Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 2, Summer 2024, Serial No. 46
ISSN: 2322-4347 , E-ISSN: 2980-8979

Covert communication in the presence of untrusted relay

M. R Yari[1] , M. Forouzesh[2], P. Azmi[2]*
Professor, Tarbiat Modares University, Tehran, Iran.

(Received: 2024/04/06, Revised: 2024/07/16, Accepted: 2024/08/03, Published: 2024/08/31)
DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.2.1.1

ABSTRACT

This work discusses covert communication and information theory security in a network with an untrusted relay. In this article, a scenario is proposed and evaluated in which the source and destination are equipped with multiple antennas and communicate with each other by the help of a single antenna untrusted relay. The warden is also considered to be equipped with multiple antennas and based on the total power received by all antennas, he decides on the present or absence of communication. Considering the limitation of the total transmit power, the constrained optimization problem is formulated to maximize the secrecy rate subject to satisfy covert communication requirements. To solve the single-objective constrained problem, the idea of converting the constrained problem into a multi-objective problem is proposed. Finally, we employ the nondominated sorting genetic algorithm (NSGA) to solve it.

If the ergodic secrecy rate is considered as a measure of efficiency, comparing the proposed solution with an exhaustive search shows a gap of about 6.888%, and the proposed solution is efficient. If the source employs the maximum ratio transmission method toward the untrusted relay in the first phase, the ergodic secrecy rate is improved by 9.48% and 11.53% compared to best antenna selection and random antenna selection, respectively. A higher secrecy rate can be obtained by using the maximum ratio transmission method toward the untrusted relay by the destination to transmit the artificial noise signal in the first phase. Furthermore, the greater the source's antennas, the greater the untrusted relay distance from the source.

Keywords: Covert communication, Information theory security, Untrusted relay, multi antennas techniques, NSGA.

*Corresponding Author Email: pazmi@modares.ac.ir

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۱۴-۱
شاپا الکترونیکی: 2980-8979 شاپا چاپی: 2322-4347

علمی – پژوهشی

مخابره پنهان در حضور رله غیرقابل‌اعتماد

محمدرضا یاری[۱]، مسلم فروزش[۲]، پائیز عزمی[۳*]

۱- دانشجوی دکتری دانشگاه تربیت مدرس، تهران، ایران. ۲- استادیار دانشگاه تخصصی فناوری‌های نوین آمل، آمل، ایران. ۳- استاد، دانشگاه تربیت مدرس، تهران، ایران.

(دریافت: ۱۴۰۳/۰۱/۱۸، بازنگری: ۱۴۰۳/۰۴/۲۶، پذیرش: ۱۴۰۳/۰۵/۱۳، انتشار: ۱۴۰۳/۰۶/۱۰)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.2.1.1

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

در این مقاله به بررسی توأم مخابره پنهان و ارسال امن نظریه اطلاعاتی در یک شبکه دارای رله غیرقابل‌اعتماد پرداخته می‌شود. سناریویی پیشنهاد و مورد ارزیابی قرار می‌گیرد که منبع و مقصد در آن مجهز به چندین آنتن هستند و با کمک رلهٔ غیرقابل‌اعتماد تک آنتن با یکدیگر ارتباط برقرار می‌کنند. ناظر نیز مجهز به چندین آنتن در نظر گرفته می‌شود و بر اساس مجموع توان دریافتی توسط تمام آنتن‌ها در ارتباط باوجود یا عدم وجود مخابره، تصمیم‌گیری می‌کند. باتوجه‌به محدودیت توان کل ارسالی، مسئلهٔ بهینه‌سازی باهدف بیشینه‌کردن نرخ امن به‌شرط برقراری الزامات مخابره پنهان فرمول‌نویسی می‌شود. برای حل مسئلهٔ مقید تک‌هدفه از روش تبدیل مسئله تک‌هدفه به چندهدفه استفاده می‌شود. مسئلهٔ بهینه‌سازی چندهدفه با الگوریتم NSGAII حل می‌شود. چنانچه نرخ امن ارگودیک به‌عنوان معیار سنجش کارایی در نظر گرفته شود، مقایسه با الگوریتم جست‌وجو جامع نشان می‌دهد که روش مطرح‌شده، جهت حل مسئله بهینه‌سازی تخصیص توان با روش جست‌وجوی جامع ٪ ۶/۸۸ اختلاف دارد و روشی کارآمد هست. اگر در فاز اول منبع برای ارسال سیگنال داده از روش بیش‌ترین نرخ ارسال در جهت رله غیرقابل‌اعتماد استفاده نماید؛ نرخ امن ارگودیک نسبت به روش انتخاب بهترین آنتن و انتخاب تصادفی آنتن به ترتیب ٪ ۹/۴۸ و ٪ ۱۱/۵۳ بهبود پیدا می‌کند. همچنین با استفاده از روش بیش‌ترین نرخ ارسال به سمت رله توسط مقصد برای ارسال سیگنال نویز مصنوعی در فاز اول، نرخ امن بالاتری حاصل می‌شود. علاوه بر این، هرچقدر تعداد آنتن‌های منبع افزایش پیدا کند، لازم است که رله، فاصله بیش‌تری را تا منبع داشته باشد.

کلیدواژه‌ها: مخابره پنهان، ارسال امن نظریه اطلاعاتی،رله غیرقابل‌اعتماد، فن‌های چند آنتنی، الگوریتم NSGAI

۱- مقدمه

دسته‌ای از حملات که علیه شبکه‌های بدون سیم انجام می‌شوند؛ حملات غیرفعال هستند. حملات غیرفعال به دودستهٔ حملات شنودی[۲] و حملات آنالیز[۳] ترافیک طبقه‌بندی می‌شوند. در این مقاله راهکارهایی برای مقابله با حملات غیرفعال در سیستم مدل پیشنهادی ارائه خواهد شد. به‌عبارت‌دیگر در این مقاله این فرض وجود دارد که حملات جعل[۴] (پیام یا هویت)، دست‌کاری[۵] و قطع[۶] علیه شبکه بدون سیم انجام نمی‌شود.

راهکار متداول برای برقراری امنیت، استفاده از الگوریتم‌های رمزنگاری هست[۱]. در به‌کارگیری الگوریتم‌های رمزنگاری، این فرض وجود دارد که شنودگران قابلیت محاسباتی محدودی دارند؛ بنابراین در زمان مناسب نمی‌توانند پیام را رمزگشایی نمایند و زمانی که رمزگشایی صورت گیرد، اطلاعات اعتبار خود را از دست می‌دهند [۲].

باتوجه‌به قانون مور[۷]، قابلیت محاسباتی تجهیزات همیشه در حال افزایش هست. همچنین ظهور فنّاوری‌هایی نظیر محاسبات کوانتوم سبب می‌شود؛ توان محاسباتی تجهیزات به‌شدت افزایش پیدا کند. باتوجه‌به قانون مور و ظهور محاسبات کوانتوم، این نتیجه گرفته می‌شود که فرض توان محدود محاسباتی شنودگران رفته‌رفته کارایی خود را از دست می‌دهد[۳]. از سوی دیگر روش-

* رایانامه نویسنده مسئول: pazmi@modares.ac.ir

[2] Eavesdropping
[3] Traffic analysis
[4] Fabrication
[5] Modification
[6] Interruption
[7] Moore's law

های رمزنگاری نمی‌توانند، مانع حملاتی همچون حملات آنالیز ترافیک شوند[۴].

از مطالب فوق این نتیجه حاصل می‌شود که امروزه برای برقراری امنیت شبکه‌های بدون سیم فن‌های رمزنگاری به‌تنهایی کافی نیستند. پژوهشگران استفاده از امنیت در لایه فیزیکی[۱] (PLS) را به‌عنوان لایه اول دفاعی شبکه پیشنهاد می‌دهند[۵].

یکی از راهکارهای مقابله با حملات آنالیز ترافیک، مخابره پنهان[۲] هست. یکی از کاربردهای مهم مخابره پنهان در مخابرات نظامی باهدف پنهان‌کردن ارتباطات برای جلوگیری از تشخیص وجود مخابره توسط نیروهای دشمن هست. در این کاربردها اگر دشمن از وجود مخابره آگاه شود ممکن است عملیاتی نظامی انجام دهد. درصورتی‌که وجود مخابره از ناظر موجود در شبکه پنهان باشد، ناظر موجود در شبکه شانسی برای حملات شنودی نیز نخواهد داشت؛ بنابراین مخابره پنهان به‌نوعی مانع حملات شنودی ناظر نیز می‌شود.

در پژوهش‌های متنوعی سعی شده است که از مشخصات لایه فیزیکی نظیر نویز، تداخل، محوشدگی و غیره جهت فریب ناظر موجود در شبکه استفاده شود[۶-۱۳]؛ به‌طوری‌که فرستنده پیام خود را بر روی کانال نویزی برای گیرنده ارسال می‌نماید و ناظر موجود در شبکه قصد دارد، وجود یا عدم وجود مخابره بین گره‌های شبکه را کشف نماید.

در مخابرهٔ پنهان، مخابره در T اسلات زمانی انجام می‌شود که در هر اسلات زمانی n سمبل ارسال می‌شود[۱۲]. ناظر بر اساس انرژی دریافت شده در هر اسلات زمانی تصمیم می‌گیرد که آیا در اسلات زمانی مشخص ارسال داده، انجام‌شده است یا خیر.

فرض Ψ_0 بیانگر این مطلب هست که فرستنده در اسلات زمانی مشخص داده‌ای را ارسال نکرده است و فرض Ψ_1 بیانگر ارسال داده در اسلات زمانی مشخص هست. $\mathrm{P}(\Psi_1) = \rho$ و $\mathrm{P}(\Psi_0) = 1 - \rho$ به ترتیب احتمال ارسال و عدم ارسال داده هستند. در چنین شرایطی خطای تشخیص ارسال یا عدم ارسال در ناظر از رابطهٔ زیر محاسبه می‌گردد.

$$\mathbb{P}_e = (1-\rho).\mathbb{P}_{FA} + \rho.\mathbb{P}_{MD} \qquad (۱)$$

در رابطهٔ فوق $\mathbb{P}_{FA}$ احتمال هشدار اشتباه[۳] هست. یعنی احتمال عدم ارسال داده، درحالی‌که ناظر تصمیم بر ارسال داده گرفته است. همچنین $\mathbb{P}_{MD}$ احتمال از دست دادن آشکارسازی[۴] هست. یعنی احتمال آن‌که ارسال داده صورت پذیرد اما ناظر تصمیم بر عدم ارسال داده بگیرد.

در ادبیات مخابره پنهان، زمانی گفته می‌شود، فرستنده با گیرنده دارای مخابره پنهان هست که رابطه زیر در مخابره برقرار باشد.

$$for\ any\ \varepsilon \geq 0, \mathbb{P}_{MD} + \mathbb{P}_{FA} \geq 1 - \varepsilon, as\ n \to \infty \qquad (۲)$$

در بسیاری از مواقع به سبب اثر سایه[۵] یا فاصله‌ی زیاد گیرنده و فرستنده لینک مستقیمی بین آن‌ها وجود ندارد. در چنین مواردی با استفاده از رله می‌توان به‌نوعی چندگانگی مکانی[۶] ارسال را فراهم آورد[۱۴]. در این حالت به سبب فاصله‌ی مکانی آنتن‌های مجازی که ایجاد می‌شود، بسیار بهتر از چندگانگی چندین آنتن، قابلیت اطمینان[۷] مخابره بهبود پیدا می‌کند[۱۵]. در سیستم مدل موردبررسی منبع و مقصد به چندین آنتن مجهز هستند اما باتوجه‌به عدم وجود لینک مستقیم بین آن‌ها چندگانگی چندین آنتن به‌تنهایی کارآمد نیست و استفاده از رله در چنین شرایطی کمک‌کننده هست.

رله علاوه بر نقش یاری‌رسان ممکن است، نقش شنودگر[۸] را نیز داشته باشد، در چنین شرایطی به رله، رله غیرقابل‌اعتماد گفته می‌شود[۱۶]. در این مقاله فرض می‌شود که رله غیرقابل‌اعتماد است. جهت جلوگیری از شنود اطلاعات توسط رله از ارسال امن نظریه اطلاعاتی[۹] استفاده می‌شود.

در سال ۱۹۷۵ مدل کانال شنودی آقای وینر مطرح شد[۱۷]. بر اساس مدل کانال شنودی زمانی که کانال شنودی نسخه تضعیف یافته تری نسبت به کانال اصلی باشد، دست‌یابی به امنیت کامل در یک کانال بدون حافظه گسسته امکان‌پذیر هست[۱۷]. بر اساس کار آقای وینر مطالعات فروانی درزمینه‌ی ارسال امن نظریه اطلاعاتی شکل گرفت. سیستم مدل کلی ارسال امن نظریه اطلاعاتی شامل دو گره قانونی آلیس و باب هست. شنودگر ایو نیز قصد دارد به محتوی پیام ارسالی بین آلیس و باب پی ببرد. هدف آلیس، استفاده از ابزارها و فن‌هایی هست که به‌وسیله‌ی آن‌ها بتواند، پیام را به‌صورت محرمانه به باب تحویل دهد. برای دست‌یابی به این هدف، آلیس از مشخصات لایه فیزیکی نظیر نویز، تداخل، محوشدگی، چندگانگی و غیره بهره می‌برد[۱۸]؛ با استفاده از این ابزارها سعی می‌کند یک مزیت در کانال اصلی نسبت به کانال شنودی ایجاد کند.

یکی از مفاهیم مهم در ارسال امن نظریه اطلاعاتی، ظرفیت (نرخ) امن[۱۰] هست. در ارسال امن نظریه اطلاعاتی ظرفیت (نرخ) امن بیانگر بالاترین نرخ ارسال به سمت کاربر قانونی هست، به‌نحوی‌که محرمانگی و اطمینان[۱۱] ارسال به طور هم‌زمان تضمین شود. ظرفیت محرمانه به‌صورت زیر تعریف می‌شود.

[1] Physical Layer Security
[2] Covert communication
[3] False alarm
[4] Miss Detection
[5] Shadowing
[6] Space diversity
[7] Reliablity
[8] Eavesdropper
[9] Information-theoretic security
[10] Secrecy capacity (Rate)
[11] Reliablity

$$C_s = [C_B - C_E]^+ \quad (۳)$$

در رابطه فوق، C_B و C_E به ترتیب ظرفیت شانون کانال گیرنده اصلی و کانال شنودگر هستند. همچنین $[x]^+ = \max(x, 0)$ هست. درصورتی‌که کانال‌ها گوسی در نظر گرفته شوند، ظرفیت امن از رابطهٔ زیر محاسبه می‌گردد.

$$C_s = [\log_2(1+\gamma_d) - \log_2(1+\gamma_e)]^+ \quad (۴)$$

در رابطهٔ فوق γ_d و γ_e به ترتیب سیگنال به نویز[1] (SNR) دریافتی در مقصد و شنودگر هستند.

کانال‌های مخابراتی بدون سیم، دارای تغییرات زمانی، مکانی و فرکانسی هستند. روابط ۳ و ۴ بیانگر ظرفیت یا نرخ امن لحظه-ای هستند. یکی از معیارهایی که برای بررسی اثر تغییرپذیر بودن کانال‌های بدون سیم استفاده می‌شود، میانگین‌گیری آماری از ظرفیت امن لحظه‌ای هست. با میانگین‌گیری از نرخ امن لحظه-ای، نرخ امن ارگودیک[2] (ESR) به دست می‌آید. در [۷] برای محاسبه ESR از روش شبیه‌سازی مونتو-کارلو[3] استفاده‌شده است.

یکی از راه‌حل‌های برجسته برای برقراری ارسال امن نظریه اطلاعاتی و مخابره پنهان بکار بردن سیگنال نویز مصنوعی[4] هست. نکته بسیار مهم در به‌کاربردن سیگنال نویز مصنوعی این است که اثر مخرب آن در شنودگر و ناظر بسیار بالا باشد، در عوض اثر مخرب بسیار کمی را در گیرنده اصلی داشته باشد. در شکل۱ روش‌های گوناگون ارسال سیگنال نویز مصنوعی نمایش‌داده‌شده است. این روش‌ها عبارت‌اند از:

۱- تداخل بر اساس منبع:

در آن منبع یک سیگنال ترکیبی شامل سیگنال اطلاعات و سیگنال نویز مصنوعی را ارسال می‌کند. [۱۹, ۲۰] البته سناریوهایی وجود دارد که ارسال دارای چند فاز هست، منبع در یک‌فاز به ارسال سیگنال داده و در فاز دیگر به ارسال سیگنال نویز مصنوعی می‌پردازد[۷]. تداخل بر اساس منبع در شکل ۱ (الف) آورده شده است.

۲- تداخل بر اساس اخلالگر دوست:

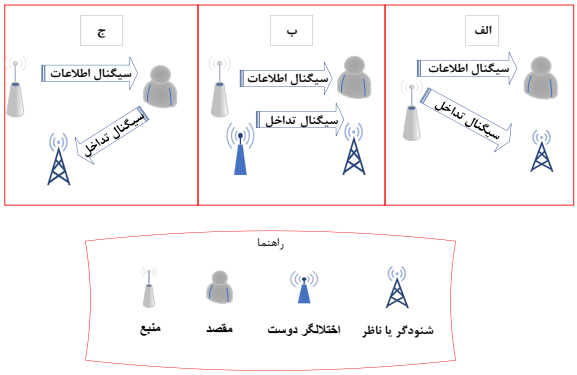
در این روش یک رله یا یک اختلالگر خارجی دوستانه[5] (FJ) مشارکت دارد تا PLS را به ارمغان آورد[۲۱-۲۳]. FJ در شکل ۱(ب) آورده شده است.

۳- تداخل مشارکتی بر اساس مقصد:

در آن مقصد جهت کاهش سیگنال به نویز در شنودگر یا فریب ناظر به ارسال سیگنال نویز مصنوعی می‌پردازد[۲۴]، [۷] و[۲۵]. تداخل مشارکتی بر اساس مقصد[6] (DBCJ) در شکل۱(ج) آورده شده است.

در میان روش‌هایی که در بالا آورده شده است، DBCJ در مقایسه با تداخل بر اساس منبع و روش FJ به‌سادگی قابل‌پیاده‌سازی هست. چون‌که در این روش مقصد از سیگنال تداخل ارسالی خود، آگاه بوده و می‌تواند خود تداخلی[7] را حذف نماید.

اگرچه به‌کارگیری نویز مصنوعی، سبب بهبود انتقال بدون سیم محرمانه می‌شود، در عوض لازم هست که توان ارسالی اضافه، هزینه‌کرد. باتوجه‌به محدود بودن توان ارسالی تجهیزات بدون سیم و همچنین افزایش تداخل در گیرنده‌های قانونی، لزوم تخصیص توان در چنین حالاتی، مشخص می‌شود.



شکل (۱): روش‌های ارسال سیگنال نویز مصنوعی

یکی دیگر از روش‌های بهبود PLS، پرتودهی هست. با استفاده از پرتودهی می‌توان سیگنال را در جهت موردنظر متمرکز کرد. به‌عنوان‌مثال، اگر سیگنال اطلاعات به سمت گیرنده قانونی متمرکز شود؛ کیفیت سیگنال دریافتی در گیرنده قانونی بهبود پیدا می‌کند. سیگنال نویز مصنوعی را نیز می‌توان به سمت گره مخرب۸ متمرکز کرد، به‌این‌ترتیب اثر سوء سیگنال نویز مصنوعی در گره مخرب افزایش پیدا می‌کند.

درصورتی‌که برای بهبود PLS از روش تولید نویز مصنوعی استفاده شود، لازم است منابع توانی اضافه به تولید نویز مصنوعی اختصاص یابد. همچنین استفاده از روش‌های پرتودهی باعث افزایش پیچیدگی محاسباتی در طراحی پرتوده می‌شود. بااین‌حال، روش‌های به‌کارگیری چندگانگی می‌توانند بهبود امنیتی را بدون نیاز به مصرف توان بیشتر و اعمال پیچیدگی برای طراحی پرتوده به ارمغان بیاورند. چندگانگی چند آنتن یک راه‌حل مناسب برای حل مسئله محوشدگی و افزایش ظرفیت کانال‌های بدون سیم است.

در این مقاله، این فرض صورت پذیرفته هست که منبع و مقصد

[1] Signal-to-Noise Ratio (SNR)
[2] Ergodic Secrecy Capacity (ESR)
[3] Monte Carlo
[4] Artifical noise
[5] Friendly Jammer
[6] Destination Based Cooperative Jamming
[7] Self interference
[۸] در مخابره پنهان و ارسال امن نظریه اطلاعاتی منظور از گره مخرب به‌ترتیب ناظر و شنودگر هست.

و شنودگر به چندین آنتن مجهز هستند؛ بنابراین با به‌کارگیری روش‌هایی چون بیش‌ترین نرخ ترکیب[1](MRC) می‌توانند کیفیت سیگنال دریافتی را بهبود دهند. همچنین می‌توانند با استفاده از پرتودهی بیش‌ترین نرخ ارسال[2] (MRT) سیگنال را در جهت مطلوب متمرکز سازند.

همان‌طور که بیان شد، در هنگام استفاده از سیگنال نویز مصنوعی، نیاز به تخصیص توان وجود دارد. در این مقاله این فرض صورت می‌پذیرد که توان کل تخصیص‌یافته برای ارسال سیگنال نویز مصنوعی و سیگنال اصلی مقدار ثابتی هست. در این مقاله مسئله بهینه‌سازی به‌گونه‌ای فرمول‌نویسی می‌شود که نرخ امن با درنظرگرفتن الزامات مخابره پنهان بیشینه شود. هدف از مسئله بهینه‌سازی یافتن فاکتور تخصیص توان بهینه بین ارسال سیگنال نویز مصنوعی و سیگنال داده هست.

در شرایطی که اندازه مسئله بهینه‌سازی بزرگ باشد، مسئله بهینه‌سازی گسسته باشد، توابع هدف یا قیدهای غیرخطی در مسئله وجود داشته باشند؛ روش‌های دقیق قادر به یافتن پاسخ مسئله در زمان مناسبی نخواهند بود. در چنین حالاتی برای یافتن بهترین جواب ممکن نزدیک بهینه در کمترین زمان، استفاده از روش‌های فراابتکاری[3] بسیار سودمند هست. یکی از روش‌های فراابتکاری موجود الگوریتم ژنتیک[4] هست.

الگوریتم ژنتیک از فرآیند انتخاب طبیعی موجود در طبیعت الهام‌گرفته است و به دسته‌ای بزرگ‌تر، به نام الگوریتم‌های تکاملی[5] (EA) تعلق دارد. در این الگوریتم از عملگرهای زیستی نظیر جهش[6]، ترکیب[7] و انتخاب[8] استفاده می‌شود [۲۶].

بسیاری از مسائل مهندسی توسط یک مسئله بهینه‌سازی مقید فرمول‌نویسی می‌شوند؛ بنابراین یافتن روش حل برای این مسائل می‌تواند بسیار ارزشمند هست. یکی از موضوعات روز پژوهشی در بحث محاسبات تکاملی، مدیریت محدودیت‌ها است[۲۷].

یکی از روش‌های فراابتکاری حل مسائل بهینه‌سازی مقید، تبدیل مسئله بهینه‌سازی تک‌هدفه به چندهدفه و حل مسئلهٔ بهینه‌سازی چندهدفه با الگوریتم‌های تکاملی هست[۲۸]. مراحل حل مسئله بهینه‌سازی چندهدفه عبارت‌اند از:

۱- نگاشت از فضای محدودیت‌ها به فضای توابع هدف

۲- ترکیب توابع هدف ناشی از محدودیت‌ها (الزامی نیست)

۳- حل مسئله بهینه‌سازی چندهدفه با الگوریتم‌های موجود برای حل مسائل چندهدفه

۴- دورانداختن پاسخ‌های امکان‌ناپذیر

۵- انتخاب بهترین پاسخ از میان پاسخ‌های باقی‌مانده

در این مقاله برای حل مسئله بهینه‌سازی تخصیص توان، از روش تبدیل مسئلهٔ بهینه‌سازی مقید تک‌هدفه به مسئله بهینه‌سازی چندهدفه و حل مسئله بهینه‌سازی چندهدفه با استفاده از الگوریتم ژنتیک با مرتب‌سازی نا مغلوب[9] نسخه شماره ۲ [10] (NSGAII) استفاده‌شده است.

۱-۱- نوآوری

در این بخش در ارتباط با نوآوری‌های مقاله در مقایسه با پژوهش‌های قبلی صحبت می‌شود.

۱- در این مقاله به بررسی حالتی پرداخته‌شده است که مقصد مجهز به چندین آنتن هست و با استفاده از ترکیب سیگنال دریافتی با روش MRC، SNR دریافتی خود را افزایش می‌دهد. در چنین حالتی رله می‌تواند باز ارسال سیگنال منبع را با توان کمتری انجام دهد. این امر سبب می‌شود، در فاز دوم، توان بیش‌تری به ارسال سیگنال نویز مصنوعی توسط منبع اختصاص داده شود و توان کمتری از رله به ناظر نشت کند. درنتیجه قابلیت تشخیص ناظر کاهش می‌یابد.

۲- در سیستم مدل مطرح‌شده، ناظر و رله غیرقابل‌اعتماد، دو گره مخرب هستند. در فاز اول جهت فریب ناظر و همچنین جلوگیری از شنود احتمالی محتوی پیام ارسالی توسط رله غیرقابل‌اعتماد، مقصد به ارسال سیگنال نویز مصنوعی می‌پردازد. نتایج حاصل نشان می‌دهد که اگر مقصد از روش MRT در جهت رله غیرقابل‌اعتماد استفاده نماید، ESR بهبود پیدا می‌کند.

۳- این فرض صورت پذیرفته است که ناظر به چندین آنتن مجهز هست و بر اساس مجموع انرژی دریافتی از تمام آنتن‌ها در ارتباط با وجود یا عدم وجود مخابره تصمیم‌گیری می‌کند.

۴- جهت حل مسئله بهینه‌سازی تخصیص توان از روش تبدیل مسئلهٔ بهینه‌سازی مقید تک‌هدفه به مسئله بهینه‌سازی چندهدفه و حل مسئله بهینه‌سازی چندهدفه با استفاده از NSGAII استفاده‌شده است.

هنگامی‌که از چندین آنتن استفاده می‌شود با بهره‌برداری از درجهٔ آزادی فضایی[11] می‌توان با صرف توان کمتر، مخابره باقابلیت اطمینان[12] را پشتیبانی کرد. انرژی کمتر سبب کاهش قابلیت ناظر در تشخیص وجود مخابره می‌شود. مهم‌ترین نوآوری، در سیستم مدل پیشنهادی چند آنتن بودن؛ مقصد و ناظر هست. بررسی توأم مخابره پنهان و امنیت نظریه اطلاعاتی در حضور

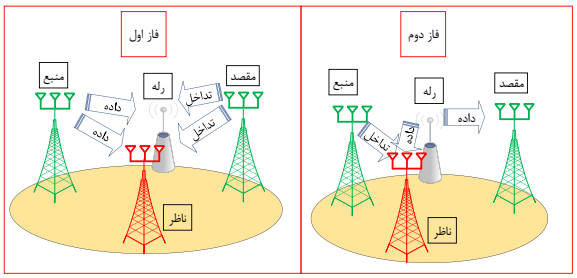
[1] Maximum Ratio Combining (MRC)
[2] Maximum Ratio Transmission (MRT)
[3] Meta-heurristic
[4] Genetic algorithm
[5] Evolutionary Algorithm (EA)
[6] Mutation
[7] Selection
[8] Crossover
[9] Non-dominated Sorting
[10] Non-dominated Sorting Genetic Algorithm
[11] Spatial degrees of freedom
[12] Reliable

رلهٔ غیرقابل‌اعتماد، در حالتی که منبع مجهز به چندین آنتن باشد و برای ارسال داده از MRT در جهت رله غیرقابل‌اعتماد استفاده می‌کند در [۷] انجام‌شده است. یکی از مسائلی که در این مقاله موردبررسی قرار می‌گیرد، بررسی MRT در جهت رله غیرقابل‌اعتماد جهت ارسال سیگنال نویز مصنوعی توسط مقصد است.

۲. سیستم مدل موردبررسی

سیستم مدل موردمطالعه در شکل ۲ آورده شده است. سیستم مدل موردمطالعه شامل یک منبع و یک مقصد هست که به ترتیب به N_s و N_d آنتن مجهز هستند. این فرض وجود دارد که به دلیل فاصله‌ی زیاد منبع و مقصد یا به دلیل اثر سایه، لینک مستقیمی بین منبع و مقصد وجود ندارد. به همین منظور از رله برای برقراری ارتباط بین منبع و مقصد استفاده‌شده است.

رله غیرقابل‌اعتماد در نظر گرفته می‌شود، به این معنی که در سطح سرویس یک کمک‌کننده هست؛ اما ممکن است، در سطح داده، در نقش شنودگر ظاهر شود و به شنود اطلاعات مبادرت ورزد. رله غیرقابل‌اعتماد دارای عملکرد تقویت و ارسال[۱] (AF) هست؛ به این معنی که سیگنال دریافتی را تقویت و باز ارسال می‌نماید.



شکل (۲): سیستم نمونه‌ی موردبررسی

برای آن که سیستم مدل مورد بررسی در مقابل حملات آنالیز ترافیک ناظر مستحکم‌تر[۲] باشد، این فرض صورت پذیرفته است که ناظر موجود در شبکه به N_w آنتن مجهز هست.

برای ارسال داده از دسترسی چندگانه تقسیم زمانی[۳] (TDMA) استفاده می‌شود. ارسال داده در دوفاز انجام می‌شود. در فاز اول، منبع سیگنال داده را به سمت رله ارسال می‌کند. به طور هم‌زمان، مقصد نیز به ارسال سیگنال نویز مصنوعی می‌پردازد. ارسال سیگنال نویز مصنوعی در فاز اول باهدف کاهش نرخ سیگنال به نویز بعلاوه تداخل[۴] (SINR) در رله غیرقابل‌اعتماد و فریب ناظر انجام می‌شود.

همان‌طور که در شکل۳ نمایش‌داده‌شده است، در فاز اول جهت ایجاد خطا در آشکارسازی مخابره توسط ناظر، منبع در برخی از اسلات‌های زمانی زوج به ارسال داده مبادرت می‌ورزد و در بقیه اسلات‌های زمانی زوج خاموش می‌ماند. منبع در اسلات‌های زمانی زوج با احتمال $\mathbb{P}_t$ تصمیم بر ارسال یا عدم ارسال داده می‌گیرد.

در فاز اول، برای ارسال سیگنال اطلاعات و سیگنال نویز مصنوعی که به ترتیب توسط منبع و مقصد انجام می‌شود. از پرتودهی MRT در جهت رله استفاده می‌شود[۵]. نتایج حاصل در[۷] نشان می‌دهد که استفاده از MRT در جهت رله برای ارسال سیگنال اطلاعات توسط منبع، سبب بهبود نرخ امن می‌شود. در این مقاله این موضوع تأیید می‌شود و نشان داده می‌شود که استفاده از MRT در جهت رله برای ارسال سیگنال نویز مصنوعی، سبب بهبود، نرخ امن می‌گردد.

در فاز دوم رله، سیگنال دریافتی در فاز اول را تقویت و مجدد باز ارسال می‌نماید. منبع نیز به طور هم‌زمان به ارسال سیگنال نویز مصنوعی می‌پردازد. ارسال سیگنال نویز مصنوعی توسط منبع باهدف فریب ناظر انجام می‌شود.

همان‌طور که در شکل ۳ نشان داده‌شده است. در فاز دوم برای ایجاد خطا در آشکارسازی مخابره توسط ناظر، رله در برخی از اسلات‌های زمانی فرد به باز ارسال اطلاعات می‌پردازد و در بقیه اسلات‌های زمانی، فرد خاموش باقی می‌ماند. رله در اسلات‌های زمانی فرد با احتمال $\mathbb{P}_t$ تصمیم بر باز ارسال یا عدم باز ارسال داده می‌گیرد.

ازآنجایی‌که رله گره‌ای تک آنتن فرض شده است، بنابراین نمی‌توان از روش MRT در جهت مقصد توسط رله جهت بهبود سیگنال دریافتی در مقصد، استفاده کرد. همان‌طور که بیان شد، در فاز دوم، ارسال سیگنال نویز مصنوعی جهت فریب ناظر توسط منبع، انجام می‌شود. برخلاف رله ناظر گره‌ای خارجی در شبکه هست و ناظر یک حمله‌کنندهٔ غیرفعال هست؛ بنابراین اطلاعات حالت کانال[۶] (CSI) ناظر در منبع مشخص نیست. باتوجه‌به مطالب بیان‌شده این نتیجه حاصل می‌شود که در فاز دوم ارسال نمی‌توان از MRT در جهت ناظر برای ارسال سیگنال نویز مصنوعی استفاده نمود.

این مخابره در قالب T اسلات زمانی که هر اسلات زمانی شامل ارسال n سمبل است، اجرا خواهد شد. قبل از راه‌اندازی شبکه، بازه‌های اسلات زمانی و شاخص اسلات‌های زمانی که منبع در آن‌ها به ارسال داده می‌پردازد، به گیرنده و رله

---

[1] Amplify-and-Forward (AF)
[2] Robust
[3] Time Division Multiple Access (TDMA)
[4] Signal-to-Interference-plus-Noise Ratio (SINR)

[۵] همانطور که بیان شد، ارسال سیگنال نویز مصنوعی با دو هدف فریب ناظر و همچنین کاهش SINR در رله غیرقابل‌اعتماد انجام می‌شود. از آن جایی که رله گره قانونی شبکه هست، این فرض انجام می‌شود که CSI رله در مقصد مشخص هست؛ بنابراین مقصد می‌تواند با متمرکز کردن سیگنال نویز مصنوعی در جهت رله مانع از حملات شنودی رله شود. در بخش نتایج مقایسه‌ای بین حالتی که از MRT در جهت رله استفاده شود، با انتخاب آنتن تصادفی، انجام می‌شود؛ نتایج حاصل نشان می‌دهد که استفاده از MRT در جهت رله کارایی سیستم مدل پیشنهادی را افزایش می‌دهد.

[6] Channel State Information (CSI)

اطلاع‌رسانی می‌شود. همچنین، بازه‌های اسلات زمانی و شاخص اسلات‌های زمانی که رله در آن‌ها به باز ارسال داده می‌پردازد، به گیرنده اطلاع رسانی می‌شود. شکل ۳ مثالی از نحوه ارسال داده در اسلات‌های زمانی گوناگون را به تصویر می‌کشد.

فرض می‌شود که تمامی گره‌های موجود به‌صورت نیم دوطرفه[1] عمل می‌کنند. همچنین فرض می‌شود که دورهٔ زمانی دقیق هر فاز ازپیش‌تعیین‌شده است و گره‌ها به‌صورت کامل با یکدیگر هم‌زمان هستند. این فرض وجود دارد که کانال بین رله و مقصد هم پاسخ هستند.

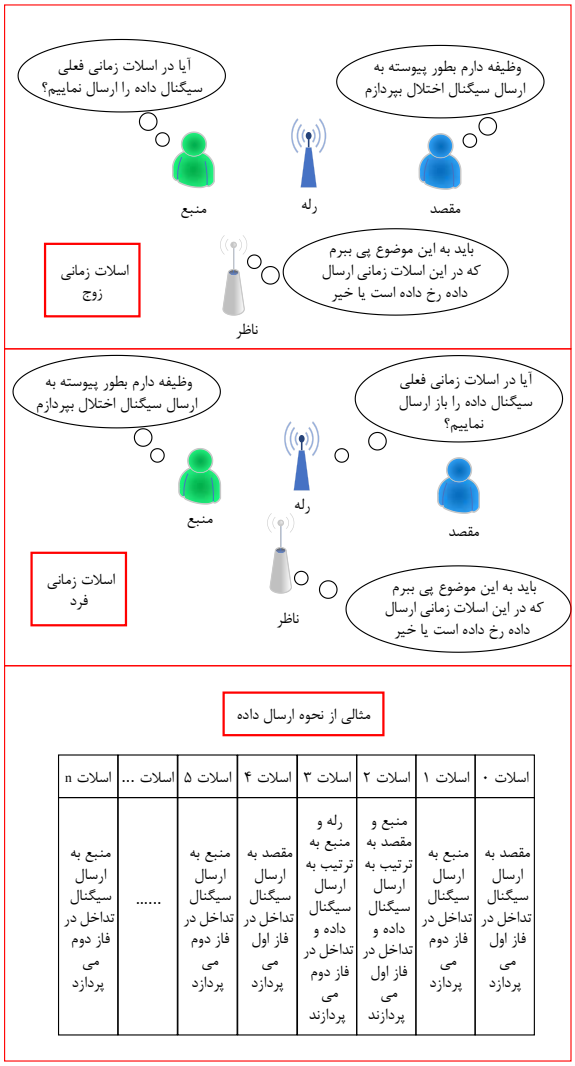
سیگنال داده، سیگنال نویز مصنوعی منبع و سیگنال نویز مصنوعی مقصد در هر اسلات زمانی به ترتیب به‌صورت $X_s^{(1)} = [x_s^{1(1)}, \dots, x_s^{n(1)}]$، $X_s^{(2)} = [x_s^{1(2)}, \dots, x_s^{n(2)}]$، $X_d = [x_d^1, \dots, x_d^n]$ هستند.

همچنین بردار سیگنال دریافتی در آنتن k ام گرهٔ m (ناظر یا مقصد) $\boldsymbol{y}_{m_k}^l = [y_{m_k}^1, \dots, y_{m_k}^n]$ هست؛ بنابراین $y_{m_k}^l$، سیگنال l ام دریافتی توسط آنتن k ام در گره m هست. بردار سیگنال دریافتی در رله $\boldsymbol{y}_r^l = [y_r^1, \dots, y_r^n]$ هست که $y_{m_k}^l \in \boldsymbol{y}_{m_k}$ و $l = 1, .., n$ است.

در ادامه فرض می‌شود که کل توان ارسالی در هر فاز P وات هست. متغیرهای تصادفی λ و ξ که $0 \le \lambda \le 1$ و $0 \le \xi \le 1$ را تعریف می‌شوند که به ترتیب بیانگر عامل تخصیص توان بین منبع و مقصد، و بین منبع و رله هستند. در فاز اول $\boldsymbol{H}_{sw}^{(1)}$، $\boldsymbol{H}_{dw}^{(1)}$، به ترتیب بیانگر ماتریس کانال منبع به ناظر و مقصد به ناظر هستند، به‌طوری‌که $\boldsymbol{H}_{sw}^{(1)} = [h_{i,j}^{sw(1)}]_{i=1,j=1}^{i=N_w,j=N_s}$، $\boldsymbol{H}_{dw}^{(1)} = [h_{i,j}^{dw(1)}]_{i=1,j=1}^{i=N_w,j=N_d}$، هستند. همچنین $\boldsymbol{h}_{sr}^{(1)}$، $\boldsymbol{h}_{dr}^{(1)}$، به ترتیب بیانگر بردار کانال منبع به رله و مقصد به رله هستند،طوری که $\boldsymbol{h}_{sr}^{(1)} = [h_1^{sr(1)}, \dots, h_{N_s}^{sr(1)}]^T$، $\boldsymbol{h}_{dr}^{(1)} = [h_1^{dr(1)}, \dots, h_{N_d}^{dr(1)}]^T$ هستند. متغییرهای $h_i^{sr(1)}$، $h_i^{dr(1)}$، $h_{i,j}^{sw(1)}$، $h_{i,j}^{dw(1)}$، متغیرهای تصادفی گوسی مختلط، مستقل و دارای توزیع یکسان[2] (i.i.d) می‌باشند. که میانگین آن‌ها برابر صفر و واریانس آن‌ها به ترتیب $\mu_{sr}^{(1)}$ ، $\mu_{dr}^{(1)}$ ، $\mu_{sw}^{(1)}$ ، $\mu_{dw}^{(1)}$ است.

در فاز دوم $\boldsymbol{h}_{sw}^{(2)}$، $\boldsymbol{h}_{rw}^{(2)}$، $\boldsymbol{h}_{rd}^{(2)}$، به ترتیب بیانگر بردار کانال منبع به ناظر، رله به ناظر، رله به مقصد هستند، $\boldsymbol{h}_{sw}^{(2)} = [h_1^{sw(2)}, \dots, h_{N_w}^{sw(2)}]$، $\boldsymbol{h}_{rw}^{(2)} = [h_1^{rw(2)}, \dots, h_{N_w}^{rw(2)}]$، $\boldsymbol{h}_{rd}^{(2)} = [h_1^{rd(2)}, \dots, h_{N_d}^{rd(2)}]$ هستند. $h_i^{sw(2)}$ ، $h_i^{rd(2)}$، $h_i^{rw(2)}$، متغیرهای تصادفی گوسی مختلط، i.i.d می‌باشند. که میانگین آن‌ها برابر صفر است و واریانس آن‌ها $\mu_{rd}^{(2)}$ ، $\mu_{sw}^{(2)}$ ، $\mu_{rw}^{(2)}$ است.

[1] Half-duplex
[2] Independent and Identically Distributed



اسلات ۰	اسلات ۱	اسلات ۲	اسلات ۳	اسلات ۴	اسلات ۵	اسلات ...	اسلات n
مقصد به ارسال سیگنال تداخل در فاز اول می پردازد	منبع به ارسال سیگنال تداخل در فاز دوم می پردازد	منبع و مقصد به ترتیب به ارسال سیگنال داده و تداخل در فاز اول می پردازند	رله و منبع به ترتیب به ارسال سیگنال داده و تداخل در فاز دوم می پردازند	مقصد به ارسال سیگنال تداخل در فاز اول می پردازد	منبع به ارسال سیگنال تداخل در فاز دوم می پردازد	.....	منبع به ارسال سیگنال تداخل در فاز دوم می پردازد

شکل (۳): نحوه ارسال در اسلات‌های زمانی مختلف

همان‌طور که بیان شد، کانال رله به مقصد و مقصد به رله هم پاسخ فرض می‌شود، بنابراین $\mu_{rd}^{(2)} = \mu_{dr}^{(1)} = \mu_{dr}$ همچنین $\boldsymbol{h}_{rd}^{(2)} = \boldsymbol{h}_{dr}^{(1)} = \boldsymbol{h}_{dr}$ هستند.

سیگنال l ام دریافتی در رله غیرقابل‌اعتماد در هر اسلات زمانی در فاز اول از رابطه زیر قابل حصول است:

$$y_r^l = \begin{cases} \sqrt{(1-\lambda)\mathrm{P}}\boldsymbol{W}_2^{\mathrm{H}}\boldsymbol{h}_{dr}x_d^l + n_r^l, & \Psi_0 \\ \sqrt{\lambda\mathrm{P}}\boldsymbol{W}_1^{\mathrm{H}}\boldsymbol{h}_{sr}^{(1)}x_s^{l(1)} + & \\ \sqrt{(1-\lambda)\mathrm{P}}\boldsymbol{W}_2^{\mathrm{H}}\boldsymbol{h}_{dr}x_d^l + n_r^l, & \Psi_1 \end{cases} \quad (۵)$$

$n_r^l \sim \mathcal{CN}(0, \sigma^2)$ نویز سفید جمع شونده در رله غیرقابل‌اعتماد است. لازم به ذکر است که کتاب کد x_d^l هم در رله و هم در ناظر ناشناخته است. درحالی‌که کتاب کد $x_s^{l(1)}$ در رله شناخته‌شده و در ناظر ناشناخته است. اگر CSI مربوط به ناظر در منبع موجود باشد، منبع می‌تواند با استفاده از شکل‌دهی پرتو فضا خالی[3] احتمال خطا آشکارسازی در ناظر را به حداکثر برساند. بااین‌وجود ازآنجایی‌که CSI ناظر موجود نیست، از MRT

[3] Null-space beamforming

در جهت رله استفاده می‌شود. بردار وزن ارسال در منبع و مقصد به ترتیب $\boldsymbol{w}_1 = \frac{\boldsymbol{h}_{sr}^{(1)}}{\|\boldsymbol{h}_{sr}^{(1)}\|}$ و $\boldsymbol{W}_2 = \frac{\boldsymbol{h}_{dr}}{\|\boldsymbol{h}_{dr}\|}$ هستند. فرض Ψ_0 و Ψ_1 به ترتیب بیانگر عدم ارسال داده توسط منبع و ارسال داده توسط منبع هستند.

باتوجه‌به رابطهٔ ۵، SINR دریافتی در رله غیرقابل‌اعتماد از رابطهٔ زیر محاسبه می‌شود.

$$\gamma_r = \begin{cases} 0, & \Psi_0 \\ \dfrac{\lambda \mathrm{P}\|\boldsymbol{h}_{sr}^{(1)}\|^2}{(1-\lambda)\mathrm{P}\|\boldsymbol{h}_{dr}\|^2 + \sigma^2} = \dfrac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{dr}+1}, & \Psi_1 \end{cases} \quad (۶)$$

در رابطهٔ فوق $\gamma_{sr} = \frac{\mathrm{P}\|\boldsymbol{h}_{sr}^{(1)}\|^2}{\sigma^2}$ و $\gamma_{dr} = \frac{\mathrm{P}\|\boldsymbol{h}_{dr}\|^2}{\sigma^2}$ هستند. در فاز دوم رله غیرقابل‌اعتماد سیگنال دریافتی را نرمالیزه کرده و آن را با توان $(1-\xi)\mathrm{P}$ ارسال می‌کند. به‌عبارت‌دیگر رله سیگنال دریافتی را با عامل G_r تقویت می‌کند که G_r از رابطه زیر به دست می‌آید.

$$G_r = \begin{cases} 0, & \Psi_0 \\ \sqrt{\dfrac{(1-\xi)\mathrm{P}}{\lambda\mathrm{P}\|\boldsymbol{h}_{sr}^{(1)}\|^2 + (1-\lambda)\mathrm{P}\|\boldsymbol{h}_{dr}\|^2 + \sigma^2}}, & \Psi_1 \end{cases} \quad (۷)$$

در ادامه رله سیگنال $x_r^l = G_r y_r^l$ را باز ارسال می‌نماید. از آنجایی که مقصد از سیگنال تداخل ارسالی خود در فاز اول آگاه است، سیگنال l ام دریافتی توسط آنتن k ام مقصد، بعد از حذف خودتداخلی از رابطهٔ زیر محاسبه می‌شود[۷, ۲۵].

$$y_{d_k}^l = \begin{cases} n_{d_k}^l, & \Psi_0 \\ G_r\sqrt{\lambda\mathrm{P}}\boldsymbol{w}_1^{\mathrm{H}}\boldsymbol{h}_{sr}^{(1)}h_k^{dr}x_s^{l(1)} + G_r n_r^l h_k^{dr} + n_{d_k}^l, & \Psi_1 \end{cases} \quad (۸)$$

در رابطهٔ فوق $\boldsymbol{n}_d^l \sim \mathcal{CN}(0_{N_d\times 1}, \sigma^2\boldsymbol{I}_{N_d\times N_d})$ هست. همان‌طور که بیان شد، در فاز دوم، رله با احتمال $\mathbb{P}_t$ تصمیم به باز ارسال داده می‌گیرد. فرض Ψ_0 و Ψ_1 به ترتیب بیانگر عدم باز ارسال داده توسط رله و باز ارسال داده توسط رله هستند. دو عملکرد رایج رله، AF و رمزگشایی و ارسال[1] (DF) هست. رله AF سیگنال دریافتی را تقویت و باز ارسال می‌نماید. عیب روش AF تقویت نویز هست. در رابطهٔ فوق $G_r n_r^l h_k^{dr}$ ترم مربوط به نویز حرارتی رله است که تقویت و باز ارسال‌شده است. در عملکرد DF لازم هست که سیگنال در رله رمزگشایی سپس باز ارسال شود، چون رله غیرقابل‌اعتماد هست، نمی‌توان از عملکرد DF استفاده کرد؛ بنابراین باوجود عیب تقویت نویز عملکردAF از این عملکرد استفاده‌شده است.

در مقصد از روش MRC استفاده می‌شود. SNR دریافتی در مقصد از رابطهٔ زیر محاسبه می‌شود.

$$\gamma_d = \begin{cases} 0, & \Psi_0 \\ \dfrac{G_r{}^2\lambda\mathrm{P}\|\boldsymbol{h}_{sr}^{(1)}\|^2\|\boldsymbol{h}_{dr}\|^2}{G_r{}^2\sigma^2\|\boldsymbol{h}_{dr}\|^2 + \sigma^2} = \dfrac{\lambda(1-\xi)\gamma_{sr}\gamma_{dr}}{\lambda\gamma_{sr} + (2-\lambda-\xi)\gamma_{dr}+1}, & \Psi_1 \end{cases} \quad (۹)$$

۳. مسئله بهینه‌سازی تخصیص توان

در این مقاله دو هدف دنبال می‌شود که عبارت‌اند از:

۱- رله غیرقابل‌اعتماد نتواند به محتوی پیام ارسالی پی ببرد.

۲- مخابره از دید ناظر پنهان باقی بماند.

برای دست‌یابی به این دو هدف، در این بخش مسئله بهینه-سازی تخصیص توان به‌گونه‌ای فرمول‌نویسی می‌شود که نرخ امن لحظه‌ای به‌شرط برقراری الزامات مخابره پنهان بیشینه شود.

۳-۱. ارسال امن نظریه اطلاعاتی

در این مقاله جهت جلوگیری از شنود اطلاعات توسط رله غیرقابل‌اعتماد از ارسال امن نظریه اطلاعاتی استفاده می‌شود. یکی از معیارهای مهم در ارسال امن نظریه اطلاعاتی نرخ امن هست. باتوجه‌به رابطهٔ ۴، نرخ امن لحظه‌ای در سیستم مدل موردمطالعه از رابطهٔ زیر محاسبه می‌شود.

$$\mathcal{R}_{sec} = \frac{\mathbb{P}_t}{2}[\log_2\left(1 + \frac{\lambda(1-\xi)\gamma_{sr}\gamma_{dr}}{\lambda\gamma_{sr} + (2-\lambda-\xi)\gamma_{dr}+1}\right) - \log_2(1 + \frac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{dr}+1})]^+ \quad (۱۰)$$

ازآنجایی‌که مخابره بین گیرنده و فرستنده در دوفاز صورت می‌پذیرد، ضریب $\frac{1}{2}$ در نظر گرفته‌شده است. همان‌طور که بیان شد، برای ایجاد خطا در آشکارسازی مخابره توسط ناظر در فاز اول منبع با احتمال $\mathbb{P}_t$ تصمیم بر ارسال داده می‌گیرد. در فاز دوم نیز به همین منظور و با همان احتمال رله تصمیم بر باز ارسال داده می‌گیرد؛ بنابراین لازم هست که ضریب $\mathbb{P}_t$ نیز برای نرخ امن لحظه‌ای در نظر گرفته شود.

۳-۲. الزامات مخابره پنهان

ناظر بر اساس توان سیگنال دریافت شده تصمیم می‌گیرد که آیا مخابره‌ای بین گره‌های شبکه صورت پذیرفته است یا خیر. اگر $\boldsymbol{h}_k^{sw(1)} = [h_{k,1}^{sw(1)}, h_{k,2}^{sw(1)}, \dots, h_{k,N_S}^{sw(1)}]$ و $\boldsymbol{h}_k^{dw(1)} = [h_{k,1}^{dw(1)}, h_{k,2}^{dw(1)}, \dots, h_{k,N_S}^{dw(1)}]$، به ترتیب سطر k ام ماتریس کانال $\boldsymbol{H}_{sw}^{(1)}$ و $\boldsymbol{H}_{dw}^{(1)}$ باشند سیگنال l ام دریافت شده توسط آنتن k ام ناظر در فاز اول به‌صورت زیر محاسبه می‌شود.

$$y_{w_k}^{l(1)} = \begin{cases} \sqrt{(1-\lambda)\mathrm{P}}\boldsymbol{W}_2{}^{\mathrm{H}}\boldsymbol{h}_k^{dw(1)}x_d^l + n_{w_k}^{l(1)}, & \Psi_0 \\ \sqrt{\lambda\mathrm{P}}\boldsymbol{W}_1{}^{\mathrm{H}}\boldsymbol{h}_k^{sw(1)}x_s^{l(1)} + \sqrt{(1-\lambda)\mathrm{P}}\boldsymbol{W}_2{}^{\mathrm{H}}\boldsymbol{h}_k^{dw(1)}x_d^l + n_{w_k}^{l(1)}, & \Psi_1 \end{cases} \quad (۱۱)$$

[1] Decode – and- Forward (DF)

نویز حرارتی در ناظر، $\boldsymbol{n}_w^{l(1)} \sim \mathcal{CN}\left(0_{N_d}, \sigma_w^2 \boldsymbol{I}_{N_w \times N_w}\right)$ هست. همچنین سیگنال l ام دریافت شده توسط آنتن k ام ناظر در فاز دوم به‌صورت زیر محاسبه می‌شود.

$$y_{w_k}^{l(2)} = \begin{cases} \sqrt{\xi \mathrm{P}} h_k^{sw(2)} x_s^{l(2)} + n_{w_k}^{l(2)}, & \Psi_0 \\ \left(y_r^l | \Psi_1\right) \times G_r h_k^{rw(2)} & \\ + \sqrt{\xi \mathrm{P}} h_k^{sw(2)} x_s^{l(2)} + n_{w_k}^{l(2)}, & \Psi_1 \end{cases} \quad (۱۲)$$

$\boldsymbol{n}_w^{l(2)} \mathcal{CN}\left(0_{N_d}, \sigma_w^2 \boldsymbol{I}_{N_w \times N_w}\right)$ نویز حرارتی در ناظر، هست.

در مخابره پنهان ناظر یک حد آستانه تصمیم‌گیری را انتخاب می‌کند و بر اساس مقایسه توان سیگنال دریافتی با حد آستانه مذکور تصمیم بر وجود یا عدم وجود مخابره می‌گیرد. ناظر در فاز اول و دوم به ترتیب $Y_w^{(1)} = \sum_{k=1}^{N_w} \sum_{l=1}^{n} \frac{\left|y_{w_k}^{l(1)}\right|^2}{n}$ و $Y_w^{(2)} = \sum_{k=1}^{N_w} \sum_{l=1}^{n} \frac{\left|y_{w_k}^{l(2)}\right|^2}{n}$ را محاسبه می‌کند. سپس در فاز اول و دوم به ترتیب براساس $Y_w^{(1)} \underset{\Psi_0}{\overset{\Psi_1}{\gtrless}} \vartheta^{(1)}$ و $Y_w^{(2)} \underset{\Psi_0}{\overset{\Psi_1}{\gtrless}} \vartheta^{(2)}$ تصمیم گیری می‌نماید.

درصورتی‌که به‌ازای $k = 0, \dots, N_w$، $\Theta_k^{(1)} = \sum_{n=1}^{l} \frac{\left|y_{w_k}^{l(1)}\right|^2}{n}$ و $\Theta_k^{(1)} = \sum_{l=1}^{n} \frac{\left|y_{w_k}^{l(2)}\right|^2}{n} = \Theta_k^{(2)}$ تعریف شوند. در این صورت $\Theta_k^{(2)} = \left(\sigma^2 + \Upsilon_k^{(2)}\right) \frac{\chi_{2n}^2}{n}$ در و $\Theta_k^{(1)} = \left(\sigma^2 + \Upsilon_k^{(1)}\right) \frac{\chi_{2n}^2}{n}$ هستند [۷] که χ_{2n}^2 متغیر تصادفی مربع کای با $2n$ درجه آزادی هست. همچنین مقادیر $\Upsilon_k^{(1)}$ و $\Upsilon_k^{(2)}$ از روابط زیر محاسبه می‌شود.

$$\Upsilon_k^{(1)} = \begin{cases} (1-\lambda)\mathrm{P}\left|\dfrac{\boldsymbol{h}_{dr}^{\mathrm{H}}}{\|\boldsymbol{h}_{dr}\|} \boldsymbol{h}_k^{dw(1)}\right|^2, & \Psi_0 \\ \lambda \mathrm{P}\left|\dfrac{\boldsymbol{h}_{sr}^{(1)\mathrm{H}}}{\left\|\boldsymbol{h}_{sr}^{(1)}\right\|} \boldsymbol{h}_k^{sw(1)}\right|^2 + & \\ (1-\lambda)\mathrm{P}\left|\dfrac{\boldsymbol{h}_{dr}^{\mathrm{H}}}{\|\boldsymbol{h}_{dr}\|} \boldsymbol{h}_k^{dw(1)}\right|^2, & \Psi_1 \end{cases} \quad (۱۳)$$

$$\Upsilon_k^{(2)} = \begin{cases} \xi P \left|h_k^{sw(2)}\right|^2, & \Psi_0 \\ (1-\xi) P \left|h_k^{rw(2)}\right|^2 & \\ + \xi P \left|h_k^{sw(2)}\right|^2, & \Psi_1 \end{cases} \quad (۱۴)$$

بر اساس قانون قوی اعداد بزرگ[1] $\frac{\chi_{2n}^2}{n}$ به عدد ۱ همگرا می‌شود. همچنین بر اساس نظریه همگرایی غالب لبزگو[2] $\frac{\chi_{2n}^2}{n}$ با عدد ۱ قابل جایگذاری هست[۷]؛ بنابراین به‌ازای $k = 1, \dots, N_w$، $\Theta_k^{(1)} \sim \left(\sigma^2 + \Upsilon_k^{(1)}\right)$ و $\Theta_k^{(2)} \sim \left(\sigma^2 + \Upsilon_k^{(2)}\right)$ هستند.

با فرض N_s و N_d به‌قدر کافی بزرگ، با به‌کارگیری قانون اعداد بزرگ $\left\|\boldsymbol{h}_{sr}^{(1)}\right\|^2$ و $\|\boldsymbol{h}_{dr}\|^2$ به ترتیب با $N_s \mu_{sr}^{(1)}$ و $N_d \mu_{dr}$ قابل جایگذاری هستند. با استفاده از قانون حد مرکزی $\boldsymbol{h}_{dr}^{\mathrm{H}} \boldsymbol{h}_k^{dw(1)}$ و $\boldsymbol{h}_{sr}^{(1)\mathrm{H}} \boldsymbol{h}_k^{sw(1)}$ به‌ترتیب به‌صورت $\mathcal{CN}(0, N_d \mu_{dr} \mu_{dw}^{(1)})$ و $\mathcal{CN}(0, N_s \mu_{sr}^{(1)} \mu_{sw}^{(1)})$ قابل تقریب زدن هستند. باتوجه‌به این مطالب $\left|\frac{\boldsymbol{h}_{sr}^{(1)\mathrm{H}}}{\left\|\boldsymbol{h}_{sr}^{(1)}\right\|} \boldsymbol{h}_k^{sw(1)}\right|^2$ و $\left|\frac{\boldsymbol{h}_{dr}^{\mathrm{H}}}{\|\boldsymbol{h}_{dr}\|} \boldsymbol{h}_k^{dw(1)}\right|^2$ متغیرهای نمایی هستند که میانگین آن‌ها به‌ترتیب $\mu_{dw}^{(1)}$ و $\mu_{sw}^{(1)}$ هست[۷].

باتوجه‌به روابط ۱۳ و ۱۴ ، تابع چگالی احتمال[3] (PDF) دو متغیر تصادفی $\Upsilon_k^{(1)}$ و $\Upsilon_k^{(2)}$ توسط روابط زیر محاسبه می‌گردد.

$$f_{\Gamma_1}\left(\Upsilon_k^{(1)}\right) = \begin{cases} \dfrac{1}{(1-\lambda)\mathrm{P}\mu_{dw}^{(1)}} e^{-\frac{\Upsilon_k^{(1)}}{(1-\lambda)\mathrm{P}\mu_{dw}^{(1)}}}, & \Psi_0 \\ \dfrac{\left[e^{-\frac{\Upsilon_k^{(1)}}{\lambda P \mu_{sw}^{(1)}}} - e^{-\frac{\Upsilon_k^{(1)}}{(1-\lambda) P \mu_{dw}^{(1)}}}\right]}{P\left(\lambda \mu_{sw}^{(1)} - (1-\lambda)\mu_{dw}^{(1)}\right)}, & \Psi_1 \end{cases} \quad (۱۵)$$

$$f_{\Gamma_2}\left(\Upsilon_k^{(2)}\right) = \begin{cases} \dfrac{1}{\xi P \mu_{sw}^{(2)}} e^{-\frac{\Upsilon_k^{(2)}}{\xi P \mu_{sw}^{(2)}}} & \Psi_0 \\ \dfrac{\left[e^{-\frac{\Upsilon_k^{(2)}}{\xi P \mu_{sw}^{(2)}}} - e^{-\frac{\Upsilon_k^{(2)}}{(1-\xi) P \mu_{rw}^{(2)}}}\right]}{P\left(\xi \mu_{sw}^{(2)} - (1-\xi)\mu_{rw}^{(2)}\right)}, & \Psi_1 \end{cases} \quad (۱۶)$$

همان‌طور که بیان شد، ناظر به ترتیب در فاز اول و دوم مقادیر $Y_w^{(1)} = \sum_{k=1}^{N_w} \Theta_k^{(1)}$ و $Y_w^{(2)} = \sum_{k=1}^{N_w} \Theta_k^{(2)}$ را محاسبه می‌کند. سپس $Y_w^{(1)}$ و $Y_w^{(2)}$ به‌ترتیب با $\vartheta^{(1)}$ و $\vartheta^{(2)}$ مقایسه می‌شوند. در صورتی که N_w به‌قدر کافی بزرگ فرض شود، بر اساس قضیه حد مرکزی تابع توزیع $Y_w^{(1)}$ و $Y_w^{(2)}$ از روابط زیر محاسبه می‌گردد.

$$Y_w^{(1)} \sim \begin{cases} \mathcal{CN}\left(\mathbb{E}\left(Y_w^{(1)} | \Psi_0\right), \boldsymbol{var}\left(Y_w^{(1)} | \Psi_0\right)\right), \Psi_0 \\ \mathcal{CN}\left(\mathbb{E}\left(Y_w^{(1)} | \Psi_1\right), \boldsymbol{var}\left(Y_w^{(1)} | \Psi_1\right)\right), \Psi_1 \end{cases} \quad (۱۷)$$

$$Y_w^{(2)} \sim \begin{cases} \mathcal{CN}\left(\mathbb{E}\left(Y_w^{(2)} | \Psi_0\right), \boldsymbol{var}\left(Y_w^{(2)} | \Psi_0\right)\right), \Psi_0 \\ \mathcal{CN}\left(\mathbb{E}\left(Y_w^{(2)} | \Psi_1\right), \boldsymbol{var}\left(Y_w^{(2)} | \Psi_1\right)\right), \Psi_1 \end{cases} \quad (۱۸)$$

در روابط فوق $\mathbb{E}\left(Y_w^{(1)} | \Psi_0\right) = N_w(1-\lambda)\mathrm{P}\mu_{dw}^{(1)} + N_w \sigma^2$، $\boldsymbol{var}\left(Y_w^{(1)} | \Psi_0\right) = N_w(1-\lambda)^2 P^2 \left(\mu_{dw}^{(1)}\right)^2$، $\mathbb{E}\left(Y_w^{(1)} | \Psi_1\right) = N_w \lambda P \mu_{sw}^{(1)} + N_w(1-\lambda)P\mu_{dw}^{(1)} +$

[1] Strong law of large numbers
[2] Lebesgue's dominated convergence theorem
[3] Probability Density Function (PDF)

$$\boldsymbol{var}\left(Y_w^{(1)}|\Psi_1\right) = N_w\lambda^2P^2\left(\mu_{sw}^{(1)}\right)^2 + N_w\sigma^2,$$
$$\mathbb{E}\left(Y_w^{(2)}|\Psi_0\right) = N_w\xi P\mu_{sw}^{(2)} + N_w(1-\lambda)^2P^2\left(\mu_{dw}^{(1)}\right)^2,$$
$$\boldsymbol{var}\left(Y_w^{(2)}|\Psi_0\right) = N_w\xi^2P^2\left(\mu_{sw}^{(2)}\right)^2 + N_w\sigma^2,$$
$$\mathbb{E}\left(Y_w^{(2)}|\Psi_1\right) = N_w(1-\xi)P\mu_{rw}^{(2)} + N_w\xi P\mu_{sw}^{(2)} + N_w\sigma^2$$
و $\boldsymbol{var}\left(Y_w^{(2)}|\Psi_1\right) = N_w(1-\xi)^2\mathrm{P}^2\left(\mu_{rw}^{(2)}\right)^2 + N_w\xi^2\mathrm{P}^2\left(\mu_{sw}^{(2)}\right)^2$ هستند.

همان‌طور که بیان شد، ناظر در فاز اول و دوم به ترتیب بر اساس $Y_w^{(1)} \underset{\Psi_0}{\overset{\Psi_1}{\gtrless}} \vartheta^{(1)}$ و $Y_w^{(2)} \underset{\Psi_0}{\overset{\Psi_1}{\gtrless}} \vartheta^{(2)}$ تصمیم بر وجود یا عدم وجود مخابره می‌گیرد؛ بنابراین احتمال هشدار اشتباه و از دست دادن آشکارسازی در هر دو فاز توسط روابط ۱۹-۲۲ محاسبه می‌گردد.

$$\mathbb{P}_{FA}^{(1)} = \mathbb{P}\left(Y_w^{(1)} > \vartheta^{(1)}|\Psi_0\right) = \mathbb{Q}\left(\frac{\vartheta^{(1)} - \mathbb{E}\left(Y_w^{(1)}|\Psi_0\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(1)}|\Psi_0\right)}}\right) \quad (۱۹)$$

$$\mathbb{P}_{MD}^{(1)} = \mathbb{P}\left(Y_w^{(1)} < \vartheta^{(1)}|\Psi_1\right) = 1 - \mathbb{Q}\left(\frac{\vartheta^{(1)} - \mathbb{E}\left(Y_w^{(1)}|\Psi_1\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(1)}|\Psi_1\right)}}\right) \quad (۲۰)$$

$$\mathbb{P}_{\boldsymbol{FA}}^{(\boldsymbol{2})} = \mathbb{P}\left(\boldsymbol{Y_w^{(2)}} > \boldsymbol{\vartheta^{(2)}}|\boldsymbol{\Psi_0}\right) = \mathbb{Q}\left(\frac{\boldsymbol{\vartheta^{(2)}} - \mathbb{E}\left(\boldsymbol{Y_w^{(2)}}|\boldsymbol{\Psi_0}\right)}{\sqrt{\boldsymbol{var}\left(\boldsymbol{Y_w^{(2)}}|\boldsymbol{\Psi_0}\right)}}\right) \quad (۲۱)$$

$$\mathbb{P}_{\boldsymbol{MD}}^{(\boldsymbol{2})} = \mathbb{P}\left(\boldsymbol{Y_w^{(2)}} < \boldsymbol{\vartheta^{(2)}}|\boldsymbol{\Psi_1}\right) = 1 - \mathbb{Q}\left(\frac{\boldsymbol{\vartheta^{(2)}} - \mathbb{E}\left(\boldsymbol{Y_w^{(2)}}|\boldsymbol{\Psi_1}\right)}{\sqrt{\boldsymbol{var}\left(\boldsymbol{Y_w^{(2)}}|\boldsymbol{\Psi_1}\right)}}\right) \quad (۲۲)$$

در روابط فوق $\mathbb{Q}(x)$ به‌صورت $\mathbb{Q}(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{y^2}{2}}dy$ تعریف می‌شود.

۳-۳. مسئله بهینه‌سازی تخصیص توان

در این بخش مسئله بهینه‌سازی تخصیص توان به‌گونه‌ای فرمول‌نویسی می‌شود که نرخ امن به‌دست‌آمده در فرمول ۱۰ بیشینه شود. همچنین الزامات مخابره پنهان که در فرمول ۲ آورده شده است، در هر دو فاز برقرار باشد. بنابراین مسئله بهینه-سازی تخصیص توان به‌صورت زیر فرمول‌نویسی می‌شود.

$$\max_{\rho,\xi} \frac{\mathbb{P}_t}{2}\left[\log_2\left(1 + \frac{\lambda(1-\xi)\gamma_{sr}\gamma_{dr}}{\lambda\gamma_{sr} + (2-\lambda-\xi)\gamma_{dr} + 1}\right) - \log_2\left(1 + \frac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{dr} + 1}\right)\right]^+,$$
$$s,t,: \quad 0 \le \rho \le 1, \quad 0 \le \xi \le 1,$$
$$\min_{\vartheta^{(1)}}\left(\mathbb{P}_{FA}^{(1)} + \mathbb{P}_{MD}^{(1)}\right) \ge 1 - \varepsilon,$$
$$\min_{\vartheta^{(2)}}\left(\mathbb{P}_{FA}^{(2)} + \mathbb{P}_{MD}^{(2)}\right) \ge 1 - \varepsilon, \quad (۲۳)$$

با کمینه گیری بر روی $\vartheta^{(1)}$ و $\vartheta^{(2)}$ بدترین الزام مخابره پنهان به ترتیب در فاز اول و دوم در نظر گرفته می‌شود. برای حل مسئلهٔ بهینه‌سازی ابتدا لازم هست که مقدار بهینه‌ی $\vartheta^{(1)}$ و $\vartheta^{(2)}$ محاسبه گردد. به‌این‌ترتیب از $\mathbb{P}_{FA}^{(1)} + \mathbb{P}_{MD}^{(1)}$ و $\mathbb{P}_{FA}^{(2)} + \mathbb{P}_{MD}^{(2)}$ به ترتیب نسبت به $\vartheta^{(1)}$ و $\vartheta^{(2)}$ مشتق گرفته می‌شود. مقادیر بهینه در پیوست ب [۲۹] آورده شده‌اند. در گام بعدی مقدار بهینه‌ی به‌دست‌آمده در روابط ۱۹ تا ۲۲ جایگذاری می‌شود. باکمی ساده‌سازی مسئله بهینه‌سازی به‌صورت زیر فرمول‌نویسی می‌شود.

$$\max_{\rho,\xi} \frac{\mathbb{P}_t}{2}\left[\log_2\left(1 + \frac{\lambda(1-\xi)\gamma_{sr}\gamma_{dr}}{\lambda\gamma_{sr} + (2-\lambda-\xi)\gamma_{dr} + 1}\right) - \log_2\left(1 + \frac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{dr} + 1}\right)\right]^+,$$
$$s,t,: \quad 0 \le \rho \le 1, \quad 0 \le \xi \le 1,$$
$$\mathbb{Q}\left(\frac{\vartheta_{opt\,2}^{(1)} - \mathbb{E}\left(Y_w^{(1)}|\psi_1\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(1)}|\psi_1\right)}}\right) - \mathbb{Q}\left(\frac{\vartheta_{opt2}^{(1)} - \mathbb{E}\left(Y_w^{(1)}|\psi_0\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(1)}|\psi_0\right)}}\right) \le \varepsilon,$$
$$\mathbb{Q}\left(\frac{\vartheta_{opt2}^{(2)} - \mathbb{E}\left(Y_w^{(2)}|\psi_1\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(2)}|\psi_1\right)}}\right) - \mathbb{Q}\left(\frac{\vartheta_{opt2}^{(2)} - \mathbb{E}\left(Y_w^{(2)}|\psi_0\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(2)}|\psi_0\right)}}\right) \le \varepsilon, \quad (۲۴)$$

۴-۳. حل مسئله بهینه‌سازی تخصیص توان

همان‌طور که بیان شد. برای حل مسئله بهینه‌سازی مقید تک‌هدفه از روش تبدیل مسئلهٔ مقید تک‌هدفه به مسئلهٔ چندهدفه و حل مسئله چندهدفه استفاده می‌شود. برای این منظور لازم است که ۵ مرحله که در مقدمه آورده شده‌اند؛مورداستفاده قرار بگیرند. مرحلهٔ اول، انجام نگاشتی از فضای محدودیت‌ها به فضای توابع هدف هست که برای این

منظور تخطی[1] از قیود رابطه ۲۴ به‌عنوان توابع هدف در مسئله چندهدفه معادل در نظر گرفته می‌شود. درنتیجه مسئله بهینه‌سازی معادل در فضای چندهدفه به‌صورت زیر فرمول‌نویسی می‌شود.

$$\begin{aligned}
&\max_{\rho,\xi} \frac{\mathbb{P}_t}{2}[log_2\left(1\right.\\
&\left.+\frac{\lambda(1-\xi)\gamma_{sr}\gamma_{dr}}{\lambda\gamma_{sr}+(2-\lambda-\xi)\gamma_{dr}+1}\right)\\
&-log_2(1+\frac{\lambda\gamma_{sr}}{(1-\lambda)\gamma_{dr}+1})]^+,\\
&\min_{\rho,\xi}\left[\frac{\mathbb{Q}\left(\frac{\vartheta_{opt\,2}^{(1)}-\mathbb{E}\left(Y_w^{(1)}|\psi_1\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(1)}|\psi_1\right)}}\right)}{\varepsilon}\right.\\
&\left.-\frac{\mathbb{Q}\left(\frac{\vartheta_{opt2}^{(1)}-\mathbb{E}\left(Y_w^{(1)}|\psi_0\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(1)}|\psi_0\right)}}\right)}{\varepsilon}-1\right]^+\\
&\min_{\rho,\xi}\left[\frac{\mathbb{Q}\left(\frac{\vartheta_{opt2}^{(2)}-\mathbb{E}\left(Y_w^{(2)}|\psi_1\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(2)}|\psi_1\right)}}\right)}{\varepsilon}\right.\\
&\left.-\frac{\mathbb{Q}\left(\frac{\vartheta_{opt2}^{(2)}-\mathbb{E}\left(Y_w^{(2)}|\psi_0\right)}{\sqrt{\boldsymbol{var}\left(Y_w^{(2)}|\psi_0\right)}}\right)}{\varepsilon}-1\right]^+
\end{aligned} \tag{۲۵}$$

انجام، مرحله۲ الزامی نیست و در شبیه‌سازی‌های این مقاله از انجام مرحلهٔ ۲ صرف‌نظر شده است.

برای حل مسئلهٔ بهینه‌سازی از الگوریتم ژنتیک استفاده می‌شود. الگوریتم ژنتیک در الگوریتم ۱ آورده شده است.

عملگر جهش، جهشی تصادفی در والد ایجاد می‌کند و به‌این‌ترتیب فرزند ایجاد می‌شود. این عملگر برای حفظ تنوع در جمعیت ضروری هست. در شبیه‌سازی‌های این مقاله از عملگر جهش گوسی استفاده‌شده است[۳۰]. این عملگر، یک عملگر مرسوم در مسائل بهینه‌سازی دارای فضای جست‌وجوی پیوسته هست.

در عملگر ترکیب دو والد با یکدیگر ترکیب می‌شوند و به‌این‌ترتیب جمعیت فرزندان ایجاد می‌شود. در شبیه‌سازی‌های مربوط به این مقاله از عملگر ترکیب حسابی استفاده‌شده است[۳۱]. هدف از الگوریتم انتخاب این هست که اهمیت بیش‌تری به اعضای برجسته جامعه داده می‌شود. یکی از انواع عملگرهای انتخاب، انتخاب رقابتی دوتایی هست[۳۲]؛ در شبیه‌سازی‌های این مقاله از الگوریتم انتخاب رقابتی باینری استفاده‌شده است.

الگوریتم (۱) :الگوریتم ژنتیک[۳۳]

۱-ایجاد جمعیت اولیه
۲- محاسبه میزان برازندگی راه‌حل
۳- انتخاب
۴- انجام تقاطع← ایجاد جمعیت فرزندان
۵- انجام جهش← ایجاد جمعیت جهش‌یافتگان
۶- در صورت برآورده نشدن شرایط خاتمه به ۲ برگرد در غیر این صورت پایان.

الگوریتم ژنتیک برای بهینه‌سازی تک‌هدفه و چندهدفه یکسان هست و تفاوت آن‌ها در بخش‌های انتخاب والدین و نیز انتخاب اعضای اصلی جمعیت جدید هست. یکی از نسخه‌های چندهدفه الگوریتم ژنتیک، NSGAII هست[۳۲] که در این مقاله از آن استفاده‌شده است.

در الگوریتم NSGAII هر شخص در جمعیت دو ویژگی دارد:
۱- مرتبه: همان شماره جبهه مربوط به شخص هست.
۲- فاصله ازدحامی محلی: فاصله ازدحامی شخص در جبهه‌ای است که در آن قرار دارد.

در هنگام مقایسه بین دو راه‌حل درصورتی‌که مرتبه آن‌ها متفاوت باشد، شخص دارای مرتبهٔ کمتر ترجیح داده می‌شود. در غیر این صورت اگر مرتبهٔ آن‌ها یکسان باشد، شخص دارای فاصله ازدحامی بیشتر ترجیح داده خواهد شد[۳۲].

الگوریتم (۲): مرتب‌سازی نا مغلوب[۳۲]

۱- شمارنده جبهه‌ها را برابر یک قرار بده.
۲- اولین عضو از جمعیت P را به مجموعه P' اضافه کن.
۳- به‌ازای هر $p \in P$، طوری که $p \notin P'$:
- $P' = P' \cup \{p\}$
- به‌ازای هر $q \in P'$، طوری که $q \neq p$
  - اگر p بر q غلبه کند: q را ، از مجموعه P' حذف کن.
  - در غیر این صورت، اگر q بر p غلبه کند، p را از مجموعه P' حذف کن.

۴- اگر $P' = \emptyset$، پایان. در غیر این صورت : اعضای P'، را به جبهه k اضافه کن و از مجموعه P، حذف کن. یک واحد به شمارنده جبهه k اضافه کن و به مرحله ۲ بازگرد.

[1] Violation

الگوریتم (۳): فاصله ازدحامی [۳۲]

۱- $l = |I|$ در نظر بگیر. ($|I|$، بیانگر سایز مجموعه I هست.)

۲- به‌ازای هر $i \in I$، $I[i]_{distance} = 0$، در نظر بگیر.

۳- به‌ازای هر تابع هدف : m

- مجموعه I، را در راستای تابع هدف m مرتب می‌نماییم.
- $I[1]_{distance} = I[l]_{distance} = \infty$، قرار می‌دهیم.
- به‌ازای $i = 2, \dots, (l-1)$
- ✓ $I[i]_{distance} = I[i]_{distance} + (I[i+1].m - I[i-1])$ [۱]

بعد از حل مسئلهٔ بهینه‌سازی چندهدفه بیان‌شده در رابطهٔ ۲۵، مجموعه جواب‌های جبهه پارتو[۲] به دست می‌آیند. حال از میان این مجموعه جواب‌ها، آن‌هایی که در قیود مسئله بهینه-سازی ۲۴ صدق نمی‌کنند، حذف می‌شوند. از میان پاسخ‌های باقی‌مانده، پاسخ دارای بالاترین نرخ امن به‌عنوان پاسخ مسئله در نظر گرفته می‌شود. لازم به ذکر هست که اگر M و N به ترتیب تعداد توابع هدف و تعداد تکرارهای الگوریتم NSGAII باشند، پیچیدگی رویکرد مرتب‌سازی نامغلوب برابر $O(MN^2)$ هست.

۴. نتایج و بحث

جهت سادگی محاسبات فرض می‌شود، $\mu_{sw}^{(2)} = \mu_{sw}^{(1)} = \mu_{sw}$، $\mu_{sr}^{(1)} = \mu_{sr}$ ، $\mu_{rw}^{(2)} = \mu_{rw}$ ، $\mu_{dw}^{(1)} = \mu_{dw}$هست. این فرض انجام می‌شود که $\mu_{ij} = d_{ij}^{-\alpha}$ به‌ازای $i \in \{s,d,r\}$ و $j \in \{w,d,r\}$ هست. d_{ij} فاصله گره i و j هست. α نیز بیانگر توان افت مسیر هست. پارامترهای شبیه‌سازی سیستم مدل موردمطالعه در جدول ۱ آورده شده است.

برای توصیف یک EA از پارامترهای کمی و پارامترهای کیفی استفاده می‌شود. پارامترهای کیفی، پارامترهای سطح بالایی هستند که ساختار کلی یک الگوریتم تکاملی را مشخص می‌نمایند و از طریق آن‌ها تمایز میان الگوریتم‌های تکاملی گوناگون برقرار می‌گردد. به‌عنوان‌مثال، یکی از پارامترهای کیفی عملگر ترکیب است که می‌تواند عملگر ترکیب حسابی باشد. دستهٔ دیگری از پارامترها، پارامترهای کمی هستند. پارامترهای کمی، پارامترهای سطح پایینی هستند که به توصیف یک EA خاص می‌پردازند.[۳۴] پارامترهای کمی و کیفی EA که برای شبیه‌سازی‌های این مقاله استفاده‌شده است به ترتیب در جدول ۲ و ۳ آورده شده است.

جدول (۱). پارامترهای شبیه‌سازی سیستم مدل

نام	پارامتر	مقدار
σ^2	توان نویز در رله و مقصد	-۵۰ dBw
σ_w^2	توان نویز در ناظر	-۵۰ dBw
$\mathbb{P}_t$	احتمال ارسال داده در هر اسلات زمانی	۰/۵
$\mathbf{P}$	کل توان ارسالی در هر اسلات زمانی	۱۰ dBw
$\mathbf{1-\varepsilon}$	حد پایین خطای آشکارسازی در ناظر	۰/۹
$\boldsymbol{N_s}$	تعداد آنتن منبع	۱۶
$\boldsymbol{N_d}$	تعداد آنتن مقصد	۱۶
$\boldsymbol{N_w}$	تعداد آنتن ناظر	۱۶
	مکان منبع	(-۵،۰)
	مکان مقصد	(۵،۰)
	مکان رله	(۰،۰)
	مکان ناظر	(۰،-۵)

جدول (۲). پارامترهای کیفی EA مورداستفاده

نام	مقدار
بازنمایی	عدد حقیقی
عملگر ترکیب	عملگر ترکیب حسابی
عملگر جهش	عملگر جهش گوسی
عملگر انتخاب والدین	انتخاب رقابتی

شکل ۴، ESR را برحسب کل توان ارسال در هر شکاف زمانی نمایش می‌دهد. همان‌طور که مشاهده می‌شود، ESR یک تابع افزایشی نسبت به‌کل توان ارسالی است. دلیل این امر این است که سیگنال نویز مصنوعی، فقط در گره‌های غیرقانونی تأثیر مخرب دارد و هیچ تأثیری در مقصد به دلیل حذف خود تداخلی نخواهد داشت. برای حل مسئله بهینه‌سازی مقید تک‌هدفه ، از روش تبدیل مسئله مقید به مسئله چندهدفه سپس حل مسئله چندهدفه با الگوریتم NSGAII استفاده‌شده است. ازاین‌رو به‌منظور تأییدیه‌ای بر روش مطرح‌شده، نتایج حاصل از آن با مونتوکارلو مقایسه می‌شود. (لازم به ذکر است درروش مونتوکارلو از روش جست‌وجو جامع نیز استفاده‌شده است تا مقدار بهینه مسئله و شکاف بهینه روش حل پیشنهادی محاسبه شود). همان‌طور که دیده می‌شود، بین حل پیشنهادی با روش جست‌وجوی جامع 6/88 % شکاف وجود دارد که انگر کارایی روش حل و تحلیل‌های موجود در این مقاله هست.

در[۷] به بررسی سیستم مدلی که منبع چند آنتن و مقصد تک آنتن پرداخته‌شده است. در مقایسه با نمودار ۳ الف در [۷]، در کار ما ESR افزایش‌یافته است. علت این موضوع مجهز بودن مقصد به 16 آنتن هست. مقصد از روش MRC استفاده می‌کند و SNR دریافتی‌اش را بهبود می‌دهد. این امر سبب می‌شود که رله باز ارسال داده منبع را با توان کمتری انجام دهد و توان بیش‌تری به ارسال سیگنال نویز مصنوعی توسط منبع در فاز دوم اختصاص داده شود. به‌این‌ترتیب قابلیت تشخیص ناظر کاهش پیدا می‌کند.

از سوی دیگر در فاز اول، استفاده از MRT توسط مقصد در

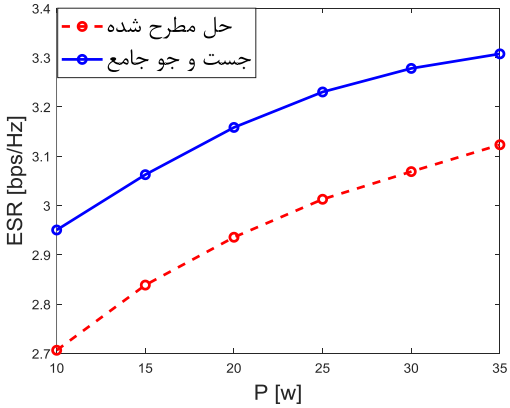
[۱] که در آن $I[i].m$، بیانگر m امین تابع هدف شخص i از مجموعه I است.

[2] Pareto front

جهت رله غیرقابل‌اعتماد برای ارسال سیگنال نویز مصنوعی سبب کاهش SINR در رله غیرقابل‌اعتماد می‌گردد. این امر نیز سبب بیش‌ترشدن ESR در مقایسه با [۷] می‌گردد.

جدول (۳). پارامترهای کیفی EA مورداستفاده

نام	پارامتر	مقدار
G_N	تعداد نسل‌ها	۱۰۰
P_S	تعداد اعضای جمعیت	۵۰
M_R	نرخ جهش	۰/۰۲
M_P	درصد جهش بر روی اعضا جمعیت	۳۰ ٪
C_P	در صد ترکیب بر روی اعضا جمعیت	۷۰ ٪
M_s	گام جهش	۰/۱

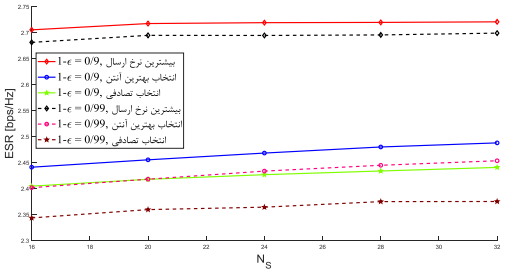


شکل (۴): ESR بر اساس کل توان ارسال در هر اسلات زمانی

شکل ۵، ESR را برحسب تعداد آنتن‌های منبع به تصویر می‌کشد. این شکل کارایی روش MRT بکار گرفته‌شده را با دو روش انتخاب بهترین آنتن و انتخاب آنتن تصادفی مقایسه می‌کند. درروش انتخاب بهترین آنتن، منبع آنتنی را برای ارسال انتخاب می‌کند که دارای بیش‌ترین بهره کانال با رله باشد. در انتخاب آنتن تصادفی همان‌طور که از نام آن پیدا است منبع یک آنتن را به‌صورت تصادفی انتخاب می‌کند. همان‌طور که مشاهده می‌شود روش MRT، ESR بیشتری را نسبت به دو روش دیگر دارد که به ترتیب و به طور میانگین % 9/48 و % 11/53 بیشتر از انتخاب بهترین آنتن و انتخاب تصادفی آنتن هست.

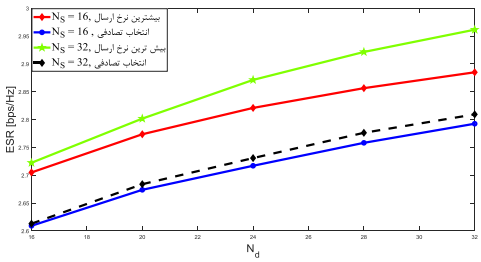
این شکل اثر حد پایین احتمال خطای آشکارسازی در ناظر یعنی $1-\varepsilon$ را نیز مورد ارزیابی قرار می‌دهد. همان‌طور که در شکل دیده می‌شود، هنگامی‌که احتمال خطای آشکارسازی قابل‌پذیرش از % 90 به % 99 افزایش یابد، ESR به‌طور میانگین % 4/02 کاهش می‌یابد. دلیل این امر این است که با افزایش احتمال خطای آشکارسازی قابل‌پذیرش لازم است که سیگنال داده با توان پایین‌تر و سیگنال تداخل با توان بیشتری ارسال شود، این امر موجب کاهش در ESR می‌شود.

در نمودار۳ ب، به بررسی اثر $1-\varepsilon$ در سیستم مدلی ناظر تک آنتن هست، پرداخته شده است. در مقایسه با [۷] با افزایش $1-\varepsilon$ میزان کاهش ESR کمتر است. علت این موضوع چند آنتن بودن ناظر هست. چند آنتن بودن ناظر سبب می‌شود، پاسخ‌های امکان‌پذیر[۱] محدودتر شوند و با کاهش $1-\varepsilon$، ESR بهبود چندانی حاصل نشود.



شکل (۵): ESR بر اساس تعداد آنتن منبع

در شکل ۶ اثر ESR، برحسب تعداد آنتن‌های مقصد نشان داده‌شده است. همان‌طور که مشاهده می‌شود، ESR در هر دو حالت انتخاب آنتن تصادفی و MRT در جهت رله، یک تابع افزایشی نسبت به تعداد آنتن‌های مقصد هست. دلیل این امر، این است که مقصد با استفاده از MRC سیگنال دریافتی خود را بهبود می‌دهد. این شکل، کارایی روش MRT بکار گرفته‌شده را با روش انتخاب آنتن تصادفی مقایسه می‌کند. درروش انتخاب آنتن تصادفی، مقصد یک آنتن را به‌صورت تصادفی انتخاب می‌کند. همان‌طور که مشاهده می‌شود، MRT به ترتیب در حالت مجهز بودن منبع به 16 و 32 آنتن% 3/49 و % 4/46 ESR بیشتری را نسبت به حالت انتخاب تصادفی آنتن ارائه می‌دهد.

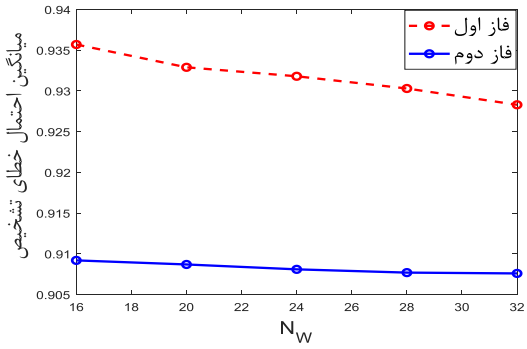


شکل (۶): ESR بر اساس تعداد آنتن مقصد

شکل ۷ اثر تعداد آنتن ناظر را در احتمال خطای تشخیص وجود یا عدم وجود مخابره در ناظر را بیان می‌دارد. همان‌طور که در شکل مشاهده می‌شود هرچقدر ناظر به تعداد آنتن بیشتری مجهز باشد می‌تواند احتمال خطای تشخیص خود را کاهش دهد. در [۷]، در ابتدا به بررسی سناریویی پرداخته می‌شود که یک ناظر تک آتنه در شبکه وجود دارد. سپس به حالت ناظران هم-دست و ناظران غیر هم‌دست بسط داده می‌شود.

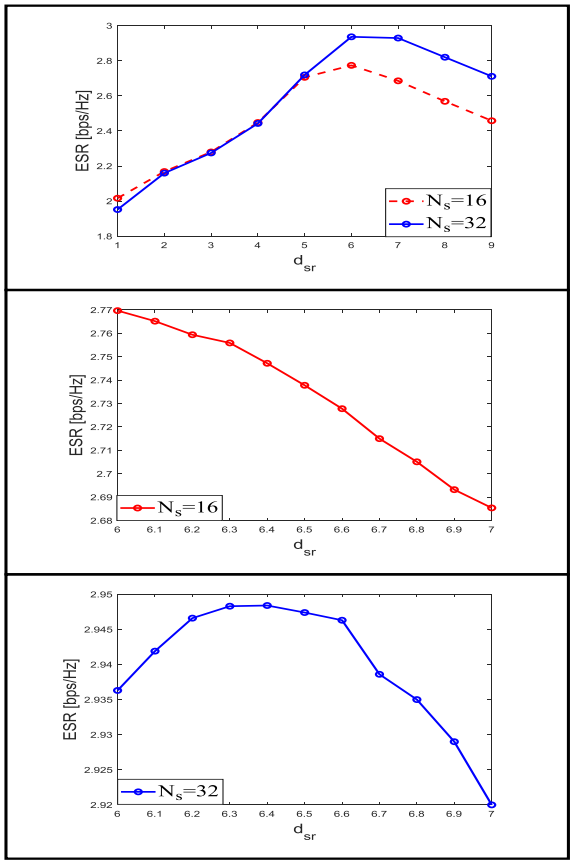
باتوجه‌به نمودار ۶ در [۷]، میانگین احتمال خطای تشخیص ناظر نسبت به حالتی که ناظر تک آنتن باشد، کاهش پیداکرده است. نکته دیگری که با مقایسه با نمودار ۶ در [۷] حاصل می‌شود، این است که حضور چند ناظر در شبکه نسبت به ناظر چند آنتن تأثیر بیش‌تری در کاهش میانگین احتمال خطا در ناظر دارد.

[۱] پاسخ‌هایی که قیدهای مسئله را برآورده می‌سازند.



شکل (۷): اثر تعداد آنتن ناظر بر روی میانگین احتمال خطای تشخیص ناظر

با فرض ثابت‌بودن مکان تمامی گره‌ها به‌جز رله، رله بر روی خط واصل منبع و مقصد از منبع به سمت مقصد جابه‌جا می‌شود. شکل ۸، ESR را برحسب مکان رله نمایش می‌دهد. منظور از d_{sr}، فاصله رله تا منبع هست. نتایج حاصل نشان می‌دهد که به‌ازای تعداد مشخصی آنتن منبع، موقعیتی وجود د دارد که اگر رله غیرقابل‌اعتماد در آن قرار بگیرد، ESR بیشینه می‌شود. هنگامی‌که منبع 16آنتن استفاده می‌کند، فاصله‌ی بهینه رله تا منبع عددی در بازه [6,6.1] هست. با فرض استفاده منبع از 32 آنتن، فاصله بهینه رله تا منبع در بازه [6.4,6.5] هست. یکی از نتایج حاصل از شکل ۸ این است که هرچقدر رله‌ی غیرقابل-اعتماد به منبع نزدیک‌تر باشد، لازم است منبع از تعداد آنتن کمتری استفاده کند. زیرا در این غیر این صورت نشت اطلاعات در شنودگر بیشتر خواهد شد و نرخ امن شبکه کاهش می‌یابد.



شکل (۸): اثر مکان رله بر ESR

۵. نتیجه‌گیری

در این مقاله به مطالعه ارسال امن نظریه اطلاعاتی و مخابره پنهان در یک شبکه دارای رله غیرقابل‌اعتماد پرداخته شده است. در سیستم مدل موردمطالعه رله غیرقابل‌اعتماد سعی می‌کند داده‌های موجود در سیگنال دریافتی را استخراج کند، درحالی‌که هدف ناظر پی‌بردن به وجود مخابره در شبکه است. برای مقابله با این دو تهدید امنیتی پیشنهاد می‌شود که مقصد و منبع به ترتیب در فاز اول و دوم به ارسال سیگنال تداخل مبادرت ورزند. در این سیستم نمونه یک راهبرد تخصیص توان ارائه می‌شود تا ضمن برقراری الزامات مخابره پنهان در هر دوفاز ارسال داده، نرخ امن بیشینه شود. برای حل مسئله بهینه‌سازی مقید تخصیص توان از روش تبدیل به مسئله چندهدفه و حل مسئله چندهدفه با الگوریتم NSGAII استفاده می‌شود، مقایسه نتایج با روش جست‌وجو جامع نشان‌دهنده کارآمد بودن روش حل مذکور برای حل مسئله تخصیص توان است.

در سیستم مدل مورد بررسی، در فاز اول منبع برای ارسال داده از روش MRT در جهت رله استفاده می‌کند، نتایج حاصل از این گزارش نشان می‌دهد این روش از روش‌های انتخاب بهترین آنتن و روش انتخاب آنتن تصادفی بهتر عمل می‌کند. مقصد نیز جهت ارسال سیگنال تداخل از روش MRT در جهت رله استفاده می‌نماید، نشان‌داده‌شده است این روش عملکرد بهتری را نسبت به روش انتخاب آنتن تصادفی دارا هست. همچنین، نتیجه گرفته می‌شود که هرچقدر ناظر از تعداد آنتن بیشتری بهره‌مند باشد می‌تواند میانگین احتمال خطای آشکارسازی خود را کمتر نماید. علاوه بر این، هرچقدر تعداد آنتن‌های منبع افزایش پیدا کند، لازم است که رله، فاصله بیش‌تری را تا منبع داشته باشد.

۶. مراجع

[1] S. Blackburn and S. D. Galbraith, "Certification of secure RSA keys," *Electronics Letters*, vol. 36, no. 1, pp. 29-30, 2000, doi: 10.1049/el:20000035.

[2] J. Han, X. Zeng, X. Xue, and J. Ma, "Physical Layer Secret Key Generation Based on Autoencoder for Weakly Correlated Channels," in *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, 2020: IEEE, pp. 1220-1225, doi: 10.1109/ICCC49849.2020.9238931.

[3] M. Adil, S. Wyne, and S. J. Nawaz, "On quantization for secret key generation from wireless channel samples," IEEE Access, vol. 9, pp. 21653-21668, 2021, doi: 10.1109/ACCESS.2021.3055561.

[4] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26-31, 2015, doi: 10.1109/MCOM.2015.7355562.

[5] L. Mucchi *et al.*, "Physical-layer security in 6G networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901-1914, 2021, doi: 10.1109/OJCOMS.2021.3103735.

[6] K. S. K. Arumugam, M. R. Bloch, and L. Wang, "Covert communication over a physically degraded relay

63, no. 23, pp. 6285-6298, 2015, doi: 10.1109/TSP.2015.2465301.
[21] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," EURASIP Journal on Wireless Communications and Networking, vol. 2009, pp. 1-10, 2010, doi: 10.1155/2009/452907.
[22] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003-5011, 2009, doi: 10.1109/TWC.2009.090323.
[23] F. Samsami, P. Baei, M. Forouzesh, S. M. J. Asgari Tabatabaee, "The analysis and design of secure wireless networks in the presence of users with different security needs based on covert communication and secure transmission of information theory in the presence of a friendly jammer", Jornal of Electronical & Cyber Defence, vol. 9 no. 4, 2022, Doi:https://dor.isc.ac/dor/20.1001.1.23224347.1400.9.4.6.9(In Persian)
[24] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682-694, 2013, doi: 10.1109/TIFS.2013.2248730.
[25] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 341-355, 2017, doi: 10.1109/TIFS.2017.2750102.
[26] M. Mitchell, *An Introduction to Genetic Algorithms*. 1996.
[27] C. A. C. Coello and E. M. Montes, "Constraint-handling in genetic algorithms through the use of dominance-based tournament selection," *Advanced Engineering* Informatics, vol. 16, no. 3, pp. 193-203, 2002, doi: 10.1016/S1474-0346(02)00011-3.
[28] C. A. C. Coello, "A comprehensive survey of evolutionary-based multiobjective optimization techniques," *Knowledge and Information systems*, vol. 1, no. 3, pp. 269-308, 1999, doi: 10.1007/BF03325101.
[29] M. Yari, P. Azmi, "Covert communication with untrusted relay," Thesis, Tarbiat modares Univ, Se, 2020 .(In Persian)
[30] R. Hinterding, "Gaussian mutation and self-adaption for numeric genetic algorithms," in *Proceedings of 1995 IEEE International Conference on Evolutionary Computation*, 1995, vol. 1: IEEE, p. 384, doi: 10.1109/ICEC.1995.489178.
[31] M. Furqan, H. Hartono, E. Ongko, and M. Ikhsan, "Performance of Arithmetic Crossover and Heuristic Crossover in Genetic Algorithm Based on Alpha Parameter," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 19, no. 1, pp. 31-36, 2017, doi: 10.9790/0661-1905013136.
[32] K. Deb, S. Agrawal, A. Pratap, and T. Meyarivan, "A fast elitist non-dominated sorting genetic algorithm for multi-objective optimization: NSGA-II," in *International conference on parallel problem solving from nature*, 2000: Springer, pp. 849-858, doi: 10.1007/3-540-45356-3_83.
[33] M. A. Albadr, S. Tiun, M. Ayob, and F. Al-Dhief , "Genetic algorithm based on natural selection theory for optimization problems," *Symmetry*, vol. 12, no. 11, p. 1758, 2020, doi: 10.3390/sym12111758.
[34] A. E. Eiben and S. K. Smit, "Parameter tuning for configuring and analyzing evolutionary algorithms," *Swarm and Evolutionary Computation*, vol. 1, no. 1, pp. 19-31, 2011, doi: 10.1016/j.swevo.2011.02.001.

channel with non-colluding wardens," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018: IEEE, pp. 766-770, doi: 10.1109/ISIT.2018.8437505.
[7] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, 2020, doi: 10.1109/TCOMM.2020.2978206.
[8] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Covert Communication Using Null Space and 3D Beamforming," *arXiv preprint arXiv:1907.01350*, 2019, doi: 10.1109/TVT.2020.2997074.
[9] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Transactions on Wireless* Communications, vol. 17, no. 7, pp. 4766-4779, 2018, doi: 10.1109/TWC.2018.2831217.
[10] K. Shahzad, "Relaying via cooperative jamming in covert wireless communications," in *2018 12th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2018: IEEE, pp. 1-6, doi: 10.1109/ICSPCS.2018.8631772.
[11] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517-8530, 2018, doi: 10.1109/TWC.2018.2878014.
[12] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9 ,pp. 6193-6206, 2017, doi: 10.1109/TWC.2017.2720736.
[13] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 317-320, 2018, doi: 10.1109/LWC.2018.2872058.
[14] A. Nosratinia, T. E. Hunter ,and A. Hedayat, "Cooperative communication in wireless networks," *IEEE communications Magazine*, vol. 42, no. 10, pp. 74-80, 2004, doi: 10.1109/MCOM.2004.1341264.
[15] A. S. Shah and M. S. Islam, "A survey on cooperative communication in wireless networks," *International Journal of Intelligent Systems and Applications*, vol. 6, no. 7, p. 66, 2014, doi: 10.5815/ijisa.2014.07.09.
[16] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1027-1053, 2016, doi: 10.1109/COMST.2016.2633387.
[17] A. D. Wyner, "The wire- tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355-1387, 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.
[18] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773-1828, 2018, doi: 10.1109/COMST.2018.2878035.
[19] D. Fang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Cooperative jamming protocols in two hop amplify-and-forward wiretap channels," in *2013 IEEE International Conference on Communications (ICC)*, 2013: IEEE, pp. 2188-2192, doi: 10.1109/ICC.2013.6654852.
[20] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Transactions on Signal Processing* ,vol.