Distributed and Cheat-Proof Spectrum Contention Scheme for IEEE 802.22 WRAN Networks

Kenneth Ezirim, Ligon Liu, Ping Ji
Department of Computer Science
Graduate Center CUNY, New York, USA
Email: {kezirim,lliu}@gc.cuny.edu, pji@jjay.cuny.edu

Shamik Sengupta
Department of Computer Science and Engineering
University of Nevada, Reno, USA
Email: ssengupta@unr.edu

***Abstract*—IEEE 802.22 wireless regional area networks (WRANs) are cognitive radio-based wireless networks that opportunistically access sub-900 MHz TV bands for their operations. IEEE 802.22 WRANs are continuously faced with self-coexistence problems. The adaptive on-demand spectrum contention (ODSC) protocol has been proposed as a possible solution to the problem of self-coexistence in such networks. Unfortunately, the design of ODSC protocol contains some major flaws, which makes the scheme cheat-prone and less efficient for resolution of spectrum contentions among networks. In this paper, we highlight the main problems associated with the implementation of ODSC as a spectrum contention protocol. We propose a scalable and cheat-proof scheme for spectrum contention that guarantees fairness and system efficiency. We show the performance of proposed scheme with different network topologies. Simulation results show substantial improvement in system performance via channel reuse, with significant levels of fairness in spectrum utilization.**

I. Introduction

IEEE 802.22 is a standardized specification that allows unlicensed secondary users (SU) to exploit the unused TV bands on zero-interference basis. The standard is used by wireless regional area networks to access TV bands located at the sub-900 MHz [1]. The introduction of this specification is part of the several efforts being made to alleviate the problem of spectrum scarcity among cognitive radio networks. Just like cognitive radio devices, IEEE 802.22 devices are required to observe spectrum etiquette by performing routine spectrum sensing and evacuating upon detection of the licensed users' presence. Several primary user protection mechanisms have been suggested in [2], which address primary-secondary spectrum etiquette. The issue of secondary-secondary spectrum etiquette, however deals with the ability of secondary users to coexist in same spectrum environment. In a system where the operating range of networks overlap geographically, the ability to coexist is a major challenge. Self-coexistence has become an important issue to address, given that the unused spectrum resources are now commodities of intense demand as been shown in [3] [4] [5] [6] [7] [8]. Hence, there is need for self-coexistence protocols and schemes that will enhance access to the often-scarce spectrum resources.

The Adaptive On-Demand Spectrum Contention (ODSC) protocol is a self-coexistence oriented protocol, designed specifically for WRAN networks [9] [10]. The ODSC protocol leverages the MAC messaging on the inter-network communication channel to provide inter-network spectrum sharing among coexisting WRAN networks. The protocol is designed to allow WRAN networks to compete for shared spectrum by simply exchanging and comparing randomly generated contention priority numbers (CPNs). Several flaws have been identified with the ODSC protocol, which can jeopardize the fairness guarantees and also impact negatively on system performance. ODSC protocol is prone to random number generator manipulation, where participants can manipulate the generated CPNs in order to win the contention process. The contention destination can easily ignore or overlook the ODSC request sent by contention sources and declare itself the winner of the contention process. Given the above scenarios, it becomes possible for one or more participants to "hijack" available spectrum resources, thereby eroding the fairness that the ODSC protocol was designed to provide.

In this paper, we address vulnerabilities associated with the ODSC protocol. We propose a modified version of the protocol that mitigates the possibility of CPN manipulation by spectrum contenders, thereby promoting fairness and self-coexistence. We also investigate and propose ways to improve system utility, leveraging the proposed spectrum contention scheme. The rest of this paper is organized as follows. In section II, we provide an insight into the system model of coexisting IEEE 802.22 WRAN networks. In section III, we present an overview of the Adaptive ODSC protocol and discuss its vulnerabilities. Section IV discusses our proposed spectrum contention scheme and highlights the enhancements made to improve fairness and system utility. Section V presents the performance evaluation via computer simulation. Final conclusions are drawn in section VI.

II. System Model

Consider a typical deployment scenario of multiple WRAN networks, each consisting of a base station (BS) and related customer premise equipment (CPE). The communication range of a WRAN network could extend up to 100 km [11] [12] and may overlap with other WRAN networks in its vicinity. Spectrum resources that are not being used by the licensed incumbents are allocated in such a way as to mitigate interference during the operation of the WRAN networks. A typical deployment of WRAN networks is illustrated in Figure 1. Suppose there are n IEEE 802.22 WRAN networks in the system. The BSs of these networks participate in spectrum contention to gain access to a specific channel. The system of WRAN networks can be represented as an undirected interference or conflict graph $G = \{N, E\}$ where $N = \{N_i\}$ is the set of vertices denoting the WRAN networks and $n = |N|$. E is a set of undirected edges denoting the existence of interference constraints existing between any given two networks. For instance, if an edge (i, k) exists in E for a channel C_j, then both N_i and N_k cannot operate simultaneously on channel C_j without interference. Assuming

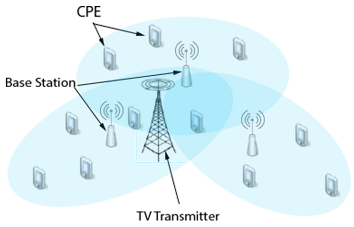


Fig. 1: A typical system of WRAN networks

N_k is the contention destination currently occupying channel C_j, then possible contenders or set of contention sources is defined as the set $N^c = N \setminus N_k \cup \{N_i : (i,k) \in E\}$.

We assume that in the system, there are m available channels. Each channel is partitioned into synchronized superframes which is further partitioned into 16 frames of fixed length. Each frame is further divided into Data Transmission Period (DTP) and Beacon Period (BP) just like in CBP protocol [11]. Availability of the channels is time-variant and largely dependent on the activities of the licensed incumbents. Without loss of generality, we assume that all WRAN networks are aware of the system topology that imposes the operational constraints on the use of the available frequency bands. Primary-secondary etiquette is strictly observed in the system. The secondary-secondary etiquette is enforced by allowing WRAN networks to request spectrum contention instead of blindly grabbing any available channel for transmission. Utility derived by WRAN networks is dependent on the throughput obtained while operating on the channels. We assume that when two WRAN networks are in close proximity and transmitting on the same frequency band(s), interference will occur. As a result, no utility is derived since the interference could exceed the signal to interference and noise ratio (SINR) requirements, causing the transmissions to fail [10].

III. Conventional ODSC Protocol

The ODSC protocol is a distributed, cooperative, and real-time spectrum sharing protocol. The fundamental idea of the protocol is based on allowing BSs of coexisting WRAN networks to contend for shared spectrum resources on an on-demand basis [11]. The ODSC scheme works as follows. An occupant of a channel, referred to as contention destination (DST), regularly send ODSC announcement messages (ODSC_ANN), informing neighbors of the occupied channel. A spectrum-demanding network, also known as contention source (SRC), upon receiving such announcements prepares an ODSC request message (ODSC_REQ) and forwards it to a randomly selected DST. The ODSC_REQ message includes a CPN which can be either a real number uniformly selected from the range $[0, 1]$ or an integer selected uniformly at random from the range $[0, 2^x - 1]$ with x being an arbitrary integer generally accepted in the system. DSTs maintain an ODSC_REQ window during which they expect to receive ODSC_REQ from channel contenders. At the end of the ODSC_REQ window, if any ODSC_REQ was received, a DST generates a CPN and compares it with the CPNs from other SRCs. If the DST's CPN is smallest (highest priority) among all CPNs compared, it will send an ODSC_RSP message to all SRCs indicating contention failure. Otherwise, the winner SRC will receive an ODSC_RSP indicating contention success while other SRCs receives messages indicating contention failure. The winner SRC acknowledges the outcome of the spectrum contention process by sending an acknowledgement message (ODSC_ACK) indicating the time when it intends to acquire the contended channel. All DSTs that are within operating range of the winner SRC will have to schedule channel release and broadcast an ODSC release message (ODSC_REL). The ODSC_REL contains information about the channel to be released, the channel release time and winner SRC identification.

Vulnerabilities: The ODSC protocol is far from a perfect protocol for fostering self-coexistence of WRAN networks. We can identify some of the loopholes in the protocol design that could jeopardize self-coexistence among the networks. Some of the assumptions made in ODSC protocol include: 1) CPNs are actually generated uniformly at random from the range specified and agreed upon by the system of WRAN networks; 2) DSTs, serving as arbiters during spectrum contention processes, are honest and unbiased; 3) CPN collisions are rare or practically impossible.

The first assumption deals with the generation of the CPNs used in spectrum contentions. Prior to the deployment of the WRAN networks, a decision is reached on the criteria used in deciding the winner of a spectrum contention. With this information, the BSs might be tempted to manipulate their CPNs in order to win the contention. The second assumption grants unlimited authority to incumbent DSTs to decide the outcome of spectrum contentions. DSTs can reach decisions in favor of themselves, regardless of the CPNs sent by SRCs. Even though the possibility of CPN collisions is quite negligible depending on the range $w = 2^x$, it is still important to address such situations. In the ODSC system, a criterion is usually adopted for spectrum contention resolution; for instance the owner of the smallest CPN wins. With this knowledge, some contenders might decide to generate the smallest possible CPN value in order to win a spectrum contention. This makes CPN collisions more frequent. The best approach to conduct spectrum contention is to hide the criterion for spectrum contention resolution from participants, thereby forcing them to use random CPN generators. However, this approach is simply inapplicable in ODSC because DSTs still reserve the right to: 1) decide the criterion; and 2) announce the winner of the spectrum contention. Also the protocol failed to consider repeated spectrum contentions that can lead to channel reuse.

IV. Modified ODSC Protocol

In this section, we propose a distributed and cheat-proof spectrum contention protocol, otherwise known as Modified ODSC. MODSC addresses issues related to the ODSC protocol. Our approach supports an open and distributed decision-making process, which involves every network contender. Also, it eliminates the need for a fixed range in generating CPN numbers, such that CPNs can be any number within the interval $[0, \infty]$. As we have stated earlier, spectrum contentions are conducted to decide which network gets the opportunity to operate on a contended channel. To encourage self-coexistence

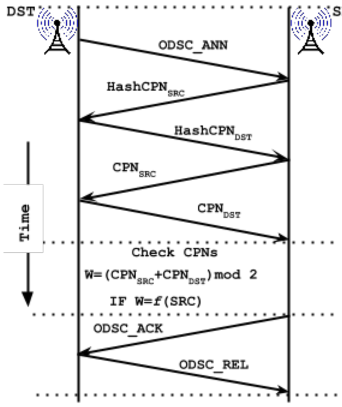


Fig. 2: Modified ODSC Scheme

among the WRAN networks, the spectrum contention process must be fair to all participant networks. This means that the process must be devoid of bias and cheating. Therefore, all networks participating in spectrum contention should be able to determine the winner in a distributed manner. This eliminates the monopoly enjoyed by DSTs in making spectrum contention decisions.

An illustration of MODSC message exchange is shown in Figure 2. The MODSC scheme commences with the broadcast of ODSC_ANN messages by DSTs. Leveraging the ODSC_REQ message broadcast, potential participants in a spectrum contention first exchange hashes of generated CPNs. Then later the participants exchange the actual CPNs. This procedure is introduced to make it impossible for any participating network to manipulate or adjust its CPN in order to win the spectrum contention. After the exchange of the CPNs, each network checks the hashes of received CPNs against the actual CPN received from neighboring networks. The spectrum contention decision is then made using all CPNs of participants. The winner of the contention process broadcasts an ODSC_ACK messages, and the DST occupying the contended channel will broadcast an ODSC_REL message. If there is more than one ODSC_ACK message at the end of the contention process, then all participants are then required to broadcast an ODSC_ACK. The winner would be the participant that had the majority of the votes.

While exchanging CPNs, a malicious BS may delay sending a CPN in order to first read the CPN of fellow contender. Reading a contender's CPN gives the BS an opportunity to manipulate its CPN. To resolve this delay-induced cheating problem described above, we apply the zero knowledge proof (ZKP) technique. The ZKP technique is a method by which parties can prove to one another that their declarations are true without conveying any extra information apart from the declarations themselves. To implement this technique, spectrum contenders are required to exchange irreversibly hashed values of their CPNs before their actual CPNs are exchanged. The hashed CPNs can prove generation time of the later-to-be-exchanged CPNs without exposing their actual values. The hash function used for this purpose can be any irreversible hash function with no known collisions beyond certain input size, such as SHA1 and SHA256. An additional requirement due to use of hash functions is the need for CPNs to be sufficiently long to prevent dictionary attacks and minimize the rare possibility of collisions. A digest size of 128 bits has been shown to be sufficient to protect the hash value of the CPNs from collisions [13]. BSs have a fixed broadcast window to exchange their hashed CPNs with each other. All contenders then exchange their actual CPNs after all hashed CPNs have been exchanged. Then validation of CPNs follows with each contender, comparing hashes of the received CPNs with the hashed CPNs received earlier on. At the end of the comparison, the decision function is applied to determine the winner. If the validation process fails, then other contenders are notified and the spectrum contention is annulled by majority vote.

A. Spectrum Contention Resolution Schemes

We considered two spectrum contention resolution schemes, namely pairwise and n-wise. With these resolution schemes, all participating networks unanimously reach a decision on the winner of a spectrum contention. There are no criteria involved and all participants arrive at the same conclusion using a decision function.

1) Pairwise Spectrum Contention Resolution

Pairwise spectrum contention entails that only two BSs are involved in the contention process. The process initiated by a contention source interested in an advertised channel. Suppose two BSs N_i and N_k generated and exchanged CPNs x and y respectively. The decision function $D(x, y)$ for the spectrum contention resolution is given as

$$D(x, y) = F(x, y) \oplus G(x, y) \qquad (1)$$

where $\oplus$ is an XOR logical operator. The function $F(x, y) \in \{0, 1\}$ is defined as $F(x, y) = (x + y)$ mod 2 and $G(x, y) \in \{0, 1\}$ is defined such that $G(x, y) = 0$ when $x < y$, and $G(x, y) = 1$ when $x > y$. In a case where $x = y$, the spectrum contention is repeated. The function $G(x, y)$ introduces uncertainty in $D(x, y)$ by taking into consideration the relative values of x and y. The computation of $D(x, y)$ is carried out independently by the BSs and the outputs expected to be the same, provided CPNs are not manipulated. We assume that prior to the spectrum contention, contenders have agreed to a injective function $f : N_i \rightarrow \{0, 1\}$ that uniquely maps each contender to an element in $\{0, 1\}$. By this means, each participant will know who won the contention after computing $D(x, y)$.

2) N-wise Spectrum Contention Resolution

Given a scenario where spectrum contention can involve more than two BSs, the decision function derived for pairwise spectrum contention resolution cannot be used. If the pairwise spectrum contention resolution is used, at least O(log n) spectrum contentions would be required to decide the winner, with n being the number of contending BSs. The decision function for n contenders will be a function with n input parameters denoted as $\mathbf{x} = \{x_i \mid x_i \in \mathbb{Z}^+\}_{i=1}^{n}$. We define the function as

$$D(\mathbf{x}) = D(\{x_1, \cdots, x_n\}) = \left[\sum_{i=1}^{n} x_i\right] \text{ mod } n \qquad (2)$$

$D(\mathbf{x}) \in \{i\}_{i=0}^{n-1}$ is inherently uniformly distributed assuming that the randomly generated CPN values were also uniformly generated, that is, $D(\mathbf{x}) \sim U(0, n-1)$. The earlier decision function cannot be applied because $F(\mathbf{x}) \oplus G(\mathbf{x}) \nsim U(0, n-1) \;\; \forall x_i \in \mathbb{Z}^+$. With the help of the decision function $D(\mathbf{x})$ and a predefined mapping function $f : N_i \rightarrow \{i\}_{i=0}^{n-1}$, each participant has an equal chance to emerge as the winner of a spectrum contention. The simultaneous and independent computation of $D(\mathbf{x})$ to reach a unanimous decision in a distributed manner rids the malicious DSTs of the capability of altering spectrum contention outcomes.

B. Non-cheatability and Collusion Proof

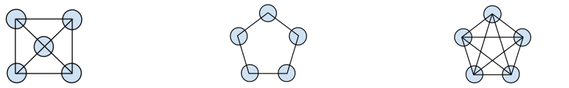
Distributed and cheat-proof spectrum contention emphasizes non-cheatability in terms of CPN manipulation. Spectrum contention processes should also be collusion-proof. This means that no group of WRAN networks can collude to alter the outcome of spectrum contention in their favor. Suppose that spectrum contention is a game and each network selects a CPN independently of the other networks. We can consider the choice of a particular CPN x_j as a pure strategy such that $x_j \in [x_{min}, x_{max}]$ is a pure strategy. Using a random CPN generator with a probability mass function Pr(x), a mixed strategy of these pure strategies can be derived. Regardless of strategies (pure or mixed) implemented by the players (BSs), no player should have an advantage over another in winning the spectrum contention game. The spectrum contention should present to every player with equal opportunity to win, provided the CPNs are not tampered with. Therefore the decision function must meet the non-cheatability and collusion-proof criteria to be considered applicable in deciding winners of spectrum contentions.

Definition 1. *A non-cheatable decision function $D(\boldsymbol{x})$ need to satisfy the following condition: Each player has a strategy s_0 that guarantees at least $\frac{1}{n}$ to win regardless of other players' strategies(i.e. $Pr(D(\boldsymbol{x}) = k) \geqslant \frac{1}{n}$ when $x_k \sim s_0$).*

Definition 2. *A collusion-proof decision function $D(\boldsymbol{x})$ need to satisfy the following condition: For a colluding set of players, $C \subset \{N_1 \ldots N_n\}$, regardless of the collusion scheme $Pr(\{x_{k \in C}\})$, $Pr(D(\boldsymbol{x}) \in C) \leq \frac{\|C\|}{n}$.*

The non-cheatability condition assures that regardless of the strategy employed by players, the probability of winning remains the same for all. Collusion-proof condition ensures that collusion among players cannot increase their chances of winning the game. This condition is obviously necessary for every individual player. Thus, for every individual player N_i, there exists a strategy s_0 such that if all other players are to collude, s_0 still guarantees a fair winning probability $\frac{1}{n}$ to the individual players. That is, $Pr(D(\mathbf{x}) = N_i) \geqslant \frac{1}{n}$ if $x_i \sim s_0$.

Proof: We adopt the decision function of equation 2 for the proof. All users share the same CPN domain which includes all integers ranging from 0 to $r-1$, $r \gg n$. For player N_i generating an arbitrary CPN number a, if $Pr(x_i = a \mid a \in 0 \ldots r-1) = \frac{1}{r}$ then the probability of N_i to win can be expressed as $Pr((\sum_{k=1}^{n} x_k) \bmod n = i) = \frac{1}{n}$. Note that i is an index mapped to player N_i. Suppose the joint distribution of other players except N_i can be expressed as $Pr(\{x_k\}_{k \in \{1 \ldots n\} \setminus i})$. We can calculate the distribution of Pr($\sum_{k \in \{1 \ldots n\} \setminus i} x_k$) with x_k falling with the range of integers in $[0 \ldots (n-1)(r-1)]$. The upper bound of r_{max} is evidently equivalent to $(n-1)(r-1)$. Let us denote the sum of other players' CPNs as $Y = \sum_{k \in \{1 \ldots n\} \setminus i} x_k$. Since $Pr(x_i = a \mid a \in 0 \ldots r-1) = \frac{1}{r}$ and $r \gg n$, we have that $\forall z : \; Pr((z + x_i) \; mod \; n = k) \approx \frac{1}{n}$ and $\sum_{y \in 0 \ldots r_{max}} Pr(Y = y) = 1$. Therefore, $Pr((Y + x_k) \bmod n = k) = \sum_{y \in 0 \ldots r_o} Pr(Y = y) \cdot Pr((y + x_i) \bmod n = k) = \frac{1}{n}$. ■



(a) Wheel (b) Cycle (c) Complete

Fig. 3: Different Network Topologies

V. Numerical and Simulation Results

In this section, we present a numerical analysis and performance evaluation of ODSC and MODSC spectrum contention schemes. The network topologies shown in Figure 3 are used in our analysis. We assume that there is a single channel for the entire system of WRAN networks. We adopt the Beacon Period Framing (BPF) protocol that guarantees reliable, efficient and scalable internetwork communication [11]. Jain's fairness index is used in quantifying the degree of fairness in the system. System utility is measured in terms of the number of superframes used by networks without any interference. Depending on network topology, an additional spectrum contention can be conducted before the end of a superframe. This leads to reallocation of the same channel to another non-interfering WRAN network, which we refer to as channel reuse. Channel reuse is possible if there is at least a single WRAN network, whose operations on the contended channel will not interfere with the operations of the winner network from the previous contention(s). It is important to note that since the winner of a spectrum contention is decided simultaneously, losers will know instantly whether to initiate another spectrum contention for a possible channel reuse. The knowledge of network topology also helps losers to ascertain conflicting scenarios and avoid initiating spectrum contention. We denote channel reuse as the parameter r, which represents the number of spectrum contentions that can be conducted or allocations that can be made for the same channel. For instance, $r = 3$ indicates that it is possible to conduct 3 spectrum contentions in a superframe.

A. Fairness in ODSC System

Simulation results show that fairness in a system of WRAN networks implementing the ODSC protocol depends on network topology. We use the well-known Jain's Fairness Index (JFI) to measure fairness in the system. Given that the ODSC scheme is highly vulnerable, we simulated the impact the presence of malicious contenders will have on fairness in the system. We assume that the malicious contenders can make transitions between two states: active and inactive states. We note that an active malicious DST always declares itself the winner of any spectrum contention process. On the other hand,

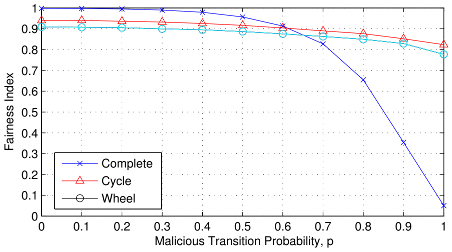


Fig. 4: Variation of Fairness with Malicious Transition Probability

an inactive malicious DST follows the specified guidelines of the protocol in determining the winner of any spectrum contention process. For experimental purposes, we assume a malicious DST makes a transition from inactive state to active state with a probability p and makes a reverse transition with a probability $1-p$. Simulation results are presented in Figure 4. The results show how fairness in the system varies with p for the select network topologies.

In this experiment, we set the number of WRAN networks $n = 20$. Also a malicious contender is selected randomly at the beginning of the simulation, invariant to the contender's position in the network topology. We observed that with low malicious transition probabilities, the ODSC protocol achieves near-optimal fairness. As we know the network topology reflects the coexistence constraints existing in the system. This explains the difference in fairness under the different network topologies. In a complete network topology, all participants are aware that only one network can operate at any time, despite the possibility of cheating occurring in the system. When p is high, we have a scenario where one network can highjack the contended channel and refuse to release it. Fairness in wheel and cycle network topologies are purely affected by the fact that more than one network can win the right to operate on the channel. This creates the possibility of adjacent winners of spectrum contention that could interfere and lay wastage of the spectrum opportunity. The winners are thus denied of their fair share of the spectrum opportunities that might arise. In general, scenarios with high p and either cycle or wheel network topology are far better and more stable in terms of fairness than scenarios with complete network topology.

B. Performance of MODSC in Different Network Topologies

Performance of the MODSC system under the three selected network topologies using the average system utility metric is illustrated in Figure 5. Average system utility is best in a system with cycle network topology, where each WRAN network has at most two neighbor WRAN networks. In a complete network topology, even though spectrum opportunity is stable, we observe a steady decline in average system utility with increasing number of networks. The results obtained emphasize the importance of placement of the WRAN networks in the expected system performance. To maximize system performance, WRAN networks have to be setup at locations where they have minimal number of neighbors. In cases where this requirement cannot be met, especially in a complete network topology scenario, MODSC ensures that self-coexistence among networks is maintained. The in-built features of the protocols against CPN manipulation, eliminate the possibility of cheating during spectrum contentions.

C. Performance Comparison of ODSC and MODSC

ODSC protocol stipulates that SRCs send spectrum contention requests on demand to contention destination DSTs. With this approach, SRCs need at least one DST to commence any spectrum contention process. Even if by chance, one or more SRCs discover that their operations on the contended channel will not interfere with the winner of the just concluded spectrum contention, no spectrum contention can be conducted until the next superframe when the winner DST sends out an ODSC_ANN message. This leads to the wastage of the spectrum opportunity, which one of the SRCs could have benefited from. Furthermore, the fact that SRCs have to randomly or systematically select a DST to contend with creates a self-coexistence problem. Consider a WRAN network with a wheel network topology depicted in Figure 6. Before spectrum contention, there is a set of DSTs $\{C, E\}$. During the contention process, the SRCs $\{A, B, F, D\}$ have to select independently one DST to contend with. Suppose those that decided to contend C are $Y_C = \{A, F\}$ and those that decided to contend with E are $Y_E = \{D, B\}$. If after the spectrum contention, F and D emerge as winners of their respective contention processes, then both BSs cannot operate without interfering with one another. According to the provisions of ODSC no spectrum contention takes place until the next superframe. As a result of this restriction, the entire spectrum opportunity is wasted.

However, with MODSC, the procedure is quite different. When a BS initiates spectrum contention request for a specific channel, all interested BSs will participate in the process. Their participation allows them to know the winner of the spectrum contention simultaneously. Then, with the help of this information and the network topology, the BSs will know exactly whether to initiate another spectrum contention before superframe ends. The BP frame size and the number of BPs in a superframe limit channel reuse, which is the same as the number of spectrum contentions that can be conducted in a given superframe. Using illustration in Figure 7 as an example, we see that in the worst case, $r = 1$ and exactly one BS emerges a winner at the end of the first round of contention. Let us assume that the winner BS is B. None of B's neighbors $\{A, F, E\}$ can initiate another spectrum contention. The remaining BSs $\{C, D\}$, with the knowledge about the network topology and winner BS, can conduct another spectrum contention. The operation of the winner of

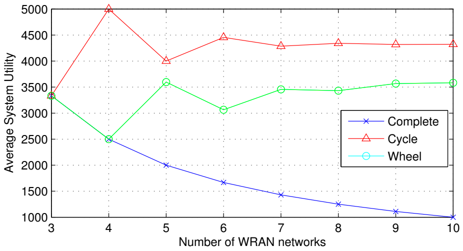


Fig. 5: Average System Utility in MODSC system

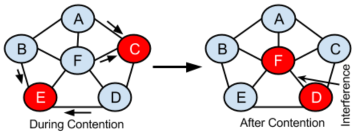


Fig. 6: ODSC Spectrum Contention Scenario

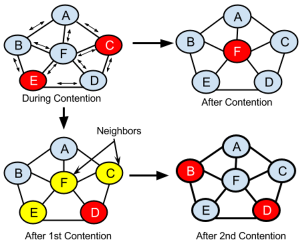


Fig. 7: MODSC Spectrum Contention Scenario

this later spectrum contention will not interfere with B's. The fact that MODSC supports channel reuse increases system utility.

Consider a system of WRAN networks with $n = 5$ and $r = 2$ for T superframes. In system with cycle network topology, each BS has equal opportunity to win either first or second round of spectrum contention. Thus, the expected system utility $E[U] \leq 2T$. In a system with a wheel network topology, the scenario is different. When the central BS, denoted as N_m, wins the expected payoff is T. However, when any other BS $N_i \neq N_m$ wins the spectrum contention the expected payoff is $2T$. Therefore, expected utility $E[U]$ in this scenario is $E[U] = \frac{(2n-1)T}{n}$. Substituting $n = 5$ in the equation and computing expected channel reuse using the expression $E[r] = E[U]/T$, we find that $E[r] < r$, which is confirmed by simulation results illustrated in Figure 9. Comparison of the performances of ODSC and MODSC based on channel reuse under wheel and cycle network topologies are shown in Figures 9 and 8 respectively.

We can clearly see that MODSC, in contrast with ODSC, guarantees more channel reuse with increasing number of WRAN networks in both cycle and wheel network topologies. Contrary to this trend, the ODSC system shows a continuous decline in channel reuse as the number of networks increase. This trend observed in ODSC system can be explained by the independent spectrum contentions conducted, which may end up in winners conflicting on the same channel. Comparing the trends in Figures 9 and 8, we can say that channel reuse is better in cycle network topology than in wheel network topology. This is also anticipated because the central WRAN network, in system with a wheel network topology, plays a significant role in determining the channel reuse.

Conclusion

In this paper, we address some of the vulnerabilities of ODSC protocol. We propose a modified version of the ODSC that fills up some of the security loopholes associated with the protocol. The MODSC protocol guarantees fairness by eliminating the possibility of cheating by malicious spectrum contenders. The protocol also gives better system performance due to channel reuse. In the future, we shall dedicate more attention to the performance of the proposed scheme in a more complex network topologies and the impact of the BP frame size and delays on channel reuse.

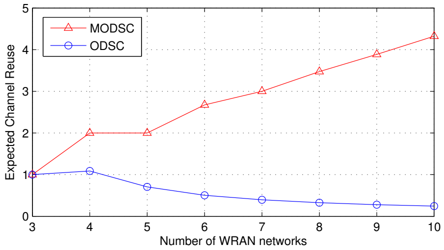


Fig. 8: Performance Comparison of ODSC and MODSC under Cycle Network Topology

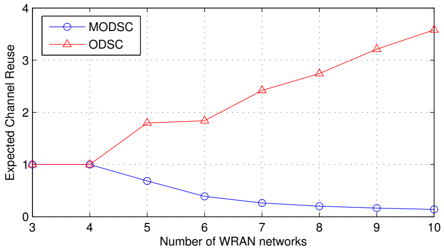


Fig. 9: Performance Comparison of ODSC and MODSC under Wheel Network Topology

References

[1] (2012) IEEE 802.22 Working Group on Wireless Regional Area Networks. [Online]. Available: http://www.ieee802.org/22/

[2] "IEEE Draft Cognitive WRAN MAC and PHY specifications: Policies and procedures for operation in the TV Bands," *IEEE P802.22/D2.0, February 2011*, pp. 1–698, March 2011.

[3] D. Grandblaise and W. Hu, "Inter base stations adaptive on demand channel contention for IEEE 802.22 WRAN self coexistence," *IEEE docs: IEEE*, pp. 802–22, 2007.

[4] K. Bian and J.-M. Park, "A coexistence-aware spectrum sharing protocol for 802.22 WRANs," in *ICCCN 2009. Proceedings of 18th Internatonal Conference on*. IEEE, 2009, pp. 1–6.

[5] L. Chen, K. Bian, L. Chen, W. Yan, and X. Li, "On the cascading spectrum contention problem in self-coexistence of cr networks," in *Proceedings of the 1st ACM workshop on Cognitive radio architectures*. ACM, 2013, pp. 3–12.

[6] D. S. Dikhit, A. Mukherjee, and A. Kumar, "IEEE 802.22 WRAN: MAC for Coexistence of Multiple CR Networks–A Survey," 2013.

[7] K. Ezirim and S. Sengupta, "Self-coexistence among CRNs using risk-motivated channel selection based deference structure," *Tsinghua Science and Technology*, vol. 18, no. 3, pp. 242–249, 2013.

[8] K. Ezirim, S. Sengupta, and E. Troia, "Channel acquisition and contention handling mechanisms for DSA in a distributed system of CRNs," in *ICNC 2013 Intl. Conf. on*. IEEE, 2013, pp. 252–256.

[9] W. Hu, "Frame Based, On-Demand Spectrum Contention Protocol Vector Messaging," Jan. 23 2014, US Patent App. 13/942,251. [Online]. Available: http://www.google.com/patents/US20140023034

[10] S. Sengupta, S. Brahma, M. Chatterjee, and N. Sai Shankar, "Self-coexistence among interference-aware IEEE 802.22 networks with enhanced air-interface," *Pervasive and Mobile Computing*, vol. 9, no. 4, pp. 454–471, 2013.

[11] W. Hu, M. Gerla, G. A. Vlantis, and G. J. Pottie, "Efficient, flexible, and scalable inter-network spectrum sharing and communications in cognitive ieee 802.22 networks," in *Cognitive Radio and Advanced Spectrum Management, 2008. CogART 2008. First Intl. Workshop on*. IEEE, 2008, pp. 1–5.

[12] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 130–138, 2009.

[13] RFC 1751 A Convention for Human-Readable 128-bit Keys. [Online]. Available: http://tools.ietf.org/html/rfc1751