Optimal Cooperator Set Selection in Social Cognitive Radio Networks

Salim Eryigit, Suzan Bayhan, Jussi Kangasharju, and Tuna Tugcu

***Abstract*—While there is a huge body of research on cooperative spectrum sensing in cognitive radio networks (CRN), incentives for cooperative behavior or the conditions under which cooperation is more likely are not explored. We model cooperation among cognitive radios (CRs) as a function of social ties among CRs. In this *social CRN* where CRs do not necessarily fulfill every cooperative sensing request, we focus on the *cooperator set selection problem*, i.e. which CRs to ask for cooperation so that resulting throughput and sensing accuracy are maximized subject to detection and false alarm probability constraints. For single channel scenario, we devise a multi-objective optimization model and obtain the solution using an evolutionary multi-objective algorithm. Our evaluations show that our solution is near-optimal in terms of throughput under legitimate operation, i.e., no malicious users, whereas it outperforms expected-throughput-optimal scheme in case of attackers. Numerical analysis demonstrates the robustness of our proposal with little loss of performance when the network is subject to common sensing attacks. In addition, our analysis underlines one significant drawback of existing works: assuming all CRs to be cooperative leads to a substantial overestimation of throughput capacity. Finally, to tackle the increasing complexity under multi-channel setting, we propose a heuristic for multi-channel cooperative sensing for the considered social CRN.**

***Index Terms*—Cognitive radio, social-awareness, cooperative spectrum sensing, social-aware sensing.**

I. Introduction

SHARING ECONOMY emerges as a new approach to services if the commodity of interest is needed not for all times but during certain periods. Spectrum sharing can be considered in this line: *secondary users* (SUs) equipped with cognitive radio (CR) capabilities access the spectrum when they need it without holding the exclusive rights for the band. Dynamic spectrum access (DSA) provides the spectrum etiquette for a number of users to share the spectrum *efficiently*, e.g., in terms of throughput or energy, or fairly. In this context, commodity is the *white space* that is the spectrum not used by the licensed users of the band, *primary users* (PUs). First, SUs have to locate these white spaces by high-accuracy spectrum sensing and release it quickly whenever a PU appears in the band. Accuracy of spectrum sensing is measured by the PU detection probability (P_d) and PU false alarm probability (P_f). While achieving high P_d is crucial for not interfering with the PUs, low P_f is essential to harvest the unused spectrum resources for SU transmission.

Cooperative spectrum sensing (CSS) improves sensing performance, especially in environments where hidden nodes exist [1]. In CSS, observations from multiple SUs are processed to decide on the state of a primary channel, which requires communication among cooperating nodes. Moreover, an SU senses for others in the hope that they sense in return when it needs the spectrum. Due to the diverse channel conditions (i.e. signal-to-noise ratio, SNR, values) and SU properties, cooperator selection has to consider this diversity and favour SUs with short sensing durations [2]. However, SUs may exhibit various sensing reliability: some may act maliciously, or some may unintentionally have low sensing accuracy, etc. CSS schemes should combat these challenges while ensuring low communication and computation overhead. These two key points are considered in the literature (e.g.,[2–4]), but the incentives for cooperation have mostly been overlooked. SUs may lack incentives to cooperate in such a model that does not account for the dynamism of cooperation, e.g., *under which conditions nodes are likely to cooperate*. Referring to real cognitive agents, e.g. human-beings, cooperation depends on the social ties between the cooperating agents. This new perspective that accounts for the SUs' cooperation behavior as a function of the social ties between SUs, distinguish our work from the existing works on CSS.

We can abstract a network in two layers: the first layer being the *wireless connectivity layer* (WCL) and the second being the *social connectivity layer* (SCL) [5]. The majority of CRN literature considers only the WCL. However, for a better grasp of the information in and about the network, CR protocols should also take the SCL into account. We call a CRN as *social CRN* if CRs operate based on the ties in the SCL. Additionally, we define a protocol as *social-aware protocol* if it exploits the knowledge in the SCL.

In this paper, we consider a CSS scenario in which each CR decides on its possible cooperators for sensing based on the information about both the SCL and WCL. For the former, it takes the willingness to cooperate and sensing reliability of other CRs into account, whereas for the latter channel conditions are considered. In a traditional CRN, when CR$_i$ requests the cooperation of CR$_j$ for sensing, CR$_j$ responds with probability 1. However, this is not the case in a social CRN as CRs may not be willing to sacrifice their energy for the benefit of others. Throughout the paper, we discuss several formulations for the *cooperation probability* of CR$_j$ for CR$_i$ based on their *social ties* (e.g., friendship, kinship).

The contributions of this paper are manifold:

Salim Eryigit is with the Dept. of Computer Engineering, Bogazici University and Idea Teknoloji Cozumleri, Turkey. E-mail: eryigit@boun.edu.tr. Tuna Tugcu is with the Dept. of Computer Engineering, Bogazici University, Turkey. E-mail: tugcu@boun.edu.tr. Suzan Bayhan and Jussi Kangasharju are with the Dept. of Computer Science, University of Helsinki, Finland. E-mail: {bayhan, jakangas@cs.helsinki.fi}.

- We develop a simple trust scheme for a CR that estimates the sensing accuracy of other CRs in Section II. Using this trust metric along with the cooperation probability of CRs, a CR can select the best possible cooperator set, e.g., avoiding malicious CRs.
- We formulate and solve the *optimal cooperator selection problem* as a probabilistic multi-objective optimization model that strikes a balance between throughput and sensing accuracy in Sections III and IV. When all the CRs are decent, our proposal's performance is within 90% of the expected throughput-optimal solution. On the other hand, in case of a malicious CR, it outperforms the expected throughput-optimal solution by 16%.
- We analyze the effect of social ties and try different cooperation probability ($p_{i,j}$) formulations in Section V. We design a flexible cooperation scheme such that it facilitates the CRs to operate also in *foreign* environments (e.g., different than home network) where they do not have any socially-connected nodes in the neighborhood. In addition, our scheme should avoid the CRs being exploited by excessive sensing. Motivated by these two points, we introduce *system willingness* and *peer willingness* concepts in Section V. Moreover, we assess the impact of certain factors specific to each CR such as location and number of social ties.
- Due to the stochastic nature of sensing in the considered social-aware model and resulting complexity for a multi-channel setting, we propose a low complexity heuristic for cooperative spectrum sensing in Section VI.

II. System Model

A. Notations and Assumptions

We consider an ad hoc CRN as in Fig. 1. All N CRs are stationary and located within each other's communication range. [1] We consider a single channel, which is primarily used by a PU following random waypoint mobility model. This channel is accessed opportunistically by CRs. As [2, 6, 7], we model the PU activity as an on-off process. We assume that the PU is active with probability P^{on} during a frame, and its state does not change within the duration of the frame.

As shown in Fig. 1, the link between CR$_i$ and CR$_j$ is marked by three values:

- **Social tie** ($w_{i,j}^{soc}$): CRs are connected to other CRs with social ties. Let $w_{i,j}^{soc}$ be the strength of the social tie between CR$_i$ and CR$_j$. Similar to [8], we assume that $w_{i,j}^{soc} = w_{j,i}^{soc}$ and they are known by CR$_i$ and CR$_j$. Practically, the social ties can be input by the users (i.e., device owners) or can be retrieved from available social services, e.g., social network sites could feed this information to the sensing module at the CR. Another way could be to apply inference techniques (e.g., using the history of association to WLANs, co-occurance at the same/nearby locations [9, 10]) to discover the similarity of visited locations and then estimate the likelihood of being socially-connected.
- **Cooperation probability** ($p_{i,j}$): It is the probability that CR$_j$ senses for CR$_i$ if asked for cooperation by CR$_i$. We assume $p_{i,j}$ is a function of $w_{i,j}^{soc}$ and consider various models for $p_{i,j}$ in Section V.

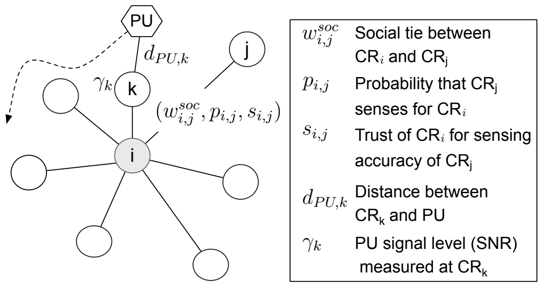

PU
$d_{PU,k}$
j
γ_k
k
$(w_{i,j}^{soc}, p_{i,j}, s_{i,j})$
i
$w_{i,j}^{soc}$ Social tie between CR$_i$ and CR$_j$
$p_{i,j}$ Probability that CR$_j$ senses for CR$_i$
$s_{i,j}$ Trust of CR$_i$ for sensing accuracy of CR$_j$
$d_{PU,k}$ Distance between CR$_k$ and PU
γ_k PU signal level (SNR) measured at CR$_k$

Fig. 1: System model: A CR and $N-1$ CRs in its range. Only some representative links are depicted.

- **Trust** ($s_{i,j}$): CR$_i$ maintains the degree of *trust* (Section II-C) it has for CR$_j$'s sensing accuracy ($s_{i,j}$). Different than $w_{i,j}^{soc}$, $s_{i,j}$ is computed at CR$_i$, may not be known by CR$_j$, and is not necessarily equal to $s_{j,i}$.

The CRN operates in a frame based manner. At the beginning of a frame, in a round-robin manner, one of the CRs is granted the right to sense and access the channel. CRs apply hard decision fusion (0: vacant, 1: occupied) for deciding on the channel state.

Let γ_j denote the PU's SNR at CR$_j$ that is given by $\gamma_j = \frac{P_{PU}^{tx} L_j G_{PU} G_j}{N_{th}}$ where P_{PU}^{tx} is PU transmission power, L_j is the path loss between the PU and CR$_j$, G_{PU} and G_j are the antenna gains for the PU and CR$_j$, and N_{th} is the noise floor [11]. The path loss model is: $L_j = \left(\frac{c}{4\pi f}\right)^2 \left(\frac{1}{d_{PU,j}}\right)^l$ where c is the speed of light, f is the channel frequency, $d_{PU,j}$ is the distance between the PU and CR$_j$, and l is the path loss exponent.

For a complex valued Phase Shift Keying channel with circularly symmetric complex Gaussian noise, we calculate the required sensing time by CR$_j$ (τ_j) to achieve specified probability of detection (P^d) and probability of false alarm (P^f) as:

$$\tau_j = \frac{\left(\mathcal{Q}^{-1}(P^f) - \mathcal{Q}^{-1}(P^d)\sqrt{2\gamma_j + 1}\right)^2}{f_s \gamma_j^2} \tag{1}$$

where $\mathcal{Q}$ is the complementary cumulative distribution of standard Gaussian and f_s is the sampling frequency [12].

B. Frame Structure

We propose a cooperation scheme that follows the steps in Fig. 2 where each frame is divided into time intervals. At the beginning of the frame (T^{req}), the candidate transmitter CR (CR$_i$) sends a packet and asks for cooperation of the selected CRs, that is denoted by $\mathcal{N}^{req}$. These requested CRs (CR$_j$s) may perform sensing for CR$_i$ based on the $p_{i,j}$ values. The second part of the frame (T^s) is dedicated to CRs that decide to cooperate with CR$_i$, denoted by $\mathcal{N}_k^{req}$. Obviously, $\mathcal{N}_k^{req} \subseteq \mathcal{N}^{req}$, but not necessarily equal to $\mathcal{N}^{req}$. After all cooperating CRs complete sensing, each CR sends its hard decision to CR$_i$ in a time-sharing manner in the reporting period (T^{rep}). CR$_i$ fuses reported sensing outcomes using OR

[1] Even though CRs are assumed to be stationary for the tractability of our analysis, our proposal also works with mobile CRs.

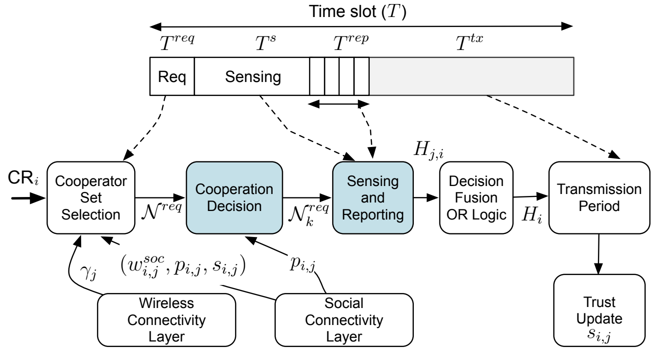


Fig. 2: Steps of the proposed sensing scheme and corresponding time period for each step in the frame structure. Steps in shaded boxes are performed by the requested CR, CR$_j$.

rule. Depending on the final decision, CR$_i$ transmits its data during the transmission period (T^{tx}) if the channel is decided to be vacant. If the fusion decision declares that the PU channel is busy, CR$_i$ stays silent till the beginning of the next frame. Below we discuss the details of each period.

- T^{req}: The requesting period is of fixed length as it is a single packet transmission that specifies which CRs are asked to cooperate. $\mathcal{N}^{req}$ may not include CR$_i$ itself if the required sensing time for CR$_i$ is too long.
- T^{s}: For the sake of simplicity, we assume that the required sensing reliability (i.e., P^d and P^f values) for each cooperating CR is identical and fixed. Given these constant P^d and P^f values, T^s equals to:
$$T^s = \max_{CR_j \in \mathcal{N}^{req}} \{\tau_j\} \tag{2}$$
where τ_j values are calculated as in (1). T^s equals to the maximum sensing time of the CRs in the requested set. However, that maximum may not be realized as CR$_j \in \mathcal{N}^{req}$ with the largest τ_j may not sense, i.e., CR$_j \notin \mathcal{N}_k^{req}$.
- T^{rep}: If we assume that a single time slot for reporting takes t^{rep}, the total required duration for reporting is:
$$T^{rep} = |\mathcal{N}^{req} \setminus \text{CR}_i| t^{rep}. \tag{3}$$
In (3), we exclude CR$_i$ from the reporting set as it does not send a report packet to itself. The size of this modified set is the maximum number of CRs that may send a report packet. Furthermore, during the slots assigned to non-cooperating CRs, CR$_i$ listens idly as it cannot know the set of sensing CRs in advance.
- T^{tx}: If CR$_i$ decides that the channel is vacant, this time period is used for transmission. Otherwise, CR$_i$ switches to a low power mode to save energy until the next frame. Let T be the length of the whole frame, then T^{tx} is:
$$T^{tx} = T - (T^{req} + T^s + T^{rep}). \tag{4}$$
Since the cooperative detection and false alarm probabilities are not known in advance due to the probabilistic nature of cooperation, their realizations may not satisfy the threshold values. Among these two criteria, we believe the detection probability is more crucial as it is for PU protection whereas false alarm probability only affects the CRN efficiency. Therefore, we forbid a CR to access the channel if the detection probability constraint is not satisfied, even if the channel is considered to be vacant.

C. Trust Metric for Sensing Accuracy Assessment

In our model, each CR tracks the performance of other CRs. We define $s_{i,j}$ as the trust of CR$_i$ for CR$_j$, which measures how accurately CR$_j$ performs sensing when requested by CR$_i$. Thus, it is a sensing reliability metric. To measure the trust, we employ a window based approach where CR$_i$ stores the evaluations regarding the last K sensing performance of CR$_j$. Let $o_{i,j,k}$ denote the kth sensing evaluation of CR$_j$ by CR$_i$. Furthermore, let $H_{j,i}$, H_i, and H be the CR$_j$'s sensing outcome, the final decision of CR$_i$ after fusing the sensing outcomes, and the PU channel's actual occupancy state, respectively. If $H_{j,i}$ is believed to be correct (false), $o_{i,j,k}$ gets the value 1 (-1). Let us focus on a single interaction between these two CRs. For OR decision fusion, six cases to consider depending on $H_{j,i}$, H_i, and H are listed in Table I.

TABLE I: Cases for sensing accuracy evaluation.

Case	$H_{j,i}$	H_i	H	Action
Case 1	0	0	0	Channel access, success
Case 2	0	1	0	No access
Case 3	1	1	0	No access
Case 4	0	0	1	Channel access, collision
Case 5	0	1	1	No access
Case 6	1	1	1	No access

Cases 1 and 4 are easy to evaluate as in both cases CR$_i$ accesses the channel and observes the ground truth. In Case 1, the transmission of CR$_i$ succeeds. Hence, CR$_i$ concludes that $H_{j,i}$ is correct, resulting in $o_{i,j,k} = 1$. On the other hand, CR$_i$ collides with the incumbent PU in Case 4. Thus, CR$_i$ concludes that $H_{j,i}$ is erroneous and sets $o_{i,j,k} = -1$. For the remaining cases, the evaluation is not straightforward since CR$_i$ does not access the channel. For these cases, we compare the decision of CR$_j$ with the majority decision of the cooperating CRs. If CR$_j$'s decision complies with the majority, it is assumed to be correct. Otherwise, it is considered as incorrect. In case of a tie where the number of cooperators is even (equal number of 0s and 1s), we break the tie by favouring the set with the higher total trust.

As the interactions are evaluated, CR$_i$ gets a sense of the reliability of other CRs. We calculate $s_{i,j}$ by using these observations. To account for a possible trend, we emphasize the recent observations. Assume the observations from $o_{i,j,1}$ to $o_{i,j,\lfloor \beta K \rfloor}$ are the most recent ones where $0 \leq \beta \leq 1$ is a system parameter denoting the percentage of observations that are considered recent. We calculate the trust value of CR$_i$ for CR$_j$ as:

$$s_{i,j} = \alpha \frac{\sum_{k=1}^{\lfloor \beta K \rfloor} o_{i,j,k}}{\lfloor \beta K \rfloor} + (1-\alpha) \frac{\sum_{\lfloor \beta K \rfloor + 1}^{K} o_{i,j,k}}{K - \lfloor \beta K \rfloor}$$

where $0 \leq \alpha \leq 1$ is the weight of recent observations. Hence, $s_{i,j}$ is a value between -1 and 1, that measures the sensing accuracy of CR$_j$ from CR$_i$'s viewpoint.

D. Social-aware Cooperative Sensing Accuracy

Let $P^{d,soc}_{\mathcal{N}^{req}}$ denote the *social-aware probability of detection* and $P^{f,soc}_{\mathcal{N}^{req}}$ denote the *social-aware probability of false alarm* of our social-aware CSS. Since a requested CR cooperates with the requester probabilistically (i.e., $p_{i,j}$), these probabilities are difficult to compute compared to traditional CSS. In the following, we present how we calculate the expected values of $P^{d,soc}_{\mathcal{N}^{req}}$ and $P^{f,soc}_{\mathcal{N}^{req}}$.

Let $\mathcal{P}(\mathcal{N}^{req})$ be the power set of $\mathcal{N}^{req}$. If we consider a subset of $\mathcal{N}^{req}$, say $\mathcal{N}^{req}_k \in \mathcal{P}(\mathcal{N}^{req})$, the probability that the realized sensing set be $\mathcal{N}^{req}_k$ (i.e. only the CRs in $\mathcal{N}^{req}_k$ sense the channel) is:

$$P(\mathcal{N}^{req}_k) = \prod_{\text{CR}_j \in \mathcal{N}^{req}_k} p_{i,j} \prod_{\text{CR}_m \in \mathcal{N}^{req} \setminus \mathcal{N}^{req}_k} (1-p_{i,m}).$$

Considering the OR rule, the probability of detection and false alarm for $\mathcal{N}^{req}_k$ are calculated as:

$$P^d(\mathcal{N}^{req}_k) = 1 - (1 - P^d)^{|\mathcal{N}^{req}_k|}.$$

$$P^f(\mathcal{N}^{req}_k) = 1 - (1 - P^f)^{|\mathcal{N}^{req}_k|}.$$

Then, the expected probability of detection for $\mathcal{N}^{req}$ is:

$$P^{d,soc}_{\mathcal{N}^{req}} = E[P^d_{\mathcal{N}^{req}}] = \sum_{\mathcal{N}^{req}_k \in \mathcal{P}(\mathcal{N}^{req})} P(\mathcal{N}^{req}_k) P^d(\mathcal{N}^{req}_k).$$

Similarly, we calculate $P^{f,soc}_{\mathcal{N}^{req}}$ as follows:

$$P^{f,soc}_{\mathcal{N}^{req}} = E[P^f_{\mathcal{N}^{req}}] = \sum_{\mathcal{N}^{req}_k \in \mathcal{P}(\mathcal{N}^{req})} P(\mathcal{N}^{req}_k) P^f(\mathcal{N}^{req}_k). \quad (5)$$

For legitimate operation, PU detection probability is crucial and has to be kept equal or above a recommended level, e.g., 0.9 according to IEEE 802.22. CR$_i$ determines its cooperation set $\mathcal{N}^{req}$ such that the expected detection probability meets the threshold. However, as some of the CRs may not participate in sensing, the realized detection probability achieved by $\mathcal{N}^{req}_k$ may be lower than the required PU detection accuracy. If that is the case, we forbid a CR to access the channel whatever the final sensing decision is.

We list the practical issues regarding calculation of $P^{d,soc}_{\mathcal{N}^{req}}$ and $P^{f,soc}_{\mathcal{N}^{req}}$ as follows:

- *Unknown $p_{i,j}$ values:* Exact $p_{i,j}$ values may not be available to CR$_i$. For such a setting, CR$_i$ can estimate $p_{i,j}$, say $\tilde{p}_{i,j}$, based on its interactions with CR$_j$. Consequently, CR$_i$ calculates $P^{d,soc}_{\mathcal{N}^{req}}$ and $P^{f,soc}_{\mathcal{N}^{req}}$ using $\tilde{p}_{i,j}$ instead of $p_{i,j}$.
- *Large neighborhood:* The number of one hop neighbors of CR$_i$ may be large. Hence, selecting $\mathcal{N}^{req}$ takes considerable time with the exponential growth of the number of subsets. Then, CR$_i$ first eliminates some candidate CRs according to for example γ_j, $p_{i,j}$ or a combination, e.g., CRs with the highest $\gamma_j p_{i,j}$ can be selected as candidates for $\mathcal{N}^{req}$.

III. Cooperator Set Selection

In our model, a CR desires to attain high throughput and cooperate with the CRs that it trusts. Below, we present these two objectives.

Throughput (C): Assume that each CR always has packets to transmit. Hence, a CR transmits for T^{tx} time units whenever it detects an idle channel successfully. In case of a false alarm or detection of the PU, CR keeps silent for T^{tx}.

Let us define our binary optimization variable x_j as:

$$x_j = \begin{cases} 1, \text{if CR}_i \text{ asks the cooperation of CR}_j \\ 0, \text{otherwise.} \end{cases}$$

For a particular assignment vector $\mathbf{x} = [x_j]$, we calculate $P^{f,soc}$ as follows:

$$P^{f,soc} = \sum_{\substack{\mathcal{N}^{req} \\ \in \mathcal{P}(N)}} P^{f,soc}(\mathcal{N}^{req}) \left[\prod_{j \in \mathcal{N}^{req}} x_j \prod_{k \notin \mathcal{N}^{req}} (1-x_k) \right].$$

The multiplicative term takes the value 1 only for the set of CRs such that $x_j = 1$. For $\mathbf{x}$, the expected throughput over the channel with Shannon capacity R bits/sec is:

$$C = (1 - P^{on})(1 - P^{f,soc}) R T^{tx}. \quad (6)$$

Trust (S): CR$_i$ desires to cooperate with the CRs towards which it has high trust values (i.e. more accurate sensing results). Hence, our second objective maximizes the minimum expected trust value of the cooperators that is expressed as:

$$S = \min\{(x_j p_{i,j} s_{i,j}) + (1 - x_j)\}. \quad (7)$$

In (7), $p_{i,j} s_{i,j}$ is the expected trust obtained from CR$_j$ if it is selected for cooperation ($x_j = 1$). The second term covers the case of unselected CRs ($x_j = 0$) to have the minimum value only occur in the set of selected CRs.

A. Problem Formulation

Given (6) and (7), we model the cooperator set selection problem as a Multi-objective Optimization Problem (MOP) [13]. In a MOP with conflicting objectives, the system has a trade-off point after which one objective can only be improved at the expense of the other. A solution is said to *dominate* another solution iff it is strictly better in at least one objective, and not worse in the remaining ones. The set of non-dominated solutions is called the *Pareto front* and the best operating point can be determined by the decision maker according to the importance of the objectives from the decision maker's perspective. We can identify $\mathcal{N}^{req}$ in terms of $\mathbf{x} = [x_j]$ as follows: $\mathcal{N}^{req} = \{CR_j, x_j = 1\}$. Then, our

MOP formulation for determining $\mathbf{x} = [x_j]$ is:

$$\textbf{Pareto-max}: \begin{cases} C{=}(1-P^{on})(1-P^{f,soc})RT^{tx} \\ S{=}\min\{(x_j p_{i,j} s_{i,j}) + (1-x_j)\} \end{cases} \quad \text{s.t.}$$

$$T^{tx}{=}T - \left(T^{req}{+}T^{s}{+}t^{rep} \sum_{j=1, j\neq i}^{N} x_j \right) \tag{8}$$

$$T^{tx} \geq 0 \tag{9}$$

$$T^{s} \geq \tau_j x_j \quad \forall j \tag{10}$$

$$P^{d,soc} \geq 0.9 \tag{11}$$

$$P^{f,soc} \leq 0.1 \tag{12}$$

$$P^{d,soc}{=} \sum_{\substack{\mathcal{N}^{req} \\ \in \mathcal{P}(N)}} P^{d,soc}(\mathcal{N}^{req}) \left[\prod_{j \in \mathcal{N}^{req}} x_j \prod_{k \notin \mathcal{N}^{req}} (1{-}x_k) \right] \tag{13}$$

$$P^{f,soc}{=} \sum_{\substack{\mathcal{N}^{req} \\ \in \mathcal{P}(N)}} P^{f,soc}(\mathcal{N}^{req}) \left[\prod_{j \in \mathcal{N}^{req}} x_j \prod_{k \notin \mathcal{N}^{req}} (1{-}x_k) \right] \tag{14}$$

$$x_j \in \{0,1\} \quad \forall j. \tag{15}$$

Const.(8) defines the value of T^{tx}. The summation $\sum_{j=1,j\neq i}^{N} x_j$ is maximum number of sensing results CR$_i$ may get from others, which equals to the number of TDMA slots CR$_i$ has to allocate. (9) states that remaining time for transmission cannot be negative, and (10) sets T^s to the maximum τ_j value of the requested CRs. (11) and (12) ensure that the selected set's expected detection and false alarm values meet the sensing requirements. We set a minimum detection probability of 0.9, and a maximum false alarm probability of 0.1. (13) and (14) define the social-aware detection and false alarm probabilities, respectively. Finally, (15) states that the variables are binary.

In the next section, we present our solution for the above problem, which finds T^{tx},T^{s}, and $\mathcal{N}^{req}$.

IV. EMOA: Evolutionary Multi-objective Optimization Algorithm

As our model is a binary integer nonlinear problem that is neither convex nor concave and difficult to solve in general, we resort to evolutionary multi-objective optimization algorithm (EMOA) [13] for its solution. EMOA stores a set of solutions referred to as *population* and each solution represents an individual of the population. The individuals in one generation mate to produce an offspring and each offspring experiences mutation with probability p_m. Next generation is composed of the generated offspring and a subset of the current population. The individuals are selected based on their *fitness* values. Below, we explain the steps of EMOA in Alg. 1.

Encoding scheme: We represent each solution as an N-bit string. The value of n^{th} bit denotes whether CR_i requests sensing from CR_n (i.e., $x_n = 1$ means CR_i asks for cooperation from CR_n). We should emphasize that this request does not necessarily imply that CR_n actually senses the channel.

Algorithm 1 EMOA

```
$iterNo = 0$
Generate the initial population, $\mathcal{B}_0$ =INITIALIZE($\mathcal{B}_0$)
**while** $iterNo < maxIter$ **do**
    Initialize the current offspring population, $\mathcal{C}_t = \emptyset$
    **while** $|\mathcal{C}_t| < C_{size}$ **do**
        Select first parent, $b_1$ =BINARYTOUR($\mathcal{B}_t$)
        Select second parent, $b_2$ =BINARYTOUR($\mathcal{B}_t$)
        Generate children, $c_1, c_2$ =CROSSOVER($b_1\ b_2$)
        Mutate children with probability $p_m$,
        $c_1$ =MUTATION($c_1$) and $c_2$ =MUTATION($c_2$)
        $\mathcal{C}_t = \mathcal{C}_t \cup c_1 \cup c_2$
    Select next generation, $\mathcal{B}_{t+1}$=SELECT($\mathcal{B}_t \cup \mathcal{C}_t$)
    $iterNo = iterNo + 1$
Select final solution, $b_{final}$ =FINALSELECT($\mathcal{B}_t$)
```

Fitness function: Fitness function represents the goodness of a solution and it is calculated based on the concept of *constrained domination*. In a constrained MOP, a solution u is said to constrained dominate another solution v if and only if: (i) both solutions are feasible and u dominates v in both objective values, or (ii) u is feasible whereas v is not, or (iii) both solutions are infeasible and the total constraint violation of u is smaller than v. In our model, (9), (11), and (12) are the critical constraints. As negative transmission time is not tolerable, we set the fitness value to $-\infty$ of the solution that violates (9). Otherwise, we calculate both objective values and the total violation regarding (11) and (12) related to a solution. Then, we calculate each solution's rank by simply counting the number of other solutions that constrained dominate this solution. Finally, the fitness of the individual equals to the difference between the number of individuals in the population and the rank of the current individual. As non-dominated solutions have rank 0, their fitness values are equal to the size of the population.

INITIALIZE: We generate the initial population of size B_{size} by randomly assigning 0 or 1 to each bit of the solution.

BINARYTOUR: To select a parent, we choose two candidate solutions using *roulette wheel selection*. Although roulette wheel selection picks the candidate solutions randomly, individuals with better fitness values are more likely to be selected. We choose the solution with better fitness value as the first parent (*binary tournament*) out of these two candidates with breaking ties arbitrarily. The other parent is selected similarly.

CROSSOVER: Crossover operation is the mating of two solutions to produce children. In our implementation, two parents mate to generate two offspring. To mate the selected parents, we employ uniform crossover strategy, which selects the i^{th} bit from a parent randomly. Since we generate two children from the parents, the i^{th} bit of the first children is obtained from a randomly selected parent and the second children gets the i^{th} bit of the other parent.

MUTATION: With probability p_m, each generated child is mutated, i.e., the value of a randomly selected position in the bit string of the individual is flipped.

SELECT: After generating the offspring population, we add them to the current population and select the best ones to form the next generation. We use two criteria for selection: *non-domination level* and its *crowding distance*. Non-domination level of a solution represents which front the solution belongs to. Non-dominated solutions with rank 0 constitute the first Pareto front, $\mathcal{I}^1$. Solutions that are only dominated by the solutions in $\mathcal{I}^1$ constitute the second Pareto front, $\mathcal{I}^2$, so on. We employ fast non-dominating sorting for finding the Pareto fronts [14]. Next, we assign crowding distances to all solutions grouped by their Pareto front. The crowding distance, denoted by d, is a measure of diversity that shows how far a given solution is from its closest (i.e., two neighboring) solutions in the same Pareto front in the objective space [15]. A solution u is considered to be better than another solution v if $u.rank < v.rank$ or $(u.rank = v.rank \land u.d > v.d)$. By using this partial ordering, we select the best B_{size} solutions to populate the next generation, $\mathcal{B}_{t+1}$.

FINALSELECT: After $maxIter$ iterations, EMOA generates the first Pareto front. We choose the solution with the largest hypervolume [16] as the final solution among the non-extremal (inner) solutions on the Pareto front. With this choice, we aim to maintain a desirable trade-off between the two objectives.

The running time complexity of the algorithm is dominated by SELECT operation. The worst case complexity of this statement when using fast non-dominating sorting is equal to $O(2B_{size}^2 2^N)$ where 2 is the number of objectives [14] and 2^N term is due to the evaluation of subsets for calculating $P^{d,soc}$ and $P^{f,soc}$. Then, the overall complexity of the algorithm is given by $O(2B_{size}^2 2^N maxIter)$. The exponential term does not constitute a problem as long as N is small ($\leq$ 10). For large values of N, the elimination procedure discussed in Section II-D should be employed to keep N small.

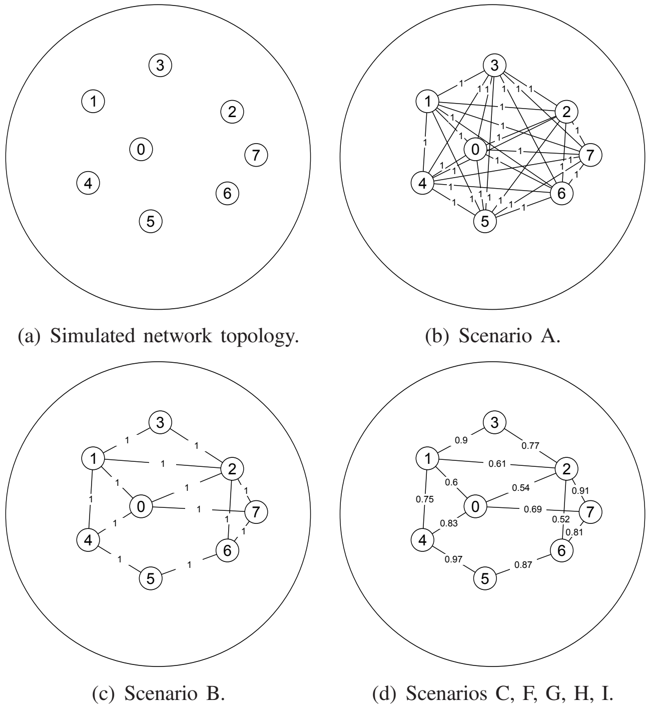
V. Numerical Analysis

In this section, we present the performance of our proposal that is obtained from experiments on our Java simulator. We aim to cover a wide range of realistic scenarios by considering various models for $p_{i,j}$. For each scenario, we compare EMOA with the expected throughput-optimal (EXP-THR-OPT) scheme that only maximizes the expected throughput without considering the trust objective. EXP-THR-OPT is found by implicit enumeration of all possible solutions. However, it becomes impossible to find even for moderate values of N due to the combinatorial nature of the problem.

We analyze a network as shown in Fig. 3(a) with eight stationary CRs and a single mobile PU. Our choice of this small network is intentional as we aim to provide insights on the operation of social-aware cooperative sensing rather than elaborating on the complexities of large-scale scenario, i.e., probabilistic nature of the problem is affected not only by social ties but also by parameters such as node locations.

As performance criteria, we concentrate on the following three metrics:

- *Realized throughput*, which occurs if the channel is vacant, and the CRs observed it as vacant, and the detection probability constraint is satisfied. When all three conditions are satisfied, the realized throughput is calculated as RT^{tx}, otherwise it is 0.
- *Missed opportunity ratio*: the ratio of *lost* vacant frames (i.e., CR does not access the channel although there is no PU traffic) to the total number of vacant frames.
- *Collision probability*: the probability that a CR accessing the channel collides with an active PU.



(a) Simulated network topology.

(b) Scenario A.

(c) Scenario B.

(d) Scenarios C, F, G, H, I.

Fig. 3: (a) Physical location of CRs (b,c,d) Social graphs used for scenarios. Edge labels denote $w_{i,j}^{soc}$.

The presented results are the average of ten runs. Table II lists the parameters of our experiments. Although the discussions we present are for the considered small network, our observations are still valid in general since a computationally efficient algorithm should work on a small set of nodes by first applying an elimination procedure to reduce the number of candidates, and then, selecting the cooperators from this smaller set.

In Fig. 3, we present the considered social graphs. An edge connecting two CRs implies that the corresponding CRs are socially tied to each other where the strength of the social tie ($w_{i,j}^{soc}$) is shown on the connecting edge. We assume that the $w_{i,j}^{soc}$ values are between 0 and 1. If that is not the case (e.g. social tie is equal to the number of mutual friends), they can still be mapped onto [0,1] interval by using some appropriate normalization (e.g. the ratio of mutual friends to total number of friends). In our network, the social ties are symmetrical but the model can also handle asymmetric values. For all scenarios, we indicate the used $p_{i,j}$ values.

TABLE II: Simulation parameters.

Parameter	**Value**
Cell radius	400 m
P^{on} (Probability of PU being active)	0.2
N (Number of CRs)	8
f_s (Sampling rate)	1 kHz
P_{PU}^{tx} (PU transmission power)	1000 mW
N_{th} (Noise floor)	-105 dB
l (Path loss exponent)	3
f (Channel frequency)	800 MHz
T (Frame length)	200 ms
T^{req} (Length of the requesting period)	5 ms
t^{rep} (Length of a single reporting slot)	5 ms
R (Channel bit rate)	10 Mbps
G_{PU} (Antenna gain of PU)	0 dB
G_j $\forall j$ (Antenna gain of CR$_j$)	0 dB
P^d (Required individual detection prob.)	0.7
P^f (Required individual false alarm prob.)	0.02
K (Window size for trust observations)	10
β (Fraction of recent observations)	0.5
α (Weight of recent observations)	0.7
Simulation length/warmup period	16000/4000 frame
EMOA parameters	
B_{size},O_{size} (Population/Offspring pop. size)	100, 20
p_m (Mutation probability)	0.05
t_{max} (Number of iterations)	100

- **Scenario A**: In this scenario, depicted in Fig. 3(b), the social graph is complete, and all the social ties are equal to 1. Hence, this scenario corresponds to the traditional sensing where CR$_j$ always senses for CR$_i$. We set $p_{i,j} = w_{i,j}^{soc} = 1 \quad \forall i, j$.
- **Scenario B**: This scenario shown in Fig. 3(c) represents the case of binary social ties which implies that not all CRs are socially connected. Furthermore, the number of connected nodes for each CR differs. For instance, CR$_0$ has a large number of neighbors, whereas CR$_3$ does not. We set $p_{i,j} = w_{i,j}^{soc}$ and $w_{i,j}^{soc} \in \{0, 1\} \quad \forall i, j$.
- **Scenario C**: This scenario shown in Fig. 3(d) is based on the previous one with a slight difference on $w_{i,j}^{soc}$ values. Here, $p_{i,j}$ is set as $p_{i,j} = w_{i,j}^{soc}$ and $w_{i,j}^{soc} \in [0, 1] \quad \forall i, j$.
- **Scenario D**: In this scenario, CR$_j$ determines its cooperation probability based on how much it has already contributed to the whole CRN, rather than deciding based on its social ties. Let us define *system willingness* (w_j^{sys}) for CR$_j$ as:

$$w_j^{sys} = 1 - \frac{\text{\# of accepted requests for other CRs}}{\text{\# of received requests from other CRs}}.$$

The second term of this equation is the ratio of accepted requests from other CRs, which can be interpreted as the system burden on CR$_j$. Thus, w_j^{sys} is inversely related to the burden put on CR$_j$. This setting may correspond to the case of an environment which is new to a CR (e.g., different than home network) where the CR does not have any social ties, or the case of bootstrapping the network. Hence, cooperation is still possible among the CRs but is restricted by w_j^{sys} parameter. That is, w_j^{sys} enables cooperation among CRs in the lack of social ties while at the same time it prevents exploitation of each CR by excessive sensing. In our setting, w_j^{sys} is a function of ratio of satisfied requests but it may also depend on internal state of a CR such as battery level. In this scenario, $p_{i,j} = w_j^{sys}$.

- **Scenario E**: Similar to the system willingness, let us define *peer willingness* as:

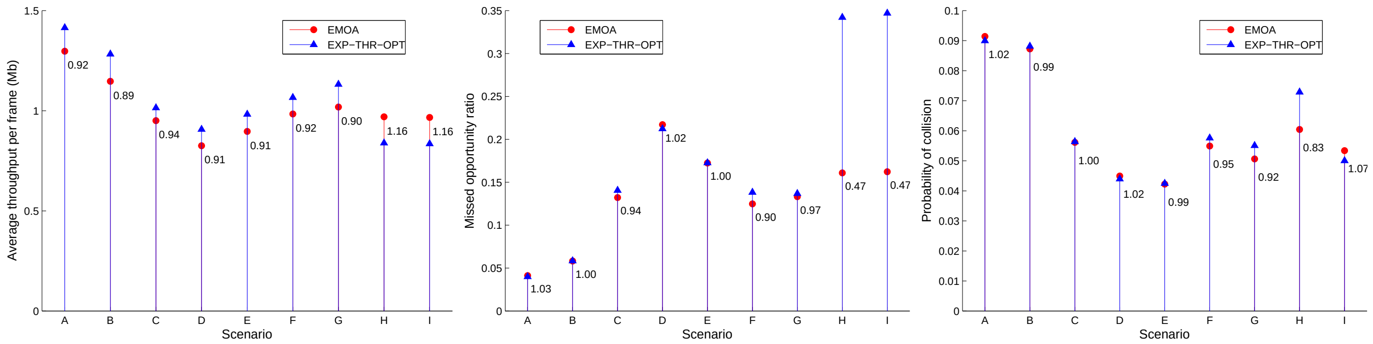
$$w_{i,j}^{peer} = 1 - \frac{\text{\# of accepted requests by CR}_j \text{ for CR}_i}{\text{\# of received requests by CR}_j \text{ from CR}_i}.$$

In other words, $w_{i,j}^{peer}$ is inversely proportional to the burden put on CR$_j$ by CR$_i$. Similar to the social tie concept, peer willingness takes one to one relations between CRs into account. However, contrary to the social tie, peer willingness dynamically evolves with time. This scenario may cover cases where CRs do not restrict total number of cooperations but want to avoid exploitation by a specific CR. In this scenario, $p_{i,j} = w_{i,j}^{peer}$.

- **Scenario F**: This case is a combination of system willingness concept with the social ties used in Scenario C. We set $p_{i,j}$ as $p_{i,j} = \max\{w_j^{sys}, w_{i,j}^{soc}\}$ for encouraging more cooperation.
- **Scenario G**: Similar to Scenario F, we define $p_{i,j}$ as the combination of system willingness, peer willingness, and social ties: $p_{i,j} = \max\{w_j^{sys}, w_{i,j}^{peer}, w_{i,j}^{soc}\}$.
- **Scenario H**: This scenario is based on Scenario F. Now, CR$_0$ is a malicious node performing spectrum sensing data falsification (SSDF) attack to the network [3]. In this type of attack, the malicious CR performs sensing, but reports the reverse of its sensing result to degrade the environmental awareness of CR$_i$. Hence, CR$_0$ always reports the inverse of its sensing result to other CRs. We select CR$_0$ as the malicious user to analyze as a worst case due to its central location and high number of social ties.
- **Scenario I**: This final scenario is very similar to Scenario H. The only difference is that CR$_0$ now always reports the existence of PU when it senses for other CRs. Similar to *PU emulation (PUE) attack*, this scenario may represent the case where a selfish CR desires to use the spectrum itself by making others believe that spectrum is occupied.

Fig. 4 depicts the performance of EMOA and EXP-THR-OPT for all scenarios. In each of these figures, numbers on the lines mark the ratio of the performance achieved by EMOA to the one achieved by EXP-THR-OPT. From Fig. 4(a), we observe that EMOA maintains near-optimal throughput. Specifically, EMOA achieves at least 89% of the throughput of EXP-THR-OPT. Furthermore, we observe that EMOA outperforms EXP-THR-OPT under malicious user cases (Scenarios H and I) and provides a relatively stable operation. The throughput reduction of EXP-THR-OPT between Scenarios F and H is 21% whereas it is 1.5% for EMOA. As EMOA tradeoffs from throughput for maintaining high trust objective, it achieves 90% of the EXP-THR-OPT in terms of throughput when there are no malicious users.

Comparing different scenarios, we observe that the realized throughput decreases with decreasing $p_{i,j}$ values. For instance, maximum throughput is achieved in Scenario A (where all $p_{i,j} = 1$) and going from Scenario A to Scenario F causes a 25% decrease for both methods. We attribute this effect to the restriction on PU detection accuracy. That is, when expected $P^{d,soc}$ is below 0.9, CRs are forbidden to access the channel.



(a) Throughput. (b) Missed opportunity ratio. (c) Probability of collision.

Fig. 4: Performance evaluation for different scenarios.

In scenarios with low $p_{i,j}$ values, sensing is performed with low number of cooperators which may lead to low $P^{d,soc}$. The implication of this behavior (i.e., high $p_{i,j}$ resulting in high throughput) is twofold. First, we can argue that the high performance of Scenario A compared with others, say Scenario C, may lead to over-estimation of the network throughput if social behavior of CRs are neglected. For example, a CRN would be expected to provide throughput as in Scenario A although only about 72% of that value (Scenario C) would be achieved. This substantial difference between the expected and the realized capacity is critical especially for services that require certain capacity guarantees. Second, it may indicate that CRs benefit from being social. Hence, they have the incentive to be social and cooperative.

Fig. 4(b) shows the missed opportunity ratio. We should recall that an opportunity is missed either due to a false alarm or due to low detection probability. Hence, it reflects the throughput loss more than just the false alarm. For the scenarios under legitimate operation (scenarios excluding the attacks), we see that high $p_{i,j}$ values result in more aggressive channel usage thereby resulting in low missed opportunity ratio. On the other hand, EXP-THR-OPT wastes almost one third of the frames in case of an attack. As seen already in Fig. 4(a), EMOA provides robust operation also in terms of missed opportunity ratio. The increase in missed opportunities between Scenarios F and H is 29% and 147% for EMOA and EXP-THR-OPT, respectively.

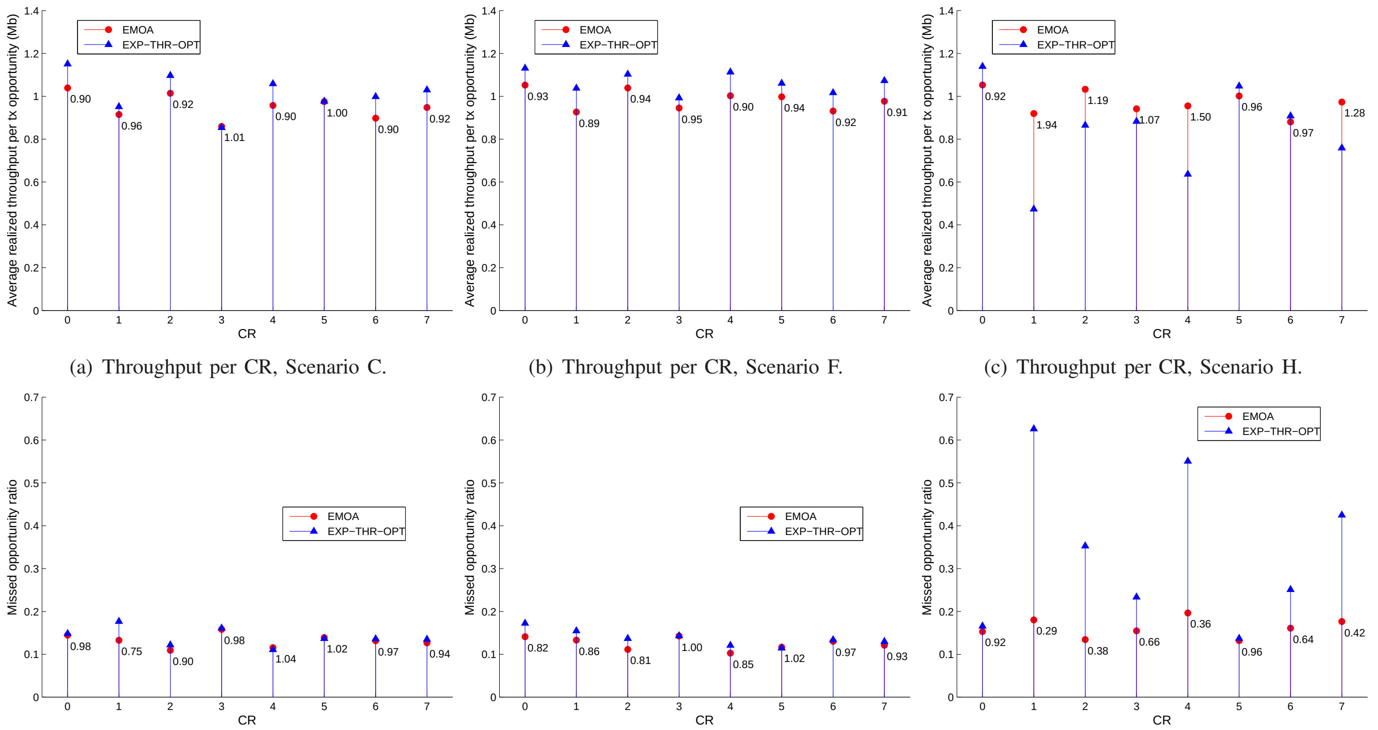
We can observe similar behavior in terms of collision probability, as shown in Fig. 4(c). Aggressive channel access (high $p_{i,j}$) causes more collisions. However, all of the values are within the tolerable limits (i.e., below 0.10 corresponding to tolerable misdetection probability) as our scheme prevents CRs from accessing the channel without a satisfactory detection probability. The increase for Scenario H (where CR$_0$ reports 0 when it senses and PU is active) compared to Scenario F is still within the limits due to the low P^{on} value. For a PU channel with higher PU traffic (i.e., higher P^{on}), this aggressive access may lead to harmful interference to the PU. However, as CRNs aim to operate on PU channels with low P^{on}, we do not provide additional interference avoidance mechanisms to our solution. Scenario I shows a decrease in collision probability as this time CR$_0$ always reports 1 regardless of the actual PU state, which results in less collisions at the expense of very high missed opportunity ratio as depicted in Fig. 4(b).

In Fig. 5, we show the individual performances of CRs in terms of throughput and missed opportunities for selected scenarios: Scenario C, F, and H. With this analysis, we aim to gain insights to the following aspects: (i) how each CR's performance differs depending on its social ties, (ii) whether the performance gap between EMOA and EXP-THR-OPT for a specific CR depends on its social properties, and (iii) whether some CRs, e.g., CRs with low social connectivity, benefit from different $p_{i,j}$ models more than the others. For (i) and (ii), we focus on a single scenario whereas for (iii) we compare different scenarios.

Fig. 6 summarizes the social ties associated with each CR. For CR$_i$, *node degree* denoted by n_i is the number of directly connected nodes; *aggregate social tie* denoted by δ_i is the sum of $w_{i,j}^{soc}$ across all links of CR$_i$; and *average social tie* denoted by $\tilde{\delta}_i$ is the ratio of aggregate social tie to the node degree, i.e., $\tilde{\delta}_i = \delta_i / n_i$. For Scenario C in which only social ties are considered for cooperation, we observe that CRs with low δ_i and n_i, e.g., CR$_3$ and CR$_5$, have the lowest throughput. However, we should note that the throughput depends on both the social ties in the SCL, $P^{f,soc}$ in (6), and sensing time in WCL, T^{tx} in (6). Since we fix required sensing accuracy for each cooperating CR, $P^{f,soc}$ depends only on number of cooperators (see (5)), whereas T^{tx} is also a function of the sensing time τ. Thus, the physical location of a CR as well as its neighbors determines the length of the sensing period and therefore T^{tx}.

We observe the effect of physical location in the diverging performance between CR$_1$ and CR$_0$. Although both have high δ_i and n_i, CR$_0$ has significantly higher throughput owing to its central location. The received PU signal has high SNR on average at this receiver which facilitates CR$_0$ to have a short sensing time, τ. Therefore, when it is CR$_0$'s turn to transmit, it can usually be one of the sensing CRs. This results in savings in terms of reporting time, which implies longer transmission time and thereby higher throughput.

While we observe some correlation between δ_i and throughput of a CR, we do not observe that between $\tilde{\delta}_i$ and throughput for our setting. We should also mention that these assessments may not be applicable for all network topologies. As a



(a) Throughput per CR, Scenario C.

(b) Throughput per CR, Scenario F.

(c) Throughput per CR, Scenario H.

(d) Missed opportunities per CR, Scenario C.

(e) Missed opportunities per CR, Scenario F.

(f) Missed opportunities per CR, Scenario H.

Fig. 5: Performance values per CR for selected scenarios.

TABLE III: Throughput decrease (%) in case of an SSDF attack (Scenarios F and H).

	CR$_1$	CR$_2$	CR$_3$	CR$_4$	CR$_5$	CR$_6$	CR$_7$
EMOA	1	1	1	4	0	5	0
EXP-THR-OPT	54	22	11	43	1	11	29

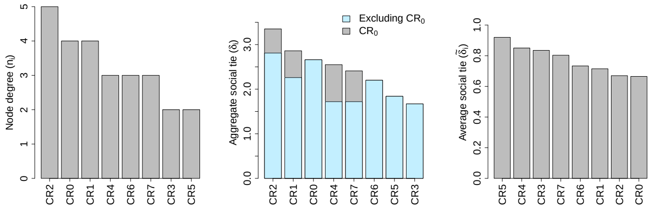
counterexample, consider a CR, say CR$_x$, with 100 neighbors within the communication range and connected to each one of them with weak social ties, say $w_{x,j}^{soc} = 0.25$. On the other hand, consider another CR, say CR$_y$, again with 100 neighbors. This time let us assume that CR$_y$ is strongly connected to only a few of its neighbors (assume $w_{y,j}^{soc} = 1$ for these neighbors) and very weakly connected to the remaining ones (assume $w_{y,j}^{soc} = 0.05$). Even though $\delta_x > \delta_y$ and $\tilde{\delta}_x > \tilde{\delta}_y$, the performance of CR$_y$ will be better as it can rely on its strongly tied neighbor for cooperation.

Regarding the performance gap between EMOA and EXP-THR-OPT, we observe that the performance gap approaches to 0 when n_i is low. This is expected as there are fewer options for both schemes and EMOA has higher likelihood of choosing cooperators as EXP-THR-OPT does. For example, in Scenario C, while EXP-THR-OPT achieves higher throughput for CRs with high n_i, both methods are almost the same for CRs with low n_i, CR$_3$ and CR$_5$. That means EMOA is almost as good as EXP-THR-OPT for CRs with low social ties.

Comparing Figs. 5(a), 5(b) and 5(c), we conclude that CR$_1$, CR$_3$ and CR$_5$ benefit most if system willingness is activated on top of social willingness – going from Scenario C to F. The increases for these nodes are 9%, 16% and 8% for EXP-THR-OPT, respectively. On the other hand, the gains for other CRs are marginal (below 5%). Hence, the system willingness concept benefits CRs with low n and δ most.

For the SSDF attack case (Scenario H), Table III lists the decrease in throughput for each CR compared to Scenario F for both methods. The trust objective used in EMOA minimizes the effects of the attack whereas EXP-THR-OPT fails avoiding the attacker, which results in significant throughput decrease. All CRs connected to CR$_0$ are affected by the attack: CR$_1$, CR$_2$, CR$_4$, and CR$_7$. Additionally, the throughput decrease is larger for those CRs that have few social ties excluding the tie with CR$_0$ (see Fig. 6(b)). For CR$_2$, the decrease is lower as EMOA selects more trustworthy neighbors that can meet the required $P^{d,soc}$ and $P^{f,soc}$ values. We attribute the throughput decrease for CR$_3$ and CR$_6$ – the nodes that are not connected to CR$_0$ directly– to the system willingness concept that encourages cooperation despite the lack of social ties between nodes. These CRs occasionally cooperate with CR$_0$, which degrades the sensing accuracy and in return leading to lower throughput. However, the decrease is smaller compared to CRs that have strong ties with CR$_0$. This side effect of system willingness stems from encouraging cooperation among weakly connected or not connected nodes. This attitude is more vulnerable to attacks and may cause larger number of CRs to be affected compared to cooperation among only strongly connected CRs. Finally, we should stress that EMOA achieves at least 90% of EXP-THR-OPT under normal operation, and performs significantly better for the attack scenario.

Figs. 5(d), 5(e), and 5(f) show the missed opportunity ratio for each CR. Regarding Scenario C, we observe that the missed opportunity ratios are very close to each other, within 0.05 range. Adding system willingness (Scenario F) decreases the missed opportunities in general as the number of possible cooperators increases. However, there is an increase for EXP-THR-OPT compared to Scenario C for CR_0, CR_2, and CR_4. Hence, we can state that CRs with large and/or strong social ties are adversely affected with more uncertainty in cooperation behavior for EXP-THR-OPT. For Scenario H, EMOA limits the missed opportunities to at most 20% for all CRs. On the contrary, EXP-THR-OPT causes intolerable missed opportunity ratios for CR_0's direct neighbors. Specifically, missed opportunity ratio is 0.35, 0.43, 0.55, and 0.63 for CR_2, CR_7, CR_4, and CR_1, respectively. That is to say, the CRs that are tied to the malicious CR starve without an attack avoidance mechanism. The trust objective in EMOA serves as an attack avoidance mechanism without bringing too much overhead.



(a) Node degree.

(b) Aggregate tie.

(c) Average tie.

Fig. 6: CR properties: node degree, aggregate social tie (with and excluding tie with CR_0), and average social tie. In the figures, CRs are sorted according to their property in decreasing order.

VI. Iterative Greedy Construction Heuristic for Multi-channel Cooperative Sensing

Due to the complexity of finding $P^{d,soc}$ and $P^{f,soc}$, EMOA becomes time consuming in case of high number of CRs or multiple primary channels. Hence, in this section we seek a lower complexity solution for such cases. As multi-channel cooperative sensing scheduling is a hard problem [17] even in a centralized setting, we devise an iterative greedy construction heuristic that assigns each channel to a dedicated transmitter and finds the set of cooperators for that transmitter.

Our assumptions are the same as before. If there are M channels, CRs $0, 1, \ldots, M-1$ are the dedicated transmitters for the first frame; CRs $M, M+1, \ldots, 2M-1$ are the transmitters for the second frame, etc. We assume that the first transmitter selects the channel for possible access among all channels and its cooperator(s) among all candidate CRs. Next, it broadcasts this information. Upon receiving the broadcast message, the second transmitter selects the channel and cooperator set among the set of remaining channels and CRs, respectively. This procedure repeats until all transmitters select some channel to sense as well as the cooperator sets. Hence, we assume a given CR can sense at most one channel for protocol simplicity. Moreover, we only employ the system willingness concept together with social ties (Scenario F) in this setting. All remaining scenarios can be utilized similarly.

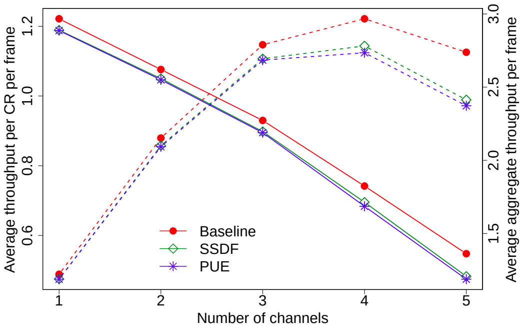


Fig. 7: Effect of increasing number of primary channels on throughput per CR (–) and aggregate throughput per time frame (- - -).

Below, we summarize the steps of channel and cooperator set selection:

1) Mark all channels and CRs as available, and all transmitters as unassigned, initially.
2) Starting with the first unassigned transmitter i, calculate utility of using CR_j for sensing available channel m as follows:
$$U_{i,j,m} = \begin{cases} \frac{1}{\tau_{m,i}}, \text{if } i = j \\ \frac{s_{i,j} \max\{w_j^{sys}, w_{i,j}^{soc}\}}{\tau_{m,j} + t^{rep}}, \text{otherwise} \end{cases}$$
where $\tau_{m,j}$ is the required sensing time for CR_j to achieve the desired P^d and P^f for channel m. The key rationale of utility design $U_{i,j,m}$ is to account for both the trust of the candidate CR as well as overheads due to sensing and reporting.
3) For each available channel, sort $U_{i,j,m}$ in descending order.
4) Starting with the highest $U_{i,j,m}$, mark CRs one by one as candidates for channel m until $P^{d,soc}$ and $P^{f,soc}$ constraints are satisfied.
5) Once all channels have their candidates assigned, select the channel with the highest total utility. Mark that channel and the candidate CRs as unavailable. Mark also the transmitter i as assigned. Go to Step 2.

We consider a network of 40 CRs that are uniformly distributed within the cell. Social ties are symmetric and assigned randomly. With 0.5 probability, the social tie between CR_i and CR_j is 0, whereas with 0.5 probability, it is uniformly random between 0.5 and 1. In case of M channels, we have M mobile PUs that are active with probability 0.5. All channels are identical and independent. All remaining parameters are the same. For malicious setting, we assign the first 5 CRs as SSDF or PUE attackers, respectively.

Fig. 7 plots the change in throughput with increasing number of channels for the baseline scenario (case of all legitimate CRs), SSDF and PUE attackers. We observe that average throughput per CR per frame decreases as the number of channels increases due to the non-scalable nature of the reporting mechanism. This issue is a well-known drawback of multi-channel operation [6]. As the number of reporters increases, there remains less time for transmission. On the other hand, average throughput per frame (total throughput of all CRs for the frame) initially increases thanks to higher number of simultaneous transmissions. However, it starts diminishing beyond a critical point (4 channels with the used parameters) as reporting takes much higher fraction of the total frame. Another point to note is the marginal decrease in throughput under malicious settings compared to the legitimate operation, which shows the robustness of the proposed method.

VII. Related Work

One key design issue related to CSS is to select the most informative nodes as well as filtering redundant information to avoid the overhead. Cacciapuoti *et al.* [4] decrease sensing redundancy by exploiting the correlations among CRs, and selecting the spatially uncorrelated ones. CR reliability should also be accounted for avoiding (intentional or unintentional) erroneous sensing reports [18]. Zeng *et al.* [19] reduce cooperation with misbehaving CRs by tracking their reputation that reflects the consistency of each CR's decision with the global network decision. Similarly, we track the reputation of CRs via recording the sensing consistency of each cooperating CR. Moreover, we account for the probabilistic nature of sensing and avoid CRs who are not very cooperative. Since lack of adequate number of cooperators results in violation of PU detection requirements, avoiding non-cooperative CRs is also vital. Kaligineedi *et al.* [20] apply outlier detection mechanisms for detecting the malicious CRs whose measurements are expected to diverge from measurements of other cooperating CRs. Our work differs from [20] as our CR reliability assessment scheme does not rely on any sensing method (e.g., energy detection [18]) whereas [20] utilizes the energy levels reported by the CRs.

Social networking perspective is not a new idea (e.g.,[21]) but has attracted relatively low interest in CR research. Simply, this approach is based on the idea that nodes have unique characteristics in terms of their interactions with other nodes or their properties (e.g., node degree, centrality). Hence, node diversity should be exploited to take the maximum benefit. In this work, we focus on CSS in a single collision domain (i.e., a mesh topology) and design a cooperation scheme to highlight how CRs can be aware of the others' cooperation behavior via considering their static (e.g., time invariant) social ties, i.e., friendship.

To the best of our knowledge, there are very few works in this line in CRN research [7, 8, 22, 23]. Güven *et al.* [22] devise a social-aware cooperation scheme that assesses each CR according to the friendship tie between the two CRs, the CR's community, and sensing history. Different from [22], we formulate the optimal cooperator selection policy and present an evolutionary multi-objective solution methodology for the formulated problem. Chen *et al.* [7] extend the primary channel recommendation scheme among CRs that is proposed in [23]. In these works, a CR that finds a primary channel idle, recommends this channel to other CRs. Chen *et al.* [8] argues that the current approaches in resource allocation/sharing represent the two extremes. *Network utility maximization* considers all users as a single entity and assigns the resources accordingly with the goal of maximizing the aggregate network utility. In contrast, game theory based approaches assume selfish users each of which considers only its own interest. Motivated by this observation, *social group utility maximization* accounts for both the selfish nature of entities as well as their cooperative behavior with the others who are socially connected. Using this new approach, each CR acts to maximize its social group utility for efficient database assisted spectrum access. Similar to our model, social ties among CRs are modelled as a rational number in [0,1] and represent how much a CR cares about other's utility.

VIII. Conclusions

In this paper, we have studied a social CRN that employs cooperative sensing. A CR may not always sense the channel for the benefit of other CRs in a social CRN, and its cooperation probability depends on the social ties. We have proposed a CR trust metric that measures the reliability of other CRs' sensing results. Using this metric, we have formulated a multi-objective optimization problem that maximizes expected throughput and sensing accuracy. Compared to a scheme that only considers the throughput, our proposal is always 90% of the expected throughput optimal solution when there are no malicious CRs, and performs significantly better in case of a malicious CR. Our numerical evaluations show that there is a substantial throughput difference between the conventional (i.e., all nodes are cooperative) and more realistic social-tie based cooperative behavior. This result is of particular importance as it highlights possible failure of a CRN in meeting the performance guarantees it promises to its subscribers. Moreover, we have also suggested and analyzed various cooperation probability formulations that focus on social ties, peer interactions, and system interactions.

As future work, we plan to extend our work to a large scale network where CRs move based on some realistic mobility patterns and social ties are modelled according to realistic human social networks.

Acknowledgment

This work is partially supported by the Turkish Ministry of Science, Industry and Technology under grant number SAN-TEZ 0410.STZ.2013-2, Bogazici University Research Fund (BAP) under grant number 7437, State Planning Organization of Turkey under grant number 07K120610, and Academy of Finland under grant number WiFiUS 284807.

References

[1] G. Ganesan and Y. Li, "Cooperative spectrum sensing in CR, part II: Multiuser networks," *IEEE Trans. on Wireless Comm.*, vol. 6, no. 6, pp. 2214–22, 2007.

[2] S. Eryigit, S. Bayhan, and T. Tugcu, "Energy-efficient multichannel cooperative sensing scheduling with heterogeneous channel conditions for CRNs," *IEEE Trans. on Vehicular Technology*, vol. 62, no. 6, pp. 2690–99, 2013.

[3] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in CRNs," in *IEEE INFOCOM*, 2008.

[4] A. S. Cacciapuoti, I. F. Akyildiz, and L. Paura, "Correlation-aware user selection for cooperative spectrum sensing in CRAHNs," *IEEE JSAC*, vol. 30, no. 2, pp. 297–306, 2012.

[5] K.-C. Chen, M. Chiang, and H. Poor, "From technological networks to social networks," *IEEE JSAC*, vol. 31, no. 9, pp. 548–72, 2013.

[6] W. S. Jeon, D. H. Lee, and D. G. Jeong, "Collaborative sensing management for CRNs with reporting overhead," *IEEE Trans. on Wireless Communications*, no. 2, 2013.

[7] X. Chen, J. Huang, and H. Li, "Adaptive channel recommendation for opportunistic spectrum access," *IEEE Trans. on Mobile Comp.*, vol. 12, no. 9, pp. 1788–1800, 2013.

[8] X. Chen, X. Gong, L. Yang, and J. Zhang, "A social group utility maximization framework with applications in database assisted spectrum access," in *Proc. of IEEE INFOCOM*, 2014, pp. 1959–67.

[9] D. J. Crandall, L. Backstrom, D. Cosley, S. Suri, D. Huttenlocher, and J. Kleinberg, "Inferring social ties from geographic coincidences," *PNAS*, vol. 107, no. 52, 2010.

[10] N. Cheng, P. Mohapatra, M. Cunche, M. A. Kaafar, R. Boreli, and V. Srikanth, "Inferring user relationship from hidden information in WLANs," in *IEEE Military Comm. Conf.*, 2012.

[11] R. Murawski, E. Ekici, V. Chakravarthy, and W. K. McQuay, "Performance of highly mobile CRNs with directional antennas," in *IEEE Int. Conf. on Comm. (ICC)*, 2011.

[12] Y.-C. Liang, Y. Zeng, E. C. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for CRNs," *IEEE Trans. on Wireless Comm.*, vol. 7, no. 4, pp. 1326–37, 2008.

[13] C. A. Floudas and P. M. Pardalos, *Encyclopedia of optimization*. Springer, 2008, vol. 1.

[14] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE Trans. on Evolutionary Computation*, vol. 6, no. 2, pp. 182–197, 2002.

[15] A. Konak, D. W. Coit, and A. E. Smith, "Multi-objective optimization using genetic algorithms: A tutorial," *Reliability Engineering and System Safety*, vol. 91, no. 9, pp. 992–1007, 2006.

[16] M. Emmerich, N. Beume, and B. Naujoks, "An EMO algorithm using the hypervolume measure as selection criterion," in *Evolutionary Multi-Criterion Optimization*, 2005, vol. 3410, pp. 62–76.

[17] C. Song and Q. Zhang, "Cooperative spectrum sensing with multi-channel coordination in CRNs," in *IEEE ICC*, 2010.

[18] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for CR applications," *IEEE Comm. Surveys Tutorials*, vol. 11, no. 1, pp. 116–30, 2009.

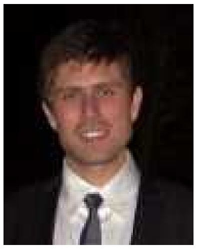
[19] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Comm. Letters*, vol. 14, no. 3, pp. 226–8, 2010.

[20] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a CR cooperative sensing system," *IEEE Trans. on Wireless Comm.*, vol. 9, no. 8, pp. 2488–97, 2010.

[21] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in DTNs," *IEEE Comm. Letters*, vol. 14, no. 11, pp. 1026–28, 2010.

[22] C. Güven, S. Bayhan, and F. Alagöz, "Effect of social relations on cooperative sensing in CRNs," in *BlackSeaCom*, 2013.

[23] H. Li, "Customer reviews in spectrum: Recommendation system in CRNs," in *IEEE DySPAN*, 2010.



Salim Eryigit (eryigit@boun.edu.tr) received his B.S. degree in Industrial Engineering from Bogazici University in 2003. He received his M.S. and Ph.D. degrees in Computer Engineering from Bogazici University in 2008 and 2014, respectively. Currently, he works as a senior research and development engineer at Idea Teknoloji, Istanbul. His current research interest include network optimization, cognitive radio networks, green communications, scheduling, and device-to-device communications.

Suzan Bayhan (bayhan@hiit.fi) received her Ph.D., M.S., and B.S. degrees in computer engineering from Bogazici University in 2012, 2006, and 2003, respectively. Currently, she works as a post-doctoral researcher at the University of Helsinki, Finland. Her research interests include modeling and analysis of cognitive radio networks, energy efficiency, mobile opportunistic networks, and content-centric networks. She received the EMEA Google Anita Borg Memorial Scholarship in 2009 and best paper award at ACM ICN in 2015.

Jussi Kangasharju (jussi.kangasharju@helsinki.fi) Jussi Kangasharju received his MSc from Helsinki University of Technology in 1998. He received his Diplome d'Etudes Approfondies (DEA) from the Ecole Superieure des Sciences Informatiques (ESSI) in Sophia Antipolis in 1998. In 2002 he received his PhD from University of Nice Sophia Antipolis/Institut Eurécom. In 2002 he joined Darmstadt University of Technology (TUD), first as post-doctoral researcher, and from 2004 onwards as assistant professor. Since June 2007 Jussi is a full professor at the Department of Computer Science at University of Helsinki. Between 2009 and 2012 he was the director of the Future Internet research program at Helsinki Institute for Information Technology (HIIT). Jussi's research interests are information-centric networks, content distribution, opportunistic networks, and green ICT. He is a member of IEEE and ACM.

Tuna Tugcu (tugcu@boun.edu.tr) received his B.S. and Ph.D. degrees in Computer Engineering from Bogazici University in 1993 and 2001, respectively, and his M.S. degree in Computer and Information Science from the New Jersey Institute of Technology in 1994. He worked as a post-doctoral fellow and visiting professor at Georgia Institute of Technology. He is currently a professor in the Computer Engineering Department, advisor to the rector and director of the Computer Center at Bogazici University. He serves in the NATO science & technology groups and IEEE standards groups. His research interests include nanonetworking, molecular communications, cognitive radio networks, and wireless networks.