Detecting Misreporting Attacks to the Proportional Fair Scheduler

Jorge F. Schmidt
Institute of Networked and Embedded Systems,
University of Klagenfurt, Austria.
Jorge.Schmidt@aau.at

Roberto López-Valcarce
Department of Signal Theory and Communications,
University of Vigo, Spain.
valcarce@gts.uvigo.es

***Abstract*—The Proportional Fair Scheduler (PFS) has become a popular channel-aware resource allocation method in wireless networks, as it effectively exploits multiuser diversity while providing fairness to users. PFS decisions on which mobile station (MS) to schedule next are based on Channel Quality Indicator (CQI) values. Since CQI values are reported by the MSs to the scheduler, network performance can be severely degraded if some malicious MSs report forged information. Previous approaches to this security issue are based either on modifying PFS, which may be undesirable in some contexts, or authenticating CQI reports by periodic transmission of challenges, which increases overhead. Instead, we propose to *detect* misreporting attackers, based on the time correlation features of the wireless channel. Our approach does not require scheduler modification, and it does not increase overhead. Simulation results under realistic settings are provided to show the effectiveness of the proposed test.**

I. Introduction

The persistent demand for permanent connectivity has determined the tremendous expansion of fourth-generation mobile wireless communication systems, such as LTE [1] and WiMax [2], and is pushing towards next-generation systems with improved capabilities [3]. To be able to deliver high data rates to a large number of users, these technologies rely on channel-aware resource allocation protocols exploiting channel state information in order to use wireless resources more efficiently. *Opportunistic schedulers* for multiuser systems constitute an example: these resource allocation schemes take advantage of physical layer (PHY) information [4], in order to exploit *multiuser diversity* (the fact that, in a system with a large number of users undergoing independent fading, it is likely that at any given time at least one user has a good channel). Among opportunistic scheduling algorithms, the Proportional Fair Scheduler (PFS) is widely recognized as an attractive choice [5], [6], providing acceptable tradeoffs between possible rates and *fairness* (this is necessary, since a scheduler which simply serves the user with the best channel at each time slot will result in poor performance for users with worse channel conditions). Analyses have shown that PFS enjoys certain optimality conditions in terms of a utility function of the long-term average rates of the users [7], [8].

Opportunistic scheduler operation is based on Channel Quality Indicator (CQI) values reported by the Mobile Stations (MS) to the scheduling entity or Base Station (BS). One serious vulnerability issue then arises, since CQI values are susceptible to forgery by a selfish or malicious MS, with the purpose of either obtaining an unfair share of network resources or disrupting network operation. This issue is referred to as *CQI misreporting attack,* and has been considered in a few recent works [9]–[12]. In [10] the fairness vulnerabilities of PFS were highlighted, and realistic misreporting attacks were described and shown to be capable of severely depleting network resources. Several means to robustify the system were then proposed in order to mitigate such attacks. Although effective, these defensive devices require modifying the original PFS and/or cell handoff mechanisms, which may not be desirable in practice and could compromise PFS optimality. The same is true about the defense measures from [11], which incorporates within the PFS operation rule an estimated trust value for each user. A different approach was proposed in [12], resorting to PHY security concepts [13]: reported CQI values are authenticated by the base station (BS) through the transmission of *challenges* from the BS to each MS. This PHY security approach avoids PFS modification, since only authenticated (thus allegedly reliable) CQI values are taken into account. The use of PHY authentication has also been used in, e.g., [14]–[18] for detecting impersonation attacks, showing that exploiting the location-dependent nature of the wireless channel is an appealing approach to address security-related issues. Nevertheless, the challenge-based PHY authentication schemes proposed in [12] result in an increased system overhead, which is highly undesirable in a wireless network.

In the present paper we develop a simple yet effective protection mechanism for PFS against CQI misreporting attacks, based on the use of the distinctive time correlation of the wireless channel. In contrast with PHY security approaches such as those in [14]–[18] which exploit the location-dependent feature of the wireless channel to protect against impersonation attacks, we propose the exploitation of the *time-dependent* characteristics of the wireless channel to protect against CQI misreporting attacks. Differently from previous PHY-based defense schemes based on CQI authentication [12], our proposed method, which is based on anomalous behavior detection, does not result in increased system overhead. In addition, it does not require modifications to the PFS either, in contrast with [10], [11], since protection is provided at the PHY layer. Specifically, we show how time variations in the histories of reported CQI values can be used in order to discriminate between malicious and honest users. The underlying idea is that CQI time series originated at an honest MS is related to the time variations in the wireless channel, and therefore to

the relative speed between BS and MS, which is bounded. This is not the case for a malicious MS, whose CQI reports typically exhibit much faster time variations. We propose to monitor the sample autocorrelation coefficient corresponding to a certain time lag in order to single out malicious MSs. Simulation results with realistic system parameters show the efectiveness of the proposed approach.

The paper is organized as follows. The communication setting, PFS basics and CQI misreporting attack are described in Sec. II. In Sec. III the time-varying characteristic of the wireless channel is described, and the proposed protection scheme is derived. Simulation results are given in Sec. IV, and conclusions are drawn in Sec. V.

II. Problem Statement

A. Communication setting

We consider a cellular system [1], [2], focusing on a scenario with N MSs within a cell moving at speeds of up to v_{m} m/s and communicating with a BS. Of these, $N_A \ll N$ are malicious, with the goal of disrupting network operation. We assume that MSs within overlapping coverages of two neighboring cells can switch between them at will, by triggering a handoff process as described in [10].

Network resources are shared over an OFDM downlink channel, where subcarriers are grouped in *resource blocks* consisting of several contiguous subcarriers over which the channel frequency response can be regarded as flat [6], [19]. The temporal dimension is sliced in *time slots* of duration T_s, i.e., a number of contiguous OFDM symbols for which the channel can be regarded as quasi-static [6], [19]. Each resource block is allocated to a single MS at each time slot. All MSs obtain their CQI values and report them to the BS in order to compete for the next time slot. Independent allocation of resource blocks is assumed, so we focus on a single resource block for clarity.

The CQI metric reported by an (honest) MS is a mapping from the signal-to-noise ratio (SNR) experienced by that MS over the corresponding resource block to a value indicating the maximum rate that the channel can support under current conditions. Based on CQI values from all N users, the BS decides on which MS to schedule over the next time slot using the PFS algorithm, described next.

B. Proportional Fair Scheduler

At each time slot, PFS selects for transmission the MS maximizing the ratio of current CQI to average throughput. In this way, low SNR users still have fair opportunities to access the channel, whereas performance is improved with respect to naive schemes (e.g., round-robin) [6]. At time slot t, PFS selects user k^* to be allocated on the next time slot as

$$k^* = \arg \max_{1 \le k \le N} \frac{\mathrm{CQI}_k(t)}{R_k(t)}, \tag{1}$$

where $\mathrm{CQI}_k(t)$ is the latest CQI value reported by the k-th user (peak feasible data rate, in case of an honest MS), and $R_k(t)$ is the monitored average throughput of the k-th user up to time slot t, which is updated as

$$R_k(t+1) = \begin{cases} \alpha \mathrm{CQI}_k(t) + (1-\alpha) R_k(t), & \text{if } k = k^*, \\ (1-\alpha) R_k(t), & \text{otherwise,} \end{cases} \tag{2}$$

where $0 < \alpha < 1$ is a fairness parameter that determines the size of the smoothing window in (2). At time $t = 0$, the average throughput is initialized as $R_k(0) = r_0$ for all k, with r_0 a small constant. If user k joins the cell at time $t = t_0$ (for example, due to a handoff from a neighboring cell), its average throughput can be initialized in different ways. We assume the BS allows the new user to set this parameter. While this is beneficial when all users behave in an honest manner, it results in added flexibility to attackers, resulting in a worst case scenario in terms of security from the network point of view [10].

C. CQI misreporting attack

From (1), PFS allocation decisions are based on CQI reports, and thus its operation is vulnerable to malicious users forging CQI values [9]–[12]. In the following, we consider the most powerful of such CQI misreporting attacks, described in [10] and termed *coordinated attack with hand-offs*, which is carried out by a set of N_A colluding attackers as follows. At time t, attacker j computes the minimum value of its reported rate that would secure the resource block at time $t+1$, i.e.,

$$m_j(t) = \left\lceil R_j(t) \cdot \max_{i \in \mathcal{H}} \frac{\mathrm{CQI}_i(t)}{R_i(t)} \right\rceil, \quad j \in \mathcal{A}, \tag{3}$$

with $\mathcal{H}$ and $\mathcal{A}$ the sets of honest users and attackers, respectively, and where the ceiling operation is included since CQI metrics are usually integer-valued[1]. The corresponding increment in reported rate is then obtained:

$$\delta_j(t) = m_j(t) - \mathrm{CQI}_j(t-1), \tag{4}$$

with $\mathrm{CQI}_j(t-1)$ the previously reported (at time slot $t-1$) CQI value. Let

$$j^* = \arg \min_{j \in \mathcal{A}} \delta_j(t). \tag{5}$$

Then, attacker j^* reports $\mathrm{CQI}_{j^*}(t) = m_{j^*}(t)$ to the BS, whereas the remaining $N_A - 1$ attackers report their true CQI values in order to conceal their malicious behavior.

Note that in order for attackers to keep obtaining time slots, they not only need to have better CQI values than honest users, but also their CQI-to-average throughput ratio must be better. If an attacker succeeds, then its average throughput increases while those of honest users decrease, so attackers need to compensate for this by reporting *rapidly increasing* CQI values. In practice, a maximum value $\mathrm{CQI}_{\max}$ exists. As remarked in [10], when an attacker reaches this value, it can trigger a handoff to a neighboring cell and back. This allows the attacker to reset its average throughput, as explained in Sec. II-B, thus allowing a sustainable attack. This scheme has

[1] A method by which attackers can estimate the value $\max_{i \in \mathcal{H}} \frac{\mathrm{CQI}_i(t)}{R_i(t)}$ is given in [10]. For simplicity, we assume this quantity is known to attackers. This case also serves as an upper bound on the power of more realistic attacks.

been shown to capture over 90% of the available time slots with just a few attackers [10].

III. Detection of Misreporting Attacks

In contrast with previous approaches based on CQI authentication [12] (which increases overhead) or scheduler modification [10], [11] (which may affect its optimality features), we propose a detection mechanism to test whether CQI values reported by an MS arise from honest behavior or not. In this way, if user k is flagged as an attacker at time t, it is excluded from the competition for the next time slot.

The key observation is that, as the time-varying characteristics of mobile wireless channels are well understood under a number of models, they allow to single out malicious users whose temporal behavior differs from which one would expect as arising from an actual physical channel. To this end, note that (honest) CQI values are directly related to the observed SNR as follows:

$$\mathrm{CQI}_k(t) = q\left[f\left(\frac{\hat{\gamma}_k^2(t)}{\hat{\sigma}_k^2}\right)\right], \tag{6}$$

where $\hat{\gamma}_k(t)$ and $\hat{\sigma}_k^2$ are the estimated values of, respectively, the channel envelope (for the considered resource block) and the noise power at the k-th MS; $f(\cdot)$ is an invertible mapping to the logarithmic (dB) domain, and $q[\cdot]$ represents a quantizer such that the CQI value falls within a discrete set of available modulation/coding alternatives (note that f and q are application specific). In practice, all such alternatives yield the same error rate while resulting in higher data rates for larger SNR values [1], [2]. Eq. (6) shows that the time variations of $\mathrm{CQI}_k(t)$ follow those of the observed SNR, and therefore those of the wireless channel (noise power fluctuations can be safely assumed to be much slower than those of the channel). This is illustrated in Fig. 1(a), which shows examples of reported CQI values along time for honest and malicious users launching the misreporting attack from Sec. II-C for two different values of initial average throughput after handoff, r_0^{Att}. The curves corresponding to attackers are noticeably different from that of an honest user, more so as attackers choose smaller values of r_0^{Att} (which result in more damage to the network, as will be discussed in Sec. IV). In addition, Fig. 1(b) suggests that the sample correlation coefficient can be useful in order to detect attackers, as discussed next.

The time-varying features of wireless mobile channels are influenced by physical factors such as multipath propagation, speed of mobile stations and/or surrounding objects, and signal bandwidth [19], [20]. For small-scale fading (i.e., over short time periods), a stationary assumption is well suited for characterizing the randomly time-varying wireless channel [21], and several models exist depending on the structure of the propagation environment. All of them exhibit strong correlation for short lags, since the channel response is a low-pass process of bandwidth much smaller than that of the transmitted signal. For example, in dense propagation environments the Rayleigh distribution is commonly used to describe the received envelope γ of a signal undergoing flat

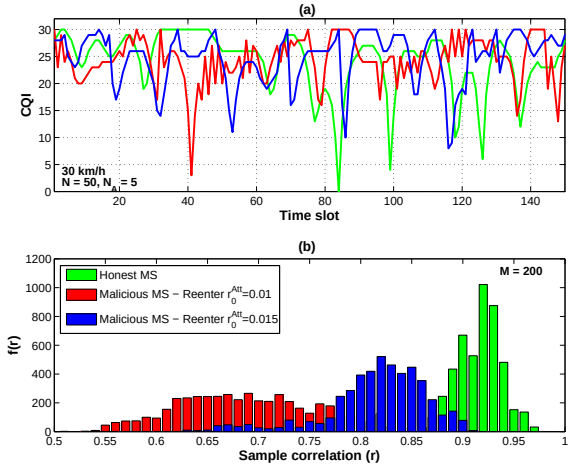

Fig. 1. Typical time histories of reported CQI values and their corresponding sample correlation distribution, for an honest MS and an attacker. Simulation parameters details are found in Sec. IV.

fading, and Jakes' model [20] is widely accepted to be a good fit for its correlation coefficient in such scenarios:

$$\rho_\gamma(\tau) \approx J_0^2(2\pi f_\mathrm{m}\tau), \tag{7}$$

with $J_0(\cdot)$ the zero-order Bessel function of the first kind, and f_m the maximum Doppler shift, related to the MS speed v, the carrier frequency f_c, and the speed of light c by $f_\mathrm{m} = f_c v/c$.

For small values of $f_\mathrm{m}\tau$, the correlation coefficient (7) will be close to one. Considering practical transmission parameters and MS speeds of interest [1], [2], and setting $\tau = T_s$ (the time slot interval), $\rho_\gamma(T_s)$ will typically be large; this also justifies the assumption that the channel remains approximately constant during a time slot. In contrast, misreporting attacks such as that from Sec. II-C tend to lower the temporal correlation of maliciously reporterd CQI sequences, when measured over several time slots, see Fig. 1(b). This allows the BS to rephrase the following hypothesis test for a given user:

$$\mathcal{H}_0: \text{ user } k \text{ is honest} \qquad \mathcal{H}_1: \text{ user } k \text{ is an attacker}, \tag{8}$$

in terms of the estimated correlation coefficient, which can be obtained as follows. Let $s_k(t) = \sqrt{f^{-1}(\mathrm{CQI}_k(t))}$, which is a quantized version of $\hat{\gamma}_k(t)/\hat{\sigma}_k$; and let

$$\mu_k(t) = \frac{1}{M-1}\sum_{i=0}^{M-2} s_k(t-i) \tag{9}$$

be the corresponding moving average over a window of $M-1$ samples. Then the correlation coefficient estimate at time slot t based on the last M received reports from user k can be expressed in terms of the vector sequence

$$\tilde{\boldsymbol{s}}_k(t) = \begin{bmatrix} s_k(t) \\ s_k(t-1) \\ \vdots \\ s_k(t-M+2) \end{bmatrix} - \mu_k(t)\mathbf{1}, \tag{10}$$

where $\mathbf{1}$ is an $(M-1)\times 1$ vector of all ones, as

$$\hat{r}_k(t) = \frac{\langle \tilde{\boldsymbol{s}}_k(t)\,,\, \tilde{\boldsymbol{s}}_k(t-1)\rangle}{\|\tilde{\boldsymbol{s}}_k(t)\| \cdot \|\tilde{\boldsymbol{s}}_k(t-1)\|}. \tag{11}$$

The proposed test at time slot t can then be written as

$$\hat{r}_k(t) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \epsilon, \tag{12}$$

where the threshold ϵ is set in order to meet a target probability of false alarm $P^{\star}_{\mathrm{FA}}$, i.e., the probability of declaring that an honest user is in fact an attacker:

$$P_{\mathrm{FA}} = \Pr\{\hat{r} < \epsilon \,|\, \mathcal{H}_0\} = F_0(\epsilon), \tag{13}$$

where F_0 denotes the CDF of (11) under $\mathcal{H}_0$. Note that the test (12) is invariant to scalings, provided that the number of quantization levels in $q[\cdot]$ is sufficiently large. Although no closed form expression is available for F_0, it can be easily evaluated numerically by means of Monte Carlo simulations if the estimation noise affecting $\hat{\gamma}_k(t)$ and $\hat{\sigma}^2_k$ can be assumed negligible. The required realizations of the channel envelope can be obtained with standard software packages, given the channel model (e.g. Jakes' as in (7)), the mobile speed, and the carrier frequency.

In practice, each MS will move at a different speed. Since the correlation coefficient is in general a decreasing function of MS speed for practical values of system parameters (being close to 1 for a stationary user). Assuming a maximum expected speed v_{m} for the mobile users, then setting the threshold ϵ to meet the target $P^{\star}_{\mathrm{FA}}$ for users moving at v_{m} m/s results in a worst-case scenario design, such that for users moving at speed $v \le v_{\mathrm{m}}$ the corresponding P_{FA} will satisfy $P_{\mathrm{FA}} \le P^{\star}_{\mathrm{FA}}$.

By monitoring $\hat{r}_k(t)$ for $k = 1, \ldots, N$, the BS can use (12) to detect malicious behavior and take appropriate measures. For example, if user k is declared an attacker at time slot t, the BS may abstain from feeding its current and future CQI reports to the PFS for a number of time slots, so that user k is not scheduled over such time window.

IV. Performance Evaluation

In order to assess the performance of the proposed scheme, we consider a setting with N_A attackers out of $N = 50$ MSs. The BS runs PFS with parameter $\alpha = 0.001$ for time slot allocation. Realistic transmission parameters are used, based on LTE specification [1]. A 2 GHz carrier frequency OFDMA system is considered, with 5.12 MHz bandwidth and 20 kHz subcarrier spacing. We focus on the allocation of consecutive time slots for a resource block consisting of 20 adjacent subcarriers (over which the channel can be considered flat). A time slot consists of 22 consecutive OFDM symbols, and thus $T_s = 1.1$ ms, during which the channel remains quasi-static. The mapping (6) from observed SNR and CQI is taken from [12] and models that of LTE:

$$\mathrm{CQI} = \begin{cases} 0, & \mathrm{SNR} \le -16, \\ \left\lfloor \frac{\mathrm{SNR}}{1.02} + 16.62 \right\rfloor, & -16 < \mathrm{SNR} < 14, \\ 30, & \mathrm{SNR} \ge 14, \end{cases} \tag{14}$$

where SNR is in dB and we assume that the estimation noise in the SNR can be neglected. Regarding channel behavior, independent flat fading channels following Jakes' model, with equal power of 0 dB, are generated for each MS. The noise power is set at $= -10$ dB for all MSs. Performance results are averaged over 100 independent realization, each spanning 1,000 time slots (1.1 s).

We start by assessing the performance of the proposed scheme under CQI misreporting attacks for a given reentry value r_0^{Att} for the attackers. The influence of this attacker-selectable parameter on system performance will be discussed subsequently.

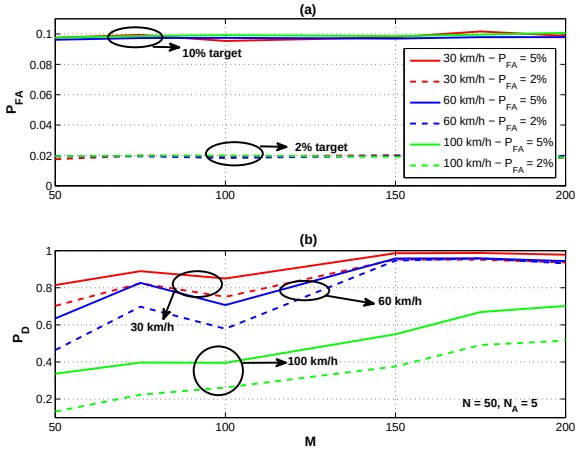

Fig. 2. Probabilities of false alarm and of detection in terms of the window size M when all MSs move at the same speed.

A. Fixed r_0^{Att}

We assume the attackers set $r_0^{Att} = 0.01 \cdot \mathrm{CQI}_{\max}$. Without protection measures, this attack may deplete roughly 99% of network resources. Fig. 2 shows false alarm (P_{FA}) and detection (P_{D}) probabilities in a setting with $N_A = 5$ attackers, considering different mobile speeds and $P^{\star}_{\mathrm{FA}}$ targets, in term of the window size M used for the computation of the sample correlation coefficient; in this case, all MSs move at the same speed. This allows to assess the accuracy in meeting false alarm targets, see Fig. 2(a). From Fig. 2(b), detection performance is seen to improve for low mobility, as could be expected, since slow users will present higher correlation values. In addition, using larger window sizes effectively improves estimation accuracy of the sample correlation coefficient, with the corresponding benefits in terms of detection. For example, with $M = 150$ a detection probability of 95% can be achieved at speeds of up to 60 km/h and 2% false alarm probability.

Fig. 3 compares scheduler performance in a setting with users moving at 60 km/h for three cases: no attack[2], attack without protection, and the proposed detection scheme using $M = 200$ and $P^{\star}_{\mathrm{FA}} = 0.1$ (users labeled as attackers at time

[2]In this case each MS gets an average of $1/N = 2\%$ time slot share.

t are not considered for scheduling in the next time slot). The proposed method is seen to be able to reclaim a sizable percentage of system resources from attackers.

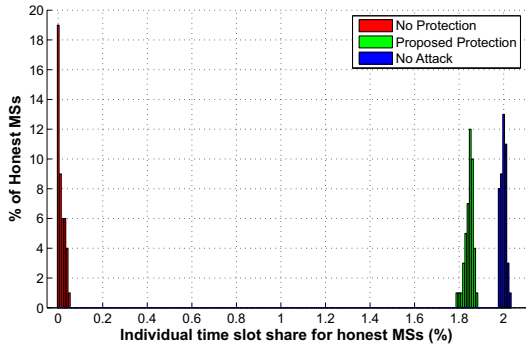

Fig. 3. Distributions of individual time slot share for honest users. Results shown for $N_A = 5$, $P_{\text{FA}} = 0.1$, $M = 200$ and all users moving at 60 km/h.

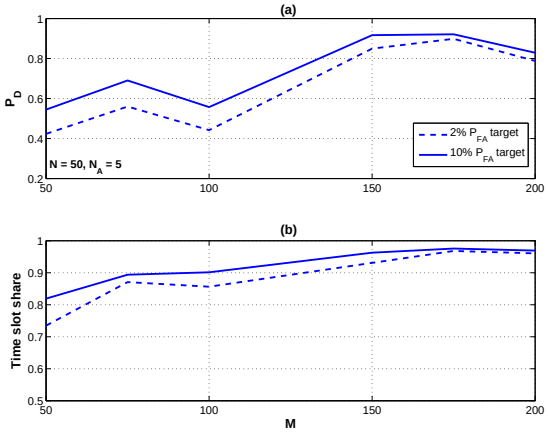

Fig. 4. P_D and time slot share for honest MSs in terms of the window size M, for MSs moving at different speeds. The threshold is set for a maximum expected speed of 60km/h.

Next we consider a more realistic scenario in which users move at different speeds, drawn from a Gaussian distribution with a mean of 40 km/h and a standard deviation of 3.16 km/h. The test threshold is set for a target $P^{\star}_{\text{FA}}$ at a maximum speed of $v_{\text{m}} = 60$ km/h, according to the worst-case approach discussed in Sec. III. As expected, achieved P_{FA} values meet the required target; in Fig. 4 results are shown for the probability of detection and the share of time slots allocated to honest users, in terms of the window size M, and again with $N_A = 5$ attackers. The protection mechanism is effective in this more realistic scenario as well: using $M = 150$, over 94% of the time slots are seen to be assigned to honest users. Similarly to what was observed in Fig. 2(b), performance is seen to improve for larger window sizes, suggesting to pick M as large as possible. However, the window size also determines the latency of the protection scheme, and thus a detection/latency tradeoff appears. The most suitable value of M is likely to be application-specific, depending on the type of network traffic. In the considered scenario, for example, there is not much incentive for using $M > 200$ even if the corresponding latency can be tolerated, as Fig. 4 shows that performance does not improve much beyond that value.

Table I summarizes results in terms of time slot allocation for different numbers of colluding attackers N_A. The proposed scheme can effectively protect against the CQI misreporting attack, even when attackers represent as much as 20% of the total number of users. Note that the percentage of system resources assigned to attackers is in all cases below what the scheduler would assign them if they behaved honestly.

TABLE I
TIME SLOT PERCENTAGE ALLOCATED TO HONEST AND MALICIOUS USERS

N_A	No Protection		Proposed method		
	Honest	Attackers	Honest	Attackers	P_{FA}
2	3.2%	96.8%	95.6%	4.4%	0.8%
4	1.2%	98.8%	96.4%	3.6%	0.9%
6	0.5%	99.5%	94.5%	5.5%	0.9%
8	0.3%	99.7%	88.3%	11.7%	0.9%
10	0.2%	99.8%	85.3%	14.7%	0.9%

Threshold adjusted for a target $P^{\star}_{\text{FA}} = 0.1$ at 60 km/h and $M = 200$. Users move at speeds of up to 60 km/h, generated as for Fig. 4.

B. *Influence of* r_0^{Att}

Throughout Sec. IV-A it was assumed that attackers used a reentry value $r_0^{Att} = 0.01 \cdot \text{CQI}_{\max}$ for their average throughputs after forcing a handoff. We focus now on the power of the CQI misreporting attack in terms of the value for r_0^{Att} set by the attackers, and the protection capabilities of the proposed test in such cases. In these experiments, all MSs are assumed to move at the same speed.

Fig. 5(a) illustrates the effectiveness of the CQI misreporting attack with $N_A = 5$ colluding attackers to deplete network resources (no detection mechanism was implemented). The attack is more powerful for lower values of r_0^{Att}, since in that case a malicious user forcing a handoff has more time slots available during which it can collaborate in the attack before its reported value reaches $\text{CQI}_{\max}$. On the other hand, the time correlation of its reported CQI values (computed with $M = 200$ in Fig. 5) becomes significantly smaller than that of an honest user, and therefore its malicious behavior has a larger probability of being detected. Thus, attackers face a power/detectability tradeoff in their choice of the reentry value r_0^{Att}. If this value is chosen too large, covert operation is possible, but the damage inflicted to the network is very limited, as shown in Fig. 5(b).

Fig. 6 illustrates this tradeoff in a setting with $N_A = 5$ attackers, and for different mobile speeds, once the proposed detection scheme is implemented (using $M = 200$ and $P^{\star}_{\text{FA}} = 0.1$). For small values of r_0^{Att}, the probability of detection is close to 1 (Fig. 6(a)), and thus the fraction of system resources captured by attackers remains small (Fig. 6(b)). For r_0^{Att} above a threshold value (which depends on mobiles' speed), P_{D} starts to drop, and attackers' share of resources increases correspondingly. However, as r_0^{Att} is

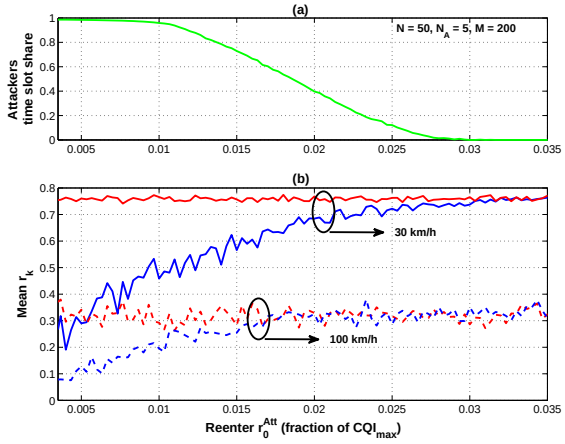

Fig. 5. Damage capability of the CQI misreporting attack (a) and mean sample correlation (b) for honest MSs (red) and attackers (blue), as a function of attackers' reentry average rate r_0^{Att}.

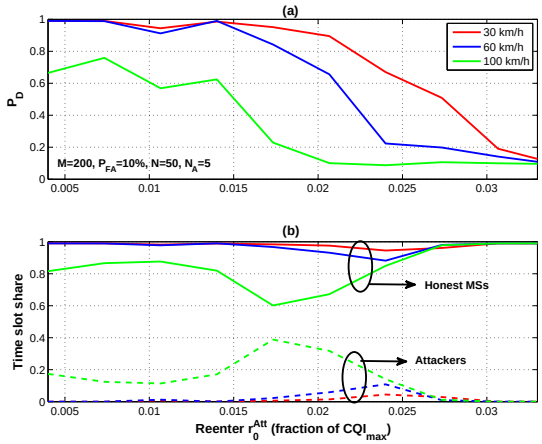

Fig. 6. P_D and time slot share for honest MSs and attackers, in terms of attackers reentry average rate.

further increased, attackers' share eventually starts to drop, due to the fact that the attack is not truly effective for very large values of r_0^{Att}, as shown in Fig. 5(b). At speeds of 100 km/h, and from the point of view of the attackers, the optimum value of r_0^{Att} in this setting is $r_0^{Att} = 0.017 \cdot \mathrm{CQI}_{\max}$, for which malicious users obtain 39% of system resources. In view of the fact that the considered attack constitutes an upper bound on the power of more realistic attacks, results from Fig. 6 clearly validate the effectiveness of the proposed protection scheme.

V. Conclusions

A novel approach for protection against CQI misreporting attacks in PFS was presented. The proposed scheme exploits the distinctive temporal features of the mobile channel in order to detect abnormal behavior from malicious user. This detection method is effective and avoids the modification of PFS, making it particularly appealing for implementation in current systems. Further, it also avoids the overhead required by previous authentication-based approaches.

Acknowledgment

Work supported by ERDF funds and the Spanish and Galician Governments (TEC2013-47020-C2-1-R COMPASS, CN 2012/260 AtlantTIC, Consolidation of Research Units GRC2013/009, TACTICA). Funding from KWF and ERDF under grant KWF-3520/23733/35457 is acknowledged.

References

[1] 3GPP, "Physical layer aspects for evolved UTRA," 3GPP technical report, TR 25.814, Ver. 1.0.3, Feb. 2006.

[2] WiMax, "IEEE standard for local and metropolitan area networks part 16: Air interface for fixed and mobile broadband wireless access systems," IEEE Std 802.16e, 2006.

[3] J. G. Andrews, S. Buzzi, W. Choi, S. Hanly, A. Lozano, A. C. K. Soong, and J. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, 2014, in press.

[4] A. Asadi and V. Mancuso, "A survey on opportunistic scheduling in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1671–1688, 2013, fourth Quarter.

[5] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1277–1294, Jun 2002.

[6] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2004.

[7] H. J. Kushner and P. A. Whiting, "Convergence of proportional-fair sharing algorithms under general conditions," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1250–1259, Jul 2004.

[8] S. Borst, "User-level performance of channel-aware scheduling algorithms in wireless data networks," *IEEE/ACM Trans. Networking*, vol. 13, no. 3, pp. 636–647, Jun 2005.

[9] S. Bali, S. Machiraju, H. Zang, and V. Frost, "A measurement study of scheduler-based attacks in 3G wireless networks," in *Passive and Active Network Measurement*. Springer, 2007, pp. 105–114.

[10] R. Racic, D. Ma, H. Chen, and X. Liu, "Exploiting and defending opportunistic scheduling in cellular data networks," *IEEE Trans. Mobile Computing*, vol. 9, no. 5, pp. 609–620, 2010.

[11] K. Pelechrinis, P. Krishanmurthy, and C. Gkantsidis, "Trustworthy operations in cellular networks: The case of PF scheduler," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 292–300, 2014.

[12] D. Kim and Y.-C. Hu, "A study on false channel condition reporting attacks in wireless networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 5, pp. 935–947, 2014.

[13] H. Wen, S. Li, X. Zhu, and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 34–39, May 2013.

[14] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. 5th ACM Workshop on Wireless Security*, ser. WiSe '06. New York, NY, USA: ACM, 2006, pp. 33–42. [Online]. Available: http://doi.acm.org/10.1145/1161289.1161297

[15] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, July 2008.

[16] ——, "Channel-based detection of sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep 2009.

[17] J. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, September 2013.

[18] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, September 2013.

[19] T. Rappaport, *Wireless Communications - Principles & Practice*. Upper Saddle River, NJ: Prentice-Hall, 1996.

[20] W. Jakes, *Microwave Mobile Communications*. New York: Willey, 1974.

[21] S. Barbarossa and A. Scaglione, "Time-varying fading channels," in *Signal Processing Advances in Wireless and Mobile Communications*, G. B. Giannakis, Y. Hua, P. Stoica, and L. Tong, Eds. Prentice Hall, 2000, pp. 1–57.