بسم الله الرحمن الرحيم

دانشکده مهندسی برق و رباتیک

پایان نامه کارشناسی ارشد مهندسی سیستم‌های الکترونیک دیجیتال

اجاره طیف در شبکه های رادیو شناختی به منظور افزایش امنیت ارسال اطلاعات

نگارنده: شکوفه وطن پور ازغندی

استاد راهنما

دکتر محمدرضا جوان

بهمن ۱۳۹۵

تقدیم به

به پاس تعبیر عظیم و انسانی شان از کلمه ایثار و از خودگذشتگان

به پاس عاطفه سرشار و گرمای امید بخش وجودشان که در این سردترین روزگاران بهترین پشتیبان است

به پاس قلب های بزرگشان که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می گراید

و به پاس محبت های بی دریغشان که هرگز فروکش نمی کند

این مجموعه را به پدر و مادر عزیزم و به کسانی که

می اندیشند و از اندیشیدن هراسی ندارند

تقدیم می کنم.

تقدیر و تشکر

وظیفه خود میدانم که از جناب آقای دکتر جوان که همواره با استقبال گرمشان پاسخگوی سوالات من بودند قدردانی نمایم. از دوست عزیزم خانم هدی علیپور که راهنماییها و تشویقهای ایشان در طی دو سال اخیر نقش بسزایی در انجام این مهم داشته صمیمانه تشکر مینمایم. همچنین، از خانواده عزیزم که همیشه همراه و همگام من بودند کمال تشکر را دارم. در پایان، از تمام کسانی که مرا در این مهم یاری رساندند سپاسگزارم.

تعهد نامه

اینجانب شکوفه وطن پور ازغندی دانشجوی دوره کارشناسی ارشد رشته مهندسی سیستم‌های الکترونیک دیجیتال دانشکده مهندسی برق و رباتیک دانشگاه صنعتی شاهرود نویسنده پایان نامه واگذاری طیف در شبکه های رادیو شناختی به منظور افزایش امنیت ارسال اطلاعات تحت راهنمائی دکتر محمدرضا جوان متعهد می شوم:

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « Shahrood University of Technology» به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.

❖ در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ

امضای دانشجو

مالکیت نتایج و حق نشر

❖ کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه های رایانه ای، نرم افزار ها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود می باشد. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.

* متن این صفحه نیز باید در ابتدای نسخه های تکثیر شده پایان نامه وجود داشته باشد .

چکیده

رادیوی شـناختی یک رهیافت مؤثر به منظور بهبود کارایی اسـتفاده از طیف اسـت. اسـاس این رهیافت تقسـیم طیف میان کاربران اولیه و کاربران ثانویه اسـت. کاربران اولیه برای اسـتفاده از طیف مورد نظر دارای مجوز بوده و اجازه دسـترسـی به طیف را در هر زمانی دارا هسـتند. کاربران ثانویه به صـورت پویا و فرصـت‌طلبانه به طیف دسـترسـی دارند با این شـرط که موجب تداخل غیرقابل تحمل برکاربران اولیه نگردند. در این پایان نامه اجاره طیف در یک شبکه رادیو شناختی مبتنی بر OFDMA به منظور حفظ امنیت ارسـال اطلاعات شـبکه اولیه مورد بررسـی قرار می‌گیرد. در این شبکه کاربران ثانویه بصورت ایستگاه‌های رله رمزگشایی و ارسال عمل کرده و به شبکه اولیه در ارسال اطلاعات کمک می‌کنند. در این شبکه فرض می‌شود پهنای باند موجود به n زیر حامل تقسیم می‌شود. شبکه اولیه به صـورت OFDM بوده و کاربر اولیه به صـورت همزمان می‌تواند از چند زیر حامل اسـتفاده نماید، در حالی که کاربران ثانویه فقط بر روی یک زیر حامل قابلیت ارسال اطلاعات را دارند. به علاوه در شبکه مورد نظر، چند کاربر متخاصم وجود دارد که سعی در شنود اطلاعات ارسالی دارند. در شبکه مورد نظر ارسال اطلاعات به صورت فریم به فریم انجام می‌شود که در آن هر فریم شامل دو بازه زمانی است. در بازه زمانی اول ایسـتگاه پایه اولیه اطلاعات را ارسـال کرده در حالی که کاربران ثانویه به ایسـتگاه پایه اولیه گوش می‌دهند. در بازه زمانی دوم کاربران ثانویه‌ای که برای کمک به ارسال اطلاعات شبکه اولیه انتخاب شده‌اند، اطلاعات دریافتی از شبکه اولیه را رمزگشایی و مجددا رمزگذاری کرده، و اطلاعات رمز شـده را به سـمت کاربر اولیه ارسـال می‌کند. سایر کاربران ثانویه، در صورت وجود، در بازه زمانی دوم اطلاعات خود را به ایسـتگاه پایه ثانویه ارسـال می‌کند. برای شـنودگر سناریوهای متفاوتی می‌توان در نظر گرفت مانند اینکه شنودگر در بازه زمانی اول، اطلاعات ارسالی از ایستگاه پایه اولیه را شنود کند و یا اینکه در بازه زمانی دوم اطلاعات ارسالی از کاربران ثانویه را شنود کند.

هدف مسـئله تخصـیص منابع پیشـنهادی، انتخاب کاربران ثانویه مناسب جهت کمک به ارسال اطلاعات شـبکه اولیه، تخصـیص زیر حامل‌ها به کاربران ثانویه، تخصـیص توان ایسـتگاه پایه اولیه و کاربران ثانویه به گونه ای اسـت که امنیت ارسـال اطلاعات شبکه اولیه تضمین شده و نرخ امن ارسال اطلاعات شبکه ثانویه بیشینه شود. جهت حل مسئله مورد نظر از روش لاگرانژ دوگان و subgradient استفاده می‌کنیم.

کلید واژه:

شبکه های رادیو شناختی، تخصیص منابع، ارتباطات مشارکتی، لاگرانژ دوگان، امنیت ارتباطات

فهرست مطالب

۱ فصل اول: مقدمه ۱

۱-۱ مقدمه ۲

۱-۲ مروری بر کارهای پیشین ۵

۱-۳ نوآوری و اهمیت مطالعه حاضر ۱۰

۱-۴ محتوای فصلهای بعد ۱۲

۲ فصل دوم: روش تحقیق ۱۳

۲-۱ سیستمهای رادیو شناختی ۱۴

۲-۲ معرفی سیستمهای رادیوشناختی ۱۷

۲-۳ سامانههای اشتراک طیفی پویا ۱۸

۲-۳-۱ اشتراک گذاری طیفی به روش ارسال زمینه ایی سیگنال ها ۱۹

۲-۳-۲ اشتراک گذاری طیفی به روش رویهمگذاری سیگنا لها ۲۰

۲-۴ طیف رادیویی ۲۰

۲-۴-۱ حسگری به صورت مشارکتی ۲۳

۲-۵ معرفی رادیو شناختی به عنوان یک لایه مقاوم در برابر شنود و اخلالگر ۲۴

۲-۶ امنیت ۲۶

۲-۷ اجاره طیف ۲۹

۲-۸ ارتباط مشارکتی ۳۰

۲-۸-۱ رفتار گره در شبکه ۳۱

۲-۸-۲ انواع رله ۳۱

۳ فصل سوم: مروری بر منابع مطالعاتی و تحقیقات انجام شده ۳۵

۳-۱ پیشگفتار ۳۶

۳-۲ مفهوم نرخ امن ۳۹

۳-۲-۱ تکنیک های دستیابی به نرخ امن غیرصفر ۴۰

۳-۲-۲ سیستم های چند زیرحاملی ۴۱

۳-۳ تخصیص منابع ۴۲

۳-۳-۱ تخصیص منابع در شبکه های شناختی مبتنی بر رله یکطرفه ۴۵

۳-۳-۲ تخصیص امن منابع در شبکههای شناختی مبتنی بر رله یک طرفه ۴۶

۳-۳-۳ بیشینه کردن مجموع نرخ امن در شبکههای شناختی مبتنی بر رله یکطرفه ۴۸

۳-۴ رله و کاربرد آن در ارسال امن ۴۹

۳-۴-۱ کانال رله بدون حافظه گسسته ۴۹

۳-۴-۲ کانال رله یکطرفه کدبرداری و ارسال ۵۰

جدول ۳-۱ نمادگذاری ۵۲

۴ فصل چهارم: اهداف و نوآوری ۵۳

۴-۱ سیستم مدل و بیان مسئله ۵۴

۴-۱-۱ مدل سیستم ۵۴

۴-۱-۲ ظرفیت کانال ۵۵

۴-۱-۳ بیان مسئله ۵۶

۲-۴ تحلیل مسئله ۵۹

۱-۲-۴ محاسبه متغیر توان ارسالی ۶۱

۵ فصل پنجم: نتیجه گیری و پیشنهاد ۶۷

۱-۵ نتایج شبیه سازی ۶۸

۲-۵ نتیجه گیری ۷۰

۳-۵ پیشنهادات ۷۰

۶ پیوست : واژگان ۷۲

فهرست شکل‌ها

شکل ۱-۴ مدل سیستم ۶۵

شکل ۴-۲ الگوریتم برنامه ۶۵

شکل ۱-۵ نرخ ثانویه روی توان ارسالی ثانویه متفاوت..... ۶۷

شکل ۵-۲ نرخ ثانویه روی نرخ اولیه مختلف..... ۶۸

شکل ۵-۳ نرخ ثانویه روی زیر حاملهای مختلف..... ۶۸

شکل ۵-۴ نرخ ثانویه روی استراق سمع کننده مختلف..... ۶۹

فصل اول: مقدمه

۱-۱ مقدمه

انتقال اطلاعات بدون رابط سیم و به‌وسیله امواج الکترومغناطیسی ارتباط بی‌سیم[۱] یا مخابرات بی‌سیم نامیده می‌شود. قدیمی‌ترین ارتباط بی‌سیم به دوران ماقبل دنیای مدرن باز می‌گردد که از دود، آتش، پرچم، و غیره برای انتقال پیام در فواصل دور استفاده می‌شود [1]. مخابرات بی‌سیم در سال ۱۸۹۷ با اختراع تلگراف بی‌سیم توسط گولیلمو مارکنی[۲] ابداع شد [2] که موفق به ارسال تلگراف بی‌سیم برای حرف S در فاصله حدود سه کیلومتری شده بود [3]. بر خلاف مخابرات با سیم که هر جفت فرستنده[۳] و گیرنده[۴] به‌وسیله رابط‌های مجزا و ایزوله از هم، به‌هم متصل می‌شوند، در مخابرات بی‌سیم کاربران در فضای آزاد مخابره کرده و تداخل[۵] زیادی بین آن‌ها وجود دارد [2]. سیستم مخابرات بی‌سیم مورد استفاده در یک منطقه جغرافیایی باید به گونه‌ای باشد که از لحاظ مخابراتی تمام منطقه را تحت پوشش قرار دهد و از دید امواج رادیویی هیچ نقطه کوری باقی نماند. همچنین، اختصاص فرکانس‌های کاری مورد استفاده باید به صورتی باشد که تداخل فرکانسی در سیستم ایجاد نشود. بنابراین پیاده‌سازی سیستم مخابراتی در یک منطقه جغرافیایی، منطقه مربوطه را به مناطق کوچک‌تری به نام سلول[۶] تقسیم‌بندی می‌کنند و فرستنده را در سلول قرار می‌دهند .

دراین‌صورت، در شبکه‌های سلولی[۷] سرویس‌دهی تنها در منطقه‌ای که سلول‌بندی شده است ممکن می‌شود و ارسال اطلاعات در هر سلول تنها از طریق ایستگاه پایه[۸] امکان‌پذیر می‌گردد. در شبکه‌های سلولی، هرگونه ارتباطات بین کاربرهای شبکه از طریق ایستگاه پایه انجام می‌شود و دو کاربر نمی‌توانند به صورت مستقیم با یکدیگر ارتباط برقرار کنند. شبکه‌های سلولی دو مزیت عمده

---

۱ Wireless Communication

۲ Guglielmo Marconi

۳ Transmitter

۴ Receiever

۵ Interference

۶ Cell

۷ Celluar Networks

۸ Base Station

دارند. اولین مزیت آن‌ها استفاده مجدد از فرکانس حامل[۱] با رعایت فاصله جغرافیایی و دیگری شکافتن سلول‌ها است. شکافتن سلول‌ها به این معنی است که در طرح اولیه شبکه سلولی، سلول را بزرگ انتخاب می‌کنند و در صورت افزایش تعداد کاربران، سلول را می‌توان به سلول‌های کوچکتری تقسیم کرد و اصطلاحا سلول را شکافت و با گذاشتن ایستگاه‌های پایه اضافه، تعداد کاربران بیشتری را سرویس‌دهی کرد. تاریخ کامل مخابرات بی‌سیم به چندین دوره اصلی تقسیم می‌گردد. دوره قبل از همگانی شدن سیستم‌های مخابراتی بی‌سیم از سال ۱۹۵۰ شروع و تا سال ۱۹۶۰ ادامه یافت. در این دوره، از مخابرات بی‌سیم جهت کاربردهای پلیسی، نظامی و هواپیمایی استفاده می‌شد و تجهیزات ارسال و دریافت، حجیم و گران قیمت بود.

نسل اول[۲] شبکه‌های مخابراتی بی‌سیم در سال‌های ۱۹۷۰ تا ۱۹۸۰ بر پایه فناوری آنالوگ[۳] و استفاده از مفهوم سلولی پدید آمد. استفاده از مخابرات بی‌سیم سلولی موجب افزایش ظرفیت[۴] سیستم، کاهش هزینه، بهبود کیفیت سرویس[۵] و کاهش توان مورد نیاز گردید. با افزایش بیش از حد تقاضا، سیستم‌های آنالوگ نسل اول قادر به تامین ظرفیت مورد نیاز برخی از مناطق شهری نبودند. به‌علاوه سیستم‌های دیجیتال[۶]، نرخ بیت[۷] و سرعت بالاتری دارند و حجم اطلاعاتی بیشتری را می‌توان در کانال‌های آن مبادله کرد. شبکه‌های مخابراتی نسل دوم[۸] در سال‌های ۱۹۸۰-۱۹۹۰ و با استفاده از فناوری دیجیتال تحقق یافت و در سال ۱۹۹۲ در اروپا به بهره برداری تجاری رسید. در این سیستم، موبایل‌ها از فرکانس‌های ۸۹۰ تا ۹۱۵ مگاهرتز و ایستگاه پایه‌ها از فرکانس‌های ۹۳۵ تا ۹۶۰ مگاهرتز

---

۱ Carrier Frequency

۲ 1G

۳ Analoge

۴ Capacity

۵ Quality Of Service (QOS)

۶ Digital

۷ Bit Rate

۸ 2G

برای ارسال سیگنال استفاده می‌کنند. همچنین، پهنای باند[۱] هر کانال[۲] رادیویی ۲۰۰ کیلوهرتز است که توسط هشت کاربر استفاده می‌شود.

همزمان با راه‌اندازی موفقیت‌آمیز شبکه‌های مخابراتی بی‌سیم نسل دوم در دهه ۱۹۹۰ میلادی، تحقیقات پیرامون شبکه‌های نسل سوم[۳] آغاز و این شبکه‌ها از سال ۲۰۰۰ به بهره‌برداری تجاری رسیدند. سیستم‌های نسل سوم، سیستم‌های مخابرات فردی[۴] نامیده می‌شوند. سیستم‌های مخابرات فردی سیستمی است که با استفاده از آن هر کاربر می‌تواند در هر زمان و هر مکان، با هر شخص دیگر به کمک یک مخابرات فردی واحد تبادل اطلاعات نماید. از مزایای عمده شبکه‌های مخابراتی نسل سوم بر شبکه‌های نسل دوم نرخ بیت بالاتر، پشتیبانی همزمان صدا و تصویر با توجه به نرخ بیت بالا، قابلیت انعطاف‌پذیری بیشتر، سرویس‌های دسترسی چندگانه همزمان برای یک کاربر و غیره است. دهه ۲۰۱۰ میلادی دهه ظهور و رشد شبکه‌های مخابراتی بی‌سیم نسل چهارم[۵] است. استفاده از چندین آنتن[۶] در ابزارهای بی‌سیم و ایستگاه پایه و همچنین استفاده از پردازش‌های مناسب، موجب بهبود سرعت انتقال داده در این شبکه‌ها گردیده است. علاوه بر این با کاستن تعداد المان‌های شبکه، معماری شبکه در این فناوری‌ها ساده‌تر شده است.

آمارهای به دست آمده درطول چند سال اول دهه۲۰۱۰ و پیش‌بینی‌های موجود برای سال‌های بعد از آن نشان‌دهنده دوبرابرشدن رشد تقاضا در بخش ترافیک داده[۷] در هر سال است. به این ترتیب پیش‌بینی می‌شود که تقاضا برای شبکه‌های داده درسال ۲۰۲۰ به ۱۰۰۰ برابر مقدار آن در سال ۲۰۱۰ برسد. همچنین با افزایش تعداد کاربران متحرک تنوع سرویس‌ها و تقاضای کاربران برای

---

[۱] Bandwith

[۲] Channel

[۳] 3G

[۴] Personal Communication Systems

[۵] 4G

[۶] Multiple Antenna

[۷] Data Traffic

بهبود پارامترهای مختلف کیفیت سرویس مانند نرخ داده[۱]، تاخیر[۲] و پوشش[۳] پیش‌بینی می‌شود که علیرغم سرویس‌های متمایز شبکه‌های نسل چهارم، این شبکه‌ها دردهه آینده قابلیت پاسخگویی به این نیازهای روزافزون کاربران را نداشته باشند. بنابراین، این عوامل موجب شده است که محققان دراندیشه تکامل شبکه‌های نسل چهارم به سمت شبکه‌های فراتر از نسل چهارم که اصطلاحا شبکه‌های نسل پنجم[۴] نامیده می‌شوند، باشند. هدف اصلی تمامی تحقیقات پیرامون فناوری‌های این نسل، ارتباط نامحدود اشیا با یکدیگر با ظرفیت ارتباطی نامحدود و کیفیت سرویس بالا است.

یک سری ملزومات برای شبکه‌های نسل پنجم تعریف شده است که برخی از آن‌ها عبارت‌اند از: کاهش قابل ملاحظه در تاخیر، افزایش قابلیت اطمینان[۵] و دردسترس بودن شبکه، افزایش کارایی طیف[۶] فرکانسی، پوشش وسیع‌تر و امنیت[۷] بیشتر جهت برآورده‌سازی این الزامات، فناوری‌های زیادی برای بهره‌گیری در شبکه‌های نسل پنجم در حال توسعه هستند که یا شکل تکامل یافته‌ای از فناوری‌های مورد استفاده در نسل‌های قبلی هستند و یا فناوری‌های جدیدی هستند که در نسل‌های قبلی مورد استفاده نبوده‌اند.

۱-۲ مروری بر کارهای پیشین

رشد روزافزون کاربران شبکه مخابراتی و نیاز رو به رشد کاربران به سرویس‌های بی‌سیم در دهه اخیر باعث ناکارآمدی تخصیص ثابت طیف فرکانسی شده است. بررسی‌های انجام شده در بهره‌وری طیفی نشان داده است که اغلب فرکانس‌های تخصیص داده شده، کم مصرف و یا بدون

---

۱ Data Rate
۲ Delay
۳ Coverage
۴ 5G
۵ Reliability
۶ Spectrum
۷ Security

مصـرف هسـتند. این امر منجر به شـکل‌گیری شبکه‌های رادیو شناختی شد که در آن کاربران ثانویه[۱] (کاربران بدون مجوز[۲]) مجاز به اسـتفاده از طیف کاربران اولیه[۳] (کاربران مجوزدار[۴]) هسـتند به شرطی که سطح معینی از کیفیت سرویس برای کاربران اولیه تضمین شود. بدین ترتیب با معرفی شبکه رادیو شـناختی و اشـتراک طیف، راه حلی برای مشکل کمبود طیف پیشنهاد شد. رادیوی شناختی[۵] ایده‌ای امیدبخش برای غلبه بر مشـکل کمیابی طیف اسـت که مخابرات بی‌سـیم امروزه با آن روبرو است. در این روش، با ایجاد امکان دسـتیابی فرصـت طلبانه برای کاربران شناختی، که همچنین کاربرانِ ثانویه نامیده می‌شوند، به طیفی که به صورت اصلی به شبکه اولیه اختصاص یافته است، کارایی طیفی بسیار بالاتری برای ارتباطات بی‌سـیم فراهم می گردد [4]. کاربران مجوزدار می توانند از طیف اختصـاص داده شـده به آن‌ها اسـتفاده کنند و کاربران دیگر حق استفاده از آن را ندارند حتی اگر کاربران مجوز دار از آن طیف استفاده نکنند.

طیف رادیویی یکی از منابع طبیعی با ارزش اسـت که سیاست‌های تخصیص طیف به صورت ثابت و افزایش خدمات بی‌سـیم در سال‌های اخیر، مسأله دستیابی به آن در بسیاری از باندها را تبدیل به موضـوع بسیار پرمعنی‌تری از کمیابی فیزیکی طیف کرده است. گزارش‌های کمیته ارتباطات فدرال[۶] شـاهدی بر این ادعا است و نشان می‌دهند که کمیابی طیف نتیجه استفاده از طیف نبوده بلکه این امر ناشی از تخصیص فرکانس ایستا است و از این‌رو بررسی روشی برای استفاده هرچه بهتر از منابع طیفی ضروری به نظر می‌رسد [8]–[5] ,[3]–[1].

ما در این مهم از اجاره طیف اسـتفاده کردیم. اجاره طیف[۷] یعنی شبکه اولیه بخشی از منابع

---

[۱] Secondary User (SU)
[۲] Unlicensed User
[۳] Primary user (PU)
[۴] Licensed user
[۵] Cognitive Radio (CR)
[۶] Federal Communications Commission (FCC)
[۷] Spectrum Leasing (SL)

خود را در اختیار شـبکه ثانویه قرار دهد مشـروط بر اینکه شـبکه ثانویه به شـبکه اولیه کمک کند تا کیفیت سـرویس شـبکه اولیه بهبود یابد. مسئله تئوری توقف بهینه[1] به این صورت است که کاربرهای اولیه تمام کاربرهای ثانویه را جستجو کرده و بهترین را به‌عنوان رله انتخاب می‌کند [2]. حال طیف را با زمان‌بندی کاربر ثانویه در شـبکه رادیو شـناختی اجاره می‌دهیم. بر این اسـاس در دو مسیر رله‌های متوالی و پروتکل رمزگشایی و ارسال[2] هر کاربر ثانویه در طیف، مجاز به همکاری در ارسال برای شبکه اولیـه اسـت و برای اینکه اجاره طیف جبران شـود هر کاربر ثانویه اطلاعات خودش را هم ارسـال می‌کند [3].

تخصـیص منابع یکی از فاکتورهای اصـلی در طراحی شبکه‌های مخابراتی بی‌سیم است که علاوه‌بر کنترل تداخل کاربران و افزایش ظرفیت شـبکه، کیفیت سـرویس درخواسـتی کاربران را نیز فراهم می‌کند. منابع شـبکه‌های مخابراتی بی‌سـیم شـامل توان ارسـالی توسـط کاربران، نرخ ارسـال داده، فرکانس‌های کاری، شـکل بی‌سیم در فرستنده‌های چندآنتنی و کدهای ارسالی است که در بین آن‌ها توان ارسـالی و طیف فرکانسـی مهم‌ترین پارامترهای تخصـیص منابع جهت کنترل کاربران و افزایش ظرفیت شبکه محسوب می‌شوند [9].

از لحاظ دردسـترس بودن اطلاعات ضـرایب کانال‌ها، نرخ و توان‌های ارسـالی در شـبکه‌های مخابراتی بی‌سیم، دو حالت کلی وجود دارد. در حالت اول، فرض می‌شود اطلاعات لحظه‌ای شبکه نظیر ضـرایب لحظه‌ای کانال در دسـترس هسـتند و استراتژی ارسال یعنی نرخ‌های داده و توام‌های ارسالی جهت بهینه‌سـازی عملکرد کیفیت سرویس به صورت متغیر با زمان تخصیص داده می‌شوند که به آن تخصـیص منابع می‌گویند. قیود این مسئله بهینه‌سازی شامل انواع محدودیت‌های کار با سیستم نظیر پیشـینه توان ارسـالی کاربران، کیفیت سـرویس‌دهی درخواستی آن‌ها پیشینه نرخ ارسال است. حالت

---

[1] Optimal Stopping Theory

[2] Decode-and-Forward (DF)

دوم زمانی است که اطلاعات مورد نیاز نظیر اطلاعات لحظه‌ای کانال در دسترس نباشد. این امر به این دلیل است که در شبکه‌های مخابراتی بی‌سیم، همواره برقرار کردن لینک فیدبکی با ظرفیت مناسب جهت فراهم کردن اطلاعات کانال در فرستنده امکان‌پذیر نیست. این امر معمولا در شبکه‌های حسگر بی‌سیم و برخی دیگر از شبکه‌های ادهاک[1] خاص اتفاق می‌افتد که در آن کانال فیدبک با ظرفیت بالا در دسترس نیست. در این حالت، استراتژی ارسال با نرخ یا توان ارسالی ثابت استفاده می‌شود و عملکرد ارتباطی شبکه برمبنای احتمال قطع اندازه‌گیری می‌گردد.

به دلیل ماهیت پخشی شبکه‌های مخابراتی بی‌سیم، تمام کاربران موجود در ناحیه تحت پوشش شبکه قادر به کشف سیگنال ارسالی توسط فرستنده‌ها هستند. بنابراین، برقراری امنیت در حضور شنودگر یکی از مسائل چالش برانگیز در شبکه‌های مخابراتی بی‌سیم است. هدف اصلی برقراری ارتباطات امن درشبکه‌های مخابراتی بی‌سیم این است که گیرنده‌های قانونی شبکه بتوانند با موفقیت پیام ارسالی توسط فرستنده‌ها را دریافت کنند و شنودگرها قادر به کشف این پیام‌ها نباشند.

برقراری امنیت در لایه‌هایی بالایی شبکه با استفاده از روش‌های رمزنگاری انجام می‌شود که مقیاس بزرگ، دینامیک و نامتمرکز شبکه‌های مخابراتی بی‌سیم چالش‌های بسیاری را بر این روش‌ها تحمیل کرده است [10]. یکی از ایده‌های نویدبخش جهت افزایش امنیت ارسال اطلاعات در مقابل حمله شنودگر، به کارگیری مشخصات لایه فیزیکی کانال بی‌سیم است که امنیت لایه فیزیکی نامیده می‌شود[2] . اخیرا مسئله برقراری امنیت لایه فیزیکی با استفاده از تئوری اطلاعات توجه زیادی را به خود جلب کرده است. مفهوم تئوری اطلاعات امنیت، اولین بار توسط شانون [3] معرفی شده است که در آن با به کارگیری سیاست‌هایی، امنیت پیام محرمانه حفظ می‌گردد. سپس wyner کانال استراق سمع کننده را معرفی نموده [11] و نشان داده است زمانی که کانال شنودگر بدتر از کانال بین فرستنده و گیرنده باشد، فرستنده و گیرنده می‌توانند به خوبی پیام محرمانه را مبادله کنند و شنودگر

[1] AD HOC

قادر به رمزگشـایی کردن هیچ اطلاعاتی نخواهد بود. هدف اصـلی این مقاله بیشینه سازی نرخ امنیتی اسـت. در [12]، نویسـندگان ظرفیت امن کانال اسـتراق‌سمع کننده گوسی را مطالعه نموده و اختلاف بین ظرفیت شـــانون کانال بین فرســـتنده و گیرنده و ظرفیت امن کانال گوســـی نامیده‌اند. همچنین، csiszar و korner کانال اسـتراق‌سمع کننده را به کانال پخشی کلی تعمیم‌داده و نشان داده‌اند زمانی که ظرفیت کانال بین فرسـتنده و شـنودگر از ظرفیت کانال بین فرستنده و گیرنده کمتر باشد ارتباط امن محقق می‌گردد [13]. بنابراین به دلیل افزایش تقاضـای انتقال داده‌ها به صورت امن، این موضوع توجه فراوانی را به خود جلب کرده است و موجب تعریفی جدیدی از نرخ با عنوان نرخ امن شده است. از دیدگاه لایه فیزیکی مفهوم نرخ امن با یک مدل کانال به نام کانال اسـتراق سـمع در پیشـنهاد شد. نرخ امن به صـورت تفاضل نرخ بین فرستنده و گیرنده (کانال اصلی) و نرخ قابل وصول بین فرستنده و شـنود اسـت.. بنابراین، برقراری امنیت لایه فیزیکی یکی از مسـائل اسـاسـی در شـبکه‌های مخابراتی بی‌سیم است و به‌همین منظور در این پایان‌نامه مسئله امنیت لایه فیزیکی شبکه در حضور شنودگر را بررسی می‌کنیم.

لازم به ذکر است که اگر نرخ بین فرستنده و شنود بیش از نرخ کانال اصلی باشد نرخ امن برابر با صـفر اسـت. در واقع شـرایط کانال، مانع رویکردهای ابتدایی امنیت لایه فیزیکی در سـیسـتم‌های تک‌آنتنی می‌شـود. به طور کلی برای دسـتیابی به یک نرخ امن غیرصـفر، اسـتفاده از سـیسـتم‌های چندآنتن الزامی اســت. اما به دلیل محدودیت اندازه و توان مصــرفی گره‌های موجود در شــبکه، پیاده‌سازی چندآنتن همیشه امکان‌پذیر نمی‌باشد. مخابرات مشارکتی یک راه موثر وجایگزین است که مزایای استفاده از سیستم‌های چند آنتن را برای گره‌های تک آنتنی فراهم می‌کند. در این راستا نقش جدیدی از رله در برای ایجاد یک ارتباط امن از منبع به مقصـد معرفی شده است. ارتباطات مشارکتی به کمک رله که در آن رله سـیگنال دریافتی از فرستنده را به گیرنده هدایت می‌کند، قابلیت اطمینان کانال فرســـتنده تا گیرنده را بهبود می‌بخشـــد و به دلیل قابلیتش در افزایش ظرفیت و کاهش توان مصـرفی توجه زیادی را به خود جلب کرده اسـت [14]. دو نوع متداول از رله‌ها، رله‌های رمزگشایی و

ارسال و تقویت ارسال نام دارند. در رله رمزگشایی و ارسال، رله سیگنال دریافتی از فرستنده را پس از رمزگشایی‌کردن، مجددا کدگذاری نموده و به گیرنده ارسال می‌کند که ما در این پایان نامه از این رله استفاده کردیم. در رله تقویت و ارسال، رله پس از دریافت سیگنال از فرستنده، آن را تقویت کرده و به گیرنده ارسال می‌کند.

۱-۳ نوآوری و اهمیت مطالعه حاضر

در سناریوی استفاده فرصت‌طلبانه[۱] از طیف، تداخل ایجادشده توسط کاربران ثانویه در کاربران اولیه باید زیرحدآستانه[۲] نگه داشته شود، در حالی که برای تضمین کیفیت سرویس[۳] در شبکه ثانویه تلاش می‌گردد. به‌طور کلی، برای کاربران شناختی و کاربران اولیه مشکل است که در یک ناحیه جغرافیایی، زمان و باند فرکانسی یکسان کار کنند. از این‌رو،تضمین کیفیت مطلوب در هر دو شبکه اولیه و ثانویه همواره از جمله چالش‌های موجود در پیاده سازی عملی شبکه‌های رادیویی شناختی بوده است. اما این امر می‌تواند با به کارگیری برخی روش‌ها از قبیل ارتباطات مشارکتی و ارسال‌های جهتی به نحو مطلوبی تحقق بخشیده شود. هدف از انجام تحقیق پیش‌رو، ارائه روش‌هایی است که علاوه‌بر تضمین کیفیت سرویس در شبکه اولیه که برای استفاده از طیف مجاز است، شرایطی را فراهم کند که کاربران ثانویه نیز به کیفیت مطلوب دست‌یافته و همزیستی میان دو شبکه خللی در ارتباطات موجود در هیچ یک از شبکه اولیه ایجاد نکند.

تخصیص مناسب منابع برای دستیابی به حداکثر مجموع نرخ امن به عنوان یک موضوع مهم در شبکه های رادیو شناختی مطرح است. برای حل این مسئله با سه چالش روبرو هستیم. یکی تعریف جدیدی از نرخ به عنوان نرخ امن که به شکل تفاضل نرخ دو کانال اصلی و شنود است و دیگری استفاده از رله برای دستیابی به نرخ امن غیر صفر که منجر به پیچیده شدن مسئله و حل آن می‌گردد.

---

[۱] Opportunistic

[۲] Threshold

[۳] Quality of Service (QoS)

از تحقیقاتی که در این زمینه با اســتفاده از رله یک طرفه در شــبکه‌های غیرشــناختی انجام شــده می‌توان به اشــاره کرد .چالش ســوم، اضــافه شــدن محدودیت‌های تداخل برای کاربران اولیه در شــبکه‌های شــناختی اســت که موجب ســخت تر شــدن حل مســئله می‌گردد که بدون درنظر گرفتن موضوع امنیت و نرخ امن به حل این دسته از مسائل پرداخته شده است.

همان طور که بیان شد اکثر کارهای انجام شده در شبکه های رادیو شناختی بر تخصیص منابع بدون متمرکز درنظر گرفتن امنیت و یا دستیابی به نرخ امن با استفاده از روش سیستم‌های چندآنتنی است. در زمینه بررسی مجموع نرخ ارسال امن و تخصیص منابع در شبکه رادیوشناختی مبتنی بر رله یک طرفه کدبرداری و ارســال انجام شــده اســت. بنابراین ما در این پایان نامه با پیشــنهاد یک شــبکه شــناختی با بهینه سازی لاگرانژ و بررسی نرخ امن در این شبکه با استفاده از رله یک طرفه کدبرداری و ارســال، به تخصیص توان و زیرحامل و انتخاب رله در این شبکه می پردازیم و نشان می دهیم برای رسیدن به نرخ امن غیر صفر استفاده از رله در شبکه های شناختی از اهمیت بیشتری نسبت به شبکه های غیرشــناختی برخوردار اســت. برای بهبود عملکرد سیستم و تکمیل انتقال اطلاعات دو کاربر، می توان از رله دو طرفه استفاده کرد. درواقع با در نظرگرفتن رله‌های دوطرفه و امکان برقرار شدن ارتباط فروســو و فراســو به طور همزمان می‌توان عملکرد ســیســتم را بهبود بخشــید. در مقایسه با کانال رله یک‌طرفه که پیام یکی از دو گره‌های منبع را به دیگری ارســال می‌کند، در کانال رله دو طرفه، دو فرســتنده از طریق یک رله تبادل اطلاعات می‌کنند؛ بنابراین کارایی طیفی برای تبادل اطلاعات بین دو گره منبع با اجازه دادن به رله برای دریافت و یا ارسال به دو گره منبع در یک زمان، بهبود می‌یابد.

در زمینه تخصــیص منابع در شــبکه‌های شناختی با رله دوطرفه در و از تحقیقات انجام شده با اســتفاده از رله کدبرداری و ارســال می‌توان به اشاره که تنها به تخصیص توان با بیشینه کردن نرخ با رله کدبرداری و ارسال پرداخته شده است. همچنین در زمینه تخصیص منابع با نرخ امن با استفاده از رله دوطرفه تحقیقات بســیار محدودی انجام شده است و بیشتر کارهایی که در این زمینه انجام شده

از رله با اســتراتژیAF و یا از رله دوطرفه با اســتفاده از ســه بازه زمانی اســتفاده شــده است. بنابراین تاکنون کاری در زمینه نرخ امن با استفاده از رله دوطرفه با دو بازه زمانی در شبکه‌های رادیو شناختی با بهینه سازی لاگرانژ انجام نشده است. از این رو، ما در این پایان نامه با پیشنهاد یک شبکه شناختی مبتنی بر رله دو طرفه کدبرداری و ارسال با دو بازه زمانی، به تخصیص منابع برای دستیابی به بیشینه نرخ امن در این شبکه می‌پردازیم.

۱-۴ محتوای فصل‌های بعد

در فصــل دوم، شبکه رادیو شناختی به عنوان راه حلی برای رفع مشکل کمبود طیف و افزایش بهره‌وری فرکانسی در شبکه های بی سیم معرفی می شود. ویژگی‌ها و ساختار کلی این شبکه و مدل های مختلف آن بیان می‌شــود. ســپس به مفهوم نرخ امن و روش‌های موجود برای دســتیابی به آن پرداخته می‌شــود. همچنین چالش های موجود در تخصــیص منابع شبکه های رادیو شناختی بیان و بررســی می شــود. در فصــل سوم، به بررسی شبکه رله های یک طرفه و ظرفیت امن در این شبکه‌ها پرداخته می‌شود و سپس منابع مطالعاتی استفاده شده در این تحقیق و سابقه تحقیقات انجام شده در زمینه تخصــیص منابع در شــبکه های شــناختی و نرخ امن مبتنی بر رله بررســی می‌شــود. در فصــل چهارم مســئله تخصــیص منابع برای دستیابی به نرخ امن و حل آن در شبکه رادیو شناختی مبتنی بر رله یک طرفه کدبرداری و ارســال مطرح می شــود. در ادامه این فصــل، تأثیر عوامل مختلف بر روی مجموع نرخ امن با ارائه نمودارهای شبیه‌سازی بررسی می‌شود. سپس در فصل پنجم مسئله تخصیص منابع برای دستیابی به نرخ امن و حل آن در شبکه رادیو شناختی مبتنی بر رله دو طرفه کدبرداری و ارســال با دو بازه زمانی مطرح می‌شود و بهبود نرخ شبکه با استفاده از رله دو طرفه نسبت به رله یک طرفه و تأثیر پارامترهای مختلف سیستم با ارائه نمودارهای شبیه سازی بررسی می‌شود. در آخر جمع بندی و نتیجه گیری این پایان نامه و همچنین ارائه پیشــنهادات و کارهای آتی در فصــل شــشم ارائه می‌شود.

فصل دوم: روش تحقیق

۱-۵ سیستم‌های رادیو شناختی

امروزه شبکه‌های رادیویی، روشی مفید جهت استفاده بهینه از منابع طیف فرکانسی دارای مجوز به شمار می‌آید. یکی از روش‌های موثر جهت سنجش طیف فرکانسی، شبکه رادیو شناختی و بکارگیری چند شبکه ثانویه به صورت مشارکتی می‌باشد. این روش در محیط‌های طبیعی با اثر محوشدگی شدید کانال، احتمال تشخیص نادرست و وقوع تداخل بر روی شبکه اولیه را کاهش می‌دهد. رادیو شناختی تکنولوژی است که دسترسی به طیف را پشتیبانی می‌کند و سیاست آن در بیشتر کشورها بر مبنای نظارت طیف می‌باشد. بنابراین رادیوشناختی به عنوان بهترین تکنولوژی امید بخش برای ارتباطات بی‌سیم آینده می‌باشد. در شبکه رادیو شناختی یک طیف برای شبکه اولیه وجود دارد که شبکه ثانویه می‌تواند به صورت توافقی با اجازه شبکه اولیه از طیف استفاده کند. این اجازه اولیه به روش‌های مختلف وجود دارد به طور مثال تا زمانی که تداخل بر روی اولیه اثر نگذارد ثانویه می‌تواند از طیف استفاده کند. شبکه‌های بی‌سیم و رادیو شناختی در ارتباطات متنوع شامل تئوری ارتباطات، شبکه مصنوعی، پردازش سیگنال، تئوری بازی، طراحی اتصال سخت افزار و نرم افزار و طراحی فرکانس رادیویی با هم همکاری دارند [15]. تقریباً تمام بخش های قابل استفاده طیف فرکانسی به کاربردهای خاص اختصاص یافته و در ظاهر با نوعی کمیابی پهنای باند مواجه هستیم؛ درحالی که اگر طیف فرکانسی مورد استفاده را مرور کنیم، متوجه می‌شویم که برخی از قسمت‌های طیف در اغلب اوقات تقریباً بدون استفاده هستند و یا بعضی اوقات و در مکان‌های خاص استفاده می‌شوند که در این شرایط استفادهٔ فرصت طلبانه از باندهای فرکانسی خالی ضروری به نظر می‌رسد.

کمیابی پهنای باند درواقع ناشی از روند کنونی تخصیص فرکانس ثابت و ناهماهنگی این روند با نیازهای واقعی در کاربرها و زمان های مختلف است. درواقع لازم است روش‌هایی برای استفاده کارا و مناسب کاربران بدون مجوز که آن‌ها را کاربران ثانویه می‌نامیم، از باندهای اختصاص یافته تدوین شود،

به نحوی که برای کاربران اصـلی دارای مجوز که آنها را کاربران اولیه می نامیم، تداخل مخرب ایجاد نشـود، یا در اصـطلاح همزیستی غیر مخربی بین کاربران اولیه و ثانویه وجود داشته باشد. لازمهٔ چنین سـازوکاری طراحی رادیوهایی اسـت که دارای توانایی های خاص باشـند. قابلیت جسـت وجوی طیف، قابلیت تصـمیم گیری و یادگیری و قابلیت تطبیق با شـرایط محیطی نمونه هایی از این توانایی ها هسـتند. رادیوشـناختی قادر اسـت از طریق حسـگری طیفی[۱]، بودن یا نبودن کاربران اصـلی فرکانس موردنظر را آشـکارسـازی نموده و از اطلاعات حاصـله در جهت بهره برداری فرصـت طلبانه از طیف[۲] اسـتفاده نماید. بنابراین در رادیوشناختی، سنجش طیف بخش مهمی برای استخراج حفره های طیفی[۳] برای سامانهٔ ثانویه است.

در یک دسته بندی دو رویکرد به اشتراک گذاری طیف فرکانسی بیان شده است [16].

- ✓ دسترسی فرصت طلبانه به طیف : که در آن یک کاربر ثانویه تنها زمانی به یک باند دسترسی دارد که این باند در حال استفاده توسط کاربر اولیه نباشد [17].
- ✓ اشتراک طیف: در آن کاربر ثانویه، همزمان با کاربر اولیه، از یک طیف فرکانسی برای انتقال داده استفاده می کنند، اما کاربر ثانویه محدودیت توان ارسالی، برای تضمین کیفیت خدمات کاربر اولیه را لحاظ می کند.

بنابراین بهره‌وری از منابع فرکانسـی یکی از اهداف توسـعهٔ فناوری سـامانه‌های ارتباطی اسـت و دلایل آن در محدودیت‌های موجود در منابع فرکانسـی و افزایش تقاضـا برای اسـتفاده از آن خلاصـه می‌شـود. یکی از نیازهای اسـاسـی در سـامانه‌های ارتباطی، ارسـال اطلاعات اسـت که با مشـکل محدودیت‌های منابع فرکانسـی مواجه هستند. همچنین مسئله اصلی این است که سامانه‌های ارتباطی کنونی در معرض اختلال و شـنود هسـتند و ما در اینجا به دنبال بسـتر ارتباطی مقاوم در برابر شنود و

[۱] Spectrum Sensing
[۲] Opportunistic Spectrum Access
[۳] Spectrum Holes

اختلال هستیم .پس استفاده نکردن بهینه از منابع فرکانسی، ناتوانی مقابله با اختلال و شنود در سامانه‌های ارتباطی کنونی یکی از چالش‌های اساسی به حساب می‌آید.

ازاین‌رو در شبکه‌های ارتباطی رادیوشناختی، با توجه به اینکه فرکانس تخصیص داده شده به این رادیوها اصلاً مشخص نیست و این رادیوها با توجه به توانایی‌ها و ویژگی هایی که دارند، باندهای فرکانسی خالی را شناسایی می‌کنند و در آن باند فرکانسی تبادل اطلاعات می‌کنند و هرلحظه امکان این وجود دارد که فرکانس خود را تغییر دهند، بنابراین طراحی این‌گونه رادیوها به دلیل نداشتن فرکانس ثابت‌کاری می‌تواند به تولید سامانه‌هایی بی‌انجامد که در برابر اختلال و شنود مقاوم باشند. ارتباط امن و مقاوم خود باعث برتری در میدان رزم و افزایش توان نظامی خواهد بود [18].

روزبه‌روز نیاز به ارسال اطلاعات به صورت بی‌سیم با میزان ارسال بالا و همچنین نیاز به کانال‌های با ظرفیت بالاتر مانند کاربردهای چندرسانه‌ای، در حال افزایش است. این تقاضای روزافزون برای نرخ‌های بالاتر و تعداد کاربران بیشتر به‌طور متناظر موجب افزایش تقاضا برای پهنای باندهای بزرگ‌تر می‌گردد. ازاین‌رو جایگزینی سامانه‌های کنونی با سامانه‌های جدیدی که قابلیت ارسال با نرخ بالاتر را داشته و در برابر اثرات ناشی از اختلال از خود مقاومت نشان دهند ضروری به نظر می‌رسد و در غیراین‌صورت، در آیندهٔ نزدیک برای ارسال اطلاعات با چالش جدی مواجه خواهیم شد. بنابراین ایده و طرح شبکه‌های رادیو شناختی، پیاده‌سازی یک پیوند رادیویی بر پایهٔ صوت و دیتا که بتواند یک ارتباط مقاوم در برابر اختلال و شنود را داشته باشد، می‌تواند سودمند باشد. همچنین پیاده‌سازی چنین شبکه‌های باعث می‌شود تا از منابع فرکانسی کاربران خاموش و یا نیمه خاموش که اطلاعاتی برای ارسال ندارند، برای ارسال اطلاعات در دیگر رادیوها استفاده نمود [19].

پیاده‌سازی فناوری رادیوشناختی در سامانه‌های ارتباطی می‌تواند به کاهش اثرات اختلال و شنود در این سامانه‌ها بی‌انجامد و همچنین می‌تواند به عنوان یک لایه ارتباطی مقاوم در برابر اختلال و شنود نسبت به شبکه‌های ارتباطی بی‌سیم موجود جایگزین شود؛ بدون اینکه سرعت تبادل اطلاعات کاسته

شـود. در این راسـتا سـامانه‌های ارتباطی مبتنی بر روشـهای طیف گسـترده[1] از نوع پرش فرکانسـی[2] پیشـنهاد شـده اسـت و این سـامانه‌ها در حال حاضر در کشور وجود دارد؛ ولی با توجه به اینکه در این سامانه‌ها، پرش‌های فرکانسی دارای الگوی خاصی هستند و این پرش‌ها به صورت منظم انجام می‌گیرند. این رادیو رله برای افزایش امنیت، بایسـتی این سامانه به سامانه‌های رمزکننده مجهز شوند، تجهیز این سـامانه به رمزکننده باعث کاهش سـرعت و کارایی این سـامانه می‌شود [20]. پایش طیف یکی از اجزا مهم در شـبکه‌های رادیو شـناختی برای استخراج منابع فرکانسی بدون استفاده است و عملکرد شبکه در استخراج این منابع برحسب دقت و کارایی توصیف می‌شود. این مسئله به‌طور کامل تجزیه و تحلیل شـده و تعداد رادیوهای ارتباطی که می‌خواهند به صـورت اجاره‌ای از منابع فرکانسـی بدون اسـتفاده رادیوهای دیگر استفاده کنند، به دست آمده است.

۱-۶ معرفی سیستم‌های رادیوشناختی

امروزه نیاز به ارسـال اطلاعات به صـورت بی‌سیم برای دسترسی به کاربردهای با میزان ارسال بالا، نظیر کاربردهای چندرسانه‌ای، روزبه‌روز در حال افزایش است. این تقاضای روزافزون برای نرخ‌های بالاتر و تعداد کاربران بیشـتر به‌طور متناظر موجب افزایش تقاضـا برای پهنای باندهای بزرگ‌تر می‌گردد. روش‌های موجود نظیر اسـتفاده از روش‌های مدولاسـیون پیچیده، کدینگ‌های مختلف، اسـتفاده از چند آنتن و روش‌های دیگر سـعی در حداکثر نمودن بهره‌وری طیفی در یک پهنای باند خاص که برای اسـتفاده کاربر موردنظر به صـورت ثابت تخصـیص یافته اسـت، داشـته و از پهنای باند موجود حداکثر اسـتفاده را برای ارسـال میزان بالاتر و یا سـرویس دهی به کاربران بیشـتر می‌نمایند[22]–[20].

برای رسـیدن به میزان ارسـال بالاتر بیش از مقادیر فعلی تنها روش ممکن، اسـتفاده از پهنای

---

[1] Spreed Spectrum

[2] Frequncy Hopping

باندهای فرکانسی بیشتر است. این روش با توجه به اینکه طیف فرکانسی یک منبع طبیعی است و قسمت‌های مختلف آن برای کاربردهای مختلف تخصیص یافته، در نگاه اول امکان‌پذیر نیست. اندازه گیری‌هایی که توسط محققان صورت گرفته است، نشان می‌دهد که از منابع فرکانسی موجود به صورت بهینه استفاده نمی‌شود و شاهد وجود منابع فرکانسی بدون استفاده در طول باند فرکانسی و نیز زمان‌ها و مکان‌های مختلف هستیم. بررسی این مشاهدات برای قسمت‌های مختلف طیف رادیویی، نتایج زیر را می‌دهد [23].

1- برخی از باندهای فرکانسی در اغلب اوقات خالی هستند.

2- برخی دیگر از باندهای فرکانسی نسبتاً شلوغ هستند.

3- بقیه باندها نیز به شدت مورد استفاده قرار می گیرند.

با در نظر گرفتن موارد اشاره شده می‌توان فهمید که کمبود منابع طیف فرکانسی که سامانه‌های مخابراتی کنونی با آن مواجه هستند، صرفاً ظاهری است. در راستای استفاده هر چه بهتر از منابع فرکانسی، لازم است که سیاست‌گذاری‌های قبلی تخصیص فرکانس مورد تجدیدنظر قرار گیرند. در حقیقت مشاهدات صورت گرفته نشان می‌دهند که منابع فرکانسی زیادی برای استفاده وجود دارند که مشکل کمبود ظاهری طیف فرکانسی، از تخصیص نیافتن و استفادهٔ مناسب از منابع فرکانسی ناشی می شود[26]–[24] .

۱-۷ سامانه‌های اشتراک طیفی پویا[1]

با در نظر گرفتن نیاز فراوان به پهنای باندهای بزرگ‌تر، به عنوان یک راه حل اولیه به نظر می‌رسد، می‌توان مشکل کمبود منابع فرکانسی را با تخصیص مجدد این منابع برای کاربردهای مختلف حل نمود. اما تخصیص مجدد منابع فرکانسی به صورت ثابت، با توجه به نبود امکان پیش بینی دقیق کاربردهای آتی و نیز مشکلاتی که برای سامانه‌ها و کاربران جاری پیش می آورد، امکان

[1] Dynamic Spectrum Sharing

پذیر نیست. با توجه به این موضوع و تجربه موفق اشتراک طیفی در قسمتی از باندهای فرکانسی، درکشور آمریکا در سال‌های اخیر استفاده از سامانه‌های اشتراک طیفی پویا به عنوان راه حل مشکل یادشده مطرح شده است.

کاربران ثانویه ازنظر استفاده از باند فرکانسی در اولویت بعدی، پس از کاربران اولیه، قرار دارند. در حقیقت این کاربران ارتباط خود را از طریق روش‌های مختلف اشتراک‌گذاری طیفی در مواقعی که حفره‌های طیفی وجود دارند، انجام می‌دهند. اصولاً دو روش عمده برای اشتراک‌گذاری طیفی مطرح شده است. در زیر این دو روش عمده معرفی می‌گردد:

۱-۷-۱ اشتراک گذاری طیفی به روش ارسال زمینه ایی[۱] سیگنال ها

در حالت کلی در این دسته از سامانه‌ها فرض بر این است که کاربران اولیه در باندهای فرکانسی حضور دارند و کاربران ثانویه با توجه به این موضوع علاقه‌مند به استفاده از باند فرکانسی هستند. کاربران ثانویه باید ارسال خود را به نحوی انجام دهند که موجب تداخل با سیگنال کاربر اولیه نگردند. به عبارت دیگر سیگنال کاربران ثانویه باید به‌صورت یک نویز برای کاربران اولیه عمل نمایند. بنابراین تا زمانی که با ارسال توان سیگنال ثانویه مقدار سطح مجاز نویز در گیرنده کاربر اولیه از حد مجاز فراتر نرود، کاربران ثانویه می‌توانند به فعالیت خود در باند فرکانسی موردنظر ادامه دهند. مقدار سطح مجاز نویز در گیرنده کاربر اولیه باید تا حدی کم باشد که کاربر اولیه برای عملکرد صحیح خود دچار مشکل نگردد. به عنوان مثال سامانه‌های باند وسیع را که امروزه برای کاربردهای با مسافت کم مورد توجه واقع شده‌اند، می توان در زمرهٔ این دسته از روش‌های اشتراک طیفی در نظر گرفت. در این نوع از سامانه‌ها، براساس قوانین مشخص شده از طریق مراجع بین‌المللی‌مخابرات، حداکثر سطح توان ارسالی که کاربر مجاز است در باندهای مختلف فرکانسی ارسال خود را با آن انجام دهد، مشخص شده است. در این نوع از سامانه‌های رادیویی اشتراک طیفی، برای اینکه سیگنال کاربر ثانویه به صورت نویز

[۱] Underlay Spectrum Sharing

برای کاربر اولیه ظاهر شود، لازم است که از روش‌های گسترده سازی طیفی استفاده گردد.

۱-۷-۲ اشتراک گذاری طیفی به روش روی‌هم‌گذاری[۱] سیگنا ل‌ها

همان طور که ذکر شـد، طبق قوانین مخابراتی و تخصـیص فرکانسـی اصـولاً برای هر باند فرکانسـی اختصـاصی، یک یا چند کاربر اولیه یا اصلی در نظر گرفته شده است. در این دسته از سامانه های اشـتراک گذاری طیفی، کاربر ثانویه تنها پس از اطمینان از فعالیت نداشـتن کاربر اولیه می تواند ارسال خود را در آن انجام دهد. در حقیقت ایده این روش مشابه روش‌های فعلی دسترسی طیفی است که در آن یک کاربر به قسـمتی از طیف که توسـط کاربر ثبت شـده‌ای اشـغال نشـده باشـد، می‌تواند دسـترسی پیدا کند. در حقیقت در این سامانه‌ها، تداخل کاربران فرعی بر روی کاربران اصلی به حداقل می‌رسد.

در این روش، هدف طراحی و توسـعه یک سـامانه مخابراتی هوشـمند است که قادر به حس کردن محیط طیفی در خلال یک محدوده وسیع فرکانسی بوده و تنها هنگامی‌که موجب تداخل در سیگنال های کاربر اولیه نشـود، ارسـال خود را انجام می‌دهد. این کاربران ثانویه با الویت ارسـال پایین، ارسال خود را از طریق رادیو هوشمند انجام می‌دهند.

۱-۸ طیف رادیویی

طیف رادیویی یک منبع طبیعی اسـت که اسـتفاده از آن برای کاربردهای متنوع، از طریق اختصـاص منابع فرکانسـی توسـط سـازمان‌ها و مراجع مرتبط با امر تخصـیص فرکانسی، در هر کشور، صـورت می‌گیرد. در زمینه سـامانه‌های اشـتراک طیفی، به کاربرانی که از طریق سازمان‌های تخصیص فرکانسـی، حق اسـتفاده از قسمت‌های خاصی از طیف فرکانسی را دارند، اصطلاحاً کاربران اولیه اطلاق می‌گردد. به عبارت دیگر کاربران اولیه را می‌توان مالکان اصـلی بخشـی از طیف فرکانسـی که مجاز به

[۱] Overlay Spectrum Sharing

فعالیت در آن هستند، در نظر گرفت. در راستای تعریف یادشده و با توجه به نبود بهره‌وری مناسب از منابع فرکانسی موجود، مفهوم جدیدی به نام حفره‌های طیفی مطرح شده است که به‌صورت زیر تعریف می‌گردد. یک حفره طیفی یک باند فرکانسی است که از ابتدا به یک کاربر اولیه تخصیص یافته است، اما در یک زمان خاص و یک منطقهٔ جغرافیایی ویژه، کاربر اولیه از این باند استفاده نمی‌کند.

دو تعداد و پهنای باند حفره‌های طیفی در طول زمان در حال تغییر است و قسمت‌هایی از طیف فرکانسی نیز که در حال استفاده توسط کاربران اولیه است، دارای چگالی توان مختلف هستند. با توجه به مشاهدات یادشده که وجود حفره‌های طیفی مختلف را نشان می‌دهد، بررسی روش‌های اشتراک طیفی پویا برای استفاده هر چه بهتر از منابع طیفی ضروری به نظر می‌رسد. مشکل نبود بهره‌وری بهینه از طیف فرکانسی را می‌توان به طور قابل توجهی از طریق معرفی کاربران ثانویه حل نمود. کاربران ثانویه، کاربرانی هستند که برای ارسال سیگنال خود از حفره‌های طیفی موجود در طیف فرکانسی بهره می‌گیرند.

بعد از مطرح شدن مفاهیم اولیه و پس از اندازه‌گیری‌های انجام شده که دلالت بر استفاده نکردن مناسب از طیف فرکانسی داشتند، ایدهٔ استفاده و پیاده سازی عملی این سامانه ها مورد توجه فراوانی قرار گرفت. وظایف یک رادیو هوشمند را می‌توان به صورت زیر دسته بندی کرد:

- ✓ تحلیل محیط رادیویی و مشاهده باند پایش طیف که مراحل زیر را در برمی‌گیرد:

  تخمین دمای تداخل محیط رادیویی[1]

  تشخیص حفره‌های فرکانسی

  شناسایی کانال که شامل مراحل زیر است:

[1]

تخمین اطلاعات حالت کانال[۱۱]

پیش بینی ظرفیت کانال

واپایش توان ارسالی و مدیریت پویای طیف.

دو وظیفهٔ اول در بخش گیرنده انجام می شود و وظیفه سوم در فرستنده صورت می گیرد، از همین جا پیداست که فرستنده و گیرنده در یک ماژول رادیوی هوشمند باید در هماهنگی کامل با یکدیگر باشند. تعریف رادیو هوشمند به این صورت مطرح شده است رادیو هوشمند یک سامانه مخابراتی بی سیم باهوش است؛ به گونه‌ای که از محیط اطراف خود دنیای بیرون آگاه است و در هر زمان با ایجاد تغییر در عامل‌های عملیاتی خود مانند توان ارسالی، فرکانس حامل، نوع و مرتبه مدولاسیون، خود را با محیط اطراف خود وفق می‌دهد. این سامانه دو هدف را دنبال می نماید:

- ✓ ارتباطات با قابلیت اطمینان بالا، در هر زمان و هر مکان که موردنیاز باشد
- ✓ استفاده بهینه از منابع فرکانسی.

ایدهٔ اصلی در تعریف سامانه‌های رادیو شناختی این است که این سامانه قابلیت حس‌کردن محیط اطراف، پردازش اطلاعات به دست آمده به طریق مناسب و تنظیم عملکرد خود بر اساس آن‌ها را داشته باشد. حس‌کردن محیط اطراف، تنها با اندازه‌گیری توان در یک باند فرکانس خاص محدود نمی‌شود، بلکه به روش‌های پیچیده‌تری نیازمند است تا بتوان تغییرات زمانی، فضایی محیط را آشکار نمود. به کمک این قابلیت، رادیویی شناختی قادر است بخش‌هایی از طیف را که در زمان و مکان خاص بدون استفاده هستند، مشخص کرده و سپس بهترین باند فرکانسی را همراه با مقدار عوامل برای عملکرد مناسب، تعیین نماید.

[۱۱] Channel State Information (CSI)

۱-۸-۱ حسگری به صورت مشارکتی

عملیات تخمین میزان ترافیک طیف در یک محدوده جغرافیایی را می‌توان به صـــورت محلی توسط یک گیرنده رادیوشناختی انجام داد و یا اینکه اطلاعات به دست آمده از چندین رادیوشناختی را با هم ترکیب کرد. عموماً حسگری مشارکتی به عنوان راه حلی برای حل مسائلی چون نبود قطعیت در تخمین توان نویز، کانال محوشـدگی[۱] و کانال سـایه افکنی[۲] معرفی می شـود. حسـگری مشـارکتی احتمال هشـدار خطا و احتمال عدم آشـکارسـازی صـحیح را به مقدار قابل توجهی کاهش می دهد. به علاوه این روش می‌تواند مسئله کاربر اولیه مخفی را حل کند و زمان حسگری را کاهش دهد.

به اشـتراک گذاشتن اطلاعات حسگری به طورکلی به دو روش سخت و نرم امکان پذیر است. در روش سخت، گیرنده ها نتایج باینری حاصل از تصمیم‌گیری در مورد بودن یا نبودن کاربر اولیه را با هم به اشـتراک گذاشته و ایستگاه مرکزی تصمیم‌گیری نهایی را براساس مجموع اطلاعات باینری به دست آمده انجام می‌دهد. در روش نرم، گیرنده‌ها، متریک‌های تصـمیم‌گیری را عیناً به اشـتراک گذاشـته به عنوان مثال انرژی اندازه‌گیری شـده و تصمیم‌گیری بر متریک نهایی حاصل انجام می‌گیرد. ترکیب نرم همواره عملکرد بهتری دارد .در یک سـامانهٔ رادیو شناختی که از طرح ساده LBT[۳] استفاده می‌کند، با اسـتفاده از روش حسـگری محلی می‌توان بخش‌های خالی طیف را بدون ایجاد تداخل برای کاربران اولیه به کار گرفت. از طرفی نشـان داده شـده اسـت که به کارگیری حسگری مشارکتی ظرفیت طیفی بسیار بالاتری را برای کاربر ثانویه فراهم می آورد.

روش حسگری مزایا معایب

- ✓ حسگری غیرمشارکتی

[۱] Fading
[۲] Shading
[۳] Listen Before Talk

- ✓ سادگی محاسباتی و پیچیدگی، مسئله گره پنهان، سایه افکنی و محوشدگی چند مسیری.
- ✓ حسگری مشارکتی

دقت بالا، کاهش زمان حسگری، جلوگیری از مشکل گره پنهان و اثر سای هافکنی، پیچیدگی، ترافیک بالا، نیاز به کانال واپایشی.

۱-۹ معرفی رادیو شـــنـــاختی به عنوان یک لایه مقاوم در برابر شـــنود و اخلالگر

در این بخش قابلیت ضداختلال شبکه های رادیو شناختی را به عنوان یک لایه ارتباطی مقاوم در مقابل شـنود و اختلال در مواقع بحران ارائه می‌شـود. با توجه به این‌که شبکه‌های رادیوشناختی جهت حل مسـئله کمبود طیف معرفی شـده‌اند، با روش‌های دسترسی طیف پویا، دسترسی طیف برای مرتبه دوم به این رادیوها داده می‌شـود، به شـرطی که در آن زمان و موقعیتی که رادیو شـناختی از شـبکه استفاده می‌کند در ارتباط کاربر اصلی مزاحمتی ایجاد نشود، این بدین معنی است که رادیو شناختی به صـورت متناوب بایسـتی طیف باند را برای آشکارسازی فعالیت کاربر اولیه پایش کند، به محض این که فعالیت کاربر اولیه آشـکار شـد، کاربران ثانویه بلافاصـله باید کانال را خالی کنند تا تداخل به کمترین مقدار خود برسد.

در مورد اختلال‌کننده‌ها، ازیک طرف اخلالگر می‌تواند قابلیت اختلال خود را با به کارگیری فنّاوری رادیو شـناختی بالا ببرد، از طرف دیگر، قابلیت جهش در میان کانال‌ها به رادیو شـناختی این امتیاز را می‌دهد که عملکرد ضـداختلال خود را بهبود ببخشـد. ینابراین عملکرد ضداختلال یک مسئله جدید و جالب در شبکه‌های رادیوشناختی است. اگر رادیوشناختی لایهٔ فیزیکی ضداختلال داشته باشد ممکن است به اختلال حساس باشد؛ یعنی با حضور اختلال کم یا تداخل، رادیو باید کانال را خالی کند. این بدین معنی اسـت که یک اختلال‌کننده می‌تواند از سـیگنال‌های با انرژی کم برای اختلال چندین کانال به طور همزمان اسـتفاده کند؛ ولی چنین الگوهایی ممکن اسـت پرهزینه باشـند، زیرا راه‌اندازی

کانال جدید و سـوئیچ رادیوها به خاطر نیاز به همزمانی فرکانسـی و زمانی، تخمین کانال و دسـت به دست کردن و ... زمانبر است.

البته مشکل اساسی آن است که کانال‌های دردسترس، ممکن است در طول زمان تغییر کنند و اطلاعات آن‌ها در میان گره‌های شـبکه تعریف نشده باشند که اگر در طراحی دقت نشود سوئیچ‌کردن کانال به شـدت گذردهی را کاهش می‌دهد، حتی ممکن اسـت شـبکه رادیو شناختی را بدون استفاده کند. در مقابل برای یک اختلال‌کننده که از ابزارهای رادیو شـناختی مشـابهی اسـتفاده می‌کند، برای هدایت حمله‌های اختلال، قابلیت سوئیچ سریع کانال، قابلیت اختلال آن را افزایش خواهد داد؛ زیرا این اخلالگر به آسانی می‌تواند چندین کانال را هم زمان مختل کند.

در مورد اختلال‌کننده‌ها فرضیات زیر را در نظر می‌گیریم:

1- اختلال‌کننده‌ها مجهز به ابزاری هسـتند که قابلیت‌های گره‌های شبکه‌های رادیوشناختی از قبیل پایش طیف و فرستنده و گیرنده RF را دارا هستند.

2- وقتی که شـبکه‌های رادیوشـناختی به کانال جدیدی سـوئیچ می کند مدت زمانی طول می کشد که اختلال کننده طیف را پایش کرده و کانال مورد نظر را پیدا کند که اگر این مدت زمان از زمان پایش شـبکه‌های رادیوشناختی بیشتر باشد، اختلال‌کننده به ناچار باید به صورت تصادفی یک کانال را مختل کند؛ بنابراین نرخ سوئیچ کانال شبکه‌های رادیوشناختی قابلیت ضداختلال آن را تشدید می‌کند که به نوبهٔ خود باعث افزایش بازدهی و پهنای باند ارسال می‌شود.

3- اختلال‌کننده‌ها اطلاعات مربوط به شـبکه‌های رادیوشـناختی را که برای انتخاب کانال و ارتباط استفاده می‌کنند نمی‌دانند.

برای کانالی که مختل می‌شـود، تنها راهی که وجود دارد، این است که اختلال‌کننده به صورت تصـادفی کانالی را برای اختلال انتخاب کند، از آنجایی که اختلال‌کننده می‌تواند کانال را با سـرعت

سوئیچ کند ممکن است به طور همزمان چندین کانال مختل شوند. در مورد اختلال‌کننده‌ها فرضیات زیر را در نظر می‌گیریم:

1- اختلال‌کننده‌ها مجهز به ابزاری هستند که قابلیت‌های گره‌های شبکه‌های رادیوشناختی از قبیل پایش طیف و فرستنده و گیرنده RF را دارا هستند.

2- وقتی که شبکه‌های رادیوشناختی به کانال جدیدی سوئیچ می کند مدت زمانی طول می کشد که اختلال کننده طیف را پایش کرده و کانال مورد نظر را پیدا کند که اگر این مدت زمان از زمان پایش شبکه‌های رادیوشناختی بیشتر باشد، اختلال‌کننده به ناچار باید به صورت تصادفی یک کانال را مختل کند؛ بنابراین نرخ سوئیچ کانال شبکه‌های رادیوشناختی قابلیت ضداختلال آن را تشدید می‌کند که به نوبهٔ خود باعث افزایش بازدهی و پهنای باند ارسال می‌شود.

3- اختلال‌کننده‌ها اطلاعات مربوط به شبکه‌های رادیوشناختی را که برای انتخاب کانال و ارتباط استفاده می‌کنند نمی‌دانند.

برای کانالی که مختل می‌شود، تنها راهی که وجود دارد، این است که اختلال‌کننده به صورت تصادفی کانالی را برای اختلال انتخاب کند، از آنجایی که اختلال‌کننده می‌تواند کانال را با سرعت سوئیچ کند ممکن است به طور همزمان چندین کانال مختل شوند.

۱-۱۰ امنیت

امنیت در شبکه‌های بی‌سیم، امنیت WLAN شبیه به خانه‌تان است. مسئله این نیست که هکرها می‌توانند اقدامات امنیتی را بشکنند، اما می‌توانند به داخل آن‌ها نفوذ و به آنچه در پی آن هستند دسترسی پیدا کنند. این اتفاق ناشی از آن است که اشخاص می‌توانند خارج از شبکه به نقطه دسترسی[۱] متصل شوند و مدیران شبکه تنظیمات پیش فرض شبکه را تغییر نمی‌دهند و یا کاربران

[۱] Access Point

ایمنی را نشناخته‌اند تا سعی کنند برای تنظیم کردن آن تلاش کنند.

هدف از تخصیص توان این است که داده با بالاترین نرخ ممکن با توجه به محدودیت‌های تداخل و همچنین با توجه به محدودیت توان تجهیزات، ارسال شود. در [17] تخصیص توان برای شبکه رله‌ی چندپرشی بررسی شده است. در این شبکه‌ها توان ارسالی، تحت محدودیت‌های تداخل و همچنین محدودیت نسبت سیگنال به نویز مورد نیاز گیرنده، حداقل شده است. همچنین تخصیص توان برای حداکثر کردن مجموع نرخ دریافت داده در یک شبکه ی رادیوشناختی با راهبرد تقویت و ارسال بررسی شده است [22].

با این حال در ساختارهای در نظر گرفته شده، یا برای همه کاربران ثانویه انتقال اطلاعات به کمک رله انجام می‌شود یا یرای همه آن‌ها انتقال داده به صورت مستقیم انجام می‌شود. یک شبکه با دو کاربر که یکی به کمک رله دریافت اطلاعات دارد و دیگری بدون کمک رله، نیز بررسی شده است[26]–[18]. در این کارها فعالیت شبکه بدون حضور یک شبکه اولیه، بررسی شده است. در برای مدیریت تداخل، یک روش برای کاهش موثر تداخل ارائه شده است .در این شبکه، کاربری که به کمک رله اطلاعات دریافت می کند، نسبت به کاربری که مستقیم داده دریافت می کند، اولویت دارد.

راهبرد تقویت و ارسال یکی از راهبردهای کارآمد(در مواقعی که رله به مقصد نزدیک‌تر است)در شبکه‌های مشارکتی است .در ساختارهای توضیح داده شده در بالا هیچ یک از این راهبرد استفاده نکرده اند. در این پایان‌نامه یک سیستم را بررسی می‌کنیم. فرستنده مرکزی داده را به ترتیب به دو کاربر تخصیص می‌دهد. یکی از کاربران مسیر به صورت مستقیم در نظر گرفته شده است و انتقال اطلاعات در یک فاز انجام می‌شود و برای کاربر دیگر، انتقال داده به وسیله رله و در دو فاز انجام می شود. در این شبکه از رله رمزگشایی و ارسال و به صورت دو طرفه غیرهمزمان در نظر گرفته می‌شود [34]–[32]. هدف یافتن ضرایب تخصیص توان در شبکه رادیوشناختی برای ارسال داده با کمک رله و ارسال مستقیم، به‌گونه‌ای که نرخ مجموع داده در شبکه، حداکثر شود. در این مهم ما ابتدا

تخصیص توان بهینه در یک شبکه رادیوشناختی لایه زیرین با انتقال داده به صورت مستقیم و به کمک رله تقویت و ارسال را بررسی کردیم [36] ,[35] ,[31].

امنیت یک امر مهم در شبکه‌های بی‌سیم به شمار می‌رود، در [37] ,[36] ,[31]، امنیت ارسال در یک شبکه بی‌سیم شامل یک منبع، یک مقصد، یک استراق سمع کننده و رله بررسی شده است. نقش رله حداکثر کردن نرخ امنیت در دو بازه زمانی است که در بازه زمانی اول منبع اطلاعات به مقصد می‌فرستد و در بازه زمانی دوم با انتخاب یک رله بهینه دوباره سیگنال ارسالی منبع را رمزگشایی و با همکاری منبع و رله استراق سمع کننده مسدود و به مقصد ارسال می‌کند. انتخاب رله و همچنین تخصیص توان بهینه در دو بازه زمانی در [38] مطرح و همکاری بین کاربران ثانویه و کاربران اولیه به عنوان رله و پاسخ به این سوال که این همکاری دو طرفه برای کاربران اولیه و ثانویه چه موقع سودمند است، در [27] داده شده است.

الگوریتم تقسیم منبع با فیدبک محدود برای شبکه های رله با مدولاسیون[۱] انجام می‌شود که مدل ارتباطی آن شامل یک گره منبع، یک گره مقصد به همراه یک رله رمزگشایی و ارسال است. ابتدا رله به این َصورت انتخاب می‌شود که بتواند نمادهای دریافتی را ارسال کند. هدف مقاله انجام شده حداکثر کردن سرعت آنی سیستم به وسیله تقسیم بهینه توان است [28]. در [29]، تخصیص توان بهینه برای حداکثر سازی نرخ امن[۲] در یک سیستم رله رمزگشایی و ارسال چند حامله در حضور یک استراق سمع کننده بررسی شده است که در [30] آن سه مدل ارسال زیر در نظر گرفته شده است:

- ✓ ارسال بدون ارتباط یعنی منبع و رله ارسال نمی‌کنند
- ✓ ارسال ارتباط مستقیم یعنی منبع در طول بازه زمانی اول پخش و رله هیچ سیگنالی ارسال نمی‌کند.

[۱] orthogonal frequency-division-multiplexing access(OFDMA)

[۲] secrecy rate

ارسال ارتباط رله یعنی سیگنال‌های پخش منبع در [39] طول بازه زمانی اول و رله در بازه زمانی دوم سیگنال رمزگذاری به مقصد ارسال می‌کند. استراتژی تطبیقی[1] حداکثر سازی نرخ امن پیشنهادی به گونه ای است که منجر به کاهش قابل توجه محاسبات در به دست آوردن توان کل سیستم می-شود [12].

۱-۱۱ اجاره طیف

یکی از کارهای دیگر رادیوشناختی اجاره طیف است که در [40] یک شبکه همکاری OFDM بر مبنای شبکه رادیو شناختی که در آن شبکه اولیه بعضی از زیر کانال‌ها را به شبکه ثانویه اجاره داده برای یک تغییرات زمان کاربر ثانویه به کاربر اولیه به عنوان رله کمک می‌کند. استراتژی همکاری که استفاده شده به این صورت است که جمع نرخ کاربران ثانویه در حالی که کیفیت سرویس اولیه را فراهم می‌کند بیشینه شود. یک مسئله بهینه سازی از ارسال شبکه اولیه انتخابی، رله انتخابی، تخصیص زیرحامل، کنترل توان و تخصیص زمان بیان شده است. در [37] اجاره طیف با مرجع همکاری که کاربران اولیه یک بخشی از تخصیص طیف را به کاربر ثانویه برای همکاری اجاره می-دهد.سیستم به گونه‌ای است که یک شنودگر سیستم را شنود می‌کند و کاربر ثانویه باید نرخ امن شبکه اولیه را تامین کند. در این مقاله بهینه سازی با پرتو افکنی در فرستنده ثانویه با چندین انتن انجام شده است. در [38] طرح اجاره طیف تطبیقی برای شبکه‌های رادیو شناختی چند کاربره مطرح شده است. بر مبنای دو راه رله متوالی و پروتکل رمزگشایی و ارسال هر کاربر شناختی هوشمندانه پروتکل اجاره طبف با همکار در انتقال اطلاعات اولیه را سوئیچ می‌کند. سیستم به گونه ای است که از دایورستی چندین کاربر سیستم ثانویه با فرمول $\log(logm)$ هنگامی که m تعداد کاریران شناختی بزرگترین باشد. در [41] یک سیستم OFDM برمبنای طرح همکاری و اتصال اجاره طیف بیان شده است. کاربر اولیه بخشی از منابع زمان و فرکانس به عنوان سود همکاری به کاربران ثانویه که نقش رله

[1] adaptive strategy

را برای کاربر اولیه بازی می‌کند اجاره می‌دهد. پارامتر بهینه کنترل اجاره منبع برای اولیه و ثانویه را با استفاده از تعادل نش بررسی کردند.

۱-۱۲ ارتباط مشارکتی

ایده‌ی اصلی یکی از روش‌های مشارکتی که در مراجع [29]–[27] به آن پرداخته شده است به این ترتیب است که ابتدا کلمه کد[۱] هر کاربر به دو قسمت تقسیم می‌شود و بخشی توسط کاربر و بخشی دیگر توسط کاربر رله، از دو مسیر محوشدگی مستقل ارسال می‌شود. در صورتی که کاربر رله موفق به دریافت صحیح نباشد به حالت غیرمشارکتی بر می‌گردد. شکل ۲-۸ ارسال به روش مشارکتی کد شده را نشان می‌دهد. در حالت کلی از روش‌های متفاوتی می‌توان در این ساختارها استفاده نمود. به عنوان مثال کدنهایی می‌تواند به صورت کدهای قالبی، کانولوشنال و یا ترکیبی از این دو باشد. همچنین چگونگی تقسیم نمودن قاب‌ها نیز می‌تواند از طریق کدهای ضربی، تکه کردن و یا کدهای پی‌درپی باشد. مشکل دیگری که کلیه‌ی روش‌های فوق دارند این است که تعداد کاربران مشارکت‌کننده به دو کاربر محدود شده است. روش دیگری در [30] ارائه شده است که از کدهای فضا-زمان برای افزایش تعداد کاربران مشارکتی استفاده می‌کند. بدین ترتیب که ابتدا هر کاربر اطلاعات خود را به مقصد و کاربران دیگر ارسال می‌کند. سپس کاربرانی که توانسته‌اند اطلاعات کاربر را بدون خطا کدبرداری نمایند به عنوان یک سیستم چند آنتن و با استفاده از کدهای فضا-زمان، اطلاعات کاربر را به سمت مقصد ارسال می‌نمایند. نکته‌ی دیگر این که با افزایش تعداد کاربران مشارکتی، کارایی سیستم مشارکتی بهبود چندانی نمی‌یابد. لذا شبکه‌هایی که می‌توانند کاربران مشارکتی زیادی داشته باشند باید به دسته‌های کوچک تقسیم شوند و مشارکت در دسته‌های کوچکتر صورت گیرد.

[۱] Code Word

چون ارسـال و دریافت همزمان در یک باند فرکانسـی عملاً امکان پذیر نمی‌باشد، لازم است که در تمامی روش‌های مشارکتی، شرط عمود بودن ارسال و دریافت در کاربران رعایت گردد. بدین معنی که سیگنال‌های ارسالی و دریافتی کاربران با یکدیگر تداخل نداشته باشند. به عنوان نمونه، در ساختار مرجع [31]، با تقسـیم زمانی و در [6] و [7] با اختصـاص کدهای عمود بر هم به هر کدام از کاربران، این موضوع در نظر گرفته شده است.

۱-۱۲-۱ رفتار گره در شبکه

برای بهتر روشن شدن مسأله‌ی مشارکت، ابتدا رفتار گره‌ها در شبکه را به صورت زیر نشان می‌دهیم. هر گره در شبکه می‌تواند یکی از سه رفتار زیر را داشته باشد:

۱- خودگرایانه[۱] : تنها اطلاعات خود را ارسال می‌کند و کمکی انجام نمی‌دهد.

۲- پشتیبان[۲] : کمک کردن به صورت یک‌طرفه انجام می‌شود.

۳- مشارکتی : کمک کردن به صورت دوطرفه است.

در مخابرات مشـارکتی انتخاب رله از اهمیت خاصی برخوردار است از مزایای آن می‌توان به موارد زیر اشاره کرد [15]:

کاهش نرخ خطای سمبل، افزایش نرخ انتقال اطلاعات، کاهش انرژی مصرفی

۲-۱۲-۱ انواع رله

۱. رله کردن شفاف[۳] که شکل موج و اطلاعات را تغییر نمی‌دهد، فقط عملیاتی ساده مانند چرخش و تقویت را روی داده انجام می‌دهد [15]. پروتکل‌های این گروه رله‌ها عبارتند از:

---

[۱] Egoistic

[۲] Supportive

[۳] Transparent Relaying

- ✓ تقویت و ارسال (AF) : در این روش، رله سیگنال دریافتی را تقویت و دوباره ارسال می‌کند. یکی از معایب این روش این است که نویز دریافتی نیز توسط رله تقویت و ارسال می‌شود. کاربردهای این رله عبارتند از: طرح مشترک پرتو افکنی[۱] همکاری (CB) و نویز مصنوعی[۲] برای بهبود امنیت تبادل روز با استفاده از شبکه‌های رله تقویت و ارسال مطرح شد [16]. در محیط های وایرلس واقعی چون کانال لینک منبع به مقصد (SD) با افزایش در زمان تغییر می‌کند، می‌توانیم از طریق لینک SD با انتقال مجدد مشترک با یک طرح رله AF قراردادی یک بهره متنوع بدست آوریم. بنابراین با تشخیص منطبقانه‌ی گره‌ی انتقالی بین گره‌های رله و منبع میتوانیم در انتظار افزایش عملکرد باشیم [17].
- ✓ پردازش خطی و ارسال۳ (LF) : این روش رله کردن شامل برخی از عملگرهای ساده‌ی خطی است که پس از تقویت بر روی سیگنال اعمال می‌شود. مثالی از چنین عملگر خطی شیفت فاز است.

پردازش غیر خطی و ارسال ۴(NLF) : در این روش برخی از عملگرهای غیر خطی روی سیگنال دریافتی عمل می‌کنند. به عنوان مثال یکی از کاربردهای آن تقویت غیرخطی سیگنال دریافتی است که نرخ خطا را حداقل می‌کند/

۲. رله کردن احیا کننده[۵] که در این روش شکل موج و اطلاعات تغییر پیدا می‌کنند و به عملگرهای باند پایه و سخت افزار های دیجیتال نیاز دارد. پروتکل‌های این گروه عبارتند از [15]:

- ✓ تخمین و ارسال۶ (EF) : در این روش از برخی از الگوریتم‌های آشکارسازی برای بازیابی سیگنال اصلی کمک گرفته می شود و سپس سیگنال آنالوگ تقویت شده و به سیگنال باند پایه تبدیل می‌شود.

---

[۱] Beamforming

[۲] Artificial Noise (AN)

[۳] Linear Process and Forward

[۴] Non Linear Process And Forward

Regenerative Relaying [۵]

[۶] Estimate and Forward

برای مثال، رله سمبل مدوله شده را تخمین می‌زند و سپس با همان مدولاسیون یا مدولاسیون دیگری ارسال می‌کند.

- ✓ فشرده سازی و ارسال[1] (CF) : این روش مشابه روش EF است با این تفاوت که رله مدل فشرده شده‌ای از اطلاعات دریافتی را به مقصد ارسال می‌کند.
- ✓ رمزگشایی و ارسال (DF) : در این روش رله سیگنال دریافتی را آشکارسازی و سپس رمزگشایی می‌کند. در مرحله‌ی بعد،سیگنال مجدداً رمزگذاری و به مقصد ارسال می‌شود.

مشکل حداکثرسازی نرخ مجموع سیستم با محدودیت توان کلی در هر سلول را به‌وسیله یک سیستم کانال ارتباطی OFDMA چندسلولی با چندین ایستگاه رله‌ای رمزگشایی و ارسال را که به انتقال ایستگاه پایه کمک می‌کند در نظر می‌گیرد [18]. امنیت شبکه‌های فیزیکی را در شبکه‌های بی سیم مشترک که با چندین رله در جایی که پروتکل‌های تقویت و ارسال و پروتکل رمزگشایی و ارسال وجود دارد را مطالعه و همچنین طرح‌های رله‌ای بهینه را بر پایه AF و DF تا بتوانیم به وسیله آن امنیت شبکه‌های بی‌سیم را در برابر حمله‌ها و نفوذهای استراق سمع‌کننده افزایش دهیم را بررسی کردیم [19]. روش تطبیق قدرت بهینه در زمان را با در نظر گرفتن قدرت متوسط طولانی مدت برای یک سیستم رله‌ای DF نشان می‌دهد، مفروض بر اینکه CSI تمام اتصالات به طور کامل در رله موجود هستند [20]. شبکه بی‌سیم با یک منبع، یک مقصد، یک استراق سمع کننده و رله‌های DF چندگانه در نظر گرفته شده است. یک طرح رله مشترک با دو بخش به این دلیل پیشنهاد می‌شود که میزان امنیت را حداکثر کند. در بخش اول, منبع اطلاعات را ارسال می‌کند که شامل سیگنال است و در زمان واحد با مقصد همکاری می‌کند تا در استراق سمع پارازیت ایجاد کرده و در رله خللی ایجاد کند. در بخش دوم یک رله سیگنال‌های رمز گشایی شده را از منبع ارسال می کند و در زمان واحد آن رله مشخص با منبع همکاری می‌کند تا در استراق سمع پارازیت ایجاد نموده البته بدون وارد آوردن خللی

[1] Compress and Forward

در مقصـد رخ می‌دهد، انتخاب یک رله بهینه همچنین تقسیم نیروهای بهینه در بین بخش‌های یک و دو پیشنهاد شده است [21].

- ✓ پالایش و ارسال[۱] (PF): سیستم‌های مخابراتی پیشرفته معمولاً گونه‌ای طراحی شده‌اند که تداخل زیادی دارند. روش PF با حذف قسمت زیادی از تداخل‌های دریافتی در رله، بر مشکل تداخل جریان‌های مختلف رله شده غلبه می‌کند.

جمع آوری و ارسال[۲] (GF) : این روش، توسعه یافته‌ی روش CF است که در آن گره رله علاوه بر اینکه اطلاعات نمونه برداری کرده از منبع را کد می‌کند اطلاعات خودش را نیز کد کرده و جمع آوری کرده و به مقصد ارسال می‌کند.

[۱] Purge and Forward

[۲] Gather and Forward

فصل سوم: مروری بر منابع مطالعاتی و تحقیقات انجام شده

۱-۱۳ پیشگفتار

در این بخش، منابع مطالعاتی استفاده شده در این تحقیق و سابقه تحقیقات انجام شده در زمینه تخصیص منابع در شبکه‌های شناختی مبتنی بر رله و نرخ امن در این شبکه‌ها را ارائه می‌کنیم. در این بخش سعی بر آن است که ابتدا با مرور این مقالات، ایده‌هایی که روی آن‌ها کار کرده ایم، مطرح شوند. یکی از مسائل مورد بررسی در شبکه‌ها تخصیص منابع است که با توجه به شرایط موجود و با هدف بهینه کردن یک تابع هدف مربوط به شبکه، منابع به صورت بهینه تخصیص می‌یابند. یکی از معمول‌ترین تابع‌های هدف در مسائل تخصیص منابع چه در حالت شناختی و چه غیرشناختی تابع مجموع نرخ ارسال است. تحقیقات انجام شده در زمینه تخصیص منابع را به دو دسته کلی شبکه‌های شناختی مبتنی بر رله و شبکه‌های با نرخ امن مبتنی بر رله دسته‌بندی کرده و به بررسی آنها می‌پردازیم.

سیستم‌های مخابرات مشارکتی که با استفاده از چندگانگی فضایی عملکرد ارتباطات را بهبود می‌بخشند در سال‌های اخیر مورد توجه زیادی قرار گرفته‌اند. ایده‌ی استفاده از رله در شبکه‌های بی‌سیم، موضوع بسیاری از تحقیقات بوده است. این ایده برای اولین بار توسط وان در میولن[۱] مطرح شد. او از روش تقسیم زمانی برای رله کردن و مطالعه تأثیرات آن بر روی ظرفیت تئوری استفاده می‌کرد و برای این کار از یک شبکه سه ترمیناله شامل منبع، رله و مقصد استفاده نمود [15]–[13]. این مفهوم در مورد شبکه‌های بزرگتر نیز می‌تواند توسعه پیدا کند. سپس در سال ۱۹۷۹ مخابرات مشارکتی برای کانال رله تخفیف یافته[۲] مطرح شد [18]–[16] ,[11]. در آن زمان آنالیزهای صورت

[۱] Van der Meeulen

[۲] Degraded Relay Channel

گرفته بر روی ظرفیت یک شبکه سه ترمیناله شامل منبع، رله و مقصد بود. در این تحقیقات مفروض این بود که همه‌ی گره‌ها در یک باند یکسان عمل می‌کنند، بنابراین سیستم به دو کانال انتشار مربوط به منبع و کانال با دسترسی چندگانه مربوط به مقصد تجزیه می‌شد.

مفهوم و ایده‌ی مخابرات مشارکتی تا حدی متفاوت از کارهای صورت گرفته بر روی کانال رله است. در حالی که در این مطالعه بیشتر، ظرفیت را در یک کانال با نویز سفید گوسی تجمعی بررسی کردند اما اکنون انگیزه مطالعات بیشتر بر روی مفهوم دایورسیتی در یک کانال محوشونده است. در کارهای صورت گرفته بر روی کانال رله، یک رله تنها به عنوان کمک برای ارسال اطلاعات منبع استفاده شده است در حالی که در مخابرات مشارکتی، منابع کلی سیستم ثابت هستند و کاربرها هم به عنوان منبع اطلاعات و هم به عنوان رله عمل می‌کنند [42]. برای رله کردن نیاز است که از گره‌های کمکی که به طور مناسب بین منبع و مقصد قرار گرفته‌اند استفاده شود. این عمل باعث بهبود ارتباط و گسترش ناحیه تحت پوشش می‌شود. در سال‌های اخیر روش‌های رله کردن متعددی از روش ساده کد برداری و ارسال گرفته تا روش‌های پیچیده‌تر رله کردن توزیع شده پیشنهاد شده است [۵۲]. این روش‌ها شامل روش کد برداری و ارسال، تقویت و ارسال[۱] و روش کد کردن مشارکتی[۲] می‌باشد. علاوه بر این با افزایش محبوبیت مخابرات مشارکتی و استفاده از رله کردن، این نکته که به واسطه آن به چه میزان عملکرد بهبود پیدا می‌کند از نکات قابل توجه است.

در [20] چند مطالعه که بر روی انتخاب رله صورت گرفته است به انتخاب تنها یک رله به عنوان رله‌ی مشارکت کننده اهمیت زیادی داده شده است. در این موارد استدلال این است که سربار ناشی از کانال‌های متعامد حداقل می‌شود و همچنین پیچیدگی فرآیند انتخاب کم می‌شود. در [21]نتیجه که طراحی یک کد زمان- فضا برای تعداد دلخواهی از رله ها مشکل است. آنها یک طرح

[۱] Amplify and Forward

[۲] Coded Cooperation

رله کردن فرصت طلبانه[1] را پیشنهاد می‌کنند که یک طرح انتخاب رله توزیع شده می‌باشد و نیاز به اطلاعات کلی وضعیت جغرافیایی برای انتخاب یک تک رله ندارد. طرح OR از کد قراردادی استفاده می‌کند. در طرح انتخاب رله به عنوان جایگزینی برای کد زمان- فضا برای چندین کاربر پیشنهاد شده است. در شبکه‌های بی‌سیم مانند شبکه‌های موردی که گره‌ها با باطری‌هایی با طول عمر محدود تغذیه می‌شوند، موضوع توان عامل مهمی در روش انتخاب رله است تا طول عمر گره حداکثر گردد. طرح OR به توان در انتخاب رله توجه نمی‌کند. در [22] نویسنده یک استراتژی انتخاب رله‌ی توان آگاه[2] را برای حداکثر کردن طول عمر شبکه پیشنهاد کرده است. در این روش از حداقل کردن توان انتقال کلی با استفاده از اختصاص توان بهینه بهره گرفته می‌شود. در [23] بازده انرژی مخابرات مشارکتی براساس انتخاب تک رله بررسی شده است. در یک شیوه‌ی انتخاب دیگر، رله براساس یک لیست اولویت انتخاب می‌شود که این لیست به سه روش ممکن است طراحی شود. در روش اول، در هر انتقال به صورت تصادفی لیست اولویت مرتب می‌گردد. در روش دیگر، در هر انتقال، گره ها براساس نسبت سیگنال به نویز دریافتی در یک لیست به طور نزولی مرتب می‌شوند و در نهایت لیست اولویت ثابت برای هر گره است که در هر انتقال نیز ثابت می‌ماند [25] ,[24].

در بیشتر موارد طرح‌های انتخاب رله تنها فرایند انتخاب را تحت یک اختصاص توان ساده بررسی می‌کنند. در [25]، انتخاب رله با در نظر گرفتن اختصاص توان بهینه بررسی شده است. در [26] اختصاص توان برای یک مدل تقویت و ارسال بررسی شده است. در مرجع مذکور، طرح اختصاص توان به منظور حداکثر کردن طول عمر، پیشنهاد شده است. برای حداکثر کردن طول عمر نیاز است که توان به طور منصفانه بین گره‌های شبکه توزیع شود تا توان انتقال کلی لازم حداقل گردد.

[1] Opportunistic Relaying

[2] Power-Aware Relay Selection

۱-۱۴ مفهوم نرخ امن

ویژگی پخش همگانی در شبکه های بی سیم امکان دریافت سیگنال توسط تمامی کاربرهای موجود در شبکه را فراهم می‌سازد. این ویژگی شبکه را نسبت به استراق سمع و شنود آسیب پذیر می‌کند. از این رو، به علت طبیعت پخش امواج رادیویی بی‌سیم، امنیت یک موضوع بسیار مهم در سیستم های بی سیم است. همچنین به دلیل افزایش تقاضای انتقال داده ها به صورت خصوصی و امن، این موضوع توجه فراوانی را به خود جلب کرده است. در [32] ابتدا بسیاری از کارهای امنیتی در لایه‌های بالایی، توسط کدگذاری و بر اساس پیچیدگی محاسباتی انجام می‌گرفت. در پروتکل استاندارد پنج لایه ای، روش‌های امنیتی بر روی تمامی لایه‌ها به جز لایه فیزیکی طراحی شده است. بنابراین، ایجاد امنیت لایه فیزیکی از هر دو دیدگاه نظری و عملی دارای اهمیت است.

ایده اولیه امنیت لایه فیزیکی [33]، بهره‌برداری از ویژگی‌های فیزیکی کانال‌های بی‌سیم به منظور انتقال پیام امن است. امنیت با دیدگاه تئوری اطلاعات امکان انتقال امن در لایه فیزیکی را فراهم می‌کند. یا پیدا کردن ظرفیت امن و تکنیک های کدینگ، ارسال پیام‌ها بدون این که توسط شنود کد برداری شوند، امکان پذیر است. امنیت با دیدگاه تئوری اطلاعات از مفهوم امنیت کامل شانون که یک ساختار ریاضی کلی از سیستم های امن ارائه کرد، سرچشمه می‌گیرد. مفهوم تئوری اطلاعات امن و کانال استراق سمع ابتدا توسط wyner [43] تعریف شد و مورد مطالعه قرار گرفت. این کانال پایه‌ای‌ترین مدل لایه فیزیکی است که مشکل امنیت ارتباطات را برطرف کرد. او نشان داد زمانی که کانال شنود نسخه تضعیف شده‌ای از کانال اصلی (کانال بین مبدأ و مقصد) باشد امکان انتقال یک پیام امن با نرخ غیرصفر امکان پذیر است. نرخی که در آن اطلاعات می‌تواند به صورت امن از منبع به مقصد مورد نظر خود منتقل شود نرخ امن و حداکثر نرخ امن از مبدأ به مقصد، ظرفیت امن نامیده می‌شود. امنیت با دیدگاه تئوری اطلاعات برای مدل‌های مختلف کانال توسعه یافت و نشان داده شد

که ظرفیت امن، تفاضل بین ظرفیت کانال اصلی و کانال استراق سمع است [44]. از تحقیقات انجام شده با دیدگاه تئوری اطلاعات و بررسی ظرفیت امن برای مدل های مختلف کانال می توان به [45] ، [46] و [47] اشاره کرد.

نرخ امن به شرایط کانال بین مبدأ و مقصد و همچنین کانال بین مبدأ و شنود بستگی دارد. شرایط کانال، مانع رویکردهای ابتدایی امنیت لایه فیزیکی در سیستم‌های تک آنتنی می‌شود. وقتی کانال بین منبع و مقصد از کانال بین منبع و شنود ضعیف تر باشد، یک نرخ امن مثبت قابل دستیابی نیست [48]؛ به عبارت دیگر، در این حالت به طور معمول نرخ امن کانال برابر با صفر خواهد بود و ایجاد یک ارتباط امن با مدل کانال استراق سمع Wyner غیرممکن است. تکنیک‌های مختلفی برای غلبه بر این محدودیت وجود دارد که در این بخش به معرفی آن‌ها خواهیم پرداخت [49].

۱-۱۴-۱ تکنیک های دستیابی به نرخ امن غیرصفر

همان طور که اشاره شد وقتی کانال اصلی از کانال شنود ضعیف تر باشد، نرخ امن مثبت قابل دستیابی نیست. یکی از روش‌ها برای غلبه بر این مشکل که در برخی از کارهای اخیر پیشنهاد شده است استفاده از سیستم‌های چندین آنتن در فرستنده و گیرنده است که برای مثال می‌توان سیستم‌های چند ورودی چند خروجی (MIMO) را نام برد [50]. در زمینه استفاده از سیستم‌های چند ورودی-چند خروجی اخیرا Pei و همکاران [51]، [9] به مطالعه مخابره امن روی کانال شناختی چند ورودی- چند خروجی پرداخته‌اند و ظرفیت امن قابل وصول با قید توان ارسالی و تداخلی را به صورت یک مسئله بهینه سازی شبه محدب فرمول کرده‌اند.

از آنجا که استفاده از چند آنتن شامل هزینه‌های سخت افزاری بالقوه قابل توجه‌ای است و عمدتاً به دلیل محدودیت اندازه و توان مصرفی گره‌های موجود در شبکه، به کارگیری این روش و پیاده سازی چند آنتن همیشه امکان پذیر نمی‌باشد، استفاده از مشارکت گره که با عنوان مخابرات مشارکتی از آن یاد می‌شود، یک راه موثر و یک جایگزین کم هزینه است که مزایای استفاده از سیستم‌های چند آنتن

را برای گره‌های تک آنتنی فراهم می‌کند [52] و روشی دیگر برای غلبه بر چالش دستیابی به نرخ امن غیر صفر است. درواقع از مخابرات مشارکتی، برای تسهیل انتقال پیام‌های محرمانه از منبع به مقصد و بهبود عملکرد ارتباطات بی‌سیم امن استفاده می‌شود.

به طور خاص، مشارکت گره از طریق رله می‌تواند نرخ امن را با بهره برداری و کاهش اثرات کانال افزایش دهد. در این سیستم، مبدأ برای ارسال پیام خود به مقصد از یک رله برای پنهان کردن پیام خود از شنود کمک می‌گیرد و داده از طریق یک یا چند رله به مقصد ارسال می‌گردد؛ به عبارت دیگر این مدل، تعمیم کانال رله [53] و کانال استراق سمع [54] است. اغلب از مشارکت برای افزایش نرخ انتقال یا تابع قابلیت اطمینان استفاده می‌شود. در [55] نقش جدیدی از رله در ایجاد یک ارتباط امن از منبع به مقصد معرفی شده است. در این راستا، استراتژی‌های مشارکت مختلفی برای کانال رله-شنود درنظر گرفته شده و ناحیه نرخ امن مربوط به آنها مشخص شده است. همچنین نشان داده است که دستیابی به یک نرخ امن کامل مثبت در [56] چندین سناریو که در آنها ظرفیت امن در غیاب رله صفر است، امکان پذیر است.

۱-۱۴-۲ سیستم های چند زیرحاملی

طیف فرکانسی می‌تواند به صورت تک‌حاملی و یا چندحاملی بین کاربران اولیه و ثانویه به اشتراک گذاشته شود [57]. در حالت اول، کاربران ثانویه و اولیه از فناوری‌های با پهنای باند وسیع (UWB)یا CDMA استفاده می‌کنند. درحالت دوم، کاربران ثانویه و اولیه طیف فرکانسی را به زیرحامل‌هایی تقسیم می‌کنند و از فناوری‌های FDMA و یا OFDMA جهت ارسال اطلاعات و دسترسی طیفی استفاده می‌کنند. سیستم‌های چند زیرحاملی با تقسیم باند فرکانسی به زیرباندهای موازی، جریان با نرخ داده بالا به جریان‌هایی با نرخ داده پایین تجزیه می‌گردد [12]. هرچه تعداد زیرحامل‌ها افزایش می‌یابد، پهنای باند هر زیرکانال باریک‌تر می‌شود. در [58] واقع با تقسیم باند فرکانسی به زیر کانال‌هایی با پهنای باند کوچک‌تر، هر زیر کانال تحت تأثیر محوشوندگی هموار قرار

می‌گیرد که پیچیدگی گیرنده را کاهش می‌دهد و توانایی سیستم‌های مخابراتی برای غلبه بر مشکل ناشی از کانال‌های فرکانس گزین، افزایش می‌یابد. به تکنیک دسترسی چندگانه با حامل‌های فرکانسی تقسیم شده عمود برهم در حالتی که حامل‌ها بین چند کاربر توزیع می‌شود، OFDMA اطلاق می‌گردد. این روش برای داشتن یک انتقال با کارایی بالا و انتقال اطلاعات با نرخ بالا در کانال‌های مخابراتی استفاده می‌شود. این روش از وقوع تداخل بین سمبل (ISI) جلوگیری می کند و همچنین از طیف فرکانسی به طور بهینه استفاده می شود [59].

رادیوشناختی نیاز به لایه فیزیکی منعطف و کارا دارد .مخابرات چند زیر حاملی به خاطر توانایی در زمینه حسگری و همچنین قابلیت پر کردن فاصله های طیفی رها شده توسط کاربر اولیه، به عنوان یک نامزد برای سیستم های رادیو شناختی پیشنهاد شده است .سیستم های رادیوشناختی مبتنی بر چند زیرحامل می توانند ملاحظات مربوط به شکل طیف را به وسیله غیرفعال کردن زیرحامل هایی که کاربر اولیه فعلاً در حال ارسال روی آن است یا زیرحامل هایی که امکان تداخل با دیگر کاربران را دارد، برآورده نمایند .علاوه بر این منابع متفاوت سیستم می تواند در جهت افزایش بازدهی مطابق با شرایط محیطی مختلف ارسال، توزیع و استفاده شود .سیستم های چند زیرحاملی، دسترسی چندگانه بسیار منعطف و تخصیص طیفی پهنای باند در اختیار را امکان پذیر می کند که می تواند در سیستم های رادیوشناختی بدون هیچ گونه افزایش پیچیدگی سخت افزاری پیاده گردد .در این سیستم چندین پارامتر مانند فضای زیر حامل، تعداد زیرحامل، مدولاسیون، کدینگ و توان می تواند تنظیم شود.

۱-۱۵ تخصیص منابع

یکی از مهم‌ترین راهکارها جهت کنترل تداخل، افزایش بهره‌وری شبکه و فراهم‌کردن کیفیت درخواستی کاربران در شبکه‌های رادیویی، تخصیص منابع است. منابع یک شبکه مخابراتی بی‌سیم، شامل توان ارسالی کاربران، باند فرکانسی و کدهای ارسال است و در این میان، توان و فرکانس مهم‌ترین و کلیدی‌ترین پارامترهای تخصیص منابع شبکه‌های رادیویی، جهت استفاده بهینه از منابع

شـبکه محسوب می‌شود. هدف تخصیص توان و فرکانس به‌گونه‌ای است که عملکرد سیستم بهینه شود و کیفیت سرویس لازم بدست آید [60].

مسـائل تخصـیص توان و فرکانس را می‌توان به صـورت مسـائل بهینه‌سازی که در آن متغیرهای مسـئله، منابع مورد نظر هستند مانند توان هر کاربر در فرکانس‌های مختلف بیان کرد. تابع هدف، تابع بهره کاربر مانند تابعی از سـیگنال به نویز کاربر و یا تابعی از توان ارسـالی کاربران اسـت. قیدهای این مسئله شامل انواع محدودیت‌های کاربران و یا سیستم است. این قیدها در شبکه‌های مخابراتی متداول، غالباً شـامل بیشـینه توان ارسـالی کاربران، کیفیت درخواستی آنها و بیشینه نرخ ارسال است [61] در شـبکه‌های رادیوشـناختی، دسـته دیگری که نشان‌دهنده راهکارهای دسترسی کاربران ثانویه به طیف فرکانسـی به این قیدها اضافه شده است. یک روش رایج برای محافظت از ارسال کاربر اولیه، اعمال قید محدودیت توان تداخل بر ارسـال کاربر ثانویه اسـت. در شبکه رادیو شناختی، مسئله تخصیص منابع از دید کاربران اولیه، مشـابه با مسئله تخصیص منابع در شبکه‌های متداول مخابراتی است. موضوع جدید، چگونگی تخصـیص منابع از دید کاربران ثانویه است که با توجه به قیدهای جدید پیچیده‌تر خواهد بود. در [40] تخصیص منابع برای دستیابی به نرخ امن، به طور کلی دو حالت درنظر گرفته می شود:

- ✓ بیشینه کردن نرخ امن با قید بیشینه توان ارسالی کاربران ثانویه و بیشینه تداخل بر کاربران اولیه
- ✓ به حداقل رساندن کل توان ارسالی با قید کمینه نرخ امن ارسال و بیشینه تداخل بر کاربران اولیه

در این پایان نامه، حالت اول یعنی بیشینه کردن نرخ امن به عنوان تابع هدف مورد بررسی قرار می گیرد.

در سـیسـتم‌های چند زیرحاملی چند کاربره، به علت موقعیت‌های مکانی متفاوت هر کاربر، دریافت و ارسـال کاربران، تضعیف‌های متفاوتی را تجربه می‌کنند. برای بهره‌مندشدن از این چندگانگی، تخصیص

بهینه منابع باید در جهت بیشـینه کردن عملکرد کلی صـورت پذیرد. بنابراین، فرایند تخصـیص نه تنها شـامل تخصـیص توان بلکه شـامل تخصـیص زیر حامل نیز می‌شـود به‌گونه‌ای که مجموعه مجزایی از زیرحامل‌ها باید به هر کاربر اختصـاص یابد. در مسائل چندکاربره و چندحاملی، چون متغیر بهینه‌سازی هر کاربر، بردار توان در زیرحامل‌های مختلف اسـت به این دسـته از مسـائل، تخصـیص منابع برداری می‌گویند. مجموعه مجزای زیر حامل‌ها، مسـئله را در گروه مسـائل بهینه‌سازی غیرمحدب و NP-hard قرار می‌گیرند و پیچیدگی محاسـباتی آنها بسـیار بالا اسـت. در حالت چندکاربره با توجه به قیدهای مربوط به کیفیت سـرویس کاربران اولیه، حجم محاسـباتی این دسـته از مسـائل بسـیار بالا اسـت. این مشکل، با وجود قیدهای دیگر برای مسئله بهینه‌سازی کاربران ثانویه تشدید خواهد شد. به همین دلیل، این دسـته از مسـائل در گروه مسـائل بهینه‌سـازی NP-hard قرار می‌گیرند. یکی از روش‌های حل این مسـائل، اسـتفاده از روش‌های جداسـازی اسـت که در آن، با استفاده از تابع دوگان مسئله بهینه‌سازی، مسـئله اولیه به زیر مسـائلی در سـطح کاربران شـبکه و یک مسئله جامع، جهت هماهنگی زیر مسائل تقسـیم می‌شـود. در مسـائل چند زیر حاملی چند کاربره، با جداسـازی مسئله به دو مسئله‌ی تخصبص فرکانس و تخصیص توان، مسئله حل می شود.

در این بخش، منابع مطالعاتی استفاده شده در این تحقیق و سابقه تحقیقات انجام شده در زمینه تخصیص منابع در شبکه‌های شناختی مبتنی بر رله و نرخ امن در این شبکه‌ها را ارائه می‌کنیم .در این بخش سـعی بر آن اسـت که ابتدا با مرور این مقالات، ایده‌هایی که روی آن‌ها کار کرده ایم، مطرح شـوند. همان طور که در فصل قبل اشاره شد یکی از مسائل مورد بررسی در شبکه ها تخصیص منابع اسـت که با توجه به شـرایط موجود و با هدف بهینه کردن یک تابع هدف مربوط به شـبکه، منابع به صورت بهینه تخصیص می یابند. یکی از معمول‌ترین تابع‌های هدف در مسائل تخصیص منابع چه در حالت شـناختی و چه غیرشـناختی تابع مجموع نرخ ارسـال اسـت. تحقیقات انجام شـده در زمینه تخصیص منابع را به دو دسته کلی شبکه‌های شناختی مبتنی بر رله و شبکه‌های با نرخ امن مبتنی بر رله دسته‌بندی کرده و به بررسی آن‌ها می‌پردازیم.

۱-۱۵-۱ تخصیص منابع در شبکه‌های شناختی مبتنی بر رله یک‌طرفه

در شبکه‌های رادیو شناختی، دسته دیگری از قیدها برای محافظت از ارسال کاربر اولیه نیز، به این قیدها اضافه شده است. مسئله تخصیص منابع در شبکه رادیو شناختی، مشابه با مسئله تخصیص منابع در شبکه‌های متداول مخابراتی است و تنها نکته جدید، چگونگی تخصیص منابع از دید کاربران ثانویه است که با توجه به قیدهای جدید پیچیده‌تر خواهد بود. از تحقیقات انجام شده در زمینه تخصیص منابع در شبکه‌های شناختی مبتنی بر رله می‌توان به اشاره کرد. در با هدف بیشینه کردن مجموع نرخ به تخصیص منابع در یک شبکه شناختی OFDMA چند کاربره با استفاده از چندین رله کدبرداری و ارسال پرداخته شده است. پیچیدگی محاسبات در الگوریتم‌های جستجو با افزایش زیرحامل‌ها و رله‌ها افزایش می‌یابد. برای غلبه بر این مشکل در این مقاله یک الگوریتم تخمین توزیع[۱] که یک الگوریتم تکاملی احتمالی است، پیشنهاد شده است.

در تخصیص منابع در یک شبکه شناختی OFDMA مبتنی بر رله DF با یک کاربر بررسی شده است. در این مقاله از تکنیک تجزیه دوگان[۲] برای انتخاب رله، تخصیص توان و زیر حامل به طور بهینه مجانبی و با هدف بیشینه کردن ظرفیت استفاده شده است و یک روش زیربهینه برای جلوگیری از پیچیدگی محاسبات روش بهینه ارائه شده است. در شبکه‌های رادیوشناختی OFDMAمبتنی بر رله مورد مطالعه قرار گرفته است و با هدف تخصیص توان و زیرحامل‌ها بین کاربران ثانویه برای رسیدن به بهترین نرخ ممکن و با در نظر گرفتن محدودیت‌های حداکثر توان تداخلی روی سیستم اولیه، به تجزیه و تحلیل سیستم‌های ثانویه با یک رله و چندین رله پرداخته شده است. با افزایش تعداد زیرحامل‌ها، رله‌ها و کاربران ثانویه، پیچیدگی محاسباتی الگوریتم بهینه به طور نمایی افزایش می‌یابد که برای رسیدن به پیچیدگی کم‌تر، دو الگوریتم زیربهینه پیشنهاد شده است که در آن‌ها تأثیر عوامل فوق روی پیچیدگی محاسباتی به صورت خطی است و این باعث

---

[۱] Estimation of Distribution Algorithm (EDA)

[۲] Dual Optimization Method

کاهش پیچیدگی محاسباتی الگوریتم شده است.

در به تخصـیص توان و انتخاب رله در شبکه شناختی با چندین رله پرداخته شده است. در این مقاله، با انتخاب توأم رله و تخصیص توان، به حداکثر رساندن نرخ سیستم رادیو شناختی با محدودیت تداخل روی کاربر اولیه بررسـی می‌شـود. ابتدا یک رویکرد مبتنی بر روش بهینه‌سازی دوگان و سپس یک روش زیر بهینه برای کاهش پیچیدگی ارائه شده است.

۱-۱۵-۲ تخصیص امن منابع در شبکه‌های شناختی مبتنی بر رله یک‌طرفه

با اضـافه شـدن مشـکل امنیت و تعریف جدید از نرخ به عنوان نرخ امن پیچیدگی حل مسئله تخصیص منابع با توجه به غیرمحدب شدن آن افزایش می‌یابد. در اینجا به تعدادی از تحقیقات انجام شـده در این زمینه اشاره می‌کنیم. با در نظر گرفتن یک شبکه غیرشناختی تک‌حاملی با یک کاربر و در حضـور یک یا، در [21] چند شـنود، از مشـارکت گره برای دسـتیابی به امنیت لایه فیزیکی با روش‌های مشـارکت کدبرداری و ارسـال، تقویت و ارسال استفاده شده است. در این مقاله‌ها دو هدف بیشـینه کردن نرخ امن با قید توان و به حداقل رسـاندن کل توان ارسالی تحت قید نرخ امن، بررسی شـده است. در [18] برای اولین هدف، یک راه حل دقیق برای روش DF با یک یا چند شنود بدست آورده شده است. برای هدف دوم، با معرفی محدودیت های اضافی به منظور کاهش پیچیدگی مسئله، یک راه حل زیربهینه ارائه شده است.

در [26] برای دستیابی به نرخ امن، رله کدبرداری و ارسال یک طرفه به کار گرفته شده است و یک مسـئله بهینه سـازی برای تخصـیص امن منابع در یک شـبکه چند کاربره غیرشـناختی بیان و بررسـی شـده اسـت. همچنین از سـیستم چند زیرحاملی استفاده شده است. در این مقاله، تخصیص منابع به عنوان یک مسـئله بهینه سـازی ترکیبی و غیر محدب فرمول شده و یک الگوریتم تخصیص منابع توزیعی و تکرار شـونده کارآمد ارائه شـده است و با استفاده از تجزیه دوگان فرم بسته ای برای تخصیص توان و زیرحامل بدست آمده است.

در [18] تخصـــیص توان برای بیشـــینه کردن نرخ امن در یک ســـیســـتم چند حاملی با رله کدبرداری و ارسال و با حضور یک شنود مطالعه شده است. سه حالت انتقال در سیستم درنظر گرفته شده است. بدون ارتباط که منبع و رله هیچ ارسالی ندارند؛ ارتباط مستقیم، منبع در طول بازه زمانی اول ســیگنال ارســال می کند درحالی‌که در بازه زمانی دوم رله هیچ ســیگنالی ارســال نمی کند؛ ارتباطات با اســتفاده از رله، منبع در طول بازه زمانی اول سیگنال ارسال می‌کند و در بازه زمانی دوم رله سیگنال دریافتی را بعد از کدگذاری مجدد به مقصد ارسال می‌کند. در این مقاله یک روش بهینه برای تخصـــیص توان و زیرحامل برای بیشـــینه کردن نرخ امن با قید توان و همچنین یک روش زیربهینه برای کاهش پیچیدگی محاســباتی پیشــنهاد شــده اســت. نشــان داده شده است راه حل زیر بهینه پیشـــنهادی وقتی تعداد زیرحامل‌ها به بی‌نهایت می‌رود به طور مجانبی بهینه اســت. همچنین نتایج عددی نشان می‌دهد حتی وقتی تعداد زیر حامل‌ها تقریباً کوچک است، عملکرد روش زیربهینه نزدیک به روش بهینه است.

با بررسی و مطالعه این دو دسته تحقیقات انجام شده دیدیم کارهایی در زمینه تخصیص منابع با هدف بیشــینه کردن نرخ امن در شــبکه شــناختی مبتنی بر رله کدبرداری و ارســال شده است. در نتیجه یک شــبکه شــناختی مبتنی بر رله یک طرفه کدبرداری و ارســال با حضور شنود در این شبکه تعریف گردید که هدف در آن بیشــینه کردن مجموع نرخ امن می‌باشــد. از دو دســته مقالات بررسی شده برای تعریف نرخ امن و همچنین قیدهای مورد نیاز برای شبکه شناختی در تعریف مسئله جدید، استفاده شده است.

مســئله امنیت و بررسی نرخ امن برای شبکه‌های شناختی و یا شبکه‌های مبتنی بر رله به طور مجزا انجام گرفته اســت ولی تاکنون کاری در زمینه بررســی امنیت و تخصیص منابع با هدف بیشینه کردن نرخ ارسال امن در شبکه رادیوشناختی مبتنی بر رله انجام شده است. در این بخش، به بررسی امنیت در شــبکه شــناختی مبتنی بر رله و تخصــیص توان، رله و زیرحامل با هدف بیشــینه کردن

مجموع نرخ ارسال امن پرداخته می‌شود. در این راستا سیستم‌های رله کدبرداری و ارسال مبتنی بر دسترسی چندگانه با تقسیم فرکانسی متعامد به علت کارایی بالا و سادگی گزینه مناسبی می‌باشند.

۳-۱۵-۱ بیشینه کردن مجموع نرخ امن در شبکه‌های شناختی مبتنی بر رله یک‌طرفه

در این بخش مدل سیستم که یک شبکه ثانویه شامل یک ایستگاه پایه را که به U کاربر ثانویه، $u = 1 \dots U$ سرویس ارائه می‌دهد، در نظر می‌گیریم. فرض می‌کنیم کاربران ثانویه نقش رله کدبرداری و ارسال را ایفا می‌کند. برای سادگی مسئله، فرض می‌کنیم چند شنود و یک کاربر اولیه در شبکه وجود دارند. در این شبکه تخصیص منابع رادیویی کانال فروسو را برای کاربران ثانویه با هدف دستیابی به حداکثر نرخ امن بررسی می‌کنیم. فرض می‌شود تکنیک OFDM در این شبکه مورد استفاده قرار می‌گیرد، به این ترتیب طیف فرکانسی سیستم به زیرحامل متعامد، $n = 1 \dots N$ تقسیم شده است که در هر پرش استفاده می‌شود. در روش اجاره طیف کاربر ثانویه در صورت استفاده همزمان از طیف باید امنیت اطلاعات سرویس کاربر اولیه را تضمین کند. آستانه تداخل به صورت مرسوم به عنوان معیار تضمین کیفیت سرویس اولیه استفاده می گردد، بنابراین با این شرط که کاربران ثانویه تداخلی بیشتر از برای کاربر اولیه ایجاد نکنند، می توانند از طیف کاربر اولیه استفاده می‌کند.

فرض می‌کنیم ارسال با رله DF و بر مبنای پروتکل نیمه دوطرفه و در دو بازه زمانی برابر انجام می‌شود در بازه زمانی اول، ایستگاه پایه سیگنال را روی همه زیرحامل‌ها ارسال می‌کند و کاربران ثانویه و شنودگر گوش می‌کنند. در بازه زمانی دوم، رله‌ها سیگنال دریافتی از ایستگاه اولیه در بازه اول را کدبرداری کرده و مجدداً کدگذاری کرده و ارسال می‌کنند و کاربران ثانویه که اولیه گوش می‌کند. در هر دو بازه زمانی کاربران ثانویه، شنود سیگنال ارسالی را دریافت می‌کند. زیرحامل‌ها در دو بازه زمانی بر مبنای جفت شدن زیر حامل ها مورد استفاده قرار می‌گیرند، بدین صورت که هر زیر حامل

در مبدأ با زیرحامل در مقصد جفت می‌شود و تنها به یک رله تخصیص می‌یابد. بنابراین در هر ارسال زیرحامل‌ها به صورت جفت شده مورد استفاده قرار می‌گیرند. بیشینه توان ارسالی که مبدأ و رله‌ها می‌توانند مورد استفاده قرار دهند، به ترتیب با مشخص می‌شوند. توان ارسالی مبدأ در بازه زمانی اول روی زیرحامل و رله برای کاربر برابر با و توان ارسالی رله روی زیرحامل در بازه زمانی دوم برابر با است. بهره کانال به صورت رایلی در نظر گرفته می‌شود. P توان ارسال شده روی کانال و توان نویز سیستم است.

۱-۱۶ رله و کاربرد آن در ارسال امن

مشارکت گره از طریق رله می‌تواند نرخ امن را با بهره‌برداری و کاهش اثرات کانال افزایش دهد. در این سیستم، مبدأ برای ارسال پیام خود به مقصد از یک رله برای پنهان کردن پیام خود از شنود کمک می‌گیرد. بنابراین در این بخش کانال رله و ظرفیت آن را بررسی می کنیم. ابتدا کانال رله در حالت کلی بررسی شده و ظرفیت کانال رله یک طرفه و شرایط بهینه برای بیشینه نمودن نرخ داده در این کانال بررسی می‌شود. کانال رله شامل یک مبدأ، یک مقصد و یک یا تعدادی گره میانی می‌باشد. این گره‌های میانی رله‌ها می‌باشند که به ارسال اطلاعات از مبدأ به مقصد کمک می کنند.

۱-۱۶-۱ کانال رله بدون حافظه گسسته

کانال رله بدون حافظه گسسته در ابتدا توسط Vender Meulen معرفی گردید. کانال بی‌حافظه به این معنی است که خروجی‌های کانال در بازه زمانی حال، مستقل از سمبل‌های دریافتی گذشته می‌باشد. ارتباط در کانال‌های دوپرشی در دو بازه زمانی صورت می‌گیرد. بازه زمانی اول برای دریافت داده‌های ارسالی از مبدأ به رله و بازه زمانی دوم برای ارسال داده‌ها از رله به مقصد می‌باشد. در سیستم‌های رله دو روش اصلی برای رله کردن وجود دارد.

- ✓ کدبرداری و ارسال DF: در این روش تمامی داده‌های ارسالی از مبدأ در رله کدبرداری می‌شوند. با استفاده از این روش رله در ارسال پیام با مبدأ همکاری می‌کند. داده‌های دریافتی مجددا کدگذاری شده و سپس ارسال می‌شوند.
- ✓ تقویت و ارسال AF: در این روش نیازی نیست که رله هیچ یک از بخش های پیام را کدبرداری کند. هر رله سیگنال نویزی دریافت شده در مرحله اول را بدون کدبرداری، تقویت و سپس ارسال می‌کند.

عیب روش AF نسبت به روش DF این است که نویز نیز در رله تقویت شده و بیشتر انتشار می‌یابد. در این پایان نامه از روش کدبرداری و ارسال استفاده شده است، بنابراین در این بخش به بررسی ظرفیت در این روش بسنده می‌کنیم.

۱-۱۶-۲ کانال رله یک‌طرفه کدبرداری و ارسال

در این بخش به بررسی کلی نرخ‌های قابل حصول در شبکه‌های رله یک طرفه کدبرداری و ارسال می‌پردازیم. کانال رله یک طرفه شامل یک فرستنده، یک گیرنده و رله است. ظرفیت کانال رله یک‌طرفه کدبرداری و ارسال به صورت زیر محاسبه می‌شود. برای بررسی ظرفیت کانال رله یک‌طرفه، یک کانال دوپرشی ساده شامل یک مبدأ، یک رله و یک مقصد را در نظر می‌گیریم. اگرچه رله و مقصد ممکن است بیش از یکی باشند. ابتدا نسبت سیگنال به نویز[۱] (SNR) به صورت زیر تعریف می‌شود:

$$SNR = gp \quad (1)$$

$$SNR_{TpTusm} = g_{TpTusm} P_{TpTusm} \quad (2)$$

$$SNR_{TusRpm} = g_{TusRpm} P_{TusRpm} \quad (3)$$

$$SNR_{Tpem} = max_{e \in \varepsilon}(g_{Tpem}) P_{TpTusm} \quad (4)$$

[۱] Signal-to-Noise-Ratio

$$SNR^{1}_{TusRusm} = g_{TusRusm} P^{1}_{TusRusm} \quad (5)$$

$$SNR^{2}_{TusRusm} = g_{TusRusm} P^{2}_{TusRusm} \quad (6)$$

که در آن g بهره کانال و p توان ارسـالی می‌باشد. همچنین $R^{s}_{TpTusmm}$ و $R_{TusRusmm}$ ، R^{m}_{TpTus}، R^{m}_{TusRp}، $R^{m}_{Tp,e}$، $R^{1}_{TusRusm}$، $R^{2}_{TusRusm}$ به ترتیب نرخ داده کلی کانال دوپرشـــی، نرخ داده پرش اول و نرخ داده پرش دوم تعریف می‌گردند.

$$R^{m}_{TpTus} = \frac{1}{2}\log\left(1 + SNR_{TpTusm}\right) \quad (7)$$

$$R^{m}_{TusRp} = \frac{1}{2}\log\left(1 + SNR_{TusRpm}\right) \quad (8)$$

$$R^{m}_{Tp,e} = \frac{1}{2}\log\left(1 + SNR_{Tpem}\right) \quad (9)$$

$$R^{1}_{TusRusm} = \frac{1}{2}\log(1 + SNR^{1}_{TusRusm}) \quad (10)$$

$$R^{2}_{TusRusm} = \frac{1}{2}\log(1 + SNR^{2}_{TusRusm}) \quad (11)$$

$$R_{TusRusmm} = R^{1}_{TusRusm} + R^{2}_{TusRusm} \quad (12)$$

که در آن SNR_{TpTusm}، SNR_{Tpem} و $SNR^{1}_{TusRusm}$ نسبت سیگنال به نویز پرش اول و SNR_{TusRpm} و $SNR^{2}_{TusRusm}$ در پرش دوم می باشـــند. نرخ داده کانال دو پرشـــی، برابر با کمینه نرخ امن ارسالی در دو بازه زمانی است

$$R_{date} = \min\left(R^{m}_{TpTus}, R^{m}_{TusRp}\right)$$

همان طور که قبلاً اشـاره شـد، ظرفیت امن تفاضـل بین ظرفیت کانال اصـلی و کانال استراق سمع است

$$R^{s}_{TpTusmm} = \left[R_{date} - max_{e\in\varepsilon} R^{m}_{Tp,e}\right] \quad (8)$$

برای دستیابی به بیشینه نرخ داده ، باید شرایطی برقرار گردد که نرخ دو پرش برابرشود .این مفهوم یک شرط بهینه برای مسئله زیر است:

$$\max \sum_{us \in US} \sum_{m=1}^{M} \eta_{TusRusmm} R_{TusRusmm} \qquad (12)$$

نمادگذاری استفاده شده در این تحقیق در جدول ارائه شده است.

Tp فرستنده اولیه	Rp گیرنده اولیه
Tus فرستنده ثانویه	Rus گیرنده ثانویه
$us = \{1, \dots, US\}$ گروه خطوط ثانویه فعال	$\varepsilon = \{1, \dots, E\}$ گروه استراق سمع کننده ها
$M = \{1, \dots, M\}$ زیرحامل ها	$\overline{R^{S,R}}$ نرخ ثانویه برای خط اولیه مدنظر سیستم
$R^{s}_{TpTusmm}$ نرخ امن لحظه‌ای از فرستنده اولیه	$R_{TusRusmm}$ نرخ امن لحظه‌ای از فرستنده ثانویه
R^{m}_{TusRp} نرخ امن احظه‌ای بین فرستنده ثانویه به گیرنده اولیه	R^{m}_{TpTus} نرخ امن لحظه‌ای بین فرستنده اولیه به فرستنده ثانویه
$R^{m}_{Tp,e}$ نرخ امن لحظه‌ای فرستنده اولیه با حضور استراق سمع کننده	g_{TpTusm} بهره کانال بین فرستنده اولیه و فرستنده ثانویه
g_{TusRpm} بهره کانال بین فرستنده ثانویه و گیرنده اولیه	$g_{TusRusm}$ بهره کانال بین فرستنده ثانویه و گیرنده ثانویه
$g_{Tp,em}$ بهره کانال بین فرستنده اولیه و کاربر متخاصن (شنودگر)	
P_{TpTusm} توان ارسالی تخصیص داده شده بین فرستنده اولیه و فرستنده ثانویه در بازه زمانی اول	P_{TusRpm} توان ارسالی تخصیص داده شده بین فرستنده ثانویه و گیرنده اولیه در بازه زمانی دوم
$P^{2}_{TusRusm}$ توان ارسالی تخصیص داده شده بین فرستنده ثانویه و گیرنده ثانویه در بازه زمانی دوم	$P^{1}_{TusRusm}$ توان ارسالی تخصیص داده شده بین فرستنده ثانویه و گیرنده ثانویه در بازه زمانی اول
$\eta_{TusRusmm} \in \{0,1\}$ یک ضریب تخصیص زیرحامل m بوسیله فرستنده ثانویه T_{us} برای ارسال به گیرنده ثانویه R_{us}	$\rho_{TpTusmm} \in \{0,1\}$ یک ضریب تخصیص زیرحامل m برای ارسال بین فرستنده و گیرنده اولیه در طول فرستنده ثانویه T_{us} در دو بازه زمانی
SNR_{TpTusm} توان اولیه در بهره کانال اولیه	SNR_{TpRusm} توان در بهره کانال بین ثانویه و اولیه
SNR_{Tpem} توان در بهره شنودگر	$SNR^{1}_{TusRusm}$ توان در بهره ثانویه در بازه اول
$SNR^{2}_{TusRusm}$ توان در بهره ثانویه در بازه دوم	

جدول ۳-۱ نمادگذاری

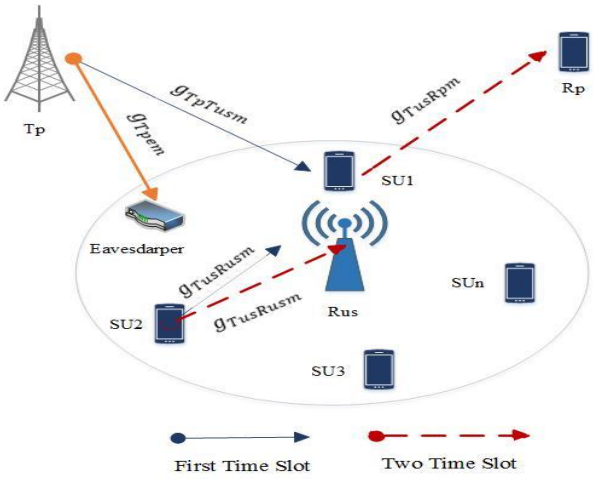
فصل چهارم: اهداف و نوآوری

۱-۱۷ سیستم مدل و بیان مسئله

۱-۱۷-۱ مدل سیستم

در این پایان نامه اجاره طیف در یک شبکه رادیو شناختی مبتنی بر OFDMA به منظور حفظ امنیت ارسال اطلاعات شبکه اولیه مورد بررسی قرار می‌گیرد. در این شبکه یک خط فرستنده اولیه Tp گیرنده اولیه Rp و $us = \{1. \dots . US\}$ جفت خطوط ثانویه فعال، فرستنده ثانویه Tus گیرنده ثانویه Rus داریم. شبکه اولیه به صورت OFDMA بوده و فرض می‌شود پهنای باند (B) موجود به $N = \{1. \dots . N\}$ زیرحامل تقسیم می‌شود. کاربر اولیه به صورت همزمان می‌تواند از چند زیرحامل استفاده نماید، در حالی که کاربران ثانویه فقط بر روی یک زیرحامل قابلیت ارسال اطلاعات را دارند. به علاوه در شبکه مورد نظر، گروه استراق سمع‌کننده‌ها $\varepsilon = \{1. \dots . E\}$ وجود دارد که سعی در شنود اطلاعات ارسالی دارد پس باید نرخ امن کاربر اولیه $R^s_{TpTusmm}$ حفظ شود بنابراین کاربران ثانویه به‌صورت ایستگاه‌های رله رمزگشایی و ارسال عمل کرده و به شبکه اولیه در ارسال اطلاعات با هدف امنیت آن‌ها کمک می‌کنند که این تصمیم‌گیری توسط شبکه کنترلر مرکزی (CNC) به همه اطلاعات کانال شامل بهره، توان کانال و... دسترسی دارد صورت می‌گیرد. در شبکه مورد نظر ارسال اطلاعات به صورت فریم به فریم انجام می‌شود که در آن هر فریم شامل دو بازه زمانی است. در بازه زمانی اول ایستگاه پایه اولیه اطلاعات را ارسال کرده در حالی که کاربران ثانویه و کاربران متخاصم به ایستگاه پایه اولیه گوش می‌دهند. در بازه زمانی دوم کاربران ثانویه‌ای که برای کمک به ارسال اطلاعات شبکه اولیه انتخاب شده‌اند، اطلاعات دریافتی از شبکه اولیه را رمزگشایی و مجددا رمزگذاری کرده، و اطلاعات رمز شده را به سمت کاربر اولیه ارسال می‌کند. سایر کاربران ثانویه، در صورت وجود، در بازه زمانی دوم اطلاعات خود را به ایستگاه پایه ثانویه ارسال می‌کند. برای شنودگر سناریوهای متفاوتی می‌توان در نظر گرفت مانند اینکه شنودگر در بازه زمانی اول، اطلاعات ارسالی از ایستگاه پایه اولیه را شنود می‌کند و در بازه زمانی دوم اطلاعات ارسالی از کاربران ثانویه اگر زیرحاملی باقی بماند ارسال می‌کند. سیستم مدل

پیشنهادی در شکل زیر نشان داده می‌شود.



شکل ۰-۱: مدل سیستم پیشنهادی در حالتی که شنودگر بازه زمانی اول را شنود می‌کند

۱-۱۷-۲ ظرفیت کانال

فرض کنید $P_{TusRusm}^{2}$ ،P_{TusRpm} ،P_{TpTusm} و $P_{TusRusm}^{1}$ به ترتیب توان تخصیص داده شده توسط فرستنده اولیه T_p به کاربر ثانویه T_{us} روی زیر حامل m در بازه زمانی اول، توان تخصیص داده شده توسط فرستنده ثانویه T_{us} به گیرنده اولیه R_p روی زیر حامل m در بازه زمانی دوم، توان تخصیص داده شده توسط فرستنده تانویه T_{us} به گیرنده ثانویه R_{us} روی زیر حامل m در بازه زمانی اول، و توان تخصیص داده شده توسط فرستنده ثانویه T_p به گیرنده ثانویه T_{us} روی زیر حامل m در بازه زمانی دوم باشد. همچنین فرض کنید گین کانال ما در هر زیر بازه مقدار ثابت و از توزیع رایلی پیروی می‌کند اما روی بازه‌های متفاوت به‌صورت IID[۱] تغییر می‌کند، g_{TpTusm} ،g_{TusRpm} ،$g_{TusRusm}$ و $g_{Tp,em}$ به ترتیب بهره کانال بین فرستنده اولیه T_p و فرستنده ثانویه T_{us} روی زیر حامل m، بهره کانال بین فرستنده ثانویه T_{us} و گیرنده اولیه R_p روی زیر حامل m، بهره کانال بین فرستنده ثانویه T_{us} و گیرنده ثانویه R_{us} روی زیر حامل m، و بهره کانال بین فرستنده اولیه T_p و شنودگر e روی زیر حامل m، و ما

[۱] IID

مسـئله را نرخ بیشـینه در نظر گرفتیم پس اگر ظرفیت کانال را بیشـینه کنیم نرخ ما با ظرفیت کانال یکی می‌شـود، $R^{s}_{TpTusmm}$ ، $R_{TusRusmm}$، R^{m}_{TusRp}، R^{m}_{TpTus}، $R^{m}_{Tp.e}$، و $\overline{R^{S.R}}$ به ترتیب نرخ امن از فرستنده اولیه T_p و فرسـتنده ثانویه T_{us} در زیرحامل m و کاربر m، نرخ امن از فرسـتنده ثانویه T_{us} و گیرنده ثانویه R_{us} در زیرحامل m و کاربر m، نرخ امن از فرستنده ثانویه T_{us} و گیرنده اولیه در زیرحامل m، نرخ امن از فرسـتنده اولیه T_p و فرستنده ثانویه T_{us} در زیرحامل m، نرخ امن از فرستنده اولیه T_p و شنودگر e در زیرحامل m، و نرخ امن مدنظر سیستم است. تعاریف پارامترهای گفته شده به‌صورت ریاضی در زیر امده است.

$$R^{s}_{TpTusmm} = \left[\min\left(R^{m}_{TpTus}.R^{m}_{TusRp}\right) - max_{e\in\varepsilon}R^{m}_{Tp.e}\right] \qquad (1)$$

$$R^{m}_{TpTus} = \frac{1}{2}\log\left(1 + g_{TpTusm}P_{TpTusm}\right) \qquad (2)$$

$$R^{m}_{TusRp} = \frac{1}{2}\log\left(1 + g_{TusRpm}P_{TusRpm}\right) \qquad (3)$$

$$R^{m}_{Tp,e} = \frac{1}{2}\log\left(1 + max_{e\in\varepsilon}(g_{Tpem})P_{TpTusm}\right) \qquad (4)$$

$$R_{TusRusmm} = \frac{1}{2}\log(1 + g_{TusRusm}P^{1}_{TusRusm}) + \frac{1}{2}\log(1 + g_{TusRus}P^{2}_{TusRusm}) \qquad (5)$$

۱-۱۷-۳ بیان مسئله

هدف مسـئله این اسـت که ما مجموع $R_{TusRusmm}$ نرخ امن از فرسـتنده ثانویه T_{us} و گیرنده ثانویه R_{us} در زیرحامل m و کاربر m ضـرب با $\eta_{TusRusmm}$ ضـریب تخصـیص داه شـده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده ثانویه T_{us} و گیرنده ثانویه R_{us} مقداری که می‌تواند بگیرد صفر و یک است را با طرح بهینه سازی لاگرانژ بیشینه کنیم. برای این مهم شرایط سیستم باید به‌گونه‌ای باشـد که مجموع ضـرب $R^{s}_{TpTusmm}$ نرخ امن از فرستنده اولیه T_p و فرستنده ثانویه T_{us} در زیرحامل m و کاربر m در $\rho_{TpTusmm}$ ضـریب تخصـیص داه شـده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده اولیه T_p و گیرنده اولیه R_p از طریق فرستنده ثانویه و این بدان معناست

$$\sum_{us\in US}\sum_{m=1}^{M}\rho_{TpTusmm}R^{s}_{TpTusmm}\geq\overline{R^{S.R}} \qquad (6)$$

(۶) بدان معناست که مجموع ضرب $R^{s}_{TpTusmm}$ نرخ امن از فرستنده اولیه T_p و فرستنده ثانویه T_{us} در زیرحامل m و کاربر us در $\rho_{TpTusmm}$ ضریب تخصیص داه شده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده اولیه T_p و گیرنده اولیه R_p از طریق فرستنده ثانویه باید از نرخ پیش فرض درنظرگرفته بیشتر یا برابر باشد که ما برای سیستم برابر در نظر گرفتیم.

$$\sum_{us\in US}\sum_{m=1}^{M}\rho_{TpTusmm}P_{TpTusm}\leq P_{p}^{max} \qquad (7)$$

(۷) بدان معناست که مجموع ضرب P_{TpTusm} توان تخصیص داده شده از فرستنده اولیه T_p و فرستنده ثانویه T_{us} در بازه اول و روی زیرحامل m در $\rho_{TpTusmm}$ ضریب تخصیص داه شده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده اولیه T_p و گیرنده اولیه R_p از طریق فرستنده ثانویه باید از بیشینه توان اولیه پیش فرض در نظر گرفته شده کمترمساوی باشد و ما در این سیستیم طوری آن‌ها را در نظر گرفتیم که حداقل برابر شود چون با این کار حتما شرط دوم که کوچکتر بودن است رخ می‌دهد.

$$\sum_{us\in US}\sum_{m=1}^{M}\eta_{TusRusmm}P^{1}_{TusRusm}\leq P_{s}^{max} \qquad (8)$$

(۸) بدان معناست که مجموع ضرب $P^{1}{}_{TusRusm}$ توان تخصیص داده شده از فرستنده ثانویه T_{us} و گیرنده ثانویه T_{us} در بازه اول و روی زیرحامل m در $\eta_{TusRusmm}$ ضریب تخصیص داه شده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده ثانویه T_{us} و گیرنده ثانویه R_{us} از طریق فرستنده ثانویه باید از بیشینه توان ثانویه پیش فرض در نظر گرفته شده کمترمساوی باشد و ما در این سیستیم طوری آن‌ها را در نظر گرفتیم که حداقل برابر شود چون با این کار حتما شرط دوم که کوچکتر بودن است رخ می‌دهد.

$$\sum_{us \in US} \sum_{m=1}^{M} (\rho_{TpTusmm} P_{TusRpm} + \eta_{TusRusmm} P^2_{TusRusm}) \leq P_s^{max} \qquad (9)$$

(۹) بدان معناست که مجموع ضرب P_{TusRpm} توان تخصیص داده شده از فرستنده ثانویه T_{us} و گیرنده ثانویه R_{us} در بازه اول و روی زیرحامل m در $\rho_{TpTusmm}$ ضریب تخصیص داه شده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده اولیه T_p و گیرنده اولیه R_p از طریق فرستنده ثانویه و ضرب $P^2{}_{TusRusm}$ توان تخصیص داده شده از فرستنده ثانویه T_{us} و گیرنده ثانویه T_{us} در بازه دوم و روی زیرحامل m در $\eta_{TusRusmm}$ ضریب تخصیص داه شده تعیین کننده زیرحامل m استفاده شده برای ارسال بین فرستنده ثانویه T_{us} و گیرنده ثانویه R_{us} از طریق فرستنده ثانویه باید از بیشینه توان ثانویه پیش فرض در نظر گرفته شده کمترمساوی باشد و ما در این سیستیم طوری آن‌ها را در نظر گرفتیم که حداقل برابر شود چون با این کار حتما شرط دوم که کوچکتر بودن است رخ می‌دهد.

$$\sum_{us \in US} \rho_{TpTusmm} + \eta_{TusRusmm} = 1 \qquad \forall m \in M \qquad (10)$$

$$\sum_{m=1}^{M} \rho_{TpTusmm} + \eta_{TusRusmm} = 1 \qquad \forall us \in US \qquad (11)$$

در (۶) نرخ امن برای خطوط اولیه، (۷) توان ارسال خطوط اولیه، (۸) و (۹) توان ارسالی سیستم ثانویه در هر دو بازه زمانی، (۱۰) و (۱۱) حالتی در هر بازه زمانی برای ارسال اولیه یا ارسالِ ثانویه استفاده می‌شود، هستند که فرمول (۱۲) بیانگر این مسئله است.

$$\max \sum_{us \in US} \sum_{m=1}^{M} \eta_{TusRusmm} R_{TusRusmm} \qquad (12)$$

۱-۱۸ تحلیل مسئله

مسئله بهینه سازی در (۶) یک مسئله بهینه سازی غیرمحدب[۱] غیرخطی[۲] مختلط [13] است. با سبک کردن ترکیب پیچیده متحمل برای تخصیص زیرحامل بهینه یک ساختار مجزا و روش تجزیه دوگان در [16] بیان شده است. ما می‌دانیم که طرح تجزیه دوگان با یک راه‌حل موثر بهینه در [14] محاسبه شده است. ابتدا با توجه به (۱) اگر $R^m_{TpTus} = R^m_{TusRp}$ باشند، بنابراین می‌توانیم مقدار P_{TpTusm} و P_{TusRpm} در (۷)، (۸) و (۹) بدست اورد.

$$R^s_{TpTusmm} = \left[\min\left(R^m_{TpTus}.R^m_{TusRp}\right) - max_{e\in\varepsilon}R^m_{Tp,e}\right] \quad \rightarrow$$

$$\frac{1}{2}\log\left(1 + g_{TpTusm}P_{TpTusm}\right) = \frac{1}{2}\log\left(1 + g_{TusRpm}P_{TusRpm}\right) \quad \rightarrow$$

$$P_{TpTusm} = \frac{g_{TusRpm}P_{TusRpm}}{g_{TpTusm}} \qquad (13)$$

$$P_{TusRpm} = \frac{g_{TpTusm}P_{TpTusm}}{g_{TusRpm}} \qquad (14)$$

$$P_{TusRpmm} = P_{TusRpm} + P_{TpTusm}$$

تابع لاگرانژ مسئله بهینه سازی (۱۲) به‌صورت زیر بدست می‌آید

[۱] nonconvex

[۲] nonlinear

$$L(p.\theta.\zeta.\lambda.\gamma) = \sum_{use\epsilon US}\sum_{m=1}^{M} R_{TusRusmm} + \theta\left(\sum_{use\epsilon Us}\sum_{m=1}^{M} R^{S}_{TpTusmm} - \overline{R^{S,P}}\right) + \zeta\left(P_p^{max} - \sum_{use\epsilon US}\sum_{m=1}^{M} P_{TpTusm}\right) + \lambda\left(P_s^{max} - \sum_{use\epsilon US}\sum_{m=1}^{M}(P_{TusRpm} + P^{2}_{TusRusm})\right) + \gamma\left(P_s^{max} - \sum_{use\epsilon US}\sum_{m=1}^{M} P^{1}_{TusRusm}\right) \quad (15)$$

هر ضـرایب لاگرانژ $p.\theta.\zeta.\lambda.\gamma$ متناظر با (۷)،(۸)،(۹) و (۱۰) و p بردار توان فرستنده متغیر با استفاده از تابع لاگرانژ در (۱۵) تابع دوگان به‌صورت زیر

$$g(\theta.\zeta.\lambda.\gamma) = \max_{p.\rho.\eta} L(p.\theta.\zeta.\lambda.\gamma) \quad (16)$$

$$g(\theta.\zeta.\lambda.\gamma) = \max_{p,\rho,\eta} \sum_{use\epsilon US}\sum_{m=1}^{M} R_{TusRusmm} + \theta\left(\sum_{use\epsilon Us}\sum_{m=1}^{M} R^{S}_{TpTusmm} - \overline{R^{S,P}}\right) + \zeta\left(P_p^{max} - \sum_{use\epsilon US}\sum_{m=1}^{M} P_{TpTusm}\right) + \lambda\left(P_s^{max} - \sum_{use\epsilon US}\sum_{m=1}^{M}(P_{TusRpm} + P^{2}_{TusRusm})\right) + \gamma\left(P_s^{max} - \sum_{use\epsilon US}\sum_{m=1}^{M} P^{1}_{TusRusm}\right)$$

فرمول فوق یعنی باید مقادیر $(\theta.\zeta.\lambda.\gamma)$ را طوری بدست آوریم که g ماکزیمم شود. حال باید از عبارت لاگرانژ نسـبت به ضـرایب خواسـته شـده مشـتق گرفت و مسـئله بهینه سـازی دوگان متناظر به‌صورت زیر

$$(\theta^*.\zeta^*.\lambda^*.\gamma^*) = arg \max_{\theta.\zeta.\lambda.\gamma\geq 0} g(\theta.\zeta.\lambda.\gamma) \quad (17)$$

مـا مقـدار متغیر توان ارسـالی، خطوط ثانویه انتخابی، تخصـیص زیر حامل و مقدار متغیر دوگان را می‌یابیم.

۱-۱۸-۱ محاسبه متغیر توان ارسالی

با استفاده از (۱۳)،(۱۴) و (۱۵) ما تابع لاگرانژ دوگان را در (۱۶) جایگذاری کرده و با مشتق از تابع لاگرانژ نسبت به $P_{TusRpmm}$ به معادله (۱۸) می‌رسیم.

$$\frac{\partial L(p.\theta.\zeta.\lambda.\gamma)}{\partial P_{TusRpmm}} = \frac{\theta}{2}\left(\frac{\frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}}{1+\frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}P_{TusRpm}} - \frac{\frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}}{1+\frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}P_{TusRpm}}\right) - \frac{\zeta g_{TusRpm}+\lambda g_{TpTusm}}{g_{TusRpm}+g_{TpTusm}} = 0 \qquad (18)$$

برای اینکه به (۱۸) برسیم باید از معادله لاگرانز نسبت به توان مشتق بگیریم حال وقتی که مشتق را در معادله اعمال می‌کنیم در حقیقت می‌شود مشتق از پارامترهایی که در ان‌ها $P_{TusRpmm}$ وجود دارد که به معادله زیر می‌رسیم.

$$\frac{\partial L}{\partial P_{TusRpmm}} = \theta\left(\frac{\partial R^{S}_{TpTusmm}}{\partial P}\right) - \zeta\left(\frac{\partial (P_{TpTusm}}{\partial P}\right) - \lambda\left(\frac{\partial P_{TusRpm}}{\partial P}\right) = 0 \qquad (19)$$

مشتق از $R^{S}_{TpTusmm}$ به دو صورت است مشتق از R^{m}_{TpTus} چون به‌صورت لگاریتمی $x = a\log(bu)$ است و مشتق لگاریتم $x' = a(\frac{b}{bu})$ می‌شود که فرمول‌های (۲) و (۴) به‌صورت زیر می‌شود.

$$\frac{\partial R^{m}_{TpTus}}{\partial P_{TusRpmm}} = \frac{1}{2}\frac{\frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}}{1+\frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}P_{TusRpm}} \qquad (*)$$

$$\frac{\partial R^{m}_{Tp.e}}{\partial P_{TusRpmm}} = \frac{1}{2}\frac{\frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}}{1+\frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm}+g_{TpTusm}}P_{TusRpm}} \qquad (**)$$

حال (*) و (**) را در (۱۹) جایگذاری کرده و برابر صفر قرار داده و مخرج مشترک می‌گیریم.

$$\frac{\partial L}{\partial P_{TusRpmm}} = \frac{\theta}{2}\left(\frac{\frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm} + g_{TpTusm}}}{1 + \frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm} + g_{TpTusm}}P_{TusRpm}} - \frac{\frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm} + g_{TpTusm}}}{1 + \frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm} + g_{TpTusm}}P_{TusRpm}}\right) - \frac{\zeta g_{TusRpm} + \lambda g_{TpTusm}}{g_{TusRpm} + g_{TpTusm}} = 0 \qquad (***)$$

حال ضـرب گین‌های فرسـتنده گیرنده اولیه،ثانویه را برروی جمع‌شان را h_{TusRpm} می‌نامیم و مـاکزیمم بهره شـــنودگر در بهره فرســـتنـده ثـانویـه در گیرنـده اولیه تقســـیم بر مجموعشـــان را $max_{e\in\varepsilon}(h^e_{TusRpm})$ می‌نامیم.

$$h_{TusRpm} = \frac{g_{TpTusm}g_{TusRpm}}{g_{TusRpm} + g_{TpTusm}} \qquad (20)$$

$$max_{e\in\varepsilon}(h^e_{TusRpm}) = \frac{max_{e\in\varepsilon}(g_{Tpem})g_{TusRpm}}{g_{TusRpm} + g_{TpTusm}} \qquad (21)$$

حال با جایگذاری (۲۰) و (۲۱) در (***) می‌توان به فرمول زیر رسید.

$$\rightarrow \frac{\theta}{2}\left(\frac{h_{TusRpm}}{1 + h_{TusRpm}P_{TusRpm}} - \frac{max_{e\in\varepsilon}(h^e_{TusRpm})}{1 + max_{e\in\varepsilon}(h^e_{TusRpm})P_{TusRpm}}\right) - \frac{\zeta g_{TusRpm} + \lambda g_{TpTusm}}{g_{TusRpm} + g_{TpTusm}} = 0$$

$$\lambda_{TusRpm} = \frac{2}{\theta}\frac{\zeta g_{TusRpm} + \lambda g_{TpTusm}}{g_{TusRpm} + g_{TpTusm}} \qquad (22)$$

از این اثبات مقدار توان تخصیص شده در سیستم به صورت رابطه (۲۳) می‌شود:

$$P_{TusRpmm} = \frac{1}{2}\left[\sqrt{\left(\frac{1}{max_{e\in\varepsilon}(h^e_{TusRpm})} - \frac{1}{h_{TusRpm}}\right)^2 + \frac{4}{\lambda_{TusRpm}}\left(\frac{1}{max_{e\in\varepsilon}(h^e_{TusRpm})} - \frac{1}{h_{TusRpm}}\right)} - \left(\frac{1}{max_{e\in\varepsilon}(h^e_{TusRpm})} - \frac{1}{h_{TusRpm}}\right)\right]^+ \qquad (23)$$

اینک باید از معادله لاگرانژ نسـبت به $P^1_{TusRusm}$ و $P^2_{TusRusm}$ مشـتق بگیریم تا توان تخصیص داده شده ثانویه را در بازه زمانی اول و دوم محاسبه کنیم.

$$\frac{\partial L}{\partial P^1_{TusRusm}} = \frac{1}{2}\frac{g_{TusRusm}}{1 + g_{TusRusm}P^1_{TusRusm}} - \gamma = 0 \qquad (24)$$

توان تخصیص داده شده ثانویه در بازه زمانی اول به صورت رابطه (۲۵) بدست می‌آید.

$$P^1_{TusRusm} = \left[\frac{1}{2\gamma} - \frac{1}{g_{TusRusm}}\right]^+ \qquad (25)$$

توان تخصیص داده شده ثانویه در بازه زمانی دوم به صورت رابطه (۲۷) بدست می‌آید.

$$P^2_{TusRusm} = \left[\frac{1}{2\lambda} - \frac{1}{g_{TusRusm}}\right]^+ \qquad (27)$$

انتخاب خط ثانویه و تخصیص زیرحامل را ما تعیین می‌کنیم که کدام زیرحامل برای خطوط ثانویه همکاری با اولیه کار می‌کند تخصیص داده شده رابطه (۲۸) و کدام زیرحامل برای خط ثانویه تخصیص داده می‌شوند رابطه (۲۹) را از رابطه (۷) بدست می‌آوریم.

$$\psi^1_{TusRpm} = \theta R^S_{TpTusmm} - \zeta P_{TpTusm} - \lambda P_{TusRpm} \qquad (28)$$

$$\psi^2_{TusRusm} = R_{TusRusmm} - \gamma P^1_{TusRusm} - \lambda P^2_{TusRusm} \qquad (29)$$

حال برای تخصیص زیرحامل‌ها از روابط (۳۰) و (۳۱) استفاده می‌کنیم.

$$(T^*_{us}.m^*) = arg \max_{us\in S_{us}, m\in S_m} \psi^1_{TusRpm} \qquad (30)$$

$$\left(T^*_{us'}.m'^*\right) = arg \max_{us\in S_{us}, m\in S_m} \psi^2_{TusRusm} \qquad (31)$$

S_m و S_{us} به ترتیب گروهی از زیرحامل‌های در دسترس در اولین و دومین بازه زمانی و گروهی از کاربران ثانویه هستند. برای اینکه بدانیم کدام زیر حامل تخصیص داده شده دو تا شرط می‌گذاریم که اگر $\psi^1_{TusRpm} > \psi^2_{TusRusm}$ باشد $\rho_{TpTusmm} = 1$ و اگر $\psi^1_{TusRpm} < \psi^2_{TusRusm}$ رخ داد $\eta_{TusRusmm} = 1$ شود.

زیر گرادیان‌ها از متغیرهای دوگان $(\theta.\zeta.\lambda.\gamma)$ به ترتیب به صورت زیر است

$$\Delta\theta = \sum_{us\epsilon Us}\sum_{m=1}^{M} R^S_{TpTusmm} - \overline{R^{S.P}} \qquad (32)$$

$$\Delta\zeta = P_p^{max} - \sum_{us\epsilon US}\sum_{m=1}^{M} P_{TpTusm} \qquad (33)$$

$$\Delta\lambda = P_s^{max} - \sum_{us\epsilon US}\sum_{m=1}^{M} (P_{TusRpm} + P_{TusRusm}^2) \qquad (34)$$

$$\Delta\gamma = P_s^{max} - \sum_{us\epsilon US}\sum_{m=1}^{M} P_{TusRusm}^1 \qquad (35)$$

و در پایان نحوه بروزرسانی متغیرهای دوگان صورت می‌پذیرد.

$$\theta^{t+1} = \left[\theta^t - S_\theta^{t+1}\Delta\theta^t\right]^+ \qquad (35)$$

$$\zeta^{t+1} = \left[\zeta^t - S_\zeta^{t+1}\Delta\zeta^t\right]^+ \qquad (36)$$

$$\lambda^{t+1} = \left[\lambda^t - S_\lambda^{t+1}\Delta\lambda^t\right]^+ \qquad (37)$$

$$\gamma^{t+1} = \left[\gamma^t - S_\gamma^{t+1}\Delta\gamma^t\right]^+ \qquad (38)$$

گام ۱. مقدار اولیه متغیرهای لاگرانژ $\theta(0).\zeta(0).\lambda(0).\gamma(0)$

گام ۲. بروزرسانی توان‌های ارسالی بر مبنای متغیرهای لاگرانژ در هر تکرار

گام ۲-۱. بروزرسانی متغیرهای $P^2_{TusRusm}$ و $P^1_{TusRusm}$ با استفاده از (۲۵) ، (۲۷)

گام ۲-۲. بروزرسانی متغیر P_{TpTusm} با استفاده از (۱۳)

گام ۲-۳. بروز رسانی متغیر P_{TusRpm} با استفاده از (۱۴)

گام ۳. تخصیص زیرحامل ها

گام ۳-۱. $S_M = \{1. \dots . N\} . S_{us} = Us$

گام ۳-۲. $\rho = 0$ و $\eta = 0$

گام ۳-۳. ساختن (T^*_{us}, m^*) و $\left(T^*_{us'}, m'^*\right)$ با استفاده از (۳۰) و (۳۱)

گام ۳-۴. $\rho_{Tp,Tus^*,m^*} = 1$ اگر $\psi^1_{TusRpm} \geq \psi^2_{TusRusm}$

گام ۳-۵. $\eta_{Tus^{*\prime},Rus^{*\prime},m^{*\prime}} = 1$ اگر $\psi^1_{TusRpm} < \psi^2_{TusRusm}$

گام ۳-۶. اگر $\rho_{Tp,Tus^*,m^*} = 1$ شود در نتیجه $S_M = S_M - \{m^*\}$ و $S_{us} = S_{us} - \{us^*\}$

گام ۳-۷. اگر $\eta_{Tus^{*\prime}.Rus^{*\prime}.m^{*\prime}} = 1$ شود در نتیجه $S_M = S_M - \{m'^*\}$ و $S_{us} = S_{us} - \{us'^*\}$

گام ۳-۸. اگر $S_M \neq \emptyset$ شد برو به گام ۳-۲

گام ۴. بروزرسانی متغیرهای دوگان با استفاده از زیرگرادیان و ....

گام ۴-۱. بروزرسانی متغیر θ با استفاده از (۳۵)

گام ۴-۲. بروزرسانی متغیر ζ با استفاده از (۳۶)

گام ۴-۳. بروزرسانی متغیر λ با استفاده از (۳۷)

گام ۴-۴. بروزرسانی متغیر η با استفاده از (۳۸)

گام ۵. اگر شرط حلقه برآورده نشد برو به گام ۲

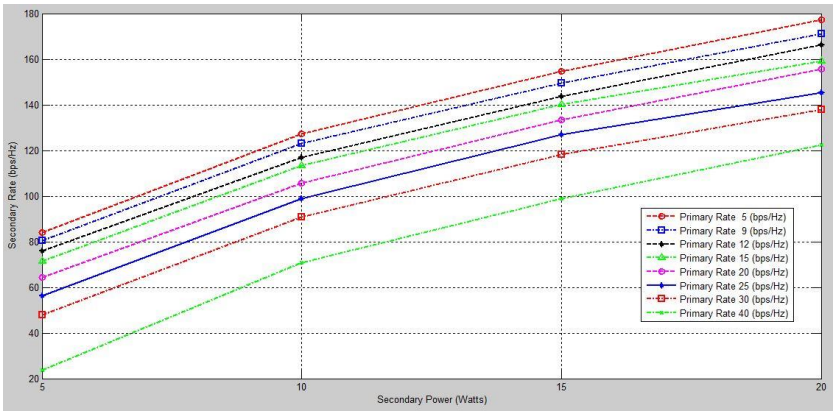
گام ۶. پایان

شکل ۴-۲ الگوریتم برای حل مسئله بهینه سازی با استفاده از طرح دوگان لاگرانژ

فصل پنجم: نتیجه گیری و پیشنهاد

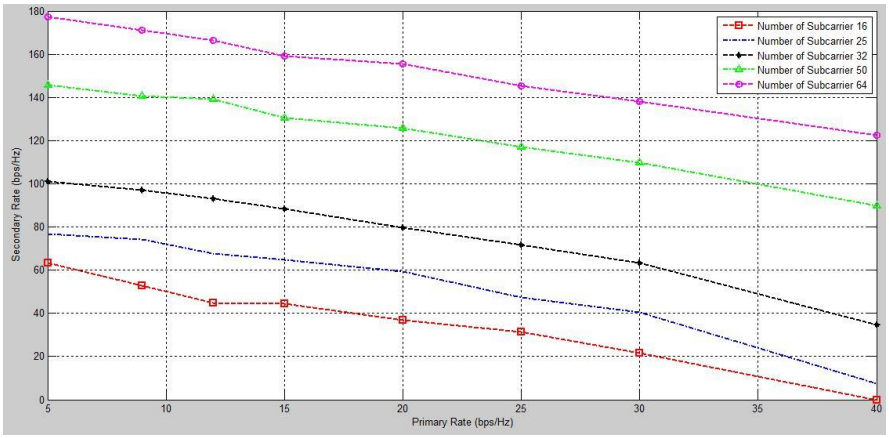
۱-۱۹ نتایج شبیه سازی

در نتایج ما توان ارسالی اولیه را ثابت ($P_p^{max} = 40\ Watts$) و مقدار زیرحامل و کاربران ثانویه را N=64 در نظر گرفته‌ایم و مقدار توان ارسالی ثانویه را تغییر داده و نرخ‌های ثانویه را محاسبه کردیم که شکل ۵-۱ مقادیر مختلف نرخ ثانویه را روی توان‌های متفاوت نشان می‌دهد. با توجه به شکل زیر می‌توان نتیجه گرفت که هر چه توان ارسالی ثانویه افزایش یابد نرخ ثانویه هم شروع به افزایش کرده و امنیت مورد نیاز برای کاربر اولیه افزایش می‌یابد.



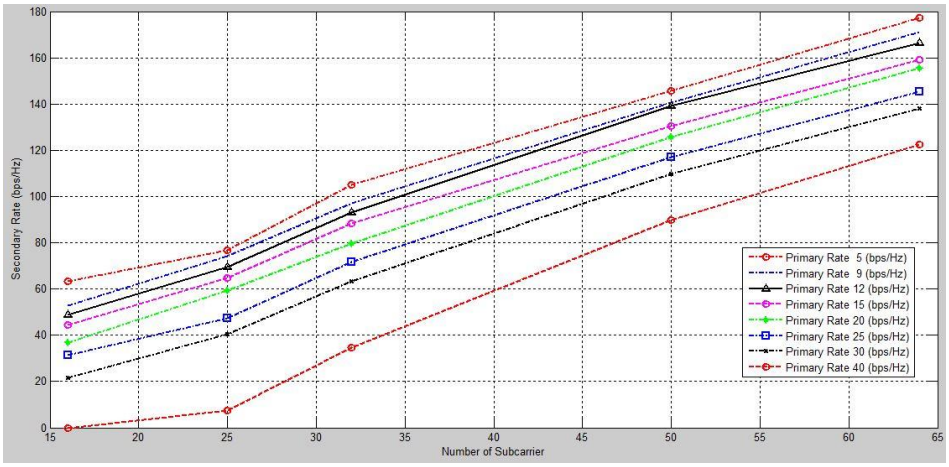
شکل ۵-۱ نرخ ثانویه روی توان ارسالی ثانویه متفاوت

در شکل (۵-۲) ما تاثیرات نرخ امن را برای کاربر اولیه روی زیرحامل‌های مختلف بررسی کردیم. در زیرحامل‌های مختلف هر چه نرخ امن اولیه افزایش یابد نرخ ثانویه شروع به کاهش میکند و این بدان معناست که کاربران ثانویه امنیت ارسال اطلاعات را برای کاربران اولیه تامین می‌کنند. در این قسمت ما $P_P^{max} = 40\text{Watts}$ و $P_s^{max} = 20Watts$ در نظر گرفتیم. ما تغییرات نرخ امن کاربر اولیه و محاسبه مجموع نرخ ثانویه سیستم و نتایج شبیه سازی رابرای زیرحامل‌های مختلف بررسی کردیم. از طرفی با افزایش زیرحامل‌ها نرخ مجموع سیستم ثانویه افزایش می‌یابد زیرا گین چندگانگی چند کاربری سیستم افزایش می‌یابد.



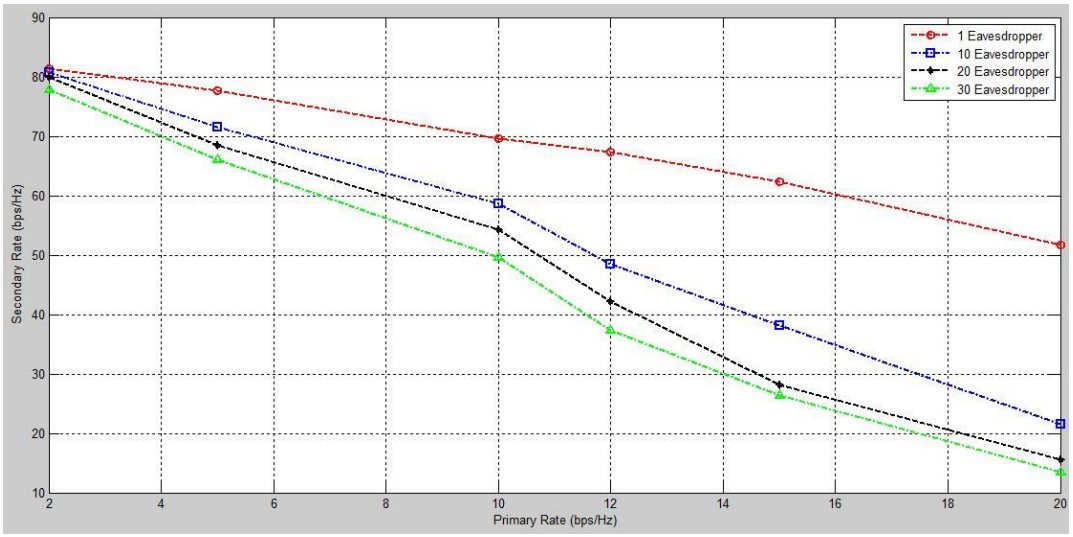
شکل ۵-۲ نرخ ثانویه روی نرخ اولیه مختلف

در شکل (۵-۳) ما تاثیر تعداد کاربران ثانویه در سیستم را بررسی کردیم و نرخ ثانویه نسبت به زیرحامل‌ها را نشان دادیم.



شکل ۵-۳ نرخ ثانویه روی زیرحامل‌های مختلف

و در نهایت تاثیر استراق سمع کننده را بر نرخ سیستم ثانویه مطالعه کردیم. نتایج در شکل (۵-۴) حاکی از این است با افزایش تعداد شنودگرها نرخ ثانویه سیستم را کاهش می‌دهد، زیرا افزایش شنودگرها افزایش بهرهای چندگانگی چندکاربره را در بر دارد و اگر نرخ امن گاربر اولیه متقاعد کننده باشد از باقی‌مانده منابع برای ارسال اطلاعات سیستم ثانویه استفاده می‌شود.



شکل ۵-۴ نرخ ثانویه روی استراق سمع کننده‌های مختلف

۱-۲۰ نتیجه گیری

نتایج شبیه سازی حاکی بر این است که ما توانستیم سیستم مدلی طراحی کنیم که کاربران ثانویه به کاربر اولیه برای امنیت اطلاعات مورد نیاز کمک می‌کند. در بازه اول کاربر ثانویه نقش رله DF را برای ارسال اطلاعات کاربر اولیه به مقصد ایفا می‌کند. در بازه دوم کاربران ثانویه اجازه دارند از طیف باقی‌مانده برای ارسال اطلاعات خودش استفاده می‌کند.

۱-۲۱ پیشنهادات

پیشـــنهاداتی که می‌توان برای کســـانی که می‌خواهند در این راســـتا گام بردارند در زیر بیان می‌شود.

- ✓ برداشت انرژی

در این پایان نامه منابع ما نامحدود در نظر گرفته شـده بود و حال می‌توان منابع را محدود در نظر گرفت.

- ✓ استفاده از رله دو طرفه

ما در این پایان نامه از رله یک‌طرفه اســتفاده کردیم و می‌توان به این صورت در نظر گرفت که علاوه بر اینکه از منابع به رله ارســال می‌شــود می‌توان از رله هم ارســال صــورت گیرد که باعث بهبود امنیت نرخ اطلاعات می‌شود.

- ✓ استفاده از رله AF در سیستم مدل

کاربران ثانویه‌ای که برای کمک به ارسال اطلاعات شبکه اولیه انتخاب شده‌اند، اطلاعات دریافتی از شــبکه اولیه را رمزگشــایی و تقویت و مجددا رمزگذاری و تقویت کرده، و اطلاعات رمز شــده را به سمت کاربر اولیه ارسال می‌کند.

پیوست : واژگان

AF	Amplify and Forward
AWGN	Additive White Guassian Noise
BER	Bit Error Rate
BLUE	Best Linear Unbiased Estimation
BPSK	Binary Phase Shift Keying
CF	Compress and Forward
CR	Cognitive Radio
CRLB	Cramer-Rao Lower Bound
CSI	Channel State Information
DF	Decode and Forward
DPC	Dirty Paper Coding
EF	Estimate and Forward
EGC	Equal Gain Combining
EPA	Equal Power Allocation
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
IEEE	Institute of Electrical and Electronics Engineers
LMMSE	Linear Minimum Mean Square Error
LS	Least Squares estimation
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
ML	Maximum Likellihood
MMSE	Minimum Mean Square Error
MRC	Maximal Ratio Combining
MSE	Mean Square Error
OFDM	Orthogonal Frequency Division Multiplexing
OPA	Optimum Power Allocation
OWRN	One-Way Relay Network
PDF	Probability Distribution Function
PU	Primary User
QoS	Quality of Service
RF	Radio Frequency
R	Relay
RMMSE	Relaxed Minimum Mean Square Error
SDMA	Space Division Multiple Access
SDR	Software Defined Radio
SIMO	Single Input Multiple Output

SINR	Signal to Interference plus Noise Ratio
SISO	Single Input Single Output
SLS	Scaled Least Squares estimation
SNR	Signal to Noise Ratio
SQP	Sequential Quadratic Programming methods
SU	Secondary User
TDD	Time Division Duplex
TWRN	Two-Way Relay Network
UHF	Ultra High Frequency
UWB	Ultra Wide Band
VHF	Very High Frequency
WRAN	Wireless Regional Area Network

مراجع

[۱] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[۲] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[۳] J. S. Gans, S. P. King, and J. Wright, "Wireless Communications: Handbook of Telecommunications Economics," *Univ. Melb.*, vol. 2, 2007.

[4] D. Zhu, J. Wang, A. L. Swindlehurst, and C. Zhao, "Downlink resource reuse for device-to-device communications underlaying cellular networks," *IEEE Signal Process. Lett.*, vol. 21, no. 5, pp. 531–534, 2014.

[5] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, 2014.

[6] J. Qiao, X. S. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, "Enabling device-to-device communications in millimeter-wave 5G cellular networks," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 209–215, 2015.

[7] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, 2009.

[8] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3541–3551, 2013.

[9] M. Chiang, P. Hande, T. Lan, and C. W. Tan, "Power control in wireless cellular networks," *Found. Trends® Netw.*, vol. 2, no. 4, pp. 381–533, 2008.

[10] Y. Sun, W. Trappe, and K. J. R. Liu, *Network-aware security for group communications*. Springer, 2008.

[11] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, 2011.

[12] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J. Sel. areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[13] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Mobile Multimedia Communications, 1999.(MoMuC'99) 1999 IEEE International Workshop on*, 1999, pp. 3–10.

[14] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[15] J. M. Peha, "Sharing spectrum through spectrum policy reform and cognitive radio," *Proc. IEEE*, vol. 97, no. 4, pp. 708–719, 2009.

[16] A. D. Wyner, "The Wire- Tap Channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[17] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. theory*, vol. 24, no. 4, pp. 451–456, 1978.

[18] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, 2010.
[20] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.
[21] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, 2011.
[22] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wirel. Commun.*, vol. 10, no. 10, pp. 3528–3540, 2011.
[23] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, 2011.
[24] J. S. Oberoi, U. Pareek, M. Naeem, and D. C. Lee, "EDA-based joint power, subcarrier allocation and relay assignment scheme for multiuser relaying in OFDMA-based cognitive radio systems," in *Signal Processing and Communication Systems (ICSPCS), 2011 5th International Conference on*, 2011, pp. 1–7.
[25] M. Shaat and F. Bader, "Asymptotically optimal resource allocation in OFDM-based cognitive networks with multiple relays," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 3, pp. 892–897, 2012.
[26] J. Guo, S. Gu, X. Wang, H. Yu, and M. Guizani, "Subchannel and power allocation in OFDMA-based cognitive radio networks," in *Communications (ICC), 2010 IEEE International Conference on*, 2010, pp. 1–5.
[27] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, 2008.
[28] T. Elkourdi and O. Simeone, "Spectrum leasing via cooperation with multiple primary users," *IEEE Trans. Veh. Technol.*, vol. 61, no. 2, pp. 820–825, 2012.
[29] M. S. Islam, G. R. Barai, and A. Mahmood, "Performance analysis of different modulation schemes using OFDM techniques in Rayleigh fading channel," *Int. J. Fundam. Phys. Sci.*, vol. 1, no. 1, pp. 22–27, 2011.
[30] W. D. Lu, Y. Gong, S. H. Ting, X. L. Wu, and N. T. Zhang, "Cooperative OFDM relaying for opportunistic spectrum sharing: Protocol design and resource allocation," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 6, pp. 2126–2135, 2012.
[31] F. He, Y. Sun, X. Chen, L. Xiao, and S. Zhou, "Optimal power allocation for two-way decode-and-forward OFDM relay networks," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 4463–4467.
[32] L. Li, X. Zhou, H. Xu, G. Y. Li, D. Wang, and A. Soong, "Simplified relay selection and power allocation in cooperative cognitive radio systems," *IEEE Trans. Wirel. Commun.*, vol. 10, no. 1, pp. 33–36, 2011.
[33] Y.-C. Liang, K.-C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Trans. Veh. Technol.*, vol. 60, no. 7, pp. 3386–3407, 2011.
[34] A. Alsharoa, F. Bader, and M.-S. Alouini, "Relay selection and resource allocation for two-way DF-AF cognitive radio networks," *IEEE Wirel. Commun. Lett.*, vol. 2, no. 4, pp. 427–430, 2013.
[35] Y. Li, M. Peng, W. Wang, and X. Zhang, "Optimal power allocation for OFDM-based two-way relaying in cognitive radio networks," in *Wireless Communications*

and Networking Conference (WCNC), 2013 IEEE, 2013, pp. 528–532.
[36] D. Yang, L. Xiao, J. Xu, and W. Li, "Joint power control and relay selection scheme for cognitive two-way relay networks," *J. Syst. Eng. Electron.*, vol. 24, no. 4, pp. 571–578, 2013.
[37] C. Zhai and W. Zhang, "Adaptive spectrum leasing with secondary user scheduling in cognitive radio networks," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 7, pp. 3388–3398, 2013.
[38] S. M. M. Toroujeni, S. M.-S. Sadough, and S. A. Ghorashi, "Spectrum leasing for OFDM-based cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2131–2139, 2013.
[39] T. Jing *et al.*, "Cooperative relay selection in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1872–1881, 2015.
[40] J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 11, pp. 4502–4507, 2008.
[41] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Top. Signal Process.*, vol. 2, no. 1, pp. 28–40, 2008.
[42] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 4, 2010.
[43] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE J. Sel. Top. Signal Process.*, vol. 5, no. 1, pp. 5–23, 2011.
[44] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *AD hoc networks*, vol. 7, no. 5, pp. 810–836, 2009.
[45] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, 2009.
[46] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, 2007.
[47] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 693–702, 2011.
[48] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, 2009.
[49] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.
[50] T. Cover and A. E. L. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. theory*, vol. 25, no. 5, pp. 572–584, 1979.
[51] S. Pietrzyk, *OFDMA for Broadband Wireless Access (Artech House Mobile Communications)*. Artech House, Inc., 2006.
[52] Z.-Q. Luo and S. Zhang, "Dynamic spectrum management: Complexity and duality," *IEEE J. Sel. Top. Signal Process.*, vol. 2, no. 1, pp. 57–73, 2008.
[53] D. P. Palomar and M. Chiang, "A tutorial on decomposition methods for network utility maximization," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1439–1451, 2006.
[54] H. N. Vu and H.-Y. Kong, "Joint subcarrier matching and power allocation in OFDM two-way relay systems," *J. Commun. Networks*, vol. 14, no. 3, pp. 257–

266, 2012.
[55] W. Yu and R. Lui, “Dual methods for nonconvex spectrum optimization of multicarrier systems,” *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, 2006.
[56] H. W. Kuhn, “The hungarian method for the assignment problem,” in *50 Years of Integer Programming 1958-2008*, Springer, 2010, pp. 29–47.
[57] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.
[58] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: A survey,” *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, 2011.
[59] A. Ghasemi and E. S. Sousa, “Collaborative spectrum sensing for opportunistic access in fading environments,” in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, 2005, pp. 131–136.
[60] J. Shen, T. Jiang, S. Liu, and Z. Zhang, “Maximum channel throughput via cooperative spectrum sensing in cognitive radio networks,” *IEEE Trans. Wirel. Commun.*, vol. 8, no. 10, 2009.
[61] M. J. Saber and S. M. Sajad Sadough, “Optimisation of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack,” *Trans. Emerg. Telecommun. Technol.*, 2014.

Abstract:

Cognitive radio is an approach in order to enhance efficiency of using spectrum. The basis of this approach is to divide the spectrum between primary and secondary users. The primary users are allowed to use the intended spectrum and can access to it any time. The secondary users access to the spectrum dynamically and opportunistic, provided to not interfere unbearably with primary users. In the present thesis we examined the spectrum leasing in cognitive radio grate based on OFDMA (Orthogonal Frequency Division Multiplexing Access) for keeping secret forwarding information of the primary grate. In this grate, the secondary users serve as decode and forward relay stations and help the primary grate in forwarding information. In this grate, it is assumed that the band width divides into n sub-carrier. The primary grate is an OFDM and the primary users can simultaneously use more and one sub-carrier, while the secondary users can only forward information on a single sub-carrier. Moreover, there are some .... users in the intended grate who attempt to eavesdrop the forwarded information. In that grate, forwarding information is made as frame to frame, in which each frame includes two periods. In the first period the primary base station forwards information, while secondary users listen to primary base station. In the second period, secondary users who have selected to help forwarding information of primary grate, encode received information from primary grate, re-decoding them, and forward the decoded information to the primary user. Other secondary users, if there are, forward their information to the secondary base station in the second period. It can assume various scenarios for eavesdropper, like that the eavesdropper eavesdrops forwarded information from primary base station in the first period, or it eavesdrops forwarded information form secondary users in second period.

The purpose of this study was to assign suggested sources, select proper secondary users to help forwarding information of primary grate, assign sub-carriers to secondary users, assign power of primary base station and secondary users, such that guaranteed the secrecy of forwarding information of primary grate and maximize the secrecy rate of secondary grate information forward. We used dual Lagrange and sub-gradient methods for solving problem.

Keywords:

Cognitive radio, cooperative communications, dual Lagrange, secrecy, spectrum leasing

Shahrood University of Technology

Faculty of Electrical and Robatic Engineering

M.Sc. Thesis in Digital Electronic Systems Engineering

A Cooperative Spectrum Leasing Scheme with Guaranteed Secrecy Rate for Primary Link

Shokufeh Vatanpour Azghandi

Supervisors:

Dr. M. Javan

Date: February 2017