طراحی یک مکانیسم تدافعی برای بهبود امنیت در لایه فیزیکی با رویکرد نظریه بازی‌ها: کاربرد در شبکه‌های اقتضایی خودرویی

مریم کاکاوند میرزایی[۱]، کارشناس ارشد؛ جلیل سیفعلی هرسینی[۲]، استادیار

۱- دانشکده فنی و مهندسی - دانشگاه گیلان - رشت - ایران - mkakavandm@gmail.com
۲- دانشکده فنی و مهندسی - دانشگاه گیلان - رشت - ایران - harsini@guilan.ac.ir

چکیده: در سال‌های اخیر رشد روزافزون تکنولوژی ارتباطات بی‌سیم و کاربرد آن در توسعه سرویس‌های داده جدید، چالش‌های جدیدی را در حوزه ارتباطات و شبکه‌های داده پیش روی محققان قرار داده است. به‌عنوان‌مثال در حوزه سیستم‌های حمل‌ونقل هوشمند ایده به‌کارگیری شبکه‌های اقتضایی خودرویی ارائه شده است. در این شبکه‌ها به‌جهت ماهیت پخش رادیویی، همیشه برای مهاجمان شبکه فرصت تأثیرگذاری روی سیستم ارتباطی وجود دارد. بنابراین مسئله امنیت برای ارسال اطلاعات حساس، بسیار مهم خواهد بود. در لایه فیزیکی شبکه، حمله‌های مهاجمان می‌تواند به یکی از دو شیوه ایجاد تداخل (پخش پارازیت) و شنود کردن صورت پذیرد. در این مقاله، یک مکانیسم تدافعی بر اساس کنترل توان فرستنده جهت مقابله با اثرهای تخریبی حمله‌های لایه فیزیکی (کنترل عملکرد مهاجم) طراحی شده است. در این مکانیسم با استفاده از روش نظریه بازی‌ها توان به‌کارگیری‌شده جهت انتقال اطلاعات توسط فرستنده و مهاجم روی زیرکانال‌های تقسیم فرکانسی متعامد یک کانال پهن باند به‌نحوی بهینه‌سازی شده است که به بهبود امنیت کانال (ظرفیت ایمن) منجر شود. شبیه‌سازی عملکرد الگوریتم ارائه‌شده در بستر یک شبکه اقتضایی خودرویی بر اساس استاندارد IEEE 802.11p انجام شده است.

واژه‌های کلیدی: امنیت در لایه فیزیکی، نظریه بازی‌ها، کنترل توان، شبکه‌های اقتضایی خودرویی.

A Game-theoretic Approach to Defensive Mechanism Design for Physical Layer Security: Application to Vehicular Ad-Hoc Networks

M. Kakavand Mirzaeei[1], MSc; J. Seifali Harsini[2], Assistant Professor

1- Department of Electrical Engineering, University of Guilan, Rasht, Iran, Email: mkakavandm@gmail.com
2- Department of Electrical Engineering, University of Guilan, Rasht, Iran, Email: harsini@guilan.ac.ir

Abstract: In the recent years the growth of wireless communications technology and its application in the development of new data services creates new challenges in the research field of data communications and networking. For example, in the field of intelligent transport systems, the concept of vehicular ad-hoc networking is presented. Because of the broadcast nature of radio environment, there are always opportunities for the network attackers to affect wireless communications systems. Hence, the issue of security for the transmission of sensitive data is of great importance. In the physical layer of the network, the attack may occur in the form of signal jamming or eavesdropping. In this paper, a defensive mechanism is designed using transmitter power control to reduce the damaging effects of these two physical layer attacks. Using a game-theoretic formulation, the mechanism optimizes OFDM subcarrier powers at both the main data transmitter and the attacker in order to improve the security of the communication channel (secrecy capacity). As an application of the proposed method, simulation results are provided for a vehicular ad-hoc network (VANET) scenario based on the IEEE802.11p standard.

Keywords: Physical-layer security, games theory, power control, vehicular ad-hoc networks (VANETs).

تاریخ ارسال مقاله: ۱۳۹۴/۱۰/۲۰
تاریخ اصلاح مقاله: ۱۳۹۴/۱۲/۲۵
تاریخ پذیرش مقاله: ۱۳۹۵/۰۲/۳۰
نام نویسنده مسئول: جلیل سیفعلی هرسینی
نشانی نویسنده مسئول: ایران - رشت - کیلومتر ۵ جاده رشت به قزوین - دانشگاه گیلان - دانشکده فنی و مهندسی.

۱- مقدمه

در دهه‌های اخیر به‌دنبال رشد فزاینده فناوری‌های ارتباطات بی‌سیم، شبکه‌های ارتباطی نوینی مانند شبکه‌های اقتضایی ارائه شده است که دارای کاربردهای مهمی در حوزه‌های نظامی، صنعتی و اجتماعی هستند [۱]. به‌عنوان‌مثال در حوزه سیستم‌های حمل‌ونقل هوشمند، ایده ایجاد یک شبکه ارتباطی بی‌سیم در میان خودروهایی که در جاده‌ها یا خیابان‌ها تردد می‌کنند، تحت عنوان شبکه اقتضایی بین‌خودرویی (VANET) مطرح شده است. در این شبکه سرویس‌های جدیدی در قالب پیام‌های کوتاه به رانندگان ارائه شده است. این پیام‌ها می‌تواند از دسته پیام‌های ایمنی که مربوط به حفظ جان سرنشینان خودروها است، بوده و یا از دسته پیام‌های غیرایمنی مثل اخبار مربوط به آب‌وهوا، اطلاعات عمومی و یا حتی اطلاعات محرمانه بین دو خودرو باشد. عدم وجود یک زیرساخت ثابت در شبکه‌های اقتضایی و نیز پویایی ساختار شبکه، زمینه حضور مهاجمان در این شبکه‌ها را تسهیل می‌کند. در واقع مهاجمان با عبور از موانع نه چندان قدرتمند این شبکه‌ها و دست‌یابی به اطلاعات موجود قادرند به اهداف خود برسند. بنابراین، مادامی که اطلاعات حساسی در این شبکه‌ها انتقال می‌یابد، ایجاد امنیت در ارتباطات امری ضروری و غیرقابل‌اجتناب است [۲].

با توجه به این‌که حمله می‌تواند به لایه‌های مختلف شبکه بی‌سیم صورت گیرد، در سال‌های اخیر تلاش‌های فراوانی در راستای ارائه پروتکل‌های امنیتی در این شبکه‌ها توسط محققان علوم کامپیوتر صورت پذیرفته است [۴-۳]. درواقع در غالب این روش‌ها که برای ایجاد امنیت از علم رمزنگاری استفاده می‌کنند، اثرهای کانال بی‌سیم ارتباطی نادیده گرفته می‌شود و تأکید اصلی بر عدم توانایی مهاجم برای شکستن رمز به‌کار گرفته شده است. بااین‌وجود، رشد توان محاسبه توسط مهاجمان همواره الگوریتم‌های امنیتی مبتنی بر علم رمزنگاری را مورد تهدید قرار داده است. به‌نحوی‌که امروزه الگوریتم‌های استاندارد رمزنگاری متقارن و غیرمتقارن مانند DES و RSA شکسته شده‌اند. اخیراً محققان علوم ارتباطات بی‌سیم به نوع دیگری از روش‌های ارتقاء امنیت موسوم به امنیت لایه فیزیکی توجه نموده‌اند که می‌توانند به‌عنوان مکملی برای پروتکل‌های امنیتی رمزنگاری محسوب شود [۵].

در حوزه امنیت لایه فیزیکی سعی می‌شود که از خصوصیت‌های کانال بی‌سیم مانند میزان محوکنندگی، تداخل و نویز برای بهبود امنیت ارتباطات در مقابل حمله‌های شنود و تخریب بهره‌برداری شود. به‌طورکلی شنود کردن اطلاعات محرمانه کاربران و نیز تخریب کانال با ارسال امواج تداخلی (پارازیت) را می‌توان در زمره حمله‌های مهاجمان به لایه فیزیکی در نظر گرفت. ازاین‌رو، این انتظار وجود دارد که استفاده از ابزار مناسب برای بهبود امنیت لایه فیزیکی بتواند به ارتقاء امنیت کلی سیستم منجر شود. در این راستا نظریه بازی‌ها به‌عنوان ابزاری کارآمد در مدل‌سازی و حل مسائل مربوط به امنیت ارتباطات شناخته شده است [۶].

در این روش موقعیت‌های قابل انتخاب در سیستم در قالب یکی از انواع بازی‌های تعریف‌شده مدل می‌شود و با استفاده از ابزار ریاضی رفتار بازیکنان در هر مرحله از بازی و مقدار هزینه و منفعت آن‌ها پیش‌بینی می‌شود. در این روش هر بازیکن می‌تواند با به‌کار گرفتن اصول علم نظریه بازی‌ها خود را به برد نزدیک کند و منفعت خود را به حداکثر ممکن برساند. لازم به ذکر است که طراحی مکانیسم دفاعی با رویکرد نظریه بازی‌ها یک مزیت مجزا بر روش‌های بهینه‌سازی ساده دارد، زیرا در این رویکرد رفتار مهاجم به‌طور صریح در مدل گنجانده شده است. درحالی‌که در روش‌های بهینه‌سازی ساده، عمل بهینه‌سازی تنها روی پارامترهای مدافع صورت گرفته و مهاجم در نظر گرفته نشده است. حتی در این روش به‌دلیل ماهیت چند بازیکنی می‌تواند رفتار مهاجم پیش‌بینی شود.

در ادامه کارهای انجام‌شده مرتبط با این مقاله معرفی و مرور شده است. یک سناریوی مخابراتی شامل یک فرستنده و گیرنده مجاز (لینک بی‌سیم) و یک مهاجم که می‌خواهد روی ارسال داده لینک بی‌سیم ایجاد تداخل نماید، توسط التمن و همکاران مورد تحلیل قرار گرفته شده است [۷]. در سناریوی مورداشاره با لحاظ نمودن هزینه توان ارسالی در فرایند بهینه‌سازی توان فرستنده لینک بی‌سیم چندکاناله، نقطه تعادل نش[۱] بازی در صفحه ۳ مقاله استخراج شده است. در این طرح تعامل بین فرستنده لینک بی‌سیم و مهاجم با یک بازی از نوع مجموع غیرصفر[۲] مدل شده است. همچنین فرض می‌شود هر دو بازیکن در شروع هر مرحله از به‌کارگیری استراتژی‌های خود، دانش کافی از محیط دارند. در یک سناریوی دیگر برای کانال‌های مخابراتی چندورودی- چندخروجی با محوکنندگی رایلی، از یک مدل بازی مجموع صفر برای حداکثر کردن اطلاعات متقابل بین یک زوج فرستنده و گیرنده (جفت رمزگذار و رمزگشا) در حضور یک گره مهاجم، استفاده شده است [۸]. همچنین نشان داده شده است که در این مدل بازی برای مهاجمی که به دنبال دسترسی به دانش ورودی کانال بی‌سیم است، بهره‌ای قابل حصول نخواهد بود. در مدلی دیگر از یک بازی استکلبرگ[۳] برای حفاظت یک منبع اطلاعات در مقابل یک شنودگر بهره گرفته شده است [۹]. در این بازی منبع برای افزایش ظرفیت امن خود با پرداخت هزینه به تعدادی گره تخریب‌گر دوست، قصد ایجاد تداخل عمدی روی گره شنودگر دارد. در یک مقاله دیگر که توسط هان و همکارانش ارائه شده است [۱۰]، بازی استکلبرگ برای مدل‌سازی مسئله دفاع در مقابل یک مهاجم هوشمند (گره‌ای که می‌تواند با یادگیری، استراتژی خود را انتخاب نماید) به‌کار گرفته شده است تا نشان دهد که اگر فرستنده اصلی از قواعد بازی برای پیش‌بینی رفتار مهاجم بهره ببرد، آنگاه اثر تخریبی یک مهاجم هوشمند بیشتر از یک مهاجم ساده نخواهد بود. همچنین پژوهشگران در [۱۱] از یک بازی مجموع صفر برای مدل‌سازی رفتار مهاجمی که می‌تواند بر اساس سطح توان خود، بین استراتژی‌های شنود و ایجاد تداخل یکی را انتخاب کند، استفاده کرده‌اند. مدل‌های بازی امنیتی برای سناریوهای

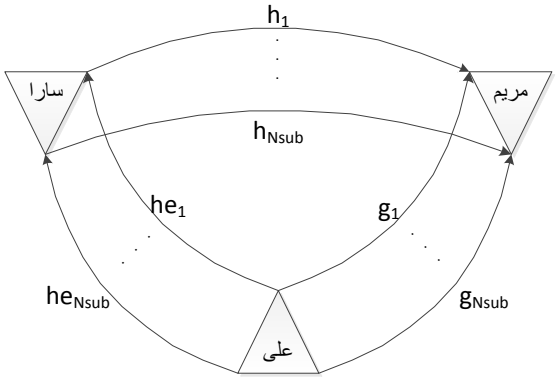
مخابراتی رادیوشناختی نیز توسعه داده شده است [۱۲، ۱۳]. به‌طورخاص در [۱۲] دو مدل بازی کاهنده تداخل برای حالت‌هایی که کاربر ثانویه فقط به یک کانال و یا به چند کانال مخابراتی دسترسی داشته باشد، ارائه شده است. در حالت دسترسی به یک کانال، ایده پرش بین کانال‌های مختلف و برای حالت دسترسی به چندین کانال، ایده توزیع تصادفی توان بین کانال‌ها برای تعیین استراتژی‌های بهینه بازی‌ها به‌کار گرفته شده است. همچنین مسئله آشکارسازی وجود مهاجم به‌وسیله فرستنده اصلی از این زاویه موردمطالعه قرار گرفته که با اختصاص یک زمان کوچک در فریم ارسال داده (مربوط به فرستنده) عمل آشکارسازی گره مهاجم بهتر صورت می‌گیرد [۱۴]. ازاین‌رو به این شیوه می‌توان امنیت لایه فیزیکی را بهبود بخشید.

در این مقاله یک سیستم مخابراتی چندکانالهٔ که از مدولاسیون تسهیم تقسیم فرکانسی متعامد (OFDM)[۴] برای انتقال داده‌ها بین یک فرستنده و گیرنده اصلی استفاده می‌کند، در نظر گرفته شده است. در این سیستم فرض شده است که مهاجم می‌تواند به‌صورت یکی از حالت‌های ایجاد تداخل چند کانالی روی لینک اصلی و یا شنود محض عمل نماید. در این مدل علاوه بر قابلیت انتخاب احتمالی حالت عملکرد مهاجم، هر دو گره‌های فرستنده اصلی و مهاجم دارای قابلیت تنظیم سطوح توان روی زیرحامل‌های مدولاسیون OFDM هستند. بر این اساس یک استراتژی دفاعی برای بهبود امنیت لایه فیزیکی با در نظر گرفتن هزینه توان ارسالی ارائه شده است. استراتژی دفاعی موردنظر در قالب یک بازی تهاجم-تدافع از نوع مجموع غیرصفر دارای یک نقطه تعادل نش یکتا است که بر اساس آن میزان منفعت فرستنده اصلی (ظرفیت امن) حداکثر می‌شود. علاوه‌براین، کاربرد الگوریتم تدافعی ارائه‌شده در محیط شبکه اقتضایی خودرویی بر مبنای استاندارد IEEE 802.11p شبیه‌سازی شده است.

ساختار این مقاله به‌صورت زیر سازمان‌دهی شده است. در بخش دوم مدل سیستم و فرمول‌بندی مسئله در قالب مدل بازی امنیتی ارائه‌شده است. در بخش سوم مقاله، روش حل مسئله در قالب یافتن نقطه تعادل نش موردبحث قرارگرفته است. در بخش چهارم بستر شبیه‌سازی شبکه اقتضایی خودرویی بررسی و نتایج ارزیابی کارایی الگوریتم ارائه شده است. نتیجه‌گیری و کارهای آتی نیز در بخش پنجم گنجانده شده است.

۲- مدل سیستم و فرمول‌بندی

یک لینک مخابراتی در شکل ۱ در نظر گرفته شده است که در آن فرستنده اصلی (سارا) داده خود را به‌سمت گیرنده (مریم) که می‌تواند یک ایستگاه ثابت یا متحرک باشد، می‌فرستد. در این مدل یک مهاجم (علی) می‌تواند به یکی از دو شیوه تخریب کانال ارتباطی فرستنده-گیرنده اصلی و یا شنود اطلاعات محرمانه کانال، روی سیستم اثر بگذارد. در مدل پیشنهادی، سارا به‌عنوان فرستنده اصلی در مبدأ ارسال پیام تصمیم دارد با مریم که در ایستگاه مقصد است به‌طور ایمن ارتباط برقرار کند و این در حالی است که علی به‌عنوان مهاجم تصمیم دارد که به این ارتباط آسیب وارد نماید. طبق فرض، علی نمی‌تواند هر دو عمل شنود و تخریب کانال را به‌طور همزمان انجام دهد. هر دو گره‌های فرستنده (سارا و علی) از OFDM جهت ارسال داده روی کانال‌های پهن باند استفاده می‌کنند، ازاین‌رو مدل ارتباطی چندکانالهٔ در نظر گرفته شده است. سارا توان انتقالش را جهت ارسال داده به‌سمت مریم بین زیرکانال‌های تقسیم فرکانسی متعامد توزیع می‌کند. به همین صورت در مورد تخریب کانال، علی توانش را بین زیرکانال‌های کانال پهن باند با هدف کاهش ظرفیت ایمن لینک اصلی سارا- مریم توزیع می‌کند.



شکل ۱: رابطه بین سارا، مریم و علی

در این مدل هر یک از کانال‌های ارتباطی بین گره‌ها (هر جفت گره) دارای محوکنندگی انتخابگر فرکانس و نویز جمع‌شونده سفید گوسی هستند. کل عرض باند به N_{sub} زیرکانال مجزا تقسیم می‌شود، به‌طوری‌که در هر زیرکانال زیرحامل جداگانه‌ای برای انتقال داده وجود دارد. بهره محوکنندگی زیرکانال‌های بین سارا و مریم با ضرایب h_i نمایش داده شده است، به‌طوری‌که $i \in [1, N_{sub}]$ است. در حالت شنود کردن بهره محوکنندگی زیرکانال‌های بین سارا و علی با ضرایب he_i نمایش داده شده است، به‌طوری‌که $i \in [1, N_{sub}]$ است. به‌علاوه در مود تخریب کردن، بهره محوکنندگی زیرکانال‌های بین علی و مریم با ضرایب g_i نشان داده شده است، به‌طوری‌که $i \in [1, N_{sub}]$ است. علی می‌تواند بین این دو حالت کاری با احتمال ρ به حالت شنود و با احتمال $(1-\rho)$ به حالت تخریب کانال تغییر وضعیت دهد. درواقع $((\rho, (1-\rho))$ یک استراتژی ترکیبی با استفاده از دو استراتژی خالص احتمال شنود و احتمال تخریب است که مجموع آن‌ها برابر یک است. استراتژی‌های خالص سارا در N_{sub} زیرحامل بر اساس سطوح توان زیرحامل‌ها مطابق رابطه (۱) تعریف شده است.

$$T = \left(T_1, T_2, \ldots, T_{N_{sub}} \right) \quad (۱)$$

به‌طوری‌که به‌ازای $i \in [1, N_{sub}]$، $T_i \geq 0$ است که این پارامتر سطح توان زیر حامل i ام را نشان می‌دهد. همچنین قید متوسط توان فرستنده به‌صورت $\sum_{i=1}^{N_{sub}} T_i \leq \bar{T}$ است که در آن $\bar{T} > 0$ اعمال شده است. پارامتر $\bar{T}$ نیز حداکثر توان متوسط تعریف‌شده برای سارا است.

به‌طور مشابه استراتژی‌های خالص علی در N_{sub} زیرحامل مطابق رابطه (۲) مشخص شده است.

$$J=\left(J_1,J_2,\ldots,J_{N_{sub}}\right) \quad (۲)$$

که در آن $i\in[1,N_{sub}]$ و $J_i\geq 0$ سطح توانی است که علی به زیرکانال i ام اختصاص می‌دهد. با فرض این‌که علی دارای حداکثر توان متوسط $\bar{J}>0$ باشد، آنگاه رابطه $\sum_{i=1}^{N_{sub}}J_i\leq \bar{J}$ برقرار است.

در این مقاله توابع سود[۵] بر اساس رابطه نرخ بیت ایمن شانون با لحاظ نمودن هزینه کرد توان ارسالی به‌ترتیب برای گره‌های سارا و علی با کمک روابط (۳) و (۴) تعریف شده است.

$$P_T(T,J)=\rho\sum_{i=1}^{N_{sub}}\left(\ln\left(1+\frac{h_i T_i}{N_i^o}\right)-\ln\left(1+\frac{he_i T_i}{Ne_i^o}\right)\right)+(1-\rho)\sum_{i=1}^{N_{sub}}\ln\left(1+\frac{h_i T_i}{g_i J_i+N_i^o}\right)-c_T\sum_{i=1}^{N_{sub}}T_i \quad (۳)$$

$$P_J(T,J)=\rho\sum_{i=1}^{N_{sub}}\ln\left(1+\frac{he_i T_i}{Ne_i^o}\right)-(1-\rho)\sum_{i=1}^{N_{sub}}\ln\left(1+\frac{h_i T_i}{g_i J_i+N_i^o}\right)-c_J\sum_{i=1}^{N_{sub}}J_i \quad (۴)$$

در روابط فوق N_i^o سطح توان نویز کانال اصلی و Ne_i^o سطح توان نویز کانال شنودگر در زیرکانال i ام هستند، به‌طوری‌که فرض بر این گرفته شده است که در رابطه (۵) صدق می‌کنند.

$$\frac{h_i}{N_i^o}\geq\frac{he_i}{Ne_i^o} \quad (۵)$$

پارامترهای c_T و c_J به‌ترتیب هزینه مصرف توان ارسالی برای گره‌های سارا و علی هستند. در رابطه (۳)، جمله اول همان ظرفیت ایمن شانون در حضور شنودگر، جمله دوم ظرفیت شانون در حضور تداخلگر و جمله سوم متوسط هزینه توانی که برای انتقال داده توسط سارا پرداخت می‌شود، تعریف می‌شود. همچنین در رابطه (۴)، جمله اول مقدار ظرفیت شنود، جمله دوم ظرفیت شانون در حضور تداخلگر و جمله سوم متوسط هزینه حمله برای علی تعریف می‌شود. در بخش بعدی مقاله، بر اساس توابع سود تعریف‌شده یک بازی از نوع مجموع غیرصفر که دارای خاصیت زیر است، طبق رابطه (۶) تعریف شده است.

$$P_T(T,J)+P_J(T,J)\neq 0 \quad (۶)$$

باید توجه نمود که در یک بازی از نوع مجموع غیرصفر بازیکنان می‌توانند استراتژی‌های خود را به‌گونه‌ای تنظیم نمایند که نتیجه بازی برای طرفین سودمند باشد.

۳- حل مسئله و یافتن نقطه تعادل نش

در مدل بازی مجموع غیرصفر درنظرگرفته‌شده بازیکنان به‌صورت عقلانی برای رسیدن به بیشترین منفعت، استراتژی‌های کنترل توان خود را انتخاب می‌کنند. بر این اساس نقطه تعادل نش طبق روابط (۷) و (۸) تعریف شده است.

$$P_T\left(T,\ J^*\right)\leq P_T\left(T^*,\ J^*\right),\ T\in S_T \quad (۷)$$

$$P_J\left(T^*,\ J\right)\leq P_J\left(T^*,J^*\right),\ \ J\in S_J \quad (۸)$$

طبق تعریف بالا، S_T و S_J به‌ترتیب مجموعه استراتژی‌های خالص برای سارا و علی هستند. نقطه $\left(T^*,\ J^*\right)$ نیز همان نقطه تعادل نش است که از دیدگاه دست‌یابی به بیشترین تابع سود، وضعیت بهینه را نشان می‌دهد. با در نظر گرفتن رابطه (۵) ظرفیت ایمن مثبت شده و مشتق دوم توابع سود نیز منفی می‌شوند. با دو بار مشتق‌گیری نشان داده شده است که:

$$\frac{\partial^2 P_T(T,J)}{\partial {T_i}^2}=\frac{-\rho\, h_i^2}{\left(h_i T_i+N_i^o\right)^2}+\frac{\rho\, he_i^2}{\left(he_i T_i+Ne_i^o\right)^2}-\frac{(1-\rho)h_i^2}{\left(h_i T_i+g_i J_i+N_i^o\right)^2}<0 \quad (۹)$$

$$\frac{\partial^2 P_J(T,J)}{\partial {J_i}^2}=-\frac{\left(T_i {g_i}^2 h_i\right)\left(h_i T_i+2g_i J_i+2N_i^o\right)}{\left(h_i T_i+g_i J_i+N_i^o\right)^2\left(g_i J_i+N_i^o\right)^2}<0 \quad (۱۰)$$

به‌دلیل مثبت بودن پارامتر احتمال ρ و وجود عبارت‌های توان دوم، جمله دوم رابطه (۹) مثبت است. همچنین به استناد نامساوی (۵) می‌توان گفت جمله اول رابطه (۹) از جمله دوم آن بزرگ‌تر است و به همین دلیل به‌خاطر علامت منفی جمله اول، جمع این دو جمله منفی خواهد بود. با توجه به منفی بودن علامت جمله سوم $\left(1-\rho\leq 0\right)$ می‌توان نتیجه گرفت که علامت رابطه (۹) همواره منفی است. با استدلالی مشابه منفی بودن رابطه (۱۰) نیز قابل توجیه است. با توجه به منفی بودن مشتق دوم در روابط (۹) و (۱۰)، می‌توان گفت که تابع $P_T\left(T,J\right)$ در T و تابع $P_J\left(T,J\right)$ در J مقعر هستند. در ادامه با توجه به ویژگی مقعر بودن توابع سود، از شرایط KKT[۶] برای دست‌یابی به نقطه تعادل نش استفاده شده است [۱۵].

قضیه۱: نقطه $\left(T^*,J^*\right)$ یک نقطه تعادل نش است، اگر و فقط اگر ثابت‌های مثبت α و β وجود داشته باشند که در معادله‌های (۱۱) و (۱۲) صدق کنند.

$$\frac{\partial P_T\left(T^*,J^*\right)}{\partial T_i}=\rho\left(\frac{h_i}{h_i T_i^*+N_i^o}\frac{he_i}{he_i T_i^*+Ne_i^o}\right)+(1-\rho)\frac{h_i}{h_i T_i^*+g_i J_i^*+N_i^o} \quad (۱۱)$$

$$-c_T\begin{cases}=\alpha & for\ T_i^*>0\\ \leq\alpha & for\ T_i^*=0\end{cases}$$

$$\frac{\partial P_J\left(T^*,J^*\right)}{\partial J_i}=\frac{(1-\rho)g_i h_i T_i^*}{(g_i J_i^*+h_i T_i^*+N_i^o)\left(g_i J_i^*+N_i^o\right)} \quad (۱۲)$$

$$-c_J \begin{cases} =\beta & for\ J_i^*>0 \\ \le\beta & for\ J_i^*=0 \end{cases}$$

به‌طوری‌که داریم:

$$\begin{cases} \alpha\ge 0 & for \sum_{i=1}^{n} T_i^* = \overline{T}, \\ \alpha = 0 & for \sum_{i=1}^{n} T_i^* < \overline{T}. \end{cases} \quad (۱۳)$$

$$\begin{cases} \beta\ge 0 & for \sum_{i=1}^{n} J_i^* = \overline{J}, \\ \beta = 0 & for \sum_{i=1}^{n} J_i^* < \overline{J}. \end{cases} \quad (۱۴)$$

نتایج قضیه ۱ به‌شکل زیر قابل تفسیر است. با توجه به تعریف نقطه تعادل نش در روابط (۷) و (۸)، چون نقطه تعادل نش بالاترین مقدار سود را معرفی می‌کند، برای رسیدن به آن مقدار باید از مشتق اول (گرادیان) با شیب مثبت استفاده کرد. درنتیجه برای مقادیر $J_i^*>0$ و $T_i^*>0$ مشتق اول برابر یک مثبت کوچک فرض می‌شود و البته مقادیر ثابت‌های مثبت α و β از طریق قیود توان متوسط فرستنده اصلی و مهاجم به‌دست خواهند آمد.

در ادامه عملکرد سیستم برای فرستنده و مهاجم در چهار حالت ممکن زیر بررسی می‌شود:

حالت اول: $J_i^*=0$ و $T_i^*=0$

حالت دوم: $J_i^*>0$ و $T_i^*=0$

حالت سوم: $J_i^*>0$ و $T_i^*>0$

حالت چهارم: $J_i^*=0$ و $T_i^*>0$

در حالت اول طبق روابط (۱۱)، (۱۲)، (۱۳) و (۱۴)، بعد از ساده‌سازی در مرحله آخر روابط (۱۵) و (۱۶) حاصل شده است.

$$\rho\left(\frac{h_i}{N_i^o}-\frac{he_i}{Ne_i^o}\right)+(1-\rho)\frac{h_i}{N_i^o}-c_T\le\alpha^* \quad (۱۵)$$

$$-c_J\le\beta^* \quad (۱۶)$$

بنابراین، باید شرایط (۱۷) و (۱۸) برقرار باشد.

$$c_T\ge-\frac{\rho\, he_i}{Ne_i^o}+\frac{h_i}{N_i^o}-\alpha^* \quad (۱۷)$$

$$c_J\ge-\beta^* \quad (۱۸)$$

این بدان معنی است که وقتی هزینه انتقال داده بیشتر از مقادیر فوق شود، فرستنده و مهاجم توانی را برای ارسال اطلاعات مصرف نمی‌کنند.

در حالت دوم نیز بعد از ساده‌سازی روابط (۱۹) و (۲۰) حاصل شده است.

$$\rho\left(\frac{h_i}{N_i^o}-\frac{he_i}{Ne_i^o}\right)+(1-\rho)\frac{h_i}{g_i J_i^*+N_i^o}-c_T\le\alpha^* \quad (۱۹)$$

$$-c_J=\beta^* \quad (۲۰)$$

با منفی شدن β^* می‌توان نتیجه گرفت که این حالت غیرقابل‌پذیرش است. البته زمانی که فرستنده اطلاعاتی را نمی‌فرستد، منطقی است که گیرنده هم توانی را صرف تخریب کانال اطلاعاتی نکند. درواقع در این حالت بین بازیکن‌ها بازی‌ای شکل نمی‌گیرد.

در حالت سوم یک دستگاه معادله غیرخطی دو معادله- دو مجهولی طبق روابط (۲۱) و (۲۲) به‌دست آمده است.

$$\rho\left(\frac{h_i}{h_i T_i^*+N_i^o}-\frac{he_i}{he_i T_i^*+Ne_i^o}\right)+(1-\rho)\frac{h_i}{h_i T_i^*+g_i J_i^*+N_i^o}-c_T=\alpha^* \quad (۲۱)$$

$$\frac{g_i h_i T_i^*}{(g_i J_i^*+h_i T_i^*+N_i^o)\left(g_i J_i^*+N_i^o\right)}-c_J=\beta^* \quad (۲۲)$$

پارامترهای مجهول در این سیستم معادله، J_i^* و T_i^* هستند. متأسفانه به‌دلیل پیچیدگی سیستم معادله‌های مذکور، ارائه یک فرم بسته جواب برحسب α^* و β^* عملی نیست. بنابراین در ادامه، پارامترهای J_i^* و T_i^* در سیستم معادله فوق با استفاده از روش‌های عددی (به‌عنوان‌مثال در MATLAB) به‌دست آمده است.

در حالت چهارم نیز بعد از ساده‌سازی روابط (۲۳) و (۲۴) حاصل شده است.

$$\rho\left(\frac{h_i}{h_i T_i^*+N_i^o}-\frac{he_i}{he_i T_i^*+Ne_i^o}\right)+(1-\rho)\frac{h_i}{h_i T_i^*+N_i^o}-c_T=\alpha^* \quad (۲۳)$$

$$(1-\rho)\frac{g_i h_i T_i^*}{\left(h_i T_i^*+N_i^o\right)\left(N_i^o\right)}-c_J\le\beta^* \quad (۲۴)$$

در این حالت طبق رابطه (۲۳) یک معادله غیرخطی ایجاد شده است که پارامتر مجهول در این معادله T_i^* است. این معادله غیرخطی به‌کمک روش‌های عددی به‌سادگی حل شده است. البته جواب به‌دست‌آمده باید در نامعادله (۲۴) صدق کند.

با تحلیل چهار حالت ذکرشده می‌توان نتیجه گرفت که توان فرستنده در دو حالت و توان مهاجم در یک حالت از چهار حالت تعریف‌شده مقادیر غیرصفر خواهند داشت.

البته لازم به‌ذکر است که جواب‌های پارامتریک برای هر یک از حالت‌های فوق باید در معادله‌های قید توان متوسط که به‌فرم معادله‌های زیر تشکیل شده است، صدق نمایند:

$$C_T(\alpha,\beta)=\sum_{i=1}^{N_{sub}} T_i(\alpha,\beta)\le \bar{T} \quad (۲۵)$$

$$C_J(\alpha,\beta)=\sum_{i=1}^{N_{sub}} J_i(\alpha,\beta)\le \bar{J} \quad (۲۶)$$

در روابط (۲۵) و (۲۶) به‌ترتیب معادله قید توان برای فرستنده و مهاجم نشان داده شده است. در بخش بعدی، الگوریتم طراحی‌شده برای حصول نقطه تعادل نش معرفی شده است.

۳-۱- الگوریتم یافتن نقطه تعادل نش

در شکل ۲ الگوریتم مراحل استخراج نقطه تعادل نش نمایش داده شده است. در این الگوریتم، پارامترهای مجهول α_{1T} و α_{1J} و α_{2J} به‌ترتیب ریشه‌های معادله‌های $C_T(\alpha_{1T},0)=\bar{T}$، $C_J(\alpha_{1J},0)=\bar{J}$ و $C_J(0,\alpha_{2J})=\bar{J}$ هستند. همچنین در آخرین بلوک الگوریتم با پیمودن پنج گام زیر نتیجه نهایی حاصل می‌شود:

گام اول: پارامتر α_0 برابر صفر و پارامتر α_1 برابر α_{1J} مقداردهی می‌شود.

گام دوم: پارامترهای مجهول دو معادله $C_J(\alpha_0,\beta_0)=\bar{J}$ و $C_J(\alpha_1,\beta_1)=\bar{J}$ که به‌ترتیب β_0 و β_1 هستند، به‌دست می‌آید.

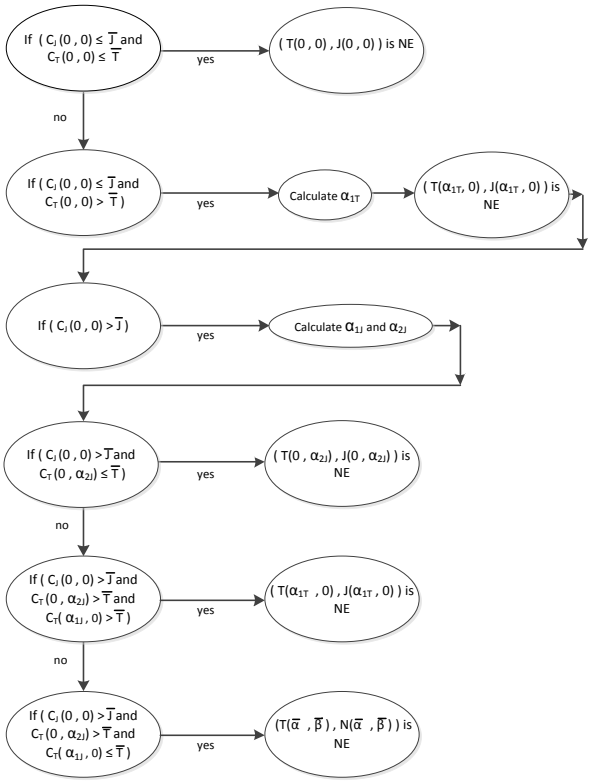
گام سوم: مقادیر $\bar{\alpha}=\frac{\alpha_0+\alpha_1}{2}$ و $\bar{\beta}=\frac{\beta_0+\beta_1}{2}$ محاسبه می‌شوند.

گام چهارم: حال معادله $C_J(\bar{\alpha},\bar{\beta})=\bar{J}$ برای یافتن نقطه $(\bar{\alpha},\bar{\beta})$ انجام می‌شود.

گام پنجم: نقطه $(\bar{\alpha},\bar{\beta})$ همان نقطه بهینه است که با استفاده از آن، نقطه تعادل نش به‌صورت $\left(T(\bar{\alpha},\bar{\beta}), J(\bar{\alpha},\bar{\beta})\right)$ به‌دست می‌آید.

لازم به‌ذکر است برای یافتن ریشه‌های معادله‌های غیرخطی فوق از روش عددی دوبخشی[۷] استفاده شده است. نقطه ابتدایی بازه در روش دوبخشی صفر است، زیرا $\alpha\ge 0$ و $\beta\ge 0$ است. نقطه انتهایی بازه بر اساس شرایط حاکم بر توان‌های فرستنده و تخریب‌گر کانال که دارای قید توان هستند به‌دست می‌آید. درواقع بازه انتهایی مقادیر پارامترهای α و β باید به‌اندازه‌ای باشد که مجموع توان‌های بهینه فرستنده و مهاجم در هر زیرکانال به‌ترتیب برابر یا کمتر از $\bar{T}$ و $\bar{J}$ باشند.

به‌دلیل پیچیدگی معادله‌ها، یک فرم بسته ریاضی برای توان‌های زیرحامل‌ها قابل حصول نیست. بنابراین نمی‌توانیم به‌صورت تحلیلی یکتا بودن جواب الگوریتم شکل ۲ را نشان دهیم. بااین‌وجود با کمک نتایج عددی که در بخش بعدی ارائه شده است در تمام موارد آزمایش الگوریتم موردنظر، وجود جواب و نیز یکتایی آن قابل‌مشاهده است.



شکل ۲: الگوریتم یافتن نقطه تعادل نش

۴- شبیه‌سازی

در این بخش نتایج ارزیابی عملکرد مکانیزم تدافعی طراحی‌شده برای یک لینک ارتباطی فرستنده-گیرنده در شبکه اقتضایی خودرویی بر مبنای استاندارد IEEE 802.11p ارائه شده است.

۴-۱- توصیف تنظیمات استفاده‌شده در آزمایش‌ها

جدول ۱ مقادیر پارامترهای به‌کاررفته در لایه فیزیکی شبکه اقتضایی خودرویی را نشان می‌دهد. در شبیه‌سازی انجام‌شده ضرایب کانال فیدینگ با توزیع رایلی به تعداد مسیرهای موجود در کانال (L_C) تولید شده و سپس اثر محوکنندگی کانال روی زیرحامل‌ها به‌صورت بهره توان محاسبه شده است. در [۱۶] نشان داده شده است که مقدار پاسخ فرکانسی در زیرحامل iام طبق رابطه (۲۷) به‌دست می‌آید.

$$H(i)=\sum_{k=0}^{L_c-1} h(k).e^{-j2\pi\frac{ik}{N_{sub}}} \quad (۲۷)$$

در این رابطه پارامتر N_{sub} تعداد کل زیرحامل‌ها را نشان می‌دهد و دامنه تغییر i از صفر تا $N_{sub}-1$ است. همچنین ضریب $h(k)$ مقدار پاسخ ضربه کانال فیدینگ روی مسیر kام است. این ضرایب در کانال فیدینگ شبکه‌های اقتضایی خودرویی در هر بازه زمانی خیلی کوچک تغییر می‌کنند و ثابت نیستند. به‌سادگی می‌توان نشان داد که بهره توان محوکنندگی روی زیرحامل iام برابر $|H(i)|^2$ است که دارای توزیع تصادفی رایلی است [۱۶].

همچنین در یک کانال سیار روابط زیر تعریف می‌شود:

$$f_D = \frac{v}{c/f_c}.\cos\theta \quad (۲۸)$$

$$L_c = \frac{\tau_{max}}{T_{sample}} \quad (۲۹)$$

$$T_{sample} = \frac{1}{2B} \quad (۳۰)$$

در رابطه (۲۸)، پارامتر f_D فرکانس داپلر ناشی از حرکت خودرو، v سرعت حرکت خودرو، f_c فرکانس حامل مدولاسیون، c سرعت انتشار نور در فضا و θ زاویه انتشار امواج از مبدأ نسبت به خودرو متحرک دیگر (یا یک ایستگاه مقصد ثابت) را نشان می‌دهد. رابطه (۲۹) نیز تعداد مسیرهای موجود در کانال فیدینگ را به پارامتر T_{sample} (یعنی زمان نمونه‌برداری از سیگنال پیوسته ورودی به کانال) و τ_{max} (یعنی ماکزیمم زمان گسترش تأخیر کانال) ارتباط می‌دهد. پارامتر T_{sample} نیز بر اساس رابطه (۳۰) به پهنای باند کانال یعنی پارامتر B ارتباط دارد.

به‌علاوه، پارامترهای نویز کانال برای زیر حامل $i \in [1,\ N_{sub}]$ برابر $N_i^o = ۰/۱$ و $Ne_i^o = ۰/۱$ در نظر گرفته شده است. سایر پارامترهای به‌کاررفته در شبیه‌سازی عبارت‌اند از: وزن‌های مربوط به هزینه‌کرد توان $c_T = c_J = ۰/۱$، مجموع توان‌های مصرف‌شده توسط فرستنده و مهاجم در تمامی زیرکانال‌ها که برابر $\bar{T} = \bar{J} = ۱$ است.

جدول ۱: مقادیر پارامترها در محیط اقتضایی خودرویی [۱۷]

پارامترهای لایه PHY	مقادیر در استاندارد IEEE 802.11p
دامنه فرکانسی	۵/۸۵۰-۵/۹۲۵GHZ
f_c	۲/۴GHZ
B	۱۰MHz
سرعت ارسال داده	۳، ۴/۵، ۶، ۹، ۱۲، ۱۸، ۲۴، ۲۷(Mbits/sec)
N_{sub}	۵۲
زمان سمبل OFDM	۸ μsec
L_c	۸
$\tau_{\max}$	۳۰۰nsec
T_{sample}	۵۰nsec
f_D	۱۰۰Hz
تعداد سمبل OFDM	۲۰۰

همچنین برای اهداف نمایش قدرت مهاجم و فرستنده در کانال، از نسبت‌های تعریف‌شده (۳۱) و (۳۲) استفاده شده است.

$$K_1 = \frac{E\left[h_i\right]}{E\left[he_i\right]} \quad (۳۱)$$

$$K_2 = \frac{E\left[h_i\right]}{E\left[g_i\right]} \quad (۳۲)$$

به‌عنوان‌مثال اگر متوسط بهره توان کانال فرستنده اصلی ثابت فرض شود، آنگاه با کاهش نسبت‌های K_1 و K_2، قدرت مهاجم در کانال افزایش پیدا می‌کند. در شبیه‌سازی صورت‌گرفته متوسط بهره توان کانال فرستنده اصلی واحد فرض شده است. درواقع با تغییر نسبت‌های K_1 و K_2، متوسط بهره‌های توان کانال‌های مهاجم-فرستنده و مهاجم-گیرنده به‌صورت روابط (۳۳)، (۳۴) و (۳۵) محاسبه شده است.

$$E\left[h_i\right] = 1 \quad (۳۳)$$

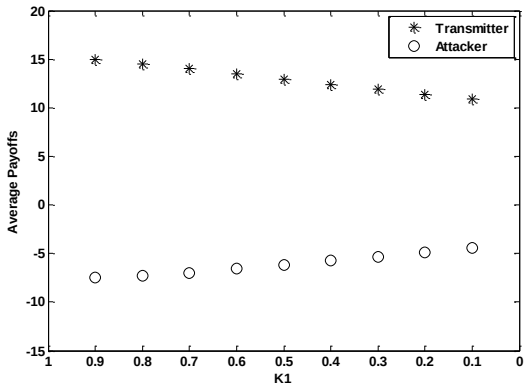
$$E\left[he_i\right] = \frac{1}{K_1} \quad (۳۴)$$

$$E\left[g_i\right] = \frac{1}{K_2} \quad (۳۵)$$

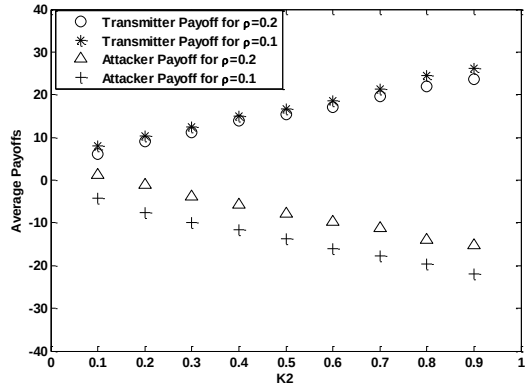
۴-۲- توصیف نتایج آزمایش‌ها

برای محاسبه تابع سود در گره‌های فرستنده و مهاجم، فرض بر این است که فرستنده ۲۰۰ نمونه OFDM در کانال ارسال می‌کند و برای هر زمان نمونه، مقادیر تابع سود محاسبه شده است و در انتها متوسط آن‌ها روی زمان ۲۰۰ نمونه به‌عنوان مقدار نهایی گزارش شده است (مقدار متوسط تابع سود).

در آزمایش اول، فرض می‌کنیم که مهاجم بسیار به گیرنده نزدیک است، ازاین‌رو $E\left[g_i\right] \approx ۱$ در نظر گرفته شده است. در شکل ۳ توابع سود برحسب پارامتر K_1 در بازه (۱ و ۰) و احتمال شنود با مقدار ۰/۲ ترسیم شده است. همان‌طور که انتظار می‌رود، با کاهش مقدار پارامتر K_1 بهره کانال شنودگر افزایش می‌یابد درحالی‌که بهره کانال فرستنده و تخریب‌گر ثابت می‌ماند. درنتیجه متوسط تابع سود برای شنودگر افزایش و برای فرستنده کاهش خواهند یافت.



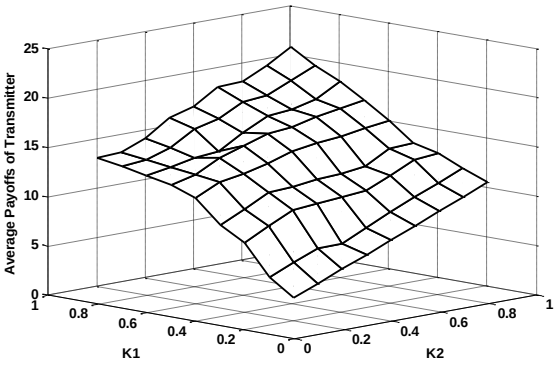
شکل ۳: مقدار متوسط تابع سود برای فرستنده و مهاجم برحسب پارامتر K_1 به‌ازای $\rho = ۰/۲$.



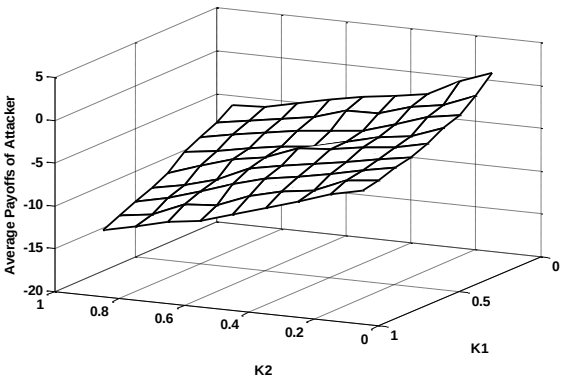
شکل ۴: مقایسه مقدار متوسط تابع سود بازیکن‌ها برحسب پارامتر K_2 در دو حالت $\rho =$ ۰/۱ و $\rho =$ ۰/۲.

در شکل ۴ فرض بر این است که مهاجم به فرستنده بسیار نزدیک است، ازاین‌رو $E\left[he_i\right] \approx$ ۱ در نظر گرفته شده است. با کاهش مقدار پارامتر K_2 در بازه (۱ و ۰) بهره توان کانال تخریب‌گر افزایش می‌یابد. بنابراین مقدار سود مهاجم زیاد شده است. در این شکل نتایج برای دو مقدار احتمال شنود برابر ۰/۱ و ۰/۲ ترسیم شده است. نتیجه قابل‌توجه در شکل ترسیم‌شده این است که با افزایش احتمال شنود، متوسط سود برای فرستنده اصلی کمتر و برای مهاجم بیشتر خواهد شد. به‌بیان‌دیگر نتیجه بازی بین فرستنده و مهاجم در شرایطی که مهاجم استفاده از حالت تخریب کانال را کاهش دهد (با کاهش ظرفیت ایمن کانال) سود کمتری را نصیب فرستنده اصلی می‌نماید.

در آزمایش سوم، هر دو پارامتر K_1 و K_2 به‌طور هم‌زمان تغییر می‌کنند و برای مقادیر بین (۱ و ۰) متوسط مقدار سود در شکل‌های ۵ و ۶ به‌ترتیب برای فرستنده اصلی و مهاجم ترسیم شده است. همان‌طور که در شکل ۵ دیده می‌شود، با کاهش پارامترهای K_1 و K_2 به‌طور هم‌زمان سود فرستنده اصلی کاهش چشم‌گیری پیدا می‌کند. دلیل این است که وضعیت کانال‌های شنود و تخریب به‌صورت توأم بهبود یافته است، بنابراین مهاجم در وضعیت برتری قرار گرفته است.

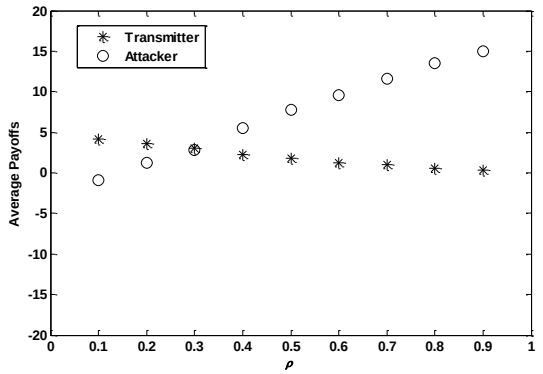


شکل ۵: نمایش افزایش مقدار متوسط سود برای فرستنده با افزایش K_1 و K_2 به‌ازای $\rho =$ ۰/۲.

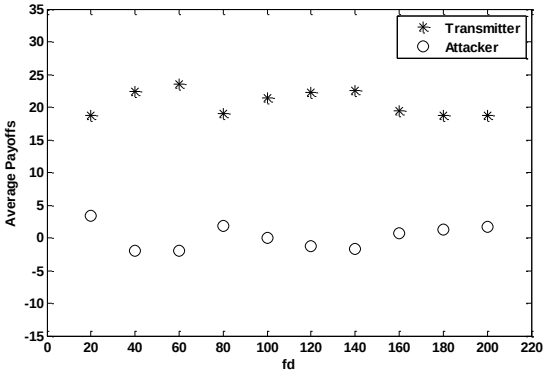


شکل ۶: نمایش مقدار متوسط سود برای مهاجم به‌ازای مقادیر مختلف K_1 و K_2 به‌ازای $\rho =$ ۰/۲.

در آزمایش پنجم پارامترهای K_1 و K_2 برابر مقدار ۰/۱ فرض شده است و با تغییر احتمال شنود، متوسط مقدار تابع سود برای دو بازیکن ترسیم شده است. در شکل ۷ که نتیجه حاصل از این آزمایش دیده می‌شود، با افزایش مقدار پارامتر ρ (احتمال شنود) مقدار متوسط سود مهاجم از یک مقدار منفی به یک مقدار مثبت تغییر می‌کند، ولی متوسط سود برای فرستنده کاهش می‌یابد. درواقع با افزایش احتمال شنود، قسمت مربوط به تخریب‌کننده کانال در تابع سود هر دو بازیکن (روابط (۳) و (۴)) به‌حدی تضعیف می‌شود که به‌تدریج اثر تخریب‌کننده کم و در نتیجه هزینه ناشی از تخریب حذف می‌شود و بیشترین تأثیر توسط شنودگر در کانال اتفاق می‌افتد (کاهش ظرفیت ایمن کانال اصلی اتفاق می‌افتد). این در حالی است که هزینه‌ای هم مشمول حال شنودگر نمی‌شود. زیرا شنودگر نیاز به صرف توان برای شنود کردن در کانال ندارد. بنابراین می‌توان ادعا کرد که مقدار متوسط سود برای مهاجم در مقادیر ρ بالاتر بیشتر است، زیرا در این نقطه به‌طور کامل عمل شنود صورت می‌گیرد و عملکرد مهاجم مشمول هیچ هزینه‌ای نیست.



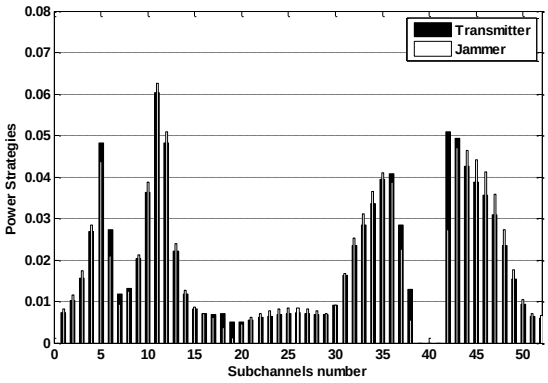
شکل ۷: نمایش مقدار متوسط تابع سود برای فرستنده و مهاجم برحسب پارامتر ρ به‌ازای $K_1 =$ ۰/۱ و $K_2 =$ ۰/۲.



شکل ۸: نمایش مقدار متوسط سود برای فرستنده و مهاجم برحسب فرکانس داپلر به‌ازای $\rho =$ ۰/۵، $K_1 =$ ۱ و $K_2 =$ ۱.

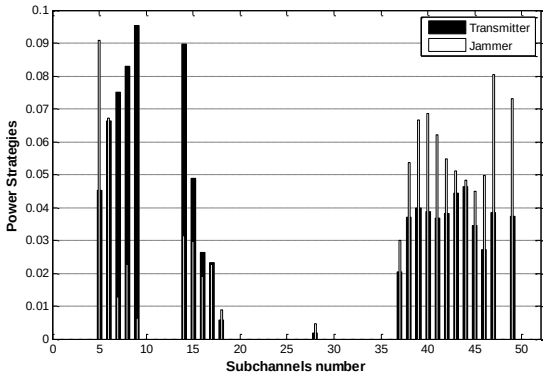
در شکل ۸، تغییر مقدار متوسط نتیجه نهایی دو بازیکن برحسب فرکانس داپلر رسم شده است. با توجه به این‌که تابع سود مورداستفاده در این مقاله به ضریب همبستگی بین ضرایب بهره کانال (به‌عنوان ممان مرتبه دوم محوکنندگی کانال) ارتباط مستقیم ندارد، بنابراین تغییر معنی‌دار افزایشی و یا کاهشی در شکل ۸ دیده نمی‌شود. بنابراین به نظر می‌رسد که توابع سود درنظرگرفته‌شده در این مقاله بیشتر برای سناریوهایی که در آن‌ها سرعت نسبی بین گره‌ها در شبکه بالا باشد (متناظر مقادیر بزرگ پارامتر f_D در جدول ۱)، مناسب هستند. به‌طور طبیعی در چنین سناریوهایی می‌توان فرض نمود که ضرایب محوکنندگی کانال در زمان‌های نمونه مجاور ناهمبسته خواهند بود، بنابراین می‌توان اثر ممان دوم در تابع سود را نادیده گرفت.

در آزمایش آخر، دو نمونه نحوه تخصیص توان بین زیرکانال‌ها توسط فرستنده و مهاجم در شکل‌های ۹ و ۱۰ نمایش داده شده است. در شکل ۹ پارامترهای K_1 و K_2 برابر مقدار ۰/۱ و احتمال شنود برابر صفر فرض شده است، یعنی مهاجم فقط عمل تخریب کانال را انجام می‌دهد. این سناریو متناظر یک مهاجم تخریب‌گر قدرتمند است. با توجه به شکل ۹ می‌توان گفت، اگرچه فرستنده سعی می‌کند از تمامی۵۲ زیرکانال برای ارسال اطلاعات استفاده کند بااین‌وجود ممکن است که در تعداد محدودی زیرکانال هیچ توانی را صرف ارسال اطلاعات نکند.



شکل ۹: نمایش تخصیص توان در۵۲ زیرکانال با احتمال شنود صفر به‌ازای $K_1 =$ ۰/۱ و $K_2 =$ ۰/۱.

در نمونه دوم که در شکل ۱۰ نشان داده شده است، پارامترهای K_1 و K_2 برابر مقدار ۰/۵ و احتمال شنود نیز برابر ۰/۵ فرض شده است. این سناریو متناظر یک مهاجم ضعیف است. همان‌گونه که در شکل دیده می‌شود در این حالت، فرستنده کل توان خود را روی تعداد انتخاب‌شده‌ای از زیرکانال‌ها (زیرکانال‌های با بهره بالاتر) توزیع می‌کند. ازاین‌جهت به الگوریتم تخصیص توان بهینه Water-filling در ادبیات مخابرات سیار شباهت دارد [۱۸].



شکل ۱۰: نمایش تخصیص توان در۵۲ زیرکانال به‌ازای $\rho =$ ۰/۵، $K_1 =$ ۰/۵ و $K_2 =$ ۰/۵.

۵- نتیجه

در این مقاله، عملکرد دفاعی یک سیستم مخابراتی نقطه‌به‌نقطه بر اساس کنترل توان به‌نحوی موردمطالعه قرار گرفته است که در آن، یک مهاجم بتواند روی ارسال اطلاعات در یکی از حالت‌های شنود و یا تخریب کانال اثر بگذارد. برای طراحی مکانیسم تدافعی در چارچوب نظریه بازی‌ها از یک مدل بازی مجموع غیرصفر برای تخصیص توان بهینه در بین زیرکانال‌های متعامد تسهیم تقسیم فرکانسی استفاده شده است. در مدل بازی درنظرگرفته‌شده، هدف فرستنده اصلی (به‌عنوان بازیکن اول) این است که بتواند حداکثر بازدهی در اطلاعات ارسالی خود به گیرنده ایجاد کند و هدف مهاجم (به‌عنوان بازیکن دوم) نیز کاهش بازدهی فرستنده است. در ادامه معادله‌های ریاضی لازم برای استخراج توان‌های بهینه دو بازیکن در نقطه تعادل نش به‌دست آمده است. به‌علاوه الگوریتمی برای انجام محاسبه‌های عددی استخراج نقطه تعادل نش ارائه شده است.

برای ارزیابی کارایی الگوریتم ارائه‌شده یک کانال ارتباطی در شبکه اقتضایی خودرویی با پارامترهای انتخاب‌شده از استاندارد IEEE 802.11p، مورد شبیه‌سازی قرار گرفته است. در این راستا با انجام آزمایش‌های گوناگون عملکرد فرستنده و مهاجم در شرایط مختلف کانال محوکننده مورد تحلیل قرار گرفته است. نتایج به‌دست‌آمده نشان داده است که در شرایطی که اطلاعات سیستم به‌طور کامل در اختیار فرستنده و مهاجم قرار دارد، مهاجم می‌تواند روی ظرفیت ایمن کانال فیزیکی (فرستنده-گیرنده اصلی) اثرهای مخربی را ایجاد کند. درعین‌حال فرستنده اصلی نیز قادر است که با توزیع مناسب توان

ارسالی در بین زیرحامل‌های خود، اثرهای تهاجم را به حداقل ممکن برساند. به‌طور حتم چنین مکانیسم تدافعی اگر به‌همراه مکانیسم‌های مبتنی بر رمزنگاری در لایه‌های بالاتر پشته پروتکل مخابراتی به‌کار گرفته شود، می‌تواند به افزایش امنیت در ارسال اطلاعات کمک نماید.

مراجع

[۱] شهرام جمالی و توفان سماپور، «کنترل ازدحام مبتنی بر تخمین در شبکه‌های موردی بی‌سیم،» *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۳، شماره ۱، صفحات ۱-۱۴، ۱۳۹۲.

[2] A. S. K. Pathan, *Security of Self-organizing Networks: MANET, WSN, WMN, VANET*, CRC Press, Taylor & Francis Group, 2011.

[3] S. Taha, and X. Shen, *Secure IP Mobility Management for VANET*, Springer Briefs in Computer Science, 2013.

[۴] محمد مؤمنی، مهدی آقاصرام، وحید شاکر، شهرام جمالی و مهدی نوشیار، «ارائه یک فیلتر جدید برای حذف نویزهای ضربه‌ای و ترکیب فیلتر پیشنهادی با الگوریتم PSO به‌منظور کشف و دفاع در برابر حملات سیل‌آسای SYN،» *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۶، شماره ۱، صفحات ۳۱۱-۳۱۹، ۱۳۹۵.

[5] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*, CRC Press, Taylor & Francis Group, 2014.

[6] T. Alpcan, and T. Basar, *Network Security: A decision and Game-theoretic Approach*, Cambridge University Press, 2011.

[7] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," *Proc. of NET-COOP2007*, Avignon, France, 2007.

[8] Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119-2123, 2004.

[9] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," *Proc. IEEE International Conference on Game Theory for Networks*, Istanbul, Turkey, 2009.

[10] D. Yang, J. Zhang, Xi. Fang, A. Richa, and G. Xue, "Optimal transmission power control in the presence of a smart jammer," *Proc. Global Communications Conference (GLOBECOM)*, CA, USA, pp. 5506-5511, 2012.

[11] A. Garnaev, and W. Trappe, "The eavesdropping and jamming dilemma in multi-channel communications," *Proc. IEEE Int. Conference on Communications (ICC)*, Budapest, pp. 2160-2164, 2013.

[12] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 4-15, 2012.

[13] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Transactions on Wireless Information Forensics and Security*, vol. 10, no. 12, pp. 2578-2590, 2015.

[14] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2155-2163, 2015.

[15] S. Boyd, and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[16] J. Vučić, *Adaptive Modulation Technique for Broadband Communication in Indoor Optical Wireless Systems*, Ph.D. Thesis, Technical University of Berlin, Berlin, 2009.

[17] ASTM2213-03, *Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2010.

[18] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

زیرنویس‌ها

[1] Nash Equilibrium

[2] Non-Zero Sum

[3] Stackelberg

[4] Orthogonal Frequency Division Multiplexing

[5] Payoff functions

[6] Karush-Kuhn-Tucker