Anti-eavesdropping Proportional Fairness Access Control for 5G Networks

Shankar K. Ghosh[1(✉)], Avirup Das[2], Sasthi C. Ghosh[2], and Nabanita Das[2]

[1] Presidency University, Bangalore 560064, India
[2] Indian Statistical Institute, Kolkata 700108, India
{sasthi,ndas}@isical.ac.in

Abstract. Due to the open access nature, communication over unlicensed band, suffers from security threats like eavesdropping. Eavesdroppers are unwanted nodes, attempting to overhear the signal transmitted between two legitimate mobile terminals (MTs), often for malicious purposes. Apart from security issues, it results in significant degradation of secrecy throughput, i.e., the throughput achieved by a legitimate user without being overheard by eavesdroppers. Since with the present technology, it is quite difficult to identify the eavesdroppers even in 5G, the average throughput of the legitimate MTs decreases when the serving base station schedules the eavesdroppers as well, based on the channel condition only. So far, the issue of eavesdropping has rarely been considered in the context of scheduling. In this paper, we propose an anti-eavesdropping proportional fairness (APF) mechanism considering the possibility of eavesdroppers. Our proposed APF technique first estimates a set of suspected eavesdroppers based on sleep mode information, and then reduces the possibility of scheduling these eavesdroppers by imposing penalties. Penalty assignments are based on past average throughput, current channel conditions and modulation/coding schemes. Both Hidden Markov model based analysis and simulations confirm that the proposed APF technique outperforms the traditional proportional fairness protocol in terms of anti-eavesdropping efficiency and secrecy throughput.

Keywords: Eavesdropping · Secrecy throughput · Proportional fairness scheduling · Hidden Markov model · Physical layer security

1 Introduction

To deal with the increasing demand for wireless data traffic in the upcoming fifth generation (5G) cellular networks, unlicensed band communication has been evolved as a promising solution. Recently, the applicability of new radio (NR), the radio access technology (RAT) for 5G systems, has been extended to unlicensed band spectrum by 3rd generation partnership project (3GPP) [1]. It is expected that the large amount of spectrum available in 2.4 GHz, 5 GHz, 6 GHz and 60 GHz unlicensed

X. Yuan et al. (Eds.): QShine 2021, LNICST 402, pp. 144–158, 2021.
https://doi.org/10.1007/978-3-030-91424-0_9

bands will significantly increase user throughput in NR systems. Although high user throughput can be ensured in unlicensed band communication, it suffers from security threats due to its open access nature [3]. Previously, Shannon's work has been extensively used to secure communication systems using shared secret keys. However, these works have several drawbacks including complexities associated with key management, distribution and key length [2]. To address these drawbacks, a new keyless information theoretic security paradigm namely *physical layer security* has been emerged. In Wyner's work [4], it has been shown that confidential communication between legitimate mobile terminals (MTs) is possible without sharing a secret key if the eavesdropper's channel is a degraded version of the intended receiver's channel. In this regard, *secrecy throughput* has been defined as the difference between the throughput obtained by the intended receiver from the system and the throughput obtained by the eavesdroppers by overhearing the receiver's channel. In presence of eavesdroppers, efficient resource allocation policy is essential to ensure high secrecy throughput. But since, with present technology, exact identification of eavesdroppers is difficult, the problem is still challenging to the research communities [2,3].

Eavesdroppers are often registered in the network as subscribed MTs and exchange signaling messages with serving base stations (BS) [5]. In such a scenario, the objective of these malicious MTs is to decode private message of any legitimate user. Since the exact identifications of eavesdroppers are not known, the serving BS often schedules eavesdroppers having good channel conditions. This in turn results in starvation of legitimate MTs. It may be noted that secrecy throughput of a legitimate user may degrade in two ways: Firstly, due to eavesdropping, i.e., the signal transmitted to the legitimate user is overheard by the eavesdroppers. Secondly, due to starvation of legitimate MTs, i.e., the average throughput obtained by the legitimate user is much less due to the resource scarcity caused by the eavesdroppers. Although exact identification of eavesdroppers' is quite difficult, the number of such malicious MTs may be known to the BS through various mathematical techniques based on random matrix theory and hypothesis testing [6]. In such a prevailing situation, it is worthy to think of a scheduling mechanism which can *reduce the possibility* of an eavesdropper being scheduled by the serving BS. It may be considered as a penalty for eavesdropping that helps to improve the secrecy throughput of good users by reducing the tendency of overhearing.

To improve user throughput in wireless data networks, a number of scheduling mechanisms have been proposed in literature. A survey of such algorithms can be found in [7]. Among these existing mechanisms, proportional fairness (PF) scheduling is of particular interest due to its ability to strike a trade-off between throughput and fairness. The goal of traditional PF scheduling is to maximize the cell throughput while ensuring fairness among the MTs. A number of variations of traditional PF have also been proposed to deal with the drawbacks incurred by traditional PF such as throughput degradation due to poor channel condition at the cell edges, blockage of signals by obstacles in millimeter wave communications (mmWave) and signal fading caused by mobility of MTs. For example, in [8],

an enhanced PF mechanism has been proposed for mmWave. Here the past average throughput decreases exponentially with current throughput degradation. Consequently, the priority of MTs residing in non line of sight region increases. The predictive finite horizon PF mechanism proposed in [9] deals with the fast fading caused by mobility of MTs by employing a data rate prediction and a future channel estimation mechanism. It may be noted that designing scheduling mechanism to reduce the performance degradation caused by eavesdroppers is quite limited in the preceding literature. In [10], a scheduling mechanism has been proposed to improve the security level in cognitive radio network. Here, the cognitive user that maximizes the achievable secrecy rate is scheduled to transmit its data packet. In [11], an optimal transmission scheduling scheme has been proposed to maximize the security of ad hoc network against eavesdropping. Here the scheduling scheme opportunistically selects a source node with the highest secrecy rate to transmit its data. In [13], the probability of success in opportunistic stationary eavesdropping attacks has been analyzed, however nothing has been suggested as preventive measure. These existing mechanisms [10,11,13] are not suitable for upcoming 5G cellular network scenarios as they are designed specifically for ad hoc and cognitive radio networks respectively.

In this work, our *objective* is to propose an anti-eavesdropping PF (APF) scheduling mechanism which can *reduce the possibility* of an eavesdropper being scheduled significantly, and therefore penalizes the eavesdroppers to reduce the tendency of overhearing. Our *contributions* are summarized as follows.

- We propose a new scheduling mechanism namely, the anti-eavesdropping proportional fairness (APF) scheduling which explicitly considers the possibility of throughput degradation by eavesdroppers. The goal of APF is to eliminate eavesdroppers while scheduling different MTs in the system. The APF mechanism first determines the set of suspected eavesdroppers based on *sleep mode information* obtained through co-operative detection [17]. In 5G systems, sleep mode is used by the MTs to save power and to increase battery life. An MT switches to sleep mode when there is no data to be transmitted [19], or to be received. In our proposed mechanism, MTs spending *less time* in sleep mode than the estimated value have higher chance of being an eavesdropper.
  Then *penalty coefficient* for each of the suspected eavesdropper is determined based on their past average throughput values. Here, the penalty coefficient represents the extent by which the possibility of scheduling the concerned eavesdropper need to be reduced. Next, *individual penalties* for each of the suspected eavesdroppers are determined based on their penalty coefficients, past average throughput values, channel conditions and modulation/coding schemes (MCS). While scheduling different MTs, individual penalties are added to the past average throughput values of the corresponding eavesdroppers. As a result, the possibility of the eavesdropper being scheduled reduces.
- We analyze the performance of our proposed APF based on Hidden Markov model (HMM). Here the sequence of scheduled MTs over an arbitrary time interval has been considered as the *hidden sequence* of legitimate MTs and eavesdroppers. In our developed model, the sequence of secrecy throughput

values has been considered as *observed sequence* and *observation likelihoods* has been computed in proportion to the secrecy throughput values. Finally, anti-eavesdropping efficiency (AE) has been computed as the probability of occurring the observed sequence from a hidden sequence consisting of *only* legitimate MTs. In other words, AE is a measure of *how close a scheduling mechanism is to the ideal situation.*

– Extensive system level simulations have been carried out to compare the performance of APF with traditional PF [7]. The HMM based analyses and simulations confirm that our proposed APF significantly outperforms the traditional PF in terms of AE, secrecy throughput and Jain's fairness index.

The rest of the paper is organized as follows. Section 2 presents the system model considered here. Section 3 describes the proposed scheduling policy with the analytical framework included in Sect. 4. Section 5 presents the simulation results and Sect. 6 concludes with future direction of research.

Table 1. List of important notations

Notation	Description
$(.)$	Indicator of scheduling mechanism (p for PF or a for APF)
$R_u^{(.)}(t)$	Past average throughput of user u at time t
$S_u^{(.)}(t)$	Secrecy throughput of user u at time t
$r_u(t)$	Achievable throughput by user u at time t
$\gamma_u(t)$	SINR received at user u at time t
$P_u(t)$	Power received by user u at time t
$N(t)$	Received noise power at time t
b	Bandwidth of a resource block
$p_k(t)$	Penalty coefficient for eavesdropper k at time t
α	Severity index
Q	Set of all users
ξ	Set of all eavesdroppers
$\tau_{ku}(t)$	Overheard throughput by eavesdropper k from legitimate user u at time t

2 System Model

Our system model consists of a new radio (NR) base station (BS) and Q the set of MTs. Within the coverage region of the BS, MTs are uniformly distributed. We consider that there exists a group of eavesdroppers that wish to decode secret messages. The individual identities of the eavesdroppers are not known to the BS. However, side information is available regarding $|\xi|$ the cardinality of the set of all potential eavesdroppers ξ. Such information is typically available through different statistical characterizations [5,6]. Based on the channel quality information (CQI) values reported by the MTs, the BS assigns resource blocks (RBs)

to the MTs based on (.), a predefined scheduling mechanism. In our case, (.) may be either p (for PF) or a (for APF).

Secrecy throughput $S_u^{(.)}(t)$ obtained by a legitimate user u ($u \in Q \setminus \xi$) at time t when (.) is used to schedule MTs has been measured as the difference between $R_u^{(.)}(t)$, the average throughput obtained by MT u from the BS upto time t and $\sum_{k \in \xi} \tau_{ku}(t)$, the total throughput obtained by all eavesdroppers by overhearing the transmitted signal to the legitimate MT u at time t. Here $\tau_{ku}(t)$ represents the individual throughput obtained by eavesdropper k by overhearing the transmitted signal to the legitimate MT u at time t. Since, channel gains of eavesdroppers' channels are much lower compared to that of the legitimate MT's channel, $R_u^{(.)}(t)$ is usually higher compared to that of $\sum_{k \in \xi} \tau_{ku}(t)$. The secrecy throughput $S_u^{(.)}(t)$ obtained by MT u at time t has been computed as:

$$S_u^{(.)}(t) = R_u^{(.)}(t) - \sum_{k \in \xi} \tau_{ku}(t) \tag{1}$$

$\gamma_u(t)$, the signal to interference plus noise ratio (SINR) received at user u at time t has been computed as:

$$\gamma_u(t) = \frac{P_u(t)}{N(t)} \tag{2}$$

$P_u(t)$ is the power received by MT u situated at distance $d(t)$ from the BS at time t and $N(t)$ is the noise power received by MT u at time t. Here $P_u(t)$ has been computed using free space path loss model. Based on $\gamma_u(t)$, achievable throughput by user u through an RB at time t has been computed as:

$$r_u(t) = b \times \log_2 (1 + \gamma_u(t)) \tag{3}$$

where b is the bandwidth of an RB in the NR base station. Based on this system model, in the next section, we propose the APF mechanism. Important notations used in this work have been summarized in Table 1.

3 Proposed APF Scheduling

In this section, we propose the APF mechanism which explicitly consider the possibility of throughput reduction due to the presence of eavesdroppers. The goal of our proposed APF mechanism is to reduce the chance of an eavesdropper being scheduled by the serving BS. We assume that $|\xi|$ the number of eavesdroppers present in the system are known to the serving BS. Such assumption is very common as can be found in [5]. Detailed operation of the proposed scheduling mechanism is described below.

Determining the Set of Suspected Eavesdroppers
In this phase, the set of suspected eavesdroppers $\xi'(t)$ is determined from the set of MTs Q based on sleep mode information obtained through energy detection technique. In 5G systems, sleep mode is used by the MTs to save power and increase battery life. An MT switches to sleep mode when there is no data to be transmitted [19]. Since, eavesdroppers have an intention to sense other MT's downlink channel, transceivers of the eavesdroppers will remain active even when there is no data to be transmitted. As a result, the transceiver will emanate a *leakage power* which may be detected by MTs residing in close proximity using energy detection technique [17].

In our proposed algorithm, a set of trusted MTs (e.g., closed access group MTs) collects the sleep mode information of their nearby MTs through energy detection technique [17] and sends that information to the BS. The BS then computes the time spent in sleep mode by correlating the measurements of various trusted MTs [18]. Once the time periods spent in sleep mode by individual MTs are computed, the set $\xi'(t)$ is determined by including $|\xi|$ MTs in *ascending order* of their sleeping time.

Remark 1. Most of the Internet traffic is variable bit rate (VBR) traffic. In case of VBR traffic call holding time is assumed to follow Pareto principle [20]. As per the Pareto principle, every call has a minimum duration of survival (say x_m) and the probability of survival of a call decreases exponentially beyond x_m. In contrast to legitimate users, the receiver of an eavesdropper remains active even when they do not have data to send. Hence, MTs spending less time in sleep mode is more probable of being an eavesdropper.

Determining the Penalty Coefficients
In this phase, $p_k(t)$ the penalty coefficient for eavesdropper k at time t is determined based on $R_k^a(t-1)$. *Penalty coefficient of eavesdropper k represent the extent by which the possibility of scheduling eavesdropper k needs to be reduced.* The value of $p_k(t)$ has been computed in proportion to $R_k^a(t-1)$, i.e., $p_k(t) = \frac{R_k^a(t-1)}{\sum_{k' \in \xi'(t)} R_{k'}^a(t-1)}$. This is quite reasonable because a higher $R_k^a(t-1)$ implies a higher possibility of having good channel conditions in recent past. Consequently, throughput degradation caused due to scheduling eavesdropper k is also expected to be high. Hence, to minimize throughput degradation, the serving BS should defer the scheduling of eavesdropper k in proportion to its past average throughput.

Determining Individual Penalty
In this phase, we determine the individual penalty for each eavesdropper k based on the penalty function $p_k(t) \times [r_k(t)]^\alpha$, where α is the severity index based on MCS. It may be noted that the penalty function explicitly considers the effect of past average throughput, present channel condition and MCS. The individual penalty of eavesdropper k increases with $p_k(t)$ which in turn is proportional to the past average throughput. This is because an eavesdropper with high past

Algorithm 1: Proposed APF mechanism

Input : Q, $|\xi|$, $R_u^a\,(t-1)\ \forall u \in Q$, $r_u\,(t)\ \forall u \in Q$, α.
Output: User u^* to be scheduled at time t.

$\xi'(t) = \phi$
for *all* $u \in Q$ **do**
  Determine sleep time of u based on leakage power measurement.
end
$\xi'(t)$ = The set of $|\xi|$ MTs taken in ascending sequence of their sleep time.
Compute $p_k(t) = \dfrac{R_k^a(t-1)}{\sum\limits_{k' \in \xi'(t)} R_{k'}^a(t-1)}\ \forall k \in \xi'(t)$.
Set $p_k(t) = 0\ \forall k \in Q \setminus \xi'(t)$.
Compute $C_u(t) = p_u(t) \times [r_u\,(t)]^\alpha\ \forall u \in Q$.
Determine the user u^* to be scheduled:

$$u^* = \arg\max_{u \in Q} \frac{r_u\,(t)}{R_u^a\,(t-1) + C_u(t)}$$

Return u^*

average throughput is expected to have good channel conditions in recent past, causing significant reduction in secrecy throughput. The individual penalty also increases with increasing $r_k(t)$ which is computed based on current SINR of the channel. This is because an eavesdropper having good channel condition at present is more likely to reduce throughput of legitimate MT, if scheduled by the serving BS. For a given SINR, throughput achieved by an user increases with improved MCS. To take care of this effect, our proposed APF increases the individual penalty exponentially with α. In our proposed scheme, the value of α is 1 for binary phase shift keying (BPSK), 2 for quadrature phase shift keying (QPSK), 3 for 16 quadrature amplitude modulation (QAM) and 4 for 64 QAM.

Assignment of RB

In this phase, RBs are assigned to the MTs based on their current throughput, past average throughput and individual penalties. It may be noted that individual penalties for all legitimate MTs are 0, i.e., $p_k(t) \times [r_k\,(t)]^\alpha = 0$ for all $k \in Q \setminus \xi'(t)$. An RB is assigned to the user u^* if the following condition holds:

$$u^* = \arg\max_{u \in Q} \frac{r_u\,(t)}{R_u^a\,(t-1) + p_u(t) \times [r_u\,(t)]^\alpha} \tag{4}$$

Thus the probability of scheduling an eavesdropper is reduced as the past average throughput value is increased by the individual penalty. The overall algorithm has been depicted in pseudo code format in Algorithm 1. The time complexity of the proposed APF is $O(|Q|^2)$.

4 Analytical Framework

In this section, we analyze the performances of our proposed APF and traditional PF [7] mechanisms based on Hidden Markov models (HMM). A HMM enables us to talk about some underlying *hidden events* based on some *observed events* and *observation likelihoods*, where the hidden events are considered as causal factors for the observed events. Observation likelihood is defined as the probability of an observation being generated from a particular *hidden state*. Here an output observation depends only on the state that produced the observation and not on any other states or observations. A detailed description of HMM can be found in [16].

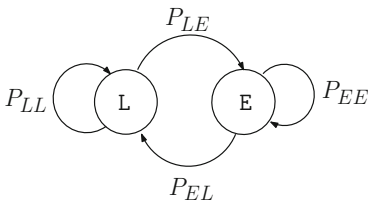

Fig. 1. Hidden Markov model

It has been assumed that time is discrete, and, in every time step t, the BS schedules an MT which may be a legitimate MT or an eavesdropper. However, the characteristic of the scheduled MT is completely unknown to the BS. Hence, the sequence of scheduled MTs over an *arbitrary time interval* I can be considered as a hidden sequence of legitimate MTs and eavesdroppers. On the other hand, the number of existing eavesdroppers and their channel gains can be known to the BS through different statistical tests [3,5]. Hence, at every time t, the BS can record $S^{(.)}(t)$ the secrecy throughput of the scheduled MT at time t. Since, the exact identity of the scheduled MT is less significant in our analysis, we are omitting the subscript in the notion of secrecy throughput for the sake of simplicity. A sequence of such secrecy throughput $S^{(.)}(t)$ over the time interval I can be considered as the observed sequence. Since, the secrecy throughput increases when the BS schedules a higher number of legitimate MTs, the observation likelihoods over I has been computed in proportion to the $S^{(.)}(t)$ values.

In ideal case, for a given observation, the hidden sequence consists of all legitimate MTs, i.e., no eavesdroppers are scheduled by the BS. Keeping this in mind, we define *anti-eavesdropping efficiency* (AE) of a scheduling mechanism as the probability of occurring the observed sequence from a hidden sequence consisting of *only* legitimate MTs. In other words, AE is a measure of *how close a scheduling mechanism is to the ideal situation.* A higher AE indicates the hidden sequence is more close to all legitimate MT sequence, i.e., the corresponding scheduling mechanism is more efficient to eliminate eavesdroppers from being scheduled. In subsequent subsections, we derive the expressions for AE.

4.1 Analyzing AE of PF

We characterize the operation of PF by an HMM consisting of two states namely L and E (shown in Fig. 1). Here the states L and E represent the states that the BS is currently serving a legitimate MT and an eavesdropper respectively. In the considered model, P_{ij}s indicate the transition probabilities from state i to state j where $i, j \in \{L, E\}$. We assume that the time interval I has n equally spaced time steps t_1, t_2, ..., t_n. Observed sequence over the time interval I is $S^p(t_1)$, $S^p(t_2)$, ..., $S^p(t_n)$. Based on the observed sequence, observation likelihoods can be computed as:

$$P\left(S^p(t_i)|L\right) = \frac{S^p(t_i)}{\sum_{k=1}^{n} S^p(t_k)}, \forall i \in [1, n]. \tag{5}$$

Since, the system consists of $|\xi|$ number of eavesdroppers, the probabilities of staying in state L and E are $1 - \frac{|\xi|}{|Q|}$ and $\frac{|\xi|}{|Q|}$ respectively. Hence, the initial probability distribution π can be computed as $\pi = (\pi_L, \pi_E)$, where $\pi_L = 1 - \frac{|\xi|}{|Q|}$ and $\pi_E = \frac{|\xi|}{|Q|}$. Following similar logic, the self transition probability P_{LL} in state L can be computed as $P_{LL} = 1 - \frac{|\xi|}{|Q|}$.

Now, AE of PF is the probability of getting the observation $S^p(t_1)$, $S^p(t_2)$, ..., $S^p(t_n)$ from a hidden sequence of all Ls, i.e., $P\left(S^p(t_1), S^p(t_2), \ldots, S^p(t_n)|L, L, \ldots, L\right)$. To compute this probability we have adopted the formation presented in [16]. We compute V^p, the AE of PF, i.e., $P\left(S^p(t_1), S^p(t_2), \ldots, S^p(t_n)|L, L, \ldots, L\right)$, as follows:

$$\begin{aligned} V^p &= \pi_L \left[P_{LL}\right]^{n-1} \prod_{i=1}^{n} P\left(S^p(t_i)|L\right) \\ &= \left(1 - \frac{|\xi|}{|Q|}\right)^n \prod_{i=1}^{n} \frac{S^p(t_i)}{\sum_{k=1}^{n} S^p(t_k)} \end{aligned} \tag{6}$$

4.2 Analyzing AE of APF

The operation of our proposed APF can also be characterized by a two state HMM as described for PF, however the transitions probabilities $P'_{ij}s$ are different from PF. At each time t, the APF determines a suspected set of eavesdroppers $\xi'(t)$ and imposes penalties on each of these eavesdroppers. As a result, at most $\xi \cap \xi'(t)$ set of eavesdroppers may be eliminated from being scheduled. Hence, at least $\xi \setminus \xi \cap \xi'(t)$ set of eavesdroppers are present for being scheduled at time t. Accordingly, for APF mechanism, the self transition probability $P'_{LL}(t)$ for state L at time t can be computed as $P'_{LL}(t) = 1 - \frac{|\xi \setminus \xi \cap \xi'(t)|}{|Q|}$. It may be noted that $P'_{LL}(t)$ boils down to P_{LL} when $\xi \cap \xi'(t) = \phi$, the null set. Hence, the

average self transition probability over the time interval I can be computed as $P'_{LL} = \frac{1}{n}\sum_{i=1}^{n} P'_{LL}(t_i)$. Since, $P'_{LL}(t_i) \geq P_{LL}\ \forall i \in [1, n]$, we get $P'_{LL} \geq P_{LL}$.

The computation of initial probability distribution is similar to that of PF, i.e., π'_L the probability of starting from state L in APF can be computed as $\pi'_L = 1 - \frac{|\xi|}{|Q|}$. Denoting by $S^a(t_1)$, $S^a(t_2)$, ... , $S^a(t_n)$ the observation sequence for APF mechanism, V^a the AE for APF mechanism can be computed as:

$$\begin{aligned} V^a &= P\left(S^a(t_1), S^a(t_2), \ldots, S^a(t_n) | L, L, \ldots, L\right) \\ &= \pi'_L \left[P'_{LL}\right]^{n-1} \prod_{i=1}^{n} P\left(S^a(t_i)|L\right) \\ &= \left(1 - \frac{|\xi|}{|Q|}\right)\left[\frac{1}{n}\sum_{k=1}^{n}\left(1 - \frac{|\xi \setminus \xi \cap \xi'(t_k)|}{|Q|}\right)\right]^{n-1} \\ &\times \prod_{i=1}^{n} \frac{S^a(t_i)}{\sum_{k=1}^{n} S^a(t_k)} \end{aligned} \tag{7}$$

5 Results and Discussions

In this section, we evaluate the performance of our proposed APF mechanism based on HMM based analysis and system level simulations. We consider secrecy throughput, AE and Jain's fairness index (J) as performance evaluation metrics. Secrecy throughput and AE have already been defined in Sects. 2 and 4 respectively. To measure fairness in achieved throughput among the legitimate MTs we have used the well known *Jain's fairness index* (J) [14]. Here J has been computed as:

$$J = \frac{\left(\sum_{i \in Q \setminus \xi} R_i^{(\cdot)}(t)\right)^2}{|Q| \sum_{i \in Q \setminus \xi} R_i^{(\cdot)}(t)^2}$$

5.1 Simulation Setup

To evaluate the performance of our proposed scheme, we have prepared a MATLAB based simulator. We consider a simulation environment similar to that of [12]. Our simulation environment consists of a cell with radius 500 m. Within the coverage region of the cell, MTs are distributed uniformly. We vary the number of MTs from 10 to 100. We have considered an NR BS situated at the center of the cell. Height of the BS measured from the ground has been set to 2 m. All

Table 2. Parameter settings

Parameters	Values	Parameters	Values
Cell radius	500 m	Number of MTs	10–100
Eavesdropper (%)	30%	BS height	2 m
Bandwidth	20 MHz	Transmit power	24 dBm
Noise power	−90 dBm	α	2

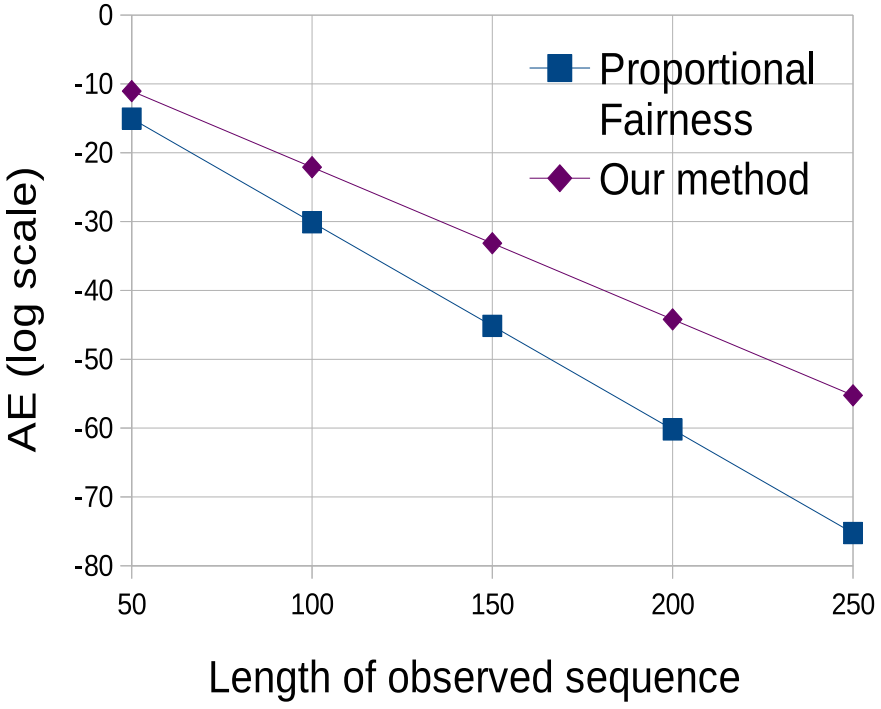

Fig. 2. AE vs. length of observed sequence (analysis)

MTs are equipped with an omni-directional transceiver, and are served by the common BS. We consider that all MTs are in line of sight with the serving BS. Transmitting power of the AP has been set to 24 dBm. The carrier frequency of the AP has been set to 28 GHz according to the 5G NR FR2 band standard [15]. We have considered *free space path loss model* to calculate the received signal strength at the MT end. In the considered simulation environment, MTs are moving according to *random way point* mobility model. While computing past average throughput at time t, we have given same weight to the current throughput and past average throughput at time $t-1$. We consider that the channel gain of an overheard channel is exponentially distributed with parameter β, where β is uniformly random within $[1\times10^{-7}, 2\times10^{-7}]$ [3]. In our considered scenario, 10%

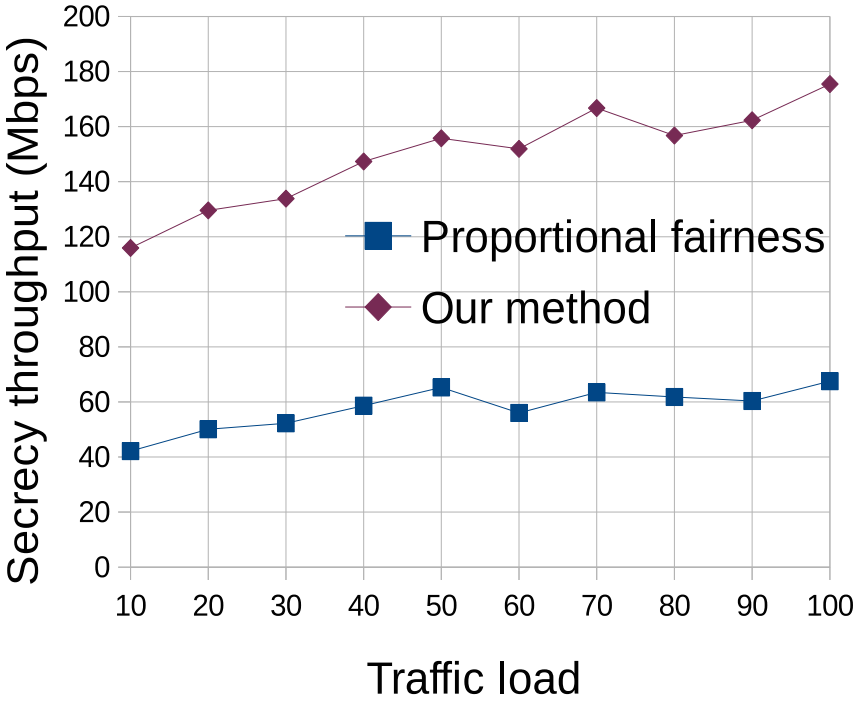

Fig. 3. Secrecy throughput vs. traffic load (simulation)

of the total MTs have been considered as *trusted nodes*. The trusted nodes send the sleep mode status of their neighboring MTs to the BS in every transmission time interval (TTI). The BS decides the sleep mode status of an MT depending upon the majority neighbor's decision. Important parameters considered in our simulations are depicted in Table 2.

5.2 Results

Figure 2 depicts the effect of the length of the observed sequence on AE. Here the results have been obtained based on the analytical models developed in Sect. 4. Results show that the AE decreases with increasing the length of observed sequence for both approaches. However, our proposed APF outperforms the traditional PF [7] in terms of AE. The performance gain in our approach increases with increasing length of the observed sequence. The reasons behind are as follows. The probability of at least one eavesdropper being scheduled increases with increasing the time interval I. As a result, the AE decreases for both the approaches. However, the proposed APF can eliminate eavesdroppers from being scheduled by imposing penalties. Such probability of elimination increases in larger time intervals. As a result, the performance gain in APF increases monotonically with the length of the considered time interval.

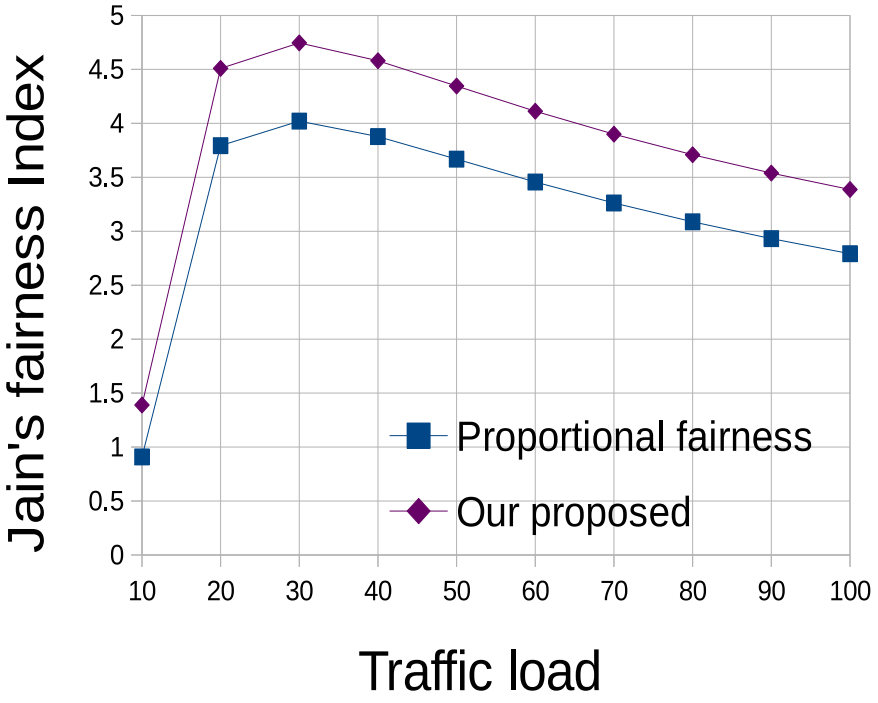

Fig. 4. Jain's fairness index vs. traffic load (simulation)

Figure 3 depicts the effect of traffic load on secrecy throughput. Here the traffic load varies from 10 MTs to 100 MTs with a step of 10 MTs. Results reported in this section represent the average results obtained from 10000 independent runs. The result shows that our proposed APF mechanism significantly outperforms the traditional PF mechanism. The reasons behind are as follows. The secrecy throughput depends on two factors: (a) the throughput obtained by the legitimate MTs from the system, and (b) the throughput obtained by the eavesdroppers by overhearing the transmitted signal to the legitimate MTs. Since, the channel gain of the overheard channel is significantly lower compared to the original channel allocated to the legitimate MTs, throughput obtained by the legitimate MTs takes the decisive role towards determining secrecy throughput. Since, our proposed approach can eliminate eavesdroppers while scheduling different MTs as obtained from the analytical results (Fig. 2), throughput obtained by the legitimate MTs in APF is better compared to that of traditional PF. This results in higher secrecy throughput in our proposed approach. *Both analysis and simulation results generate a consensus that our proposed APF can effectively eliminate eavesdroppers while scheduling different MTs.*

Figure 4 shows the effect of traffic load on the Jain's fairness index. Here also the traffic load varies from 10 MTs to 100 MTs with a step of 10 MTs. The result shows that our proposed APF mechanism significantly improves the Jain's fairness index compared to the traditional PF mechanism as the traffic load increases beyond 20 MTs. The reason behind is as follows. The traditional PF often schedules eavesdroppers having good channel conditions. This results in starvation of some legitimate MTs when the traffic load is beyond a certain threshold (20 MTs in our case). On the other hand, being equipped with side information such as time spent in sleep mode and number of eavesdroppers, our proposed APF reduces the chance of scheduling an eavesdropper. Consequently, in our approach, possibility of starvation is quite low. As a result, the APF mechanism outperforms the traditional PF in terms of Jain's fairness index. The possibility of starvation increases with increasing traffic load for both the approaches, resulting in decreasing trend for J.

6 Conclusions and Future Research Scope

In this work, APF scheduling mechanism has been proposed to avoid eavesdroppers while scheduling different MTs in the system. Moreover, the anti-eavesdropping efficiency of the proposed APF has been analyzed based on HMM. The APF mechanism reduces the chance of an eavesdropper being scheduled by assigning penalties to a suspected set of eavesdroppers. Both analysis and simulation results confirm that the APF mechanism significantly outperforms the traditional PF in terms of secrecy throughput, anti-eavesdropping efficiency and Jain's fairness index.

To determine a more accurate probability distribution to capture the exact set of eavesdroppers, we are planning to employ the carrier frequency offset (CFO) information. The CFO information is related to the user specific transceiver and is less affected by the environment. For further characterization of eavesdropping behaviours, we aim to deploy random matrix theory (RMT) to analyze the multi-dimensional CFO data.

References

1. Lagen, S., et al.: New radio beam-based access to unlicensed spectrum: design challenges and solutions. IEEE Commun. Surv. Tutor. **22**(1), 8–37 (2020)
2. Hamamreh, J.M., Furqan, H.M., Arslan, H.: Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1773–1828 (2019)
3. Wu, Y., Zheng, J., Guo, K., Qian, L.P., Shen, X., Cai, Y.: Joint traffic scheduling and resource allocations for traffic offloading with secrecy provisioning. IEEE Trans. Veh. Technol. **66**(9), 8315–8332 (2017)
4. Wyner, A.D.: The Wire-tap channel. Bell Syst. Tech J. **54**(8), 1355–1387 (1975)
5. Chorti, A., Perlaza, S.M., Han, Z., Poor, H.V.: Physical layer security in wireless networks with passive and active eavesdroppers. In: Proceedings of IEEE Global Communications Conference (GLOBECOM), pp. 4868–4873 (2012)

6. Chen, H., Tao, X., Li, N., Xia, S., Sui, T.: Physical layer data analysis for abnormal user detecting: a random matrix theory perspective. IEEE Access **7**, 169508–169517 (2019)
7. Capozzi, F., Piro, G., Grieco, L.A., Boggia, G., Camarda, P.: Downlink packet scheduling in LTE cellular networks: key design issues and a survey. IEEE Commun. Surv. Tutor. **15**(2), 678–700 (2013)
8. Ma, J., Aijaz, A., Beach, M.: Recent results on proportional fair scheduling for mmWave-based industrial wireless networks. arXiv:2007.05820 (2020)
9. Margolies, R., et al.: Exploiting mobility in proportional fair cellular scheduling: measurements and algorithms. IEEE/ACM Trans. Netw. **24**(1), 355–367 (2016)
10. Zou, Y., Wang, X., Shen, W.: Physical-layer security with multiuser scheduling in cognitive radio networks. IEEE Trans. Commun. **61**(12), 5103–5113 (2013)
11. Yajun, W., Tongqing, L., Chuanan, W.: An anti-eavesdrop transmission scheduling scheme based on maximizing secrecy outage probability in ad hoc networks. China Commun. **13**(1), 176–184 (2016)
12. Firyaguna, F., Bonfante, A., Kibilda, J., Marchetti, N.: Performance evaluation of scheduling in 5G-mmWave networks under human blockage. arXiv:2007.13112v1 (2020)
13. Balakrishnan, S., Wang, P., Bhuyan, A., Sun, Z.: On success probability of eavesdropping attack in 802.11ad mmWave WLAN. In: Proceedings of IEEE International Conference on Communications (ICC), pp. 1–6 (2018)
14. Guo, C., Zhang, Y., Wang, X.: A Jain's index perspective on α fairness resource allocation over slow fading channels. IEEE Commun. Lett. **17**(4), 705–708 (2013)
15. Carfano, G., Murguia, H., Gudem, P., Mercier, P.: Impact of FR1 5G NR jammers on UWB indoor position location systems. In: Proceedings of International Conference on Indoor Positioning and Indoor Navigation (IPIN), pp. 1–8 (2019)
16. Jurafsky, D., Martin, J.H.: Hidden Markov Models. Speech and Language Processing, Draft of October 2, 2019
17. Sawant, R., Nema, S.: SNR analysis in cooperative spectrum sensing for cognitive radio. In: International Conference on Advances in Communication and Computing Technology (ICACCT). Sangamner 2018, pp. 392–396 (2018). https://doi.org/10.1109/ICACCT.2018.8529340
18. Armi, N., Saad, N.M., Zuki, Y.M., Arshad, M.: Cooperative spectrum sensing and signal detection in cognitive radio. In: 2010 International Conference on Intelligent and Advanced Systems, Kuala Lumpur, Malaysia, 2010, pp. 1–5. https://doi.org/10.1109/ICIAS.2010.5716151
19. Lauridsen, M., Berardinelli, G., Tavares, F.M.L., Frederiksen, F., Mogensen, P.: Sleep modes for enhanced battery life of 5G mobile terminals. In: The proceedings of IEEE Conference on Vehicular Technology (VTC) (2016)
20. Chang, B., Chen, J.: Cross-layer-based adaptive vertical handoff with predistive RSS in heterogeneous wireless networks. IEEE Trans. Veh. Technol. **57**(6), 3679–3692 (2008)