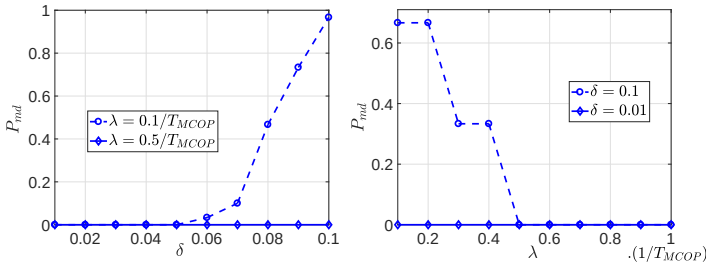


Fig. 24: Misdetection probability (P_{md}) vs. : (a) Threshold δ, and (b) LTE arrival rate λ.

queue stays empty and denoted this parameter by η. A device is saturated if $\eta = 0$, i.e., it always has a frame to transmit.

In Fig. 22, we show the effect of the arrival rate on the attempt rate for different levels of saturation. We implemented a Type 1 misbehavior strategy where the eNB transmits class 3 frames but reduces the contention window to $q_m = 0.5q$. The eNB misbehaved half the time ($\alpha = 0.5$). Figure 22(a) shows the saturation levels of both LTE and Wi-Fi with and without LTE misbehavior when the Wi-Fi traffic is always saturated and one eNB competes with five APs. Figure 22(b) shows the respective attempt rates. Here, the arrival rate is normalized by $1/T_{\text{MCOP}}$ which is the maximum service rate (transmissions per second) that meets the medium capacity. In Fig. 22(a), we note that η always equals zero for the Wi-Fi APs, as they are backlogged by design. For the LTE station, we observe that when the LTE misbehaves, saturation occurs at a higher arrival rate indicating that the LTE gains an advantage in accessing the channel sooner.

Figure 22(b) shows that when the arrival rate is low, misbehavior has no effect on the attempt rate of the Wi-Fi. However, when λ increases and the devices approach saturation, the gap between the attempt rate, with and without misbehavior, increases. As expected, the attempt rate gap remains constant after saturation is reached (and is consistent with the results shown in Fig. 19).

Figures 22(c) and 22(d) show the same experiments, but when the APs remain unsaturated while the arrival rate for the LTE increases. The unsaturated condition for the Wi-Fi is also evident in Fig. 22(c), where the Wi-Fi queue is empty over 70% of the time for any λ. From Fig. 22(c), we further observe that the gain from misbehavior is practically diminished. The LTE saturates almost at the same rate $\lambda = 0.6$. Further, we observe in Fig. 22(d) that the LTE misbehavior increases the LTE attempt rate in an imperceptible manner. This makes misbehavior detection less necessary compared to saturated conditions.

Finally, we evaluated the misdetection probability P_{md} under unsaturated traffic conditions. In Fig. 24(a), we show P_{md} as a function of the threshold δ, for Type 1 misbehavior with $q_m = 0.5q$ and $\alpha = 0.5$. As expected for $\lambda = \frac{0.5}{T_{\text{MCOP}}}$ (i.e., under saturated conditions as seen in Fig. 22 (a)), we have almost perfect detection. Under unsaturated conditions ($\lambda = \frac{0.1}{T_{\text{MCOP}}}$), the method of excluding observations that yield idle times larger than expected during a backoff process enables us to have a reasonable P_{md} with careful selection of δ. Misdetection becomes very small for $\delta \leq 0.05$, however, for this range, the AP is required to collect a large number of observations to avoid false alarms. Generally, this range of δ is only required whenever the LTE is found operating under unsaturated traffic conditions. Figure 24(b) shows P_{md} as a function of the arrival rate λ at the LTE, for Type 1 misbehavior. As expected, P_{md} approaches zero as we approach saturation.

8 Conclusion

We studied the problem of LTE misbehavior under the LTE-LAA protocol for coexistent LTE and Wi-Fi systems. We outlined several misbehavior scenarios and developed a suite of implicit monitoring techniques that enable the Wi-Fi system to estimate the operational parameters of the LTE, without decoding LTE signals. This is a desired property as Wi-Fi devices are not necessarily equipped with LTE receivers. Our methods rely on operations in the signal domain to identify and classify LTE transmissions. We evaluated these techniques using an experimental setup and verified their efficiency in practical scenarios.

We further developed a behavior evaluation framework in which a central hub collects all observations from a distributed set of monitoring APs to build a behavior profile for the eNBs and detect misbehavior. We extended our detection method to work reliably for both unsaturated and saturated traffic. We evaluated

the performance of our detector via simulations and showed that LTE misbehavior can cause a significant performance degradation for Wi-Fi devices. However, such misbehavior was detectable by our framework with very high probability while achieving a low false alarm probability. Although our framework focuses on the coexistence between LTE and Wi-Fi systems, our ideas can be extended to other coexistence scenarios.

ACKNOWLEDGEMENTS

I. Samy, X. Han, L. Lazos, and M. Li were supported in part by NSF grant CNS-1731164. M. Krunz was supported in part by NSF (grants CNS-1910348, CNS-1731164, CNS-1813401) and by the Broadband Wireless Access Applications Center (BWAC). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of NSF. Y. Xiao's work was supported in part by the National Natural Science Foundation of China under Grant 62071193 and the Key R&D Program of Hubei Province of China under Grant 2020BAA002.

REFERENCES

[1] I. Samy, L. Lazos, Y. Xiao, M. Li, and M. Krunz, "LTE misbehavior detection in Wi-Fi/LTE coexistence under the LAA-LTE standard," in *Proceedings of WiSec Conference*, 2018, pp. 87–98.

[2] FCC, "Second memorandum opinion and order: In the matter of unlicensed operation in the TV broadcast band and additional spectrum for unlicensed devices below 900 MHz in the 3 GHz band," https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-260A1.pdf, 2010.

[3] Qualcomm, "Qualcomm whitepaper: Extending LTE advanced to unlicensed spectrum," https://www.qualcomm.com/media/documents/files/white-paper-extending-lte-advanced-to-unlicensed-spectrum.pdf, 2013.

[4] FCC, "FCC 16-89: Use of spectrum bands above 24 GHz for mobile radio services, et al." https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-89A1_Rcd.pdf, 2016.

[5] GSA, "https://gsacom.com/paper/lte-5g-market-statistics-march-2021/."

[6] ——, "https://gsacom.com/paper/unlicensed-shared-spectrum-report-july-2019/."

[7] V. Sathya, M. I. Rochman, and M. Ghosh, "Measurement-based coexistence studies of laa & wi-fi deployments in chicago," *IEEE Wireless Communications*, 2020.

[8] H. He, H. Shan, A. Huang, L. X. Cai, and T. Q. Quek, "Proportional fairness-based resource allocation for LTE-U coexisting with Wi-Fi," *IEEE Access*, vol. 5, pp. 4720–4731, 2016.

[9] Y. Li, F. Baccelli, J. G. Andrews, T. D. Novlan, and J. C. Zhang, "Modeling and analyzing the coexistence of Wi-Fi and LTE in unlicensed spectrum," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6310–6326, 2016.

[10] Z. Guan and T. Melodia, "CU-LTE: Spectrally-efficient and fair coexistence between LTE and Wi-Fi in unlicensed bands," in *Proc. of the INFOCOM Conference*, 2016, pp. 1–9.

[11] J. Xiao and J. Zheng, "An adaptive channel access mechanism for LTE-U and WiFi coexistence in an unlicensed spectrum," in *Proc. of the ICC Conference*, 2016, pp. 1–6.

[12] Q. Chen, G. Yu, and Z. Ding, "Optimizing unlicensed spectrum sharing for LTE-U and WiFi network coexistence," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2562–2574, 2016.

[13] S. Zinno, G. Di Stasi, S. Avallone, and G. Ventre, "On a fair coexistence of LTE and Wi-Fi in the unlicensed spectrum: A survey," *Computer Communications*, 2017.

[14] I. Samy and L. Lazos, "Optimum priority class selection under Wi-Fi/LTE coexistence," in *Proc. of the ICC Conference*, 2019, pp. 1–7.

[15] X. Han, I. Samy, and L. Lazos, "Energy-efficient LTE/Wi-Fi coexistence," in *Proc. of the ICC Conference*, 2020, pp. 1–7.

[16] M. Hirzallah and M. Krunz, "Intelligent tracking of network dynamics for cross-technology coexistence over unlicensed bands," in *Proc. of the ICNC Conference*, 2020, pp. 698–703.

[17] A. H. Y. Abyaneh, M. Hirzallah, and M. Krunz, "Intelligent-CW: AI-based framework for controlling contention window in WLANs," in *Proc. of the DySPAN Symposium*, 2019, pp. 1–10.

[18] M. Hirzallah, M. Krunz, and Y. Xiao, "Harmonious cross-technology coexistence with heterogeneous traffic in unlicensed bands: Analysis and approximations," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 690–701, 2019.

[19] M. Hirzallah, Y. Xiao, and M. Krunz, "Matchmaker: An inter-operator network sharing framework in unlicensed bands," in *Proc. of the SECON Conference*, 2019, pp. 1–9.

[20] ——, "On modeling and optimizing LTE/Wi-Fi coexistence with prioritized traffic classes," in *Proc. of the DySPAN Symposium*, 2018, pp. 1–10.

[21] S. Sagari, I. Seskar, and D. Raychaudhuri, "Modeling the coexistence of LTE and WiFi heterogeneous networks in dense deployment scenarios," in *Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 2301–2306.

[22] R. Ratasuk, M. A. Uusitalo, N. Mangalvedhe, A. Sorri, S. Iraji, C. Wijting, and A. Ghosh, "License-exempt LTE deployment in heterogeneous network," in *Wireless Communication Systems (ISWCS), 2012 International Symposium on*, 2012, pp. 246–250.

[23] 3GPP TS 37.213 version 15.0.0 Release 15, "LTE; physical layer procedures for shared spectrum channel access," 2018.

[24] T. Tao, F. Han, and Y. Liu, "Enhanced LBT algorithm for LTE-LAA in unlicensed band," in *Proc. of the PIMRC Symposium*, 2015, pp. 1907–1911.

[25] R. Yin, G. Yu, A. Maaref, and G. Y. Li, "LBT-based adaptive channel access for LTE-U systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6585–6597, 2016.

[26] J. Tan, S. Xiao, S. Han, Y.-C. Liang, and V. C. Leung, "QoS-aware user association and resource allocation in LAA-LTE/WiFi coexistence systems," *IEEE Transactions on Wireless Communications*, vol. 18, no. 4, pp. 2415–2430, 2019.

[27] J. Tan, L. Zhang, Y.-C. Liang, and D. Niyato, "Deep reinforcement learning for the coexistence of LAA-LTE and WiFi systems," in *Proc. of the ICC Conference*, 2019, pp. 1–6.

[28] X. Ying, R. Poovendran, and S. Roy, "Detecting lte-u duty cycling misbehavior for fair sharing with wi-fi in shared bands," in *Proc. of the PIMRC Symposium*, 2017, pp. 1–7.

[29] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 5, pp. 502–516, 2005.

[30] J. Tang, Y. Cheng, and W. Zhuang, "Real-time misbehavior detection in IEEE 802.11-based wireless networks: An analytical approach," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 146–158, 2014.

[31] M. Li, S. Salinas, P. Li, J. Sun, and X. Huang, "MAC-layer selfish misbehavior in ieee 802.11 adhoc networks: Detection and defense," *IEEE Trans. on Mobile Computing*, vol. 14, no. 6, pp. 1203–1217, 2015.

[32] Y. Zhang and L. Lazos, "Vulnerabilities of cognitive radio MAC protocols and countermeasures," *IEEE Network*, vol. 27, no. 3, pp. 40–45, 2013.

[33] M. Hirzallah, W. Afifi, and M. Krunz, "Full-duplex spectrum sensing and fairness mechanisms for Wi-Fi/LTE-U coexistence," in *Proc. of the GlOBECOM Conference*, 2016, pp. 1–6.

[34] A. L. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE journal on selected areas in communications*, vol. 25, no. 6, 2007.

[35] Y. Zhang and L. Lazos, "Countering selfish misbehavior in multi-channel MAC protocols," in *Proc. of the INFOCOM Conference*, 2013, pp. 2787–2795.

[36] M. Raya, J. Hubaux, and I. Aad, "DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots," in *Proc. of MobiSys*, 2004, pp. 84–97.

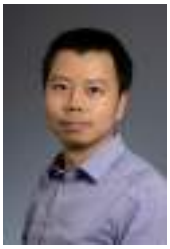
[37] S. Gollakota and D. Katabi, "Zigzag decoding: Combating hidden terminals in wireless networks," in *Proc. of the ACM SIGCOMM Conference*, 2008, pp. 159–170.

Islam Samy received his B.S. degree in Electrical Engineering from Alexandria University in 2011 and the M.Sc. degree in wireless communication from Nile University in 2014. He is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, The University of Arizona, where he is also a Graduate Research Assistant. His main research interests include secure and fair resource allocation for heterogeneous coexisting systems, wireless communication, and information theory.

Xiao Han received a B.S. degree in Electrical Engineering from Northwest A&F University, Xianyang, China, in 2016, and M.S. degree in Electrical and Computer Engineering from University of Arizona, Tucson, United States, in 2019. He is currently working toward the Ph.D. degree in Computer Science at University of South Florida, Tampa, United States. His research interests include wireless networks and network security.

Loukas Lazos is a Professor of Electrical and Computer Engineering at the University of Arizona. Dr. Lazos received his Ph.D. degree in Electrical Engineering from the University of Washington in 2006. His research interests are in the areas of network security, privacy, and wireless communications. His current research focuses on secret-free authentication methods for IoT devices, integrity verification of physical properties, secure and fair channel access for emerging wireless technologies, and fair resource allocation for heterogeneous coexisting technologies, and private information retrieval. Dr. Lazos is the recipient of the US National Science Foundation (NSF) Faculty Early CAREER Development Award (2009) for his research in security of multi-channel wireless networks. He has served as a technical program chair for the IEEE CNS conference, the IEEE GLOBECOM symposium on communications and information systems security and the IEEE DSPAN workshop. He is an associate editor for the IEEE Transactions on Information and Forensics Security journal and the IEEE Transactions on Mobile Computing journal. He has also served and continues to serve on the organization and technical program committees of many international conferences and on expert panels of several government agencies.

Ming Li is an Associate Professor in the Department of Electrical and Computer Engineering of University of Arizona, and also affiliated with the Computer Science Department. He was an Assistant Professor in the Computer Science Department at Utah State University from 2011 to 2015. He received his Ph.D. in ECE from Worcester Polytechnic Institute, MA, in 2011. His main research interests are wireless and cyber security, with current emphases on cross-layer optimization and machine learning in wireless networks, wireless physical layer security, privacy enhancing technologies, and cyber-physical system security. He received the NSF Early Faculty Development (CAREER) Award in 2014 and the ONR Young Investigator Program (YIP) Award in 2016. He was a recipient of the best paper award from ACM WiSec 2020. Currently he serves on the editorial boards of IEEE TWC, TMC and TDSC. He is a senior member of IEEE, and a member of ACM.



Yong Xiao is a Professor in the School of Electronic Information and Communications at the Huazhong University of Science and Technology (HUST), Wuhan, China. He is also the associate group leader of the network intelligence group of IMT-2030 (6G promoting group) and the vice director of 5G Verticals Innovation Laboratory at HUST. Before he joins HUST, he was a research assistant professor in the Department of Electrical and Computer Engineering at the University of Arizona where he was also the center manager of the Broadband Wireless Access and Applications Center (BWAC), an NSF Industry/University Cooperative Research Center (I/UCRC) led by the University of Arizona. His research interests include machine learning, game theory, distributed optimization, and their applications in cloud/fog/mobile edge computing, semantic communications, wireless networks, and Internet-of-Things (IoT).

Marwan Krunz is a Regents Professor at the University of Arizona. He holds the Kenneth VonBehren Endowed Professorship in ECE and is also a Professor of Computer Science. He directs the Broadband Wireless Access and Applications Center (BWAC), a multi-university NSF/industry center that focuses on next-generation wireless technologies. He also holds a courtesy appointment as a Professor at the University of Technology, Sydney. Previously, he served as the site director for the Connection One center. Dr. Krunz's research is on resource management, network protocols, and security for wireless systems. He has published more than 300 journal articles and peer-reviewed conference papers, and is a named inventor on 12 patents. His latest h-index is 61. He is an IEEE Fellow, an Arizona Engineering Faculty Fellow, and an IEEE Communications Society Distinguished Lecturer (2013-2015). He received the NSF CAREER award. He served as the Editor-in-Chief for the IEEE Transactions on Mobile Computing. He also served as editor for numerous IEEE journals. He was the TPC chair for INFOCOM'04, SECON'05, WoWMoM'06, and Hot Interconnects 9. He was the general vice-chair for WiOpt 2016 and general co-chair for WiSec'12. Dr. Krunz served as chief scientist for two startup companies that focus on 5G and beyond systems and machine learning for wireless communications.