LTE Misbehavior Detection in Wi-Fi/LTE Coexistence Under the LAA-LTE Standard

Islam Samy
Dept. of Electrical and Computer
Engineering, University of Arizona
islamsamy@email.arizona.edu

Loukas Lazos
Dept. of Electrical and Computer
Engineering, University of Arizona
llazos@email.arizona.edu

Yong Xiao
Dept. of Electrical and Computer
Engineering, University of Arizona
yongxiao@email.arizona.edu

Ming Li
Dept. of Electrical and Computer
Engineering, University of Arizona
lim@email.arizona.edu

Marwan Krunz
Dept. of Electrical and Computer
Engineering, University of Arizona,
and University of Technology Sydney
krunz@email.arizona.edu

ABSTRACT

In this paper, we consider the fair coexistence between LTE and Wi-Fi systems in unlicensed bands. We focus on the misbehavior opportunities that stem from the heterogeneity of the coexisting systems and the lack of explicit coordination mechanisms. We show that a selfishly behaving LTE can gain an unfair share of the spectrum resources through the manipulation of the parameters defined in the LAA-LTE standard, including the manipulation of the backoff mechanism of LAA, the traffic class, the clear channel assignment threshold and others. We develop a detection mechanism for the Wi-Fi system that can identify a misbehaving LTE system. Our mechanism advances the state of the art by providing an accurate monitoring method of the LTE behavior under various topological scenarios, *without explicit cross-system coordination.* Deviations from the expected behavior are determined by computing the statistical distance between the protocol-specified and estimated distributions of the LAA-LTE protocol parameters. We analytically characterize the detection and false alarm probabilities and show that our detector yields high detection accuracy at very low false alarm rate, for a wise choice of statistical parameters.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; • **Networks** → *Protocol testing and verification*;

KEYWORDS

LTE-Unlicensed, LTE-LAA, Wi-Fi, Spectrum access, Coexistence, Backoff manipulation, Misbehavior detection

1 INTRODUCTION

The dramatic growth in demand for wireless services has fueled a severe shortage in radio spectrum, especially in the overcrowded unlicensed bands. The regulatory approach for meeting this galloping demand is to allow the coexistence of competing wireless technologies (e.g., LTE Unlicensed and Wi-Fi coexisting in the 5GHz U-NII band) [1–5]. This shared spectrum paradigm poses novel challenges for the secure, efficient, and fair resource access. Many of these challenges stem from the heterogeneity of the coexisting systems, the system scale, and the lack of explicit coordination mechanisms between them. The fundamentally different spectrum access mechanisms and PHY-layer capabilities–dynamic vs. fixed access, schedule-based vs. random access, interference-avoiding vs. interference-mitigating, etc.–create a complex and interdependent ecosystem, without a unified control plane.

Some recent efforts have addressed the problem of fair coexistence of LTE/Wi-Fi and Wi-Fi/Zigbee under benign settings (e.g., [6–14]). Theoretical and experimental studies showed that the Wi-Fi performance seriously degrades in the presence of an LTE Unlicensed system, even if the LTE remains protocol-compliant [15, 16]. Several mechanisms proposed standard modifications to mitigate the protocol unfairness. Two main approaches were promoted: a duty cycle-based LTE-U based on Carrier-Sensing Adaptive Transmission (CSAT) mechanism introduced by Qualcomm [17] and a channel sensing-based Licensed-Assisted Access LTE (LAA-LTE) based on the Listen-Before-Talk (LBT) mechanism [18]. For the former approach, it was shown that adjusting the LTE duty cycle can improve fairness [19,20]. For the LBT mechanism-based LAA, Jeon *et al.* showed that controlling the Clear Channel Assessment (CCA) threshold can be beneficial for the fair coexistence [21]. Follow-up works achieved further improvements by dynamically adapting the contention window (CW) size [22,23].

However, the impact of deliberate violation of the coexistence etiquette to gain an unfair share of spectrum occupancy has not been studied at length. Ying *et al.* were among the first that considered the problem of misbehavior when cycle-based LTE-U and Wi-Fi coexist [24]. The authors recognized that the LTE duty cycle is unilaterally controlled by the LTE system, and can therefore be abused to increase the spectrum share of the LTE. They proposed a monitoring mechanism that accurately estimates the duty cycle followed by the LTE and allows a spectrum manager detect any misbehavior. The proposed scheme is not applicable to LAA-LTE standard, which is embraced by most LTE operators and the standardization bodies [18].

WiSec '18, June 18–20, 2018, Stockholm, Sweden

ACM ISBN 978-1-4503-5731-9/18/06. . . $15.00
https://doi.org/10.1145/3212480.3212485

In this paper, we are the first to propose a mechanism for detecting misbehavior under LAA-LTE.

Our methods build upon the extensive prior art on misbehavior detection in channel access for homogeneous networks, e.g., [25–29], with notable differences. First, heterogeneous networks do not share common coordination channels for communicating explicit control information such as network allocation vector fields, device IDs, reservation messages (RTS/CTS), etc. Without explicit coordination, detecting the state and monitoring the behavior of stations operating under a different technology become challenging, as the messages exchanged by one system are undecodable at any other. Relevant challenges include determining which system occupies the channel, for how long, at what locality, with what range, which stations collided, to name a few. Moreover, although the LAA-LTE and Wi-Fi standards follow the same carrier-sense multiple access (CSMA) principles, they adopt different channel contention parameters that affect the overall system behavior under various conditions of coexistence. Determining a system's behavior requires accurate estimation of protocol parameters using only implicit monitoring. Note that Wi-Fi devices may not be equipped with LTE receivers and vise versa, thus complicating the monitoring mechanism.

In this paper, we address the problem of misbehavior at the system level when heterogeneous technologies coexist. Specifically, we consider a misbehaving LAA-LTE system that coexists with a Wi-Fi deployment. The LTE aims at occupying the shared spectrum for a longer fraction of time by manipulating the channel access mechanism of LAA. We propose a framework that enables the Wi-Fi to detect the misbehavior of LTE, taking into account the absence of any means for explicit coordination. Our framework relies on implicit sensing mechanisms that provide the Wi-Fi with accurate approximations of the operational parameters used by the misbehaving LTE. Parameters of interest include the defer time before an attempt of channel access, the backoff period for new and retransmitted frames, the LTE priority class, and the CW size. Our contributions are summarized as follows:

- We are the first to study and formulate the problem of channel access misbehavior of LAA-LTE 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 monitoring mechanism that does not rely on signal decoding for estimating relevant LAA-LTE protocol parameters. We develop an implicit sensing mechanism that goes beyond simple LTE transmission detection, to determine the existence of hidden stations, identify retransmitted frames, and specify the LTE priority class. These are essential parameters for accurately estimating the overall LTE behavior.
- We propose a novel misbehavior detection mechanism based on Jensen-Shannon (JS) divergence [30]. We analytically evaluate the threshold for detecting misbehavior based on the JS metric and characterize the detection and false alarm probabilities.
- We validate our theoretical results via extensive simulations and show that our detector yields near-perfect detection capabilities and a negligible false alarm rate.

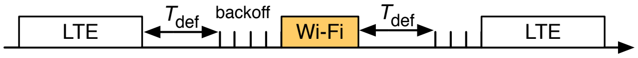


Figure 1: Backoff between two consecutive transmissions.

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 analyze the detection scheme performance in Section 6. We summarize the main contributions of this work in Section 7.

2 BACKGROUND AND RELATED WORK

2.1 LAA-LTE Release 14

We consider an LTE system that follows the LAA-LTE specification, as described in LTE Release 14 [18]. The standard defines four traffic priority classes with channel access parameters listed in Table 1. Classes C_1 and C_2 are suitable for transmitting control messages and short frames, whereas classes C_3 and C_4 accommodate longer LTE frames. The channel access mechanism of LAA-LTE is shown in Fig. 1 and is described in the following steps.

(1) Upon the completion of the previous LTE transmission, the LTE station 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 higher priority classes to compensate for the longer frame size. If the channel stays idle during T_{init}, the LTE 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 ($P_{th} \approx -73$ dBm according to [18]), for at least $4\mu s$, the channel is inferred to be idle. Otherwise, it is inferred to be busy.

(2) The LTE station initializes the backoff counter to a value N uniformly selected in $[\![0, q-1]\!]$, where q is the CW size, which is initially set to a minimum value $q_{\min}$.

(3) The LTE station decrements its backoff counter by one with every idle slot. If a slot is sensed to be busy, the station 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 LTE station transmits a frame with maximum duration of T_{MCOP}. The station then waits for an ACK/NACK. If it receives an ACK, the transmission round for the given frame is completed. Otherwise, the process is repeated from Step 2 by doubling the CW size.

We note that the priority classes differ in both the defer time and allowed CW sizes. As will be shown later, this difference can be exploited by LTE stations to shorten the time between consecutive transmissions.

2.2 Related Work

Whereas there is a wealth of interest in channel access misbehavior for homogeneous networks, misbehavior between coexisting

Table 1: Parameters for different priority classes.

Priority Class	p	$q_{\min}$	T_{MCOP} (ms)	Allowed q sizes
C_1	1	4	2	$\{4, 8\}$
C_2	1	8	3	$\{8, 16\}$
C_3	3	16	8 or 10	$\{16, 32, 64\}$
C_4	7	16	8 or 10	$\{16, 32, \ldots, 1024\}$

technologies is relatively new. The work closest to ours is reported in [24]. However, the authors considered the misbehavior in the LTE-U protocol that adopts a duty cycle channel access model. 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 ones. Possible LTE misbehavior is detected by a central node called the spectrum manager, which has prior knowledge on the permitted duty cycle for the LTE. In this paper we consider misbehavior under the LAA-LTE standard that implements a CSMA-like channel access model and involves drastically different misbehavior actions and remedies. Our work is similar to that of [24] in that we also employ a central node we call the hub to analyze the LTE behavior.

The LTE/Wi-Fi coexistence in a benign setting has sparked a lot of interest due to the unfairness in channel access opportunities (e.g., [14] and references therein). Ratasuk *et al.* [16] showed that LTE outperforms Wi-Fi by replacing one of the Wi-Fi deployments with an LTE cell and comparing the respective throughput. Hirzallah *et al.* [31] showed that different access protocols for Wi-Fi and LTE can cause an increase in the collision rate and latency for both systems. They suggested a CCA threshold adaptation mechanism to promote fairness between the two systems. The idea of adapting the backoff parameters of the LTE to achieve fair coexistence with Wi-Fi is also studied in [21–23]. However, these works assumed that all stations are always trustful and protocol-compliant.

Misbehavior detection for channel access in homogeneous networks has been extensively studied, especially for the IEEE 802.11 family of protocols (e.g., [25–28, 32, 33]). Tang *et al.* proposed a real-time misbehavior detection mechanism, depending on an indicator function that represents the difference between the number of successful transmissions and the number of expected transmissions, under a fair channel allocation [27]. Li *et al.* used multiple backoff counter observations to calculate the probability that a monitored station remains protocol-compliant [28]. Misbehavior was detected by comparing this probability to a threshold. Toledo *et al.* applied the Kolmogorov-Smirnov test to detect misbehavior from the number of idle slots between two transmissions [32]. As all stations follow the same protocol, misbehavior is detected if the idle slot distribution of a station differs from that of others.

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, the LTE and Wi-Fi systems execute channel access protocols with different parameters. For instance, the LAA-LTE backoff parameters change depending on the priority class, as shown in Table 1. Accurate estimation of the LTE behavior requires mechanisms for classifying frames 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.

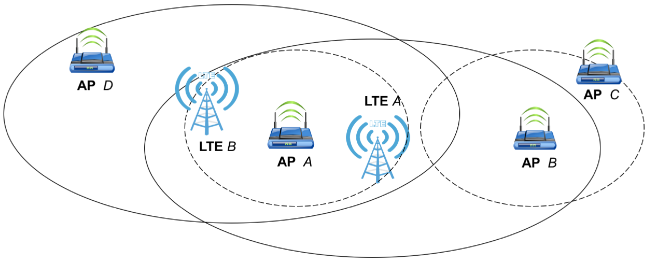


Figure 2: Coexistence between LTE and Wi-Fi. Wi-Fi and LTE stations have difference interference ranges.

3 SYSTEM AND MISBEHAVIOR MODELS

System Model: We consider the coexistence of an LAA-LTE system with N_W Wi-Fi access points (APs) over the 5GHz unlicensed band, as shown in Fig. 2. The set of all Wi-Fi APs in the vicinity of the LTE is denoted by $\mathcal{N}_W$, with $|\mathcal{N}_W| = N_W$. For a station X, we denote by $\mathcal{N}_X^{(1)}$ all transmissions that interfere with X. That LTE and Wi-Fi APs transmit at different powers, so if $Y \in \mathcal{N}_X^{(1)}$, it is not implied that $X \in \mathcal{N}_Y^{(1)}$. As an example, Wi-Fi AP B of Fig. 2 is in the interefence range of LTE A (solid line), but LTE A is not in the interference range of B (dashed line). The transmission powers for the LTE and Wi-Fi are denoted by P_l and P_w, respectively.

The LTE behavior is expected to follow the LAA-LTE standard [18], as described in Section 2.1. We consider the misbehavior of one or more LTE stations which are monitored by any Wi-Fi AP in their vicinity. The observations of the LTE behavior are assumed to be collectively available for analysis at a central hub. This assumption is made to evaluate misbehavior at the system level rather than the station level, as done in prior works on homogeneous networks. Finally, we analyze the LTE misbehavior under backlogged traffic conditions. This is the most relevant scenario for LTE misbehavior detection, as prior works have shown low performance gains under conditions of low contention [33].

Misbehavior Model: The LTE system manipulates the LAA-LTE protocol parameters by taking the following actions:

Decreased defer time p: The LTE can reduce its defer time to reduce the delay before initiating the backoff countdown process. Specifically, the LTE can select a defer time that belongs to a high priority class and transmit a frame of low priority class, with longer duration. Alternatively, the LTE can choose to ignore the defer time overall and initiate the backoff countdown immediately after the previous transmission is terminated, or a busy slot has ended.

CCA threshold manipulation: Another manipulation strategy for the LTE is to avoid freezing its backoff counter in the presence of an active Wi-Fi AP. This scenario can occur in benign settings when the active Wi-Fi is a hidden terminal to the LTE, or due to the power asymmetry between LTE and Wi-Fi. The two scenarios can be illustrated with the assistance of Fig. 2. Assume that Wi-Fi B acts as a monitor for the behavior of the LTE. The LTE is outside the interference range of C and therefore does not freeze its backoff counter when C is active. This may be perceived by B, who is within the interference range of C, as misbehavior. Moreover, B freezes its backoff counter when the LTE is active, but the converse does not hold due to the transmission power asymmetry.

Backoff process manipulation: The LTE system can manipulate the backoff process of LAA by selecting its backoff counter from a smaller window range $N \in [\![0, q_m - 1]\!]$, where $q_m < q$. The value of q_m can be selected from high-priority classes, so that the LTE appears to be protocol-compliant. Moreover, the LTE can avoid increasing its CW size after a collision to reduce latency between two consecutive channel access attempts. This can be done by simply ignoring any mandated CW size increase for a given priority class after a collision or by taking advantage of the low CW sizes allowed in high priority classes. We emphasize that there is an inherent difficulty in attributing collisions to a transmitting station because, (a) collisions are receiver-dependent and (b) in a heterogeneous setting, one system cannot decode the transmissions of another. As an example, the LTE station can consistently select backoff values in the range $[\![0, 3]\!]$, irrespective of the priority class. Moreover, in the event of successive collisions, it can maintain the CW to four, or increase it to eight, irrespective of the number of collisions. Essentially, all priority classes are treated as if they were of C_1 or C_2.

For the rest of this work, we consider a more general misbehavior model. In which, the LTE is protocol-compliant for α fraction of the time, while it uses a smaller CW of size q_m, for the remaining fraction of time. The value of α ranges according to some factor such as the LTE traffic demand, between zero to one. Thus, the uniformity assumption of the chosen backoff counter is not guaranteed within this misbehavior model. Let X denote the distribution of the backoff counter followed by the misbehaving LTE. The probability of selecting a backoff x is given by,

$$P_{\mathrm{X}}(x) = \begin{cases} \frac{1-\alpha}{q_m} + \frac{\alpha}{q}, \ \forall \ x < q_m, \\ \frac{\alpha}{q}, \ \forall \ q_m \leq x \leq q - 1. \end{cases} \tag{1}$$

This distribution depends on the chosen priority class, and the corresponding sizes of the CW.

The LTE system can combine multiple misbehavior strategies to improve its overall performance. We emphasize that although the backoff misbehavior strategies outlined in the misbehavior model are not new, a novel arsenal of detection methods is necessary due to the lack of a common control plane and a common PHY-layer.

Overview of the Detection Mechanism: The misbehavior detection process proposed in this work consists of a behavior monitoring phase and a behavior evaluation phase, as shown in Fig. 3. During the behavior monitoring phase, the monitoring Wi-Fi APs listen to the wireless medium when they do not transmit. Each monitoring AP, overhearing the transmission of an LTE frame, estimates behavior-related parameters such as the start and end times of the LTE frame, 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). *All the parameters are implicitly estimated without decoding the LTE frame.* Monitoring APs report their observations along with the start and end times of their own Wi-Fi activity to a central hub for further processing. The reported information provides to the hub universal knowledge on the distributed observations of the Wi-Fi system.

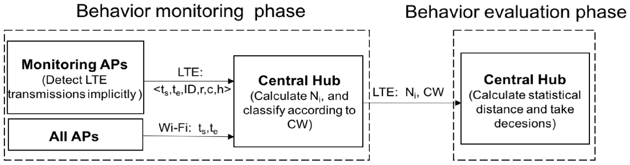

Behavior monitoring phase
Behavior evaluation phase
Monitoring APs
(Detect LTE transmissions implicitly)
LTE:
<ts,te,ID,r,c,h>
All APs
Wi-Fi: ts,te
Central Hub
(Calculate Ni, and classify according to CW)
LTE: Ni, CW
Central Hub
(Calculate statistical distance and take decesions)

Figure 3: Overview of the misbehavior detection mechanism.

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 LTE station. If this access pattern deviates from the LTE specifications for any LTE station, the station is deemed to be misbehaving. Deviation from the nominal behavior is measured through the Jensen-Shannon divergence (D_{JS}), defined for any two distributions **A** and **B** as

$$D_{JS}(\mathbf{A}||\mathbf{B}) = \frac{1}{2}D(\mathbf{A}||\mathbf{C}) + \frac{1}{2}D(\mathbf{B}||\mathbf{C}), \tag{2}$$

where $D(\cdot||\cdot)$ is the Kullback-Leibler divergence, and $\mathbf{C} = 1/2(\mathbf{A} + \mathbf{B})$. The LTE is deemed to misbehave if $D_{JS} > \delta$, where δ is a misbehavior threshold selected to satisfy desired detection and false alarm probabilities.

4 BEHAVIOR MONITORING PHASE

The key challenge in monitoring the LTE behavior is system heterogeneity. The monitoring APs cannot decode LTE transmissions as they may not be equipped with LTE receivers. In this section, we present several implicit techniques that enable 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 a non Wi-Fi signal, it performs signal processing without decoding to determine if it belongs to an LTE station. For the i^{th} LTE transmission, the AP estimates a six-tuple of information $< t_s(i), t_e(i), ID_j, r, C, h >$ where $t_s(i)$ and $t_e(i)$ denote the start and end of the i^{th} transmission, respectively, ID_j denotes an LTE ID, r denotes the retransmission round for an LTE frame, C denotes the LTE traffic class, and h is a flag that denotes if the monitoring AP is a hidden terminal to the transmitting LTE. All parameters are estimated implicitly without decoding. In the remainder of the section, we describe the parameter estimation process.

4.1 Detecting LTE Transmissions

Identifying LTE signals: The first step for estimating the LTE operating parameters is to determine when and for how long LTE stations access the wireless medium. To detect LTE transmissions, we adopt the cyclic prefix (CP)-based method proposed in [31]. Briefly, the CP detection operates as follows. LTE transmissions, like any other OFDM modulated signal, utilize the CP concept to mitigate inter-symbol interference (ISI) between two consecutive symbols. The CP is a replication of the end of an OFDM symbol, copied at the beginning of that symbol, as shown in Fig. 4.

Let L denote the length of the CP in samples and N denote the length of an OFDM symbol in samples. Parameters L and N are fixed to unique values in the LTE standard [18]. A Wi-Fi AP that cannot decode an LTE transmission can try to detect it by estimating parameters L and N via signal sampling and signal correlation.

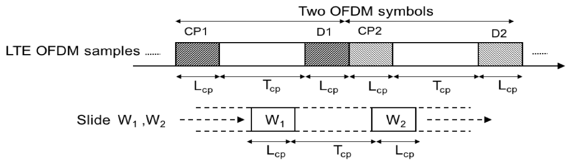


Figure 4: Detecting LTE transmissions using CP.

The AP first samples the received signal and stores the samples. The AP fixes two time windows W_1 and W_2 of length L, separated by $N - L$ samples. Then, it shifts the two windows simultaneously by one sample at the time while keeping the window separation fixed to $N - L$. For each shift n, the AP obtains the corresponding received signal samples $s_1(n)$ and $s_2(n)$ and computes the correlation $\rho(n)$ as

$$\rho(n) = \sum_{k=0}^{L-1} s_1(n-k)s_2^*(n-k-N), \tag{3}$$

where s_2^* is the complex conjugate of s_2. If $s_1 = s_2$, the correlation spikes relatively to the case of $s_1 \neq s_2$ indicating that s_1 is the CP of s_2 and that s_2 occurs $N - L$ samples away, thus confirming the LTE OFDM symbol structure. This also allows the AP to synchronize with the start of the LTE frame and determine the starting time $t_s(i)$ and end time $t_e(i)$.

Differentiating between LTE stations: Although the CP-based detection approach can identify LTE transmissions without decoding, it cannot attribute transmissions to individual LTE stations. This is necessary for building the behavioral profile of each LTE station. In an LTE system, an LTE transmission carries the station identity ID_j which is calculated as $ID_1 + 3ID_2$, where ID_1 and ID_2 define the physical-layer cell identity group and physical layer identity, respectively. The ID_1 and ID_2 fields are part of the primary synchronization signal (PSS) and secondary synchronization signal (SSS), respectively. The pair (ID_1, ID_2), which defines ID_{cell}, is unique for every LTE station, however they can only be obtained if the PSS and SSS are decoded. As shown in Fig. 5, the PSS and SSS fields appear at fixed locations in an LTE frame and also have a fixed duration in number of OFDM symbols or signal samples.

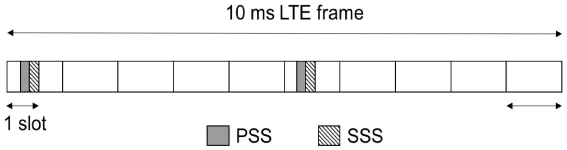


Figure 5: The PSS ans SSS fields in LTE frames.

Monitoring APs can exploit the known LTE frame structure to attribute LTE transmissions to different LTE stations. Note that we are not interested in extracting ID_j, but in attributing LTE transmissions to unique LTE stations to evaluate their individual behavior. This is achieved by exploiting the same signal correlation principle used to identify LTE transmissions. The main idea is to detect the unique header 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 LTE station will exhibit high correlation on the ID fields. Note that the IDs themselves are not decoded, because correlation of the sampled values suffices for classification purposes. A monitoring AP executes the following LTE transmission classification algorithm.

Step 1: The AP applies the CP-based LTE detection method to identify the i^{th} LTE transmission and synchronizes with the start time $t_s(i)$.

Step 2: The AP extracts the samples $s_{ID}^{(i)}$, of length L_{ID}, that correspond to ID_1 and ID_2 in the PSS and SSS fields, respectively (the two fields are contiguous).

Step 3: The AP maintains a signature database for all LTE stations. The signature of the j^{th} LTE is the sampled form s_{ID_j} of $ID_1||ID_2$. For the i^{th} LTE transmission, the AP computes the signal correlation as follows,

$$\rho_{ID}^{(i,j)} = \sum_{k=1}^{L_{ID}} s_{ID_j}^*(k)\, s_{ID}^{(i)}(k), \forall j. \tag{4}$$

Step 4: The AP attributes the i^{th} LTE transmission to LTE j that yields the maximum $\rho_{ID}^{(i,j)}$, given that $\rho_{ID}^{(i,j)} \geq \gamma_0$. Here γ_0 is a minimum correlation threshold that defines a signal match. If a match is found, the AP also replaces the current signature of LTE j with $s_{ID}^{(i)}$.

Step 5: If no correlation value exceeds γ_0, the AP adds $s_{ID}^{(i)}$ as a new LTE station signature to the database.

The correlation-based classification method presents challenges when LTE transmissions collide (with other LTE or with Wi-Fi). Although performing classification via signal cancellation in the presence of collisions is possible [34], 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.

4.2 Priority Class Estimation

The channel access behavior of an LTE station depends 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 CW.

To evaluate the compliance of an LTE station with the class parameters of the frame it transmits, the APs classify frames to one of the four classes of Table 1. This classification is performed based on the LTE frame length. As observed in Table 1, the maximum occupancy time T_{MCOT} is distinct for classes C_1, C_2, and C_3/C_4. By measuring the length of the i^{th} frame as $t_e(i) - t_s(i)$, the AP can classify the frame to the appropriate class. Note that we have implicitly assumed that in a backlogged scenario, it is in the interest of the LTE to always maximize its occupancy time once it seizes the channel. The T_{MCOP} value is the same in C_3 and C_4. Moreover, the first three CW sizes are equal for both classes. Only if a frame collides three or more times, a C_4 frame will be treated differently that a C_3 frame (there is also small difference in the defer time). 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.

4.3 CW 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. The CW is implicitly estimated by tracking the transmission round r. The latter is defined as the number of transmission attempts for successfully communicating a given frame. Initially, r is set to one and it is incremented by one with every retransmission attempt of the same frame. According to the exponential increase principle, the value of the CW doubles with every increase of r.

Parameter r is difficult to infer because a retransmission can be caused due to a collision. The monitoring AP utilizes the signal correlation method to infer r. Specifically, the AP utilizes the fact that most fields in the header and payload of a retransmitted frame remain identical to the original transmission. Therefore correlating the sampled signal between two successive transmissions allows the AP to infer that a retransmission has occurred and increase r accordingly. A monitoring AP tracks r through the following steps.

Step 1: For each LTE ID_j, the AP samples the $i - 1^{st}$ and i^{th} frames and buffers the related samples to the LTE frame header, denoted by $s_{H_j}(i-1)$ and $s_{H_j}(i)$ and of the payload, denoted by $s_{P_j}(i-1)$ and $s_{P_j}(i)$.

Step 2: The AP correlates $s_{H_j}(i-1)$ with $s_{H_j}(i)$ and $s_{P_j}(i-1)$ with $s_{P_j}(i)$ using the correlation function of (4). It computes the correlation value $\rho_H(i-1,i)$ for the header and $\rho_P(i-1,i)$ for the payload.

Step 3: If $\rho_H(i-1,i) \geq \gamma_0$ and $\rho_P(i-1,i) \geq \gamma_0$ the AP identifies the i^{th} frame as a retransmission and increases r by one. Otherwise, it sets r to zero.

From parameter r and the class priority c, the central hub can infer the CW value that should have been used by a given LTE station. For instance, the CW of a class 3 frame with $r = 2$ should be equal to 32 according to Table 1.

4.4 Hidden Terminal Discovery

The channel access behavior of an LTE station is affected by other coexisting Wi-Fi and LTE stations. coexistence is determined by the CCA threshold, which is used by the LTE to determine if the channel is idle and freeze its backoff process. In an LTE/Wi-Fi coexistence scenario, a monitoring AP faces two challenges in inferring the backoff behavior of an LTE station. First, the AP does not know if it is a hidden terminal to an LTE that it overhears due to the power asymmetry between LTE and Wi-Fi. For instance, AP K in Fig. 6 hearing a transmission from LTE A may or may not be a hidden terminal to A. Second, for LTE A and LTE B overheard at K, the AP does not know if A and B are hidden terminals. We propose two methods that enable the Wi-Fi system to deal with hidden terminals.

4.4.1 Inferring APs hidden terminals. To determine if an AP is a hidden terminal to an LTE, we exploit the channel reciprocity principle. In Fig. 6, the AP k hears the transmissions of both LTE stations, A and B. The AP needs to determine if its transmission exceeds the CCA threshold at A and B. The AP utilizes channel reciprocity as follows. For LTE A, the received power $P_{r,K}$ at AP K during the $i - 1^{st}$ LTE A transmission is given by

$$P_{r,K} = P_l |h_{k,a}^{(i-1)}|^2, \tag{5}$$

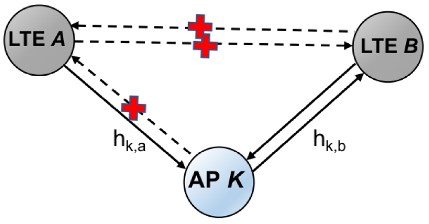


Figure 6: AP K is a hidden terminal to A but not B. LTE stations A and B are hidden terminals.

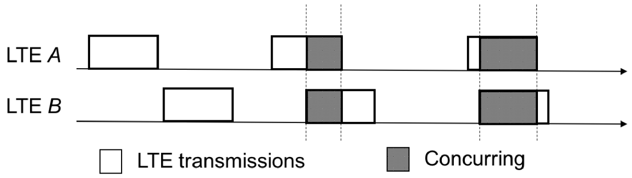


Figure 7: Transmission timeline for two LTE stations which are hidden terminals.

where $h_{k,a}^{(i-1)}$ is the impulse response of the channel between LTE A and station K and P_l is the transmit power of the LTE. Assuming that the channel does not change dramatically during the LTE backoff period (slow fading conditions), AP K can estimate the received power at LTE A side, $P_{r,A}$, when K is transmitting by

$$P_{r,A} = P_w |h_{k,a}^{(i-1)}|^2 = \frac{P_w P_{r,k}}{P_l}, \tag{6}$$

where P_w denotes the Wi-Fi transmit power. If $P_{r,A} > P_{th}$, where P_{th} is the CCA threshold employed by the LTE, then K is in the one-hop neighborhood $\mathcal{N}_{\text{LTE }A}^{(1)}$ of A. Otherwise, K is a hidden terminal to A. Repeating the same steps at all APs and sharing this information with the central hub allows the determination of all APs belong to $\mathcal{N}_{\text{LTE}}^{(1)}$, for all LTE stations. The hidden terminal inference can be fortified with repeated transmissions from the LTE. Assuming a fixed topology, the AP can compute the percentage of LTE frames for which the received power at the LTE as calculated by eq. (6) exceeds the CCA threshold. If the percentage exceeds certain threshold, the AP can declare with confidence that its activity is heard at the LTE and set the h flag reported to the central hub to FALSE.

4.4.2 Inferring LTE hidden terminals. For two or more LTE stations overheard at the same monitoring AP, the channel reciprocity principle cannot be applied, because the AP cannot estimate the channel between LTEs. This information is inferred at the central hub based on the start and end times reported for each LTE. To demonstrate this method, consider the topology of Fig. 6 where A and B are hidden terminals to each other. In this case, the frames transmitted by these two stations will concur in time, indicating that one is not aware of the other's transmissions. Here, we assume that LTE stations that belong to the same operator, will not deliberately try to interfere with each other's transmissions.

The central hub utilizes the start and end times t_s and t_e reported by the APs to determine if LTEs are hidden terminals. If concurrent frame transmissions are identified, the hub concludes that the involved LTEs are hidden terminals and therefore should not take into account each other's transmissions in their channel access pattern.

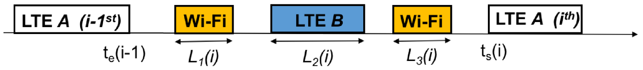


Figure 8: Estimation of the i^{th} backoff counter between two successive transmissions from LTE A.

By applying this approach for any two LTE stations, the hidden LTE terminals are specified for each LTE station.

5 BEHAVIOR EVALUATION PHASE

In the behavior evaluation phase, the central hub models and analyzes the behavior of each LTE station. The evaluation is performed in two steps. In the first step, the hub infers the channel access pattern of each LTE station through their backoff pattern. In the second step, the estimated backoff pattern is compared to the nominal pattern dictated by the LTE specification. We focus on the backoff pattern because it captures all misbehaviors described in the misbehavior model detailed in Section 3. We describe each step in detail.

5.1 Backoff Pattern Estimation

Using the LTE identities, the traffic class, and the start and end times, the central hub attributes all reported LTE frame transmissions to the respective LTE stations. Consider two successive transmissions $i-1$ and i, attributed to the same LTE ID_j. The hub can estimate the i^{th} backoff counter selected by the LTE by tracking the elapsed time between the end of the $i-1^{st}$ and the beginning of the i^{th} LTE transmission. The estimated backoff time $\hat{T}_{BO}$ is given by

$$\hat{T}_{BO}(i) = t_s(i) - t_e(i-1) - \hat{T}_f(i), \tag{7}$$

where $t_s(i)$ and $t_e(i-1)$ are the start and end times of the i^{th} and $(i-1)^{\text{th}}$ transmission, respectively, and $\hat{T}_f(i)$ is the estimated backoff freeze time. The elapsed time between two successive transmissions from LTE A is shown in Fig. 8. The central hub estimates the freeze time for the backoff counter by tracking the reported LTE and Wi-Fi activities. The freeze time $\hat{T}_f(i)$ can be written as

$$\hat{T}_f(i) = \sum_{k=1}^{|\mathcal{N}_{ID_j}|} L_k(i) + T_{\text{collision}}(i), \tag{8}$$

where $|\mathcal{N}_{ID_j}|$ is the cardinality of ID_j's one-hop neighborhood, $L_k(i)$ is the length of the frame transmitted by the k^{th} station (LTE or Wi-Fi), and $T_{\text{collision}}(i)$ is the time of the received collisions at LTE ID_j. The one-hop neighborhood of LTE ID_j is estimated using the hidden terminal discovery technique discussed in Section 4.4, by identifying all stations (Wi-Fi or LTE) whose transmissions exceed the CCA threshold at ID_j. The value of $L_k(i)$ is set to zero if station k is not reported to transmit during the i^{th} backoff period. Collisions are identified when two or more stations in $\mathcal{N}_{ID_j}$ concurrently transmit. The duration $T_{collision}$ is estimated by the hub as follows. The hub tracks the intersections among the reported t_s and t_e of all stations belong to $\mathcal{N}_{ID_j}$, in the i^{th} backoff period. For the APs, these times are reported individually from each of them. Whereas for the LTE stations, we consider that the LTE transmission is detected without collisions at least once at any monitoring APs, which reports t_s and t_e of that transmission to the hub. Here, we utilize the distributed nature of the monitoring APs for LTE's, see Section 4.1.

From the backoff period $\hat{T}_{BO}(i)$, the hub estimates the selected backoff counter $\hat{N}(i)$ for the i^{th} backoff round. Let v_i denote the number of all transmissions from stations in $\mathcal{N}_{ID_j}$, including collisions. A collision of any number of stations increases v_i by one. The backoff period for the LTE is given by

$$\hat{T}_{BO}(i) = (v_i + 1) \cdot T_{def} + (v_i + 1).p \cdot T_s + \hat{N}(i) \cdot T_s. \tag{9}$$

where T_s is the slot duration for the LTE system and p is the number of deferred slots according to the priority class (see Table 1). In (9), we add one to v_i to account for the T_{def} that the LTE has to follow after every LTE transmission. The backoff counter $\hat{N}(i)$ is given by

$$\hat{N}(i) = \frac{\hat{T}_{BO}(i) - (T_{def} + p \cdot t_s)(v_i + 1)}{t_s}. \tag{10}$$

In (10), $\hat{T}_{BO}(i)$ is obtained from eq. (7) and v_i is computed based on the Wi-Fi and LTE activities during the i^{th} backoff period. The correct estimation of $\hat{N}(i)$ requires knowledge of the priority class to determine p, as we mentioned in Section 4.2.

5.2 LTE Behavior Evaluation

In this section, we use the estimated backoff counters to detect LTE misbehavior. The evaluation of the LTE behavior is performed at the central hub after combining the backoff counters estimated from the parameters reported by different monitoring APs. Let J be the number of observations collected for a given LTE. To evaluate the LTE behavior, the hub organizes the J backoff counter estimates according to the class c and retransmission round r. This is required to compare each series of backoff counters with the uniform distribution $U(0, q(r, c) - 1)$, where $q(r, c)$ is the compliant CW size for class c and retransmission round r. We employ the techniques proposed in Section 4 for classifying the collected observations.

Once the sorting process is completed per c and r, misbehavior detection is performed by computing the statistical distance between the estimated distribution of the monitored backoff counters and $\text{U}(0, q(r, c) - 1)$. This statistical evaluation is done separately for each (c, r) pair. For simplicity, we consider that the J observations follow the same (c, r) pair, and neglect the c and r indices. We define by $\mathbf{M}$ the estimated distribution based on the J observations. $\mathbf{M}$ has a density function

$$P_{\mathbf{M}}(x) = \frac{\sum_{i=1}^{J} I(\hat{N}(i) = x)}{J}, \tag{11}$$

where $I(\cdot)$ is the indicator function. The statistical distance between $\mathbf{M}$ and $\mathbf{U}(0, q-1)$ is computed through the Jensen-Shannon divergence (D_{JS}). An LTE station is suspected of misbehavior if $D_{JS}(\mathbf{U}||\mathbf{M}) > \delta$, where δ is a threshold specified by the hub.

5.3 Determining the Threshold δ

In this section, we analyze the selection of the threshold δ as a function of J. The backoff counter distribution related to J is defined in (11). Let n_x be the number of times that $\hat{N}(i)$ is estimated to equal x. The probability $P_M(x)$ can be written as $P_M(x) = {}^{n_x}/_{J}$. We define by $\mathbf{B}$ the average of the probability distributions between $\mathbf{U}$ and $\mathbf{M}$, with $P_B(x)$ equal to,

$$P_B(x) = \frac{1}{2}\left(\frac{1}{q} + \frac{n_x}{J}\right) = \frac{n_x q + J}{2Jq}, \; \forall\, x. \tag{12}$$

Now, the distance $D_{JS}(\mathbf{U}||\mathbf{M})$ can be written as,

$$\begin{aligned} D_{JS}(\mathbf{U}||\mathbf{M}) &= \frac{1}{2}D(\mathbf{U}||\mathbf{B}) + \frac{1}{2}D(\mathbf{M}||\mathbf{B}) \\ &= \frac{1}{2q}\Big(\sum_{x=0}^{q-1}\log_2(\frac{2n}{n_x+n}) + \sum_{x=0}^{q-1}\frac{n_x}{n}\log_2(\frac{2n_x}{n_x+n})\Big). \end{aligned} \tag{13}$$

where $n = J/q$. It can be shown that $D_{JS}(\mathbf{U}||\mathbf{M})$ is a summation of q convex functions in n_x's that become zero at $n_x = n$. We select δ to achieve a zero false alarm rate. If $\mathbf{M} \sim \mathbf{U}[0, q-1]$, then $D_{JS}(\mathbf{U}||\mathbf{M})$ should be less than δ. At the same time, $D_{JS}(\mathbf{U}||\mathbf{M})$ should be greater than δ if $\mathbf{M} \sim \mathbf{X}$, the misbehavior's distribution defined in (1). Due to the convexity of $D_{JS}(\mathbf{U}||\mathbf{M})$, the maximum is achieved either at $n_{x\min} = \min_x\ n_x$ or $n_{x\max} = \max_x\ n_x$. The following inequality holds when substituting for all n_x's with $n_{x\min}$ or $n_{x\max}$,

$$D_{JS}(\mathbf{U}||\mathbf{M}) \leq \max\{D(n_{x\min}), D(n_{x\max})\}, \tag{14}$$

where

$$D(n_x) = \frac{1}{2}\Big(\log_2(\frac{2n}{n_x+n}) + \frac{n_x}{n}\log_2(\frac{2n_x}{n_x+n})\Big). \tag{15}$$

Therefore, for any chosen δ, we can define $n_{\min}$ and $n_{\max}$ to be the roots of the equation, $D(n_x) = \delta$. and by selecting such δ we are certain that no misbehavior is detected when, $n_{x\min} \geq n_{\min}$ and $n_{x\max} \leq n_{\max}$. To understand this selection, note that the $D_{JS}(\mathbf{U}||\mathbf{M})$ is a summation of $1/qD(n_x)$'s. If we guarantee that all of $D(n_x)$'s are less than δ, then we are sure that $D_{JS}(\mathbf{U}||\mathbf{M}) < \delta$. By choosing $n_{\min}$ and $n_{\max}$ to be around n, as is the case for uniform selection, such that $n_{\min} = n(1-c_1)$, and $n_{\max} = n(1+c_2)$, with c_1 and c_2 being two constants that depend on the number of observations, δ should be equal to the $\max\{D(n(1-c_1)), D(n(1+c_2))\}$.

False alarm probability: From eq.(13), the false alarm probability P_{fa} can be defined as,

$$P_{fa} \quad = \Pr\Big\{D_{JS}(\mathbf{U}||\mathbf{M}) > \delta\Big\}, \tag{16}$$

when the backoff counter is drawn uniformly from 0 to $q-1$. Due to the complexity of arriving to a closed-form formula for P_{fa}, we derive a bound in the following proposition,

PROPOSITION 1. *The false alarm probability can be bounded by,*

$$P_{fa} \leq 1 - \Big(\sum_{k=n_{\min}}^{n_{\max}}\binom{J}{k}(\frac{1}{q})^k(\frac{q-1}{q})^{J-k}\Big)^q. \tag{17}$$

PROOF. The proof is provided in Appendix A. □

Detection probability: Unlike the false alarm analysis, the detection probability is misbehavior-dependent. Here, the analysis should consider different misbehavior strategies represented by the fraction of time $1-\alpha$ that an LTE misbehaves and the extend of misbehavior represented by the selection of the contention window q_m. We derive a bound for P_d in the following proposition,

PROPOSITION 2. *The detection probability is bounded by,*

$$\begin{aligned} P_d \qquad &> (1 - \textstyle\sum_{k=n_{\min}}^{n_{\max}}\binom{J}{k}\beta^k(1-\beta)^{J-k})^{q_m} \\ &.(1 - \textstyle\sum_{k=n_{\min}}^{n_{\max}}\binom{J}{k}(\frac{\alpha}{q})^k(\frac{q-\alpha}{q})^{J-k})^{q-q_m}, \end{aligned} \tag{18}$$

where $\beta = \frac{1-\alpha}{q_m} + \frac{\alpha}{q}$.

PROOF. The proof is provided in Appendix B. □

Propositions 1 and 2 dictate the expected tradeoff between P_d and P_{fa} as a function of the detection threshold δ. For a given number of observations J, δ can be selected to satisfy this tradeoff. We evaluate this selection through the ROC curves in the following section.

Note: The Jensen-Shannon Divergence is designed for measuring the distance between two distributions of the same range. However, when $\alpha = 0$ (i.e., the LTE always misbehaves), the series of backoff counter estimates will yield zero probabilities for all x's greater than $q_m - 1$. The proposed detection scheme is still applicable here by replacing the zero probabilities with negligible (non-zero) values.

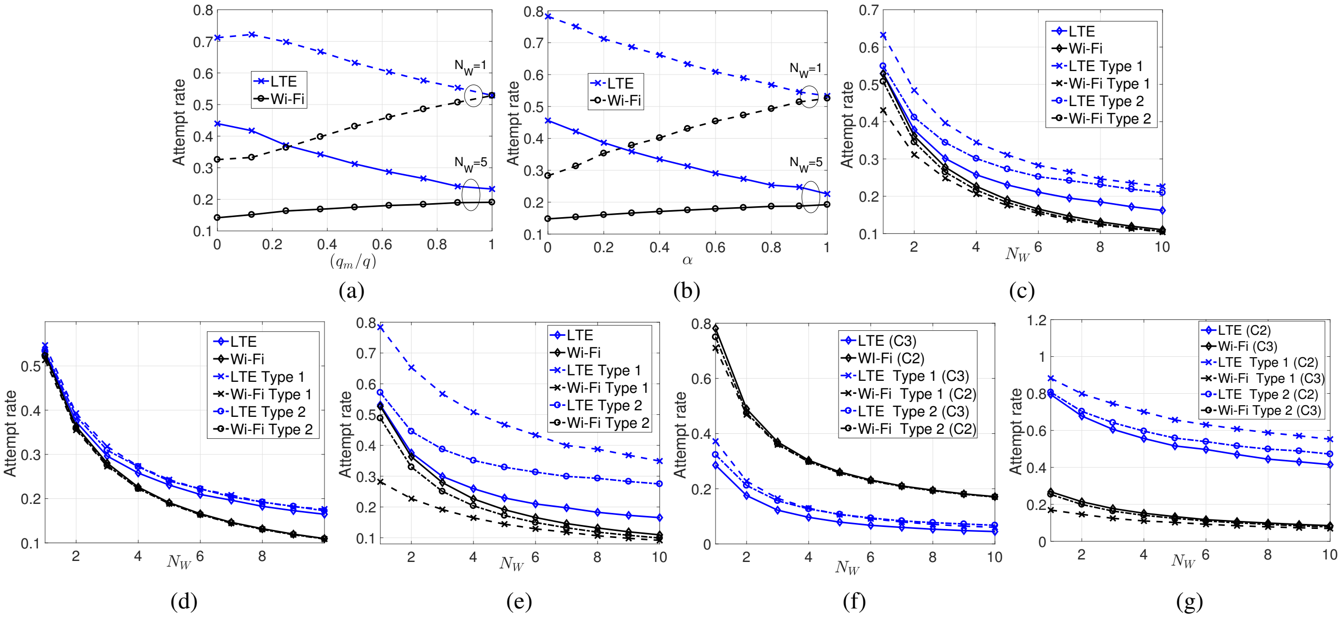
6 PERFORMANCE EVALUATION

To validate the proposed misbehavior detection framework, we implemented an event-based simulation for the LTE/Wi-Fi coexistence. Specifically, we deployed a set of terminals (LTE and Wi-Fi) in the same collision domain so that activity from every terminal affects the behavior of others. The LTE stations followed the LAA-LTE specification whereas the Wi-Fi APs implemented the IEEE 802.11e protocol. To isolate the impact of misbehavior, frame losses occurred only due to collisions (perfect channel conditions). Each experiment was run for 100,000 events, where each event corresponds to a transmission attempt by any terminal. All terminals were backlogged. For each terminal, we evaluated the transmission attempt rate defined as the number of transmission attempts, including collisions, of a terminal over the total number of attempts by any terminal. This metric indicates how frequently each terminal attempts to seize the common medium. We further evaluated the detection and false alarm probabilities under different misbehavior scenarios.

6.1 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. Misbehavior for the LTE was implemented by adopting smaller values of the default CW $q_m < q$ for various α. The LTE chose its backoff uniformly in $[0, q_m - 1]$. In Figure 9(a), we show the transmission attempt rate as a function of q_m/q, where q is the CW dictated by the LTE protocol. The value of α was set to 0.5 and we considered the coexistence of one LTE with $N_w = 1$ and $N_w = 5$ Wi-Fi APs. We observe that the Wi-Fi channel access opportunities 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 Wi-Fi). We observe that the degradation in the attempt rate of each Wi-Fi station can go up to 50%. Figure 9(b) gives similar intuition, when the fraction of time that the LTE misbehaves is varied. For this set of experiments, we fixed $q_m = 0.5q$.

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 decreased the CW to $q_m = 0.5q$, whereas in type 2 it used the nominal value of q but disregarded the CW exponential growth after collisions. In Figure 9(c), we show the attempt rate as a function of N_W, with and without LTE misbehavior, for $\alpha = 0.5$. 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



(a) (b) (c)

(d) (e) (f) (g)

Figure 9: 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 $q_m = 0.5q$, vs. number of Wi-Fi terminals for: (c) class 3-LTE and class 3-Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.5$, (d) class 3-LTE and class 3-Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.9$ (e) class 3-LTE and class 3-Wi-Fi with $q_m = 0.5q$, and $\alpha = 0$, (f) class 3-LTE and class 2-Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.5$, and (g) class 2-LTE and class 3-Wi-Fi with $q_m = 0.5q$, and $\alpha = 0.5$.

N_W. Overall, type 1 misbehavior has higher impact than type 2, as it affects all retransmission rounds. We also investigated scenarios where the LTE misbehaves all the time or a very small portion of time. Figure 9(d) shows the case of $\alpha = 0.9$. We observe that the LTE misbehavior does not have any significant effect on the Wi-Fi performance. The case of $\alpha = 0$ is shown in Fig. 9(e). The Wi-Fi performance degrades up to 40% for type 1 manipulation and about 8% for type 2. Note that at high N_W, the performance of the LTE station is always better than that of Wi-Fi stations.

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 second set of experiments, we varied the priority class and measured the achieved attempt rate. In Figure 9(f), the Wi-Fi 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 stations. As expected, the LTE gains are significant when the LTE uses a lower class than Wi-Fi and also misbehaves. These results are shown in Fig. 9(g) where we see a larger difference in performance relatively to Fig. 9(c), where the LTE and the Wi-Fi APs have the same class.

6.2 Selection of Detection Threshold δ

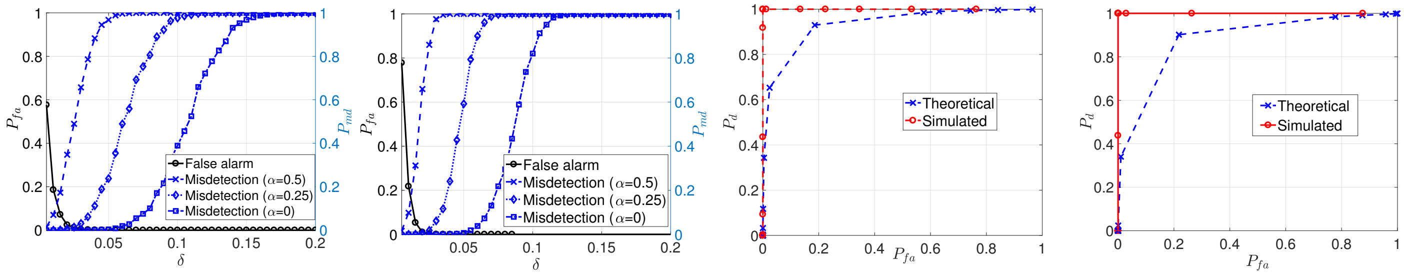
In the section, we show how to select the detection threshold δ for detecting LTE misbehavior based on the theoretical bounds derived in Propositions 1 and 2. For the misbehaving LTE, we use $q_m = 0.5q$ and vary α to $0, 0.25$ and 0.5. Figure 10(a) shows the false alarm and misdetection probability (P_{md}) for $q = 4$, as a function of δ. As expected, P_{md} increases with α and also with δ. In addition, we note an obvious tradeoff between P_{fa} and P_{md}. To select an appropriate value for δ, we equate P_{fa} with P_{md} for each value of α. We observe that for $\alpha = 0$ and $\alpha = 0.25$ the two curves intersect at $\delta \approx 0.02$ achieving an almost zero false alarm and misdetection probabilities. For $\alpha = 0.5$, the intersection of the two curves occurs at $\delta \approx 0.01$ with the false alarm and misdetection probabilities being around 0.15. Figure 10(b), presents the same tradeoff when the minimum contention window equals to $q = 16$. Although P_{md} increases at low values of δ, we observe similar performance with the case of $q = 4$, when we look at the value of δ that equates P_{md} to P_{fa}. Note that an alternative way to select δ is to fix the false alarm probability and select the δ that minimizes the misdetection probability

6.3 Receiver Operating Characteristic Curves

6.3.1 *Manipulation of the CW q.*

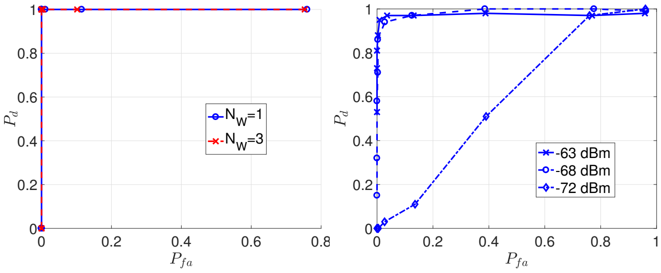
To further investigate the tradeoff between P_{fa} and P_d, we studied the receiver operating characteristic (ROC) curves using the theoretical bounds and simulations. In our simulations, we selected δ to satisfy certain false alarm probability according to the theoretical bound in Proposition 1. To measure the probability of detection, we implemented a type 1 misbehavior strategy with $q_m = 0.5q$ and $\alpha = 0.5$. To measure the probability of false alarm, we set $\alpha = 1$, i.e., no misbehavior.

Figure 10(c) shows the ROC curve using the theoretical bounds and simulation for $q = 4$ and $\alpha = 0.5$. We observe that the theoretical bounds are somewhat loose and that the true system performance is significantly better when the observation window (number of transmissions analyzed) is large. Indeed, the ROC is close to the optimal curve indicating that our system can operate with almost sure detection and almost zero false alarm probability. In Fig. 10(d), we increased the value of q to 16 and repeated our simulations. Although the theoretical curve performs worse as the theoretical bounds become looser, the simulation results still demonstrate an almost perfect detection with an almost zero false alarm probability.



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

Figure 10: False alarm (P_{fa}) and Misdetection probability (P_{md}) vs. Threshold δ: (a) $q = 4$, (b) $q = 16$, ROC curves: (c) $q = 4$, $q_m = 2$, and $\alpha = 0.5$ and (d) $q = 16$, $q_m = 8$, and $\alpha = 0.5$.



(a) (b)

Figure 11: ROC curves: (a) $q = 16$, defer ($p = 1$) and (b) $q = 16$, and $N_W = 200$.

6.3.2 Manipulation of the defer time p. In this section, we evaluate the performance of the proposed detection scheme when the LTE manipulates the defer time p before the backoff process is started. To simulate this misbehavior, we implemented an LTE that uses the defer time from traffic class C_1 (i.e., $p = 1$) while transmitting frames that belong to class C_3 ($p = 3$). Our simulations show an almost perfect ROC curve that yields perfect detection 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 an always detectable manner. For class C_3, the number of slots that the LTE shall wait before attempting any transmission should be at least three. When $p = 1$, there are situations where the LTE transmits a frame after fewer than three slots from the completion of the previous transmissions. This is a detectable phenomenon for any selection of δ that fixes the false alarm probability to a given value.

6.3.3 CCA threshold manipulation. In the last set of experiments, we evaluated the manipulation of the CCA threshold. A selection of a lower CCA threshold, increases the number of Wi-Fi APs that are ignored by the LTE, because they are considered hidden terminals. To simulate the CCA threshold manipulation scenario, we uniformly deployed multiple APs and one LTE in a square are 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. We set the carrier frequency to 5GHz

We evaluated the performance of our detector when the CCA threshold is set to -63, -68, and -72dBm (the LAA-LTE standard sets the CCA threshold to -73 dBm) and for a deployment of $N_W = 200$ APs. In Fig. 11(b), we show the ROC for the three CCA thresholds. We observe that when the CCA is lowered by more than 5dBm, the ROC is near the optimal one. However, when the CCA is lowered little, our detector is unable to detect this misbehavior at low false alarm rate. However, such misbehavior creates an imperceivable advantage for the LTE in terms of channel access opportunity. Nonetheless, even in this extreme case the detection probability is higher than the false alarm rate.

7 CONCLUSION

We studied the problem of LTE misbehavior under the LAA-LTE protocol for coexistent LTE and Wi-FI systems. We enumerated possible misbehavior scenarios for the LTE including the manipulation of the defer time, the selection of the CW, the nullification of the exponential increase backoff mechanism, and the manipulation of the CCA threshold. We developed a suite of implicit monitoring techniques that enable the Wi-Fi system to estimate the operational parameters of the LTE, without decoding the LTE signal. This is a desired property as Wi-Fi APs are not necessarily equipped with LTE receivers. Our methods relied on computing signal correlations in the signal domain to identify and classify LTE transmissions.

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 LTE stations. We employed the Jensen-Shannon distance as a measure for comparing the estimated LTE behavior to the nominal behavior dictated by the LAA-LTE standard. We theoretically analyzed the false alarm and detection probabilities and derived relevant bounds as a function of the system parameters and the misbehavior pattern of the LTE. Finally, we evaluated the performance of our detector via simulations. We showed that the LTE misbehavior can cause a significant performance degradation for the Wi-Fi stations. However, such misbehavior was detectable by our method with very high probability while achieving a low false alarm probability.

ACKNOWLEDGMENTS

This work was supported in part by NSF (grants # IIP-1265960, CNS-1409172, CNS-1563655, CNS- 1731164, CNS-1619728, and CNS-1564477) and by the Broadband Wireless Access & Applications Center (BWAC). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

REFERENCES

[1] 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.

[2] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine, and S. Pandey, "Ieee 802.11af: a standard for tv white space spectrum sharing," *IEEE Communications Magazine*, vol. 51, no. 10, pp. 92–100, 2013.

[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] 3GPP, "Tr 36.889: Feasibility study on licensed-assisted access to unlicensed spectrum," https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2579, 2015.

[5] 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.

[6] H. He, H. Shan, A. Huang, L. X. Cai, and T. Quek, "Proportional fairness-based resource allocation for LTE-U, coexisting with Wi-Fi," *IEEE Access*, 2016.

[7] 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," *arXiv preprint arXiv:1510.01392*, 2015.

[8] Z. Guan and T. Melodia, "Cu-lte: Spectrally-efficient and fair coexistence between LTE and Wi-Fi in unlicensed bands," *Networks*, vol. 4, p. 9, 2016.

[9] S. Sagari, S. Baysting, D. Saha, I. Seskar, W. Trappe, and D. Raychaudhuri, "Coordinated dynamic spectrum management of LTE-U and Wi-Fi networks," in *Proceedings of the Dynamic Spectrum Access Networks Symposium*. IEEE, 2015, pp. 209–220.

[10] A. Mukherjee, J.-F. Cheng, S. Falahati, L. Falconetti, A. Furuskär, B. Godana, H. Koorapaty, D. Larsson, Y. Yang *et al.*, "System architecture and coexistence evaluation of licensed-assisted access LTE with IEEE 802.11," in *Proceedings of the IEEE International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 2350–2355.

[11] J. Xiao and J. Zheng, "An adaptive channel access mechanism for LTE-U and WiFi coexistence in an unlicensed spectrum," in *Proceedings of the ICC Conference*. IEEE, 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] F. Cai, Y. Gao, L. Cheng, L. Sang, and D. Yang, "Spectrum sharing for LTE and WiFi coexistence using decision tree and game theory," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2016, pp. 1–6.

[14] 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.

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

[16] 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*. IEEE, 2012, pp. 246–250.

[17] Qualcomm, "Lte in unlicensed spectrum: Harmonious coexistence with wi-fi," 2014.

[18] 3GPP TS 36.213 version 14.2.0 Release 14, "Lte; evolved universal terrestrial radio access (e-utra); physical layer procedures," 2013.

[19] S. Choi and S. Park, "Co-existence analysis of duty cycle method with wi-fi in unlicensed bands," in *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*. IEEE, 2015, pp. 894–897.

[20] C. Cano and D. J. Leith, "Coexistence of wifi and lte in unlicensed bands: A proportional fair allocation scheme," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2288–2293.

[21] J. Jeon, H. Niu, Q. Li, A. Papathanassiou, and G. Wu, "Lte with listen-before-talk in unlicensed spectrum," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2320–2324.

[22] T. Tao, F. Han, and Y. Liu, "Enhanced lbt algorithm for lte-laa in unlicensed band," in *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on*. IEEE, 2015, pp. 1907–1911.

[23] 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.

[24] X. Ying, R. Poovendran, and S. Roy, "Detecting lte-u duty cycling misbehavior for fair sharing with wi-fi in shared bands," *arXiv preprint arXiv:1710.01705*, 2017.

[25] 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.

[26] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2013.

[27] 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.

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

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

[30] J. Lin, "Divergence measures based on the shannon entropy," *IEEE Transactions on Information theory*, vol. 37, no. 1, pp. 145–151, 1991.

[31] M. Hirzallah, W. Afifi, and M. Krunz, "Full-duplex spectrum sensing and fairness mechanisms for wi-fi/lte-u coexistence," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–6.

[32] 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.

[33] Y. Zhang and L. Lazos, "Countering selfish misbehavior in multi-channel mac protocols," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2787–2795.

[34] S. Gollakota and D. Katabi, *Zigzag decoding: combating hidden terminals in wireless networks*. ACM, 2008, vol. 38, no. 4.

APPENDIX A PROOF OF PROPOSITION 1

The false alarm probability can be calculated by counting the number of all possible combinations of n_x that satisfy the inequality,

$$D_{JS}(\mathbf{U}||\mathbf{M}) > \delta. \tag{19}$$

Due to the uniformity of its distribution, we can divide it by the total number of combinations to calculate P_{fa}. This way is inefficient and unpractical, especially for a large number of observations. Instead of that, we show how to derivative a bound that we guarantee that P_{fa} is always below. P_{fa} can be written as,

$$\begin{aligned} P_{fa} &= \Pr\Big\{D_{JS}(\mathbf{U}||\mathbf{M}) > \delta\Big\} \\ &= Pr\Big\{\sum_{x=0}^{q-1} D(n_x) > q\delta\Big\}. \end{aligned} \tag{20}$$

Let $D_{max} = \max\{D(n_{x_{\min}}), D(n_{x_{\max}})\}$, then D_{max} has to be greater than δ to possibly cause a false alarm, thus we can consider the following inequality,

$$\begin{aligned} P_{fa} &\leq Pr\Big\{D_{\max} > \delta\Big\} \\ &= Pr\Big\{D(n_{x_{\min}}) > \delta\Big\} + Pr\Big\{D(n_{x_{\max}}) > \delta\Big\}. \end{aligned} \tag{21}$$

As we define $n_{\min}$ and $n_{\max}$ as the roots of the equation, $D(n) = \delta$, we get

$$P_{fa} \leq Pr\{n_{x_{\min}} < n_{\min}\} + Pr\{n_{x_{\max}} > n_{\max}\}. \tag{22}$$

As we cannot expect which one is the maximum, it can be bounded again to the following

$$\begin{aligned} P_{fa} &\leq 1 - Pr\{n_{\min} \leq n_0, \ldots, n_x, \ldots, n_{q-1} \leq n_{\max}\}, \\ &\leq 1 - \Big(\sum_{k=n_{\min}}^{n_{\max}} \binom{J}{k} (\frac{1}{q})^k (\frac{q-1}{q})^{J-k}\Big)^q \end{aligned} \tag{23}$$

APPENDIX B PROOF OF PROPOSITION 2

The detection probability P_d can be written as

$$P_d = \Pr\Big\{D_{JS}(\mathbf{U}||\mathbf{M}) > \delta\Big\} \tag{24}$$

$$= Pr\Big\{\sum_{x=0}^{q-1} D(n_x) > q\delta\Big\} \tag{25}$$

when LTE misbehaves in selecting the backoff counter. Similar to the ideas used in bounding the false alarm, P_d can be written as

$$P_d \quad > Pr\{n_0, \ldots, n_{q-1} < n_{\min}, n_0, \ldots, n_{q-1} > n_{\max}\}. \tag{26}$$

To clarify that, we claim that if all n_x's either less than $n_{\min}$, or greater than $n_{\max}$, then all $D(n_x)$ have to be greater than δ, which satisfies the inside inequality in (25), and guarantees a decodable misbehavior. However, there are other possible situations in which the misbehavior can also be detected, thus we get the inequality in (26). This inequality can be further bounded as follows,

$$
\begin{aligned}
P_d \quad & > \textstyle\prod_{x=0}^{q-1} Pr\{n_x < n_{\min}, n_x > n_{\max}\} && (27)\\
& = \textstyle\prod_{x=0}^{q-1} (1 - Pr\{n_{\min} < n_x < n_{\max}\}) && (28)\\
& = \textstyle\prod_{x=0}^{q_m - 1} (1 - \sum_{k=n_{\min}}^{n_{\max}} \binom{J}{k} \beta^k (1-\beta)^{J-k}) && (29)\\
& \cdot \textstyle\prod_{x=q_m}^{q-1} (1 - \sum_{k=n_{\min}}^{n_{\max}} \binom{J}{k} (\frac{\alpha}{q})^k (\frac{q-\alpha}{q})^{J-k}) &&\\
& = (1 - \textstyle\sum_{k=n_{\min}}^{n_{\max}} \binom{J}{k} \beta^k (1-\beta)^{J-k})^{q_m} && (30)\\
& .(1 - \textstyle\sum_{k=n_{\min}}^{n_{\max}} \binom{J}{k} (\frac{\alpha}{q})^k (\frac{q-\alpha}{q})^{J-k})^{q-q_m}, &&
\end{aligned}
$$

where $\beta = \frac{1-\alpha}{q_m} + \frac{\alpha}{q}$. The probabilities, in (29), are those used in drawing the manipulated backoff counter, which are function of α and q_m.