ارائه چهارچوبی مبتنی بر نظریه بازی‌ها برای جلب مشارکت گره‌ها در فرآیند شناسایی گره‌های مخرب در شبکه‌های حسگر بی‌سیم

رحیم بجانی[۱]، دانشجوی کارشناسی ارشد؛ محمد کلانتری[۲]، استادیار؛ امیرمسعود افتخاری مقدم[۳]، دانشیار

۱- دانشکده برق و کامپیوتر - دانشگاه آزاد اسلامی واحد قزوین - قزوین - ایران - r.bejani@qiau.ac.ir
۲- دانشکده مهندسی کامپیوتر - دانشگاه تربیت دبیر شهید رجایی - تهران - ایران - mkalantari@srttu.edu
۳- دانشکده برق و کامپیوتر - دانشگاه آزاد اسلامی واحد قزوین - قزوین - ایران - eftekhari@qiau.ac.ir

چکیده: نظریه بازی‌ها به عنوان یک رویکرد جدید برای مدل کردن برخی مشکل‌های شبکه‌های حسگر بی‌سیم از جمله مسیریابی، تجمیع داده‌ها و تشخیص نفوذ مورد استفاده قرار می‌گیرد. این شبکه‌ها به دلیل داشتن محدودیت منابع انرژی و حافظه می‌توانند توسط گره‌های مخرب مورد نفوذ قرار گیرند. این گره‌ها در تلاش هستند تا با مصرف بیهوده انرژی گره‌ها باعث ایجاد اختلال در شبکه شوند. تشخیص و جلوگیری از نفوذ گره‌ها می‌تواند به عنوان یک فرایند نظارت بر فعالیت‌ها، توسط سیستم تشخیص نفوذ انجام گیرد. به دلیل مصرف انرژی بیشتر توسط IDSها، گره‌های خودخواه تمایلی به سرخوشه شدن و فعال‌سازی IDS خود ندارند. ما در این مقاله، با ارائه مکانیسمی مبتنی بر نظریه بازی‌ها، گره‌ها را مجبور می‌کنیم تا در انتخاب سرخوشه با سایر گره‌ها همکاری کنند و اطلاعات خصوصی خود از جمله هزینه سرخوشه شدن را به درستی اعلام کنند. در این انتخاب، از پارامترهای مقدار انرژی باقی‌مانده، اعتبار و فاصله گره نسبت به ایستگاه مرکزی برای محاسبه هزینه سرخوشه استفاده می‌کنیم. بعد از انتخاب سرخوشه مناسب، یک بازی بر اساس تعادل نش بیزی بین آن و سایر گره‌های خوشه ارائه داده‌ایم تا IDS به طور مداوم روشن نماند. ارزیابی‌های صورت گرفته نشان می‌دهند که مکانیسم ما، مصرف انرژی گره‌ها را کاهش داده و باعث افزایش طول عمر شبکه می‌شود.

واژه‌های کلیدی: نظریه بازی، همکاری گره‌ها، تشخیص نفوذ، شناسایی گره‌های مخرب، طراحی مکانیسم، انتخاب سرخوشه، امنیت شبکه، حسگر بی‌سیم.

A Game Theory Framework to Cooperate Nodes in Malicious Nodes Detection Process in Wireless Sensor Network

R. Bejani[1], MSc Student; M. Kalantari[2], Assistant Professor; A. M. Eftekhari Moghaddam[3], Associate Professor

1- Faculty of Electrical and Computer Engineering, Islamic Azad University of Qazvin, Qazvin, Iran, Email: r.bejani@qiau.ac.ir
2- Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran, Email: mkalantari@srttu.edu
3- Faculty of Electrical and Computer Engineering, Islamic Azad University of Qazvin, Qazvin, Iran, Email: eftekhari@qiau.ac.ir

Abstract: Game theory is used as a new approach to model some problems of wireless sensor networks such as routing, data aggregation, and intrusion detection. These networks can be vulnerable to attacks by malicious nodes due to power and memory resource limitations of nodes. These nodes try to disrupt the network with unnecessary consumption of energy. Intrusion detection and prevention is run as a process of monitoring the events occurring in a network by the IDS (Intrusion Detection System). Because of high energy consumption by the IDS, selfish nodes in the cluster are unwilling to be a cluster head and turn IDS on. In this paper, we propose a mechanism based on game theory to enforce nodes to cooperate with other nodes in cluster head election and truthfully reveal their private information including cluster head cost. In this election, we use remaining energy, reputation and distance of node from base station to calculate cluster head cost. After selecting the appropriate cluster head, we propose a game based on BNE (Bayesian Nash Equilibrium) between cluster head and other nodes, such that the CH-IDS (Cluster Head-IDS) agent is not always in 'on' state. As a result, the power of CH can be saved. The implementation results show that our proposed mechanism reduces node energy consumption and increases the network life.

Keywords: Game theory, nodes cooperation, intrusion detection, malicious nodes detection, mechanism design, cluster head election, network security, wireless sensor.

تاریخ ارسال مقاله: ۱۳۹۵/۰۴/۰۹
تاریخ اصلاح مقاله: ۱۳۹۵/۰۶/۲۴
تاریخ پذیرش مقاله: ۱۳۹۵/۰۸/۲۰
نام نویسنده مسئول: محمد کلانتری
نشانی نویسنده مسئول: ایران - تهران - لویزان - دانشگاه تربیت دبیر شهید رجائی - دانشکده مهندسی کامپیوتر.

۱- مقدمه

در سال‌های اخیر شبکه‌های حسگر بی‌سیم از زمینه تحقیقاتی به زمینه‌های کاربردی در جهان واقعی تبدیل شده است این شبکه‌ها به چند کلاس مختلف کاربردی محیط زیستی، پزشکی، خانگی و اقتصادی [۱] تقسیم شده‌اند. به دلیل وجود گره‌های مخرب و خودخواه در این شبکه‌ها و لزوم ایجاد امنیت، به روش‌های مبتنی بر پیش‌گیری و تشخیص این گره‌های بدرفتار نیاز داریم. هدف این نوع گره‌ها بالا بردن خرابی شبکه و کاهش احتمال شناسایی شدن می‌باشد. این خرابی می‌تواند همان مصرف انرژی بیش از حد در گره‌های شبکه باشد که در نتیجه آن عمر گره‌ها و کل شبکه پایین می‌آید [۲].

نظریه بازی‌ها به عنوان یک روش مبتنی بر ریاضی و یک تئوری پرکاربرد در این شبکه‌ها می‌باشد که شرایط و موقعیت‌ها را در بین عواملی بررسی می‌کند که روی یک شی یا هدف مشترک تعامل دارند [۳]. این نظریه در بسیاری از زمینه‌های کامپیوتر از جمله امنیت شبکه‌های نظیر به نظیر، تشخیص حمله‌های منع سرویس توزیع شده و تشخیص سایر حمله‌ها مورد استفاده قرار گرفته است.

ما در این مقاله سعی داریم که با استفاده از اصول نظریه بازی‌ها از جمله تئوری شهرت و راستی‌آزمایی، روشی را برای تشخیص و جلوگیری از بدرفتاری‌های این گره‌ها ارائه بدهیم و با سیستم‌های تشویق [۴]، در بین آنها انگیزه همکاری ایجاد کنیم. نوآوری‌های ارائه شده در این کار عبارتند از:

- محاسبه تعداد برش‌های زمانی مورد انتظار هر گره برای زنده ماندن، به صورت پویا در ابتدای هر برش زمانی
- ارائه یک مکانیسم و الگوریتم برای انتخاب سرخوشه بر اساس هزینه محاسبه شده هر گره با پارامترهای مقدار انرژی باقی‌مانده و اعتبار گره و فاصله از ایستگاه مرکزی
- ارائه یک بازی بیزی بین IDS سرخوشه و سایر گره‌ها، جهت مداوم روشن نبودن IDS و ترکیب آن با مکانیسم انتخاب سرخوشه.

در بخش ۲ در مورد کارهای قبلی انجام شده در زمینه‌های مرتبط با کار ما مروری شده است در بخش ۳ مکانیسم و الگوریتم پیشنهادی ما به همراه اثبات و مثال عددی ارائه شده است. در بخش ۴ نتیجه‌های حاصل از شبیه‌سازی با نتیجه روش‌های قبلی و مرتبط مورد مقایسه قرار گرفته است. در بخش ۵ نیز نتیجه‌گیری و کارهای آتی که می‌توان در راستای این مقاله انجام داد ارائه شده است.

۲- مروری بر کارهای قبلی

در این بخش کارهای قبلی انجام شده توسط سایر پژوهشگران فعال در زمینه کاربرد نظریه بازی‌ها در شبکه‌های حسگر بی‌سیم را، در دو بخش بررسی می‌کنیم در بخش ۲-۱ همکاری گره‌ها در سیستم‌های تشخیص نفوذ و در بخش ۲-۲ کاربرد طراحی مکانیسم در شبکه‌ها بررسی می‌شود.

۲-۱- همکاری گره‌ها در سیستم‌های تشخیص نفوذ

نظریه بازی برای حل برخی مسائل مربوط به شبکه‌های بی‌سیم از جمله تحمیل رفتار همکاری [۵]، پروتکل‌های مسیریابی [۶] و طراحی سیستم‌ها مورد استفاده قرار گرفته است. اخیراً کارهای زیادی برای بررسی عملکرد متقابل گره‌های نرمال و مخرب انجام شده است. Agah و همکارانش در [۷]، یک بازی جمع غیرصفر برای تشخیص نفوذ ارائه داده‌اند آنها در بازی تک مرحله‌ای با اطلاعات کامل، یک استراتژی بهینه به دست آورده‌اند. در [۸] Liu و همکارانش برای تشخیص نفوذ در شبکه‌های موردی بی‌سیم یک روش بیزی ترکیبی ارائه داده‌اند. آن‌ها یک روال برای تشخیص ارائه داده‌اند که کل مصرف انرژی را کاهش می‌دهد. در [۹] نویسندگان یک بازی غیرهمکارانه با N بازیکن ارائه داده‌اند که هدف آن‌ها جلب مشارکت گره‌ها برای تشخیص نفوذ است. منبع [۱۰] اهداف و استراتژی‌های یک نفوذگر را با رویکردی مبتنی بر انگیزش[۱] مدل‌سازی می‌کند.

در [۱۱] از یک مدل مبتنی بر بازی‌های تصادفی برای ایجاد همکاری در بین گره‌های خودخواه شبکه‌های چند گام[۲] ارائه شده است. در این بازی از معمای زندانی نظریه بازی‌ها استفاده شده و گره‌های خودخواه با هر بار بدرفتاری در هر مرحله تنبیه می‌شوند.

در [۱۲] در مورد تشخیص حمله‌های نفی سرویس توزیع شده با استفاده از نظریه بازی‌ها بحث شده است و تشخیص این حمله‌ها بر عهده IDS می‌باشد.در این کار، یک بازی بین IDS و گره‌های مخرب ارائه شده است که در آن، تعادل نش به نحوی است که گره‌ها را وادار می‌کند تا از بین دو استراتژی خودخواه و یا نرمال، استراتژی نرمال را انتخاب کنند. در این مقاله به نحوه انتخاب سرخوشه و IDS فعال اشاره‌ای نشده است. هم چنین در [۱۳] یک سیستم دفاعی در برابر حمله‌های نفی سرویس برای شبکه‌های حسگر بی‌سیم ارائه شده است که با استفاده از پارامترهای یادگیری جدید میزان دقت آن در برابر حملات افزایش داده شده و نرخ هشدار اشتباه آن پایین آورده شده است.

در [۱۴] با استفاده از طراحی مکانیسم، امکان تشکیل خوشه حتی با یک گره مطمئن نیز وجود دارد. در این مکانیسم، گره‌هایی را که تمایلی برای همکاری صادقانه با سایر گره‌ها ندارند جهت همکاری تحریک می‌شوند. این تحریک توسط سیستم اعتباردهی به گره‌ها و مکانیسم VCG[۳] انجام شده است در بخش آخر مقاله نیز یک بازی غیرهمکارانه و جمع غیرصفر بین گره انتخاب شده و گره نفوذگر ارائه شده است و با به دست آوردن تعادل نش بیزی تک مرحله‌ای، تعادل نسبی بین امنیت و مصرف انرژی ایجاد کرده است.

در [۱۵] فرض شده است که IDSها در سرخوشه‌ها فعال می‌شوند و نحوه انتخاب این سرخوشه‌ها به صورت تصادفی می‌باشد. در این روش، موارد مهمی از قبیل مقدار انرژی باقی‌مانده گره‌ها و رفتار گره‌های خودخواه در نظر گرفته نشده است. در نتیجه گره‌هایی که انرژی باقی‌مانده کمتری دارند به دلیل سرویس‌دهی به سایر گره‌ها

زودتر از بین می‌روند و گره‌های خودخواه به دلیل عدم سرویس‌دهی، بیشتر ازسایر گره‌های نرمال عمر می‌کنند.

در [۱۶] نویسندگان با وجود گره‌های خودخواه در شبکه‌های سیار، انتخاب سرخوشه مناسب برای فرآیند تشخیص نفوذ را مورد مطالعه قرار داده‌اند. با توجه به اینکه برخی از گره‌ها سعی دارند رفتار خودخواهانه از خود نشان دهند و انرژی کمتری مصرف کنند نویسندگان مکانیسمی مبتنی بر اعتبار[۴] ارائه داده‌اند تا تمام گره‌ها در تشخیص نفوذ مشارکت کنند و انرژی مصرف کنند و پاداش بگیرند. مقدار این پاداش بر اساس مدل VCG محاسبه شده است بنابراین تمام گره‌ها مجبور شده‌اند در مورد هزینه سرخوشه شدن صادق باشند. پارامترهای در نظر گرفته شده برای محاسبه هزینه سرخوشه شدن، عبارتند از مقدار انرژی باقی‌مانده گره و اعتبار آن. در این کار الگوریتم انتخاب سرخوشه به صورت مستقل از خوشه[۵] (CILE) پیاده‌سازی شده است اما در نهایت هیچ بازی بین سرخوشه و گره‌های بدرفتار ارائه نشده است.

انتخاب سرخوشه در [۱۷] بر اساس درجه ارتباط گره انجام می‌گیرد که این نوع انتخاب نیز باعث از بین رفتن انرژی چند گره خاص در خوشه می‌شود. هم چنین در [۱۸، ۱۹] انتخاب سرخوشه بر پایه مقدار انرژی باقی‌مانده گره‌ها انجام گرفته است که در آن، رفتار گره‌های خودخواه در نظر گرفته نشده است. در [۱۶، ۲۰، ۲۱] نیز از نظریه بازی‌ها برای انتخاب سرخوشه استفاده شده است و نوع گره‌ها نیز در این انتخاب در نظر گرفته شده است اما پارامترهای به کار رفته جهت محاسبه هزینه و وزن هر گره فقط انرژی و مقدار اعتبار گره می‌باشد.

در [۲۲] نویسندگان برای بررسی رفتارهای متقابل گره‌های نرمال و مخرب در شبکه‌های بی‌سیم از نظریه بازی‌ها استفاده کرده‌اند. آن‌ها فرآیند تشخیص نفوذ را با یک بازی بیزی از نوع اطلاعات ناقص مدل‌سازی کرده‌اند و سپس یک تعادل نش بیزی کامل[۶] با کمک استراتژی مخلوط و تابع شناسایی پسین[۷] به دست آورده‌اند و در هر مرحله از بازی گره‌های نرمال، باور خودشان را نسبت به گره‌های بدرفتار بروز کرده‌اند. هدف نویسندگان در این مقاله، حذف گره‌های مخرب نبوده، بلکه بعد از شناسایی گره سعی کرده‌اند بین گره مخرب و سایر گره‌ها همزیستی[۸] ایجاد کنند و از انرژی آنها برای افزایش طول عمر کل شبکه استفاده کنند. در این مقاله نیز در مورد نحوه انتخاب سرخوشه و IDS بحثی نشده است.

۲-۲- کاربرد طراحی مکانیسم

طراحی مکانیسم یک زیرشاخه از رشته اقتصاد خرد می‌باشد [۳] و از ابزار نظریه بازی‌ها برای دستیابی به اهداف از پیش تعیین شده استفاده می‌کند. تفاوت نظریه بازی با طراحی مکانیسم این است که نظریه بازی رویدادهای اتفاق افتاده بعد از رفتارها و انتخاب‌های عناصر بازی را مورد بررسی قرار می‌دهد ولی طراحی مکانیسم یک بازی با قوانین خاصی را پیشنهاد می‌دهد که عناصر مستقل، مجبور باشند استراتژی‌هایی را برگزینند که خروجی بازی برای همه عناصر بازی، مطلوب باشد یا به عبارتی دیگر، همان خروجی تابع انتخاب جمع (SCF) باشد. متعادل کردن انرژی مصرفی IDS را می‌توان با استفاده از همین طراحی مکانیسم و با تابع هزینه، مدل سازی کرد.

در [۱۶، ۲۰، ۲۱]، اطلاعات خصوصی بازیکنان یا گره‌های متحرک همان هزینه آنالیز آنهاست که به سطح انرژی گره‌ها و مقدار اعتبار آنها بستگی دارد و این هزینه به‌طور دقیق برای هر گره محاسبه نشده بلکه بر حسب سطح انرژی، کلاس‌بندی شده‌اند و تعداد برش زمانی مورد انتظار برای زنده ماندن گره (nT_i) در آن، به صورت ثابت و در ابتدای اولین برش زمانی برای هر گره محاسبه شده است. هدف این کار، ایجاد انگیزه در گره‌ها برای همکاری و دادن اطلاعات خصوصی درست در حین انتخاب سرخوشه است [۲۳]. در [۲۱] نویسندگان بعد از انتخاب سرخوشه، یک بازی تک مرحله‌ای بین سرخوشه و گره‌های عضو خوشه داده‌اند و تعادل نش بازی را محاسبه کرده‌اند. تفاوت‌های مقاله ما، با همه کارهای قبلی ذکر شده عبارتند از: تأثیر پارامتر فاصله در محاسبه هزینه، محاسبه پویای تعداد دوره‌های زمانی مورد انتظار برای زنده ماندن گره بعد از انتخاب، ارائه یک بازی بیزی چند مرحله‌ای با قابلیت به‌روزرسانی باور بازیکنان و در نهایت محاسبه تعادل نش بیزی و احتمال پسین، جهت مداوم روشن نماندن IDS.

۳- انتخاب سرخوشه با استفاده از نظریه بازی‌ها

الگوریتم‌های مختلفی برای خوشه‌بندی و تعیین سرخوشه در کارهای تحقیقاتی آمده است. این الگوریتم‌ها را می‌توان به دو دسته تقسیم کرد. در دسته اول، ابتدا خوشه تشکیل می‌شود و سپس برای آن یک سرخوشه انتخاب می‌شود [۲۴]. در دسته دوم، ابتدا گره‌های سرخوشه تعیین می‌شوند سپس سایر گره‌ها به عنوان اعضا به آن سرخوشه تعلق می‌گیرند. فرض ما در این کار، این است که خوشه تشکیل شده و ما می‌خواهیم در برش‌های زمانی[۹] برای خوشه، سرخوشه انتخاب کنیم همچنین فرض بر این است که رابطه گره‌ها در خوشه به صورت تک جهشی[۱۰] می‌باشد.

IDS را می‌توان به سه روش در شبکه فعال کرد: توزیع شده[۱۱]، متمرکز[۱۲]، توزیع شده- متمرکز.

در نوع توزیع شده عامل IDS بر روی هر گره حسگر فعال می‌شود و همه گره‌ها، رفتارهای غیرعادی گره‌های حسگر همسایه را بررسی می‌کنند. در حالی که در IDS متمرکز، IDS تنها بر روی ایستگاه پایه فعال می‌شود و داده‌های تجمیع شده گره‌های حسگر را جهت تشخیص نفوذ آنالیز می‌کند. در IDS توزیع شده- متمرکز، شبکه حسگر بی‌سیم خوشه‌بندی شده برای هر خوشه یک گره به عنوان سرخوشه (CH) انتخاب می‌شود و IDS روی آن فعال می‌شود تا رفتار گره‌های خوشه را بررسی کند [۲۵].

IDSهای توزیع شده به دلیل مصرف انرژی زیاد در کل شبکه، مناسب نیستند. همچنین IDSهای متمرکز نیز، به دلیل اینکه کل

سربار تحلیل بر عهده ایستگاه پایه می‌باشد مناسب نیستند. بنابراین روش ارائه شده ما مبتنی بر نوع توزیع شده - متمرکز می‌باشد.

در ابتدا شبکه را به صورت یک گراف غیر جهت‌دار G: (N,L) در نظر می‌گیریم که در آن N مجموعه گره و L مجموعه اتصال‌های غیر جهت‌دار تک جهشی است. شبکه را به خوشه‌های مختلفی تقسیم‌بندی می‌کنیم که هر خوشه یک مجموعه گره $n \in N$ و یک مجموعه بردار $l \in L$ دارد. فرض می‌کنیم که گره‌های خودخواه به دلیل مصرف منابع خود مانند باطری، حافظه و زمان CPU، تمایلی برای شرکت در تشخیص نفوذ ندارند. همه گره‌های موجود عقلانی در نظر گرفته شده‌اند [۲۶، ۲۷] و سعی دارند از سرویس‌های موجود حداکثر استفاده را ببرند. مقدار سرویسی که گره‌ها می‌توانند دریافت کنند به اعتبارشان بستگی دارد بنابراین گره‌ها برای دریافت سرویس بیشتر، به دریافت اعتبار بیشتر نیاز دارند و برای دریافت اعتبار بیشتر، باید با گره‌های دیگر همکاری داشته باشند و اطلاعات خصوصی درست، ارائه دهند[۲۸].

فرض می‌کنیم که در موقع تشکیل خوشه، اعتبار پیش‌فرض گره مقدار ثابت R_0 باشد. یک گره خودخواه در نتیجه رفتار خودخواهانه و دادن اطلاعات نادرست از مقدار انرژی باقی مانده‌اش، با کاهش اعتبار مواجه می‌شود و در نتیجه، وقتی مقدار آن، از یک مقدار تعریف شده- حد آستانه[۱۳] - کمتر می‌شود از سرویس‌های شبکه محروم می‌شود [۲۹]. برای محاسبه هزینه آنالیز و انتخاب سرخوشه، نمادها و پارامترهای زیر را در نظر می‌گیریم:

R_i : اعتباره گره i، در برش زمانی جاری

PS_i : سرخوشه به دلیل محدویت منابع تنها می‌تواند یک تعداد محدودی از بسته‌های هر گره را در خوشه آنالیز کند که به این تعداد محدود مجموعه نمونه‌گیری[۱۴] می‌گویند. هر گره یک مجموعه نمونه‌گیری بر اساس اعتبار دارد که آن را با PS_i نشان می‌دهند.

C: بیانگر هزینه آنالیز بسته است.

E_{ids}: بیانگر انرژی لازم برای اجرای IDS به مدت یک دوره زمانی[۱۵] است.

CH_A : سرخوشه مربوط به خوشه A، که مسئول حفاظت از گره‌های خوشه در مقابل نفوذ است.

CM_{-i} : نشانگر گره‌ها در خوشه به استثنای گره i.

برای هر گره دو عامل مؤثر در نظر می‌گیریم:

- ضریب قدرت که به صورت رابطه (۱) [۱۶، ۳۰] محاسبه می‌شود.

$$PF_i = \frac{E_i}{nT_i} \qquad (۱)$$

که در آن E_i مقدار انرژی باقی‌مانده گره است و nT_i تعداد برش‌های زمانی است که انتظار می‌رود گره زنده بماند و با رابطه (۲) [۳۱] محاسبه می‌شود.

$$nT_i = \frac{E_i}{E_{CM}} \qquad (۲)$$

که در آن E_{CM} انرژی مورد نیاز گره برای زنده ماندن به مدت یک برش زمانی است.

- ضریب فاصله که از رابطه (۳) به دست می‌آید.

$$DF_i = \frac{d_i}{\sum_{j=1}^{n} d_j} \qquad (۳)$$

$$d_i = \sqrt[2]{(x_i - x_{BS})^2 + (y_i - y_{BS})^2}$$

که در آن d_i فاصله گره از ایستگاه مرکزی است.

هزینه آنالیز هر گره می‌تواند بر اساس مقدار انرژی باقی‌مانده آن و مقدار اعتبار آن محاسبه شود مکانیسم ارائه شده ما، برای محاسبه این هزینه به دو صورت می‌باشد:

روش اول: که در آن nT_i به صورت متغیر و پویا در هر برش زمانی برای هر گره محاسبه می‌شود و ضریب فاصله هیچ تاثیری در آن ندارد. نحوه محاسبه به صورت رابطه (۴) [۱۶] می‌باشد.

$$C_i = \frac{PS_i}{PF_i} = \begin{cases} \infty & E_i < E_{ids} \\ \dfrac{\dfrac{R_i}{\sum_{j=1}^{n} R_j} \times nT_i}{E_i} & E_i >= E_{ids} \end{cases} \qquad (۴)$$

روش دوم: محاسبه هزینه همانند روش اول با nT_i پویا هست با این تفاوت که در آن، ضریب فاصله گره تا ایستگاه مرکزی نیز دخالت دارد و محاسبه آن به صورت رابطه (۵) می‌باشد.

$$C_i = \begin{cases} \infty & E_i < E_{ids} \\ \dfrac{PS_i \times DF_i}{PF_i} = \dfrac{\dfrac{R_i}{\sum_{j=1}^{n} R_j} \times \dfrac{d_i}{\sum_{j=1}^{n} d_j} \times nT_i}{E_i} & E_i >= E_{ids} \end{cases} \qquad (۵)$$

گره‌های خودخواه می‌خواهند با مصرف انرژی کمتر، PS خود را به بالاترین مقدار برسانند. با توجه به رابطه‌های (۴) و (۵) اگر انرژی باقی‌مانده گره، کمتر از انرژی مورد نیاز برای اجرای IDS در یک برش زمانی باشد هزینه آنالیز بی‌نهایت می‌شود [۱۶، ۳۰] در غیر این صورت مقدار C محاسبه می‌شود. مقدار C با PS رابطه مستقیم و با PF_i رابطه معکوس دارد. اگر گره، PS کافی داشته باشد به عبارت دیگر، اعتبار (R_i) بالایی داشته باشد، تمایلی به مصرف انرژی جهت سرخوشه شدن ندارد. از طرف دیگر اگر PF بزرگ‌تر باشد یا به عبارتی دیگر، انرژی آن بیشتر باشد هزینه کمتر می‌شود و احتمال سرخوشه شدن زیاد می‌شود.

۳-۱- ارائه مکانیسم

هر گره، اطلاعات خصوصی درباره نوع خودش دارد (مخرب یا نرمال) که آن را با θ_i ={Normal,Selfish} نشان می‌دهیم. فرض می‌کنیم که بازیکن i یک تابع مطلوبیت شبه خطی به صورت رابطه (۶) دارد [۱۸].

$$u_i(\theta_i, o(\theta_i, \theta_{-i})) = p_i - v_i(\theta_i, o(\theta_i, \theta_{-i})) \qquad (۶)$$

که در آن پارامترها به شرح زیر می‌باشند:

θ_{-i} : نوع گره‌ها در یک خوشه به استثنای i

v_i: ارزیابی هزینه بازیکن i نسبت به خروجی $o \in O$ ، در حالیکه O، مجموعه خروجی‌های ممکن است. در اینجا v_i، همان هزینه آنالیز است که بعد از انتخاب نوع گره توسط i، مشخص می‌شود.

$p_i \in R : p_i$ مقدار پرداختی به گره i توسط مکانیسم است. این مقدار در قالب اعتبار به گره داده می‌شود.

u_i پارامتر بهره‌وری هست که بازیکن سعی می‌کند آن را به بالاترین حد برساند. بازیکنان برای اینکه سود بیشتری به دست آورند ممکن است برای هزینه آنالیز یک مقدار غیرواقعی ارائه بدهند. بنابراین باید مکانیسمی ارائه دهیم که در آن استراتژی راست‌گویی، یک استراتژی غالب باشد.

برای بازی، هر گره یک نوع θ_i و یک تابع ارزیابی $v_i(\theta, o)$ انتخاب می‌کند و این مقادیر ورودی مکانیسم هستند. برای هر بردار ورودی، بردار خروجی یعنی $o = o(\theta, \ldots, \theta_n)$ و بردار پرداختی $p = (p_1, \ldots p_n)$ توسط مکانیسم محاسبه می‌شود. این پرداختی‌ها، بازیکنان را به سمت هدف مورد نظر مکانیسم، سوق می‌دهند. این هدف، همان تابع انتخاب جمع است که به صورت رابطه (۷) تعریف می‌شود [۱۶].

$$SCF = \min \sum_{i \in n} v_i(\theta_i, o(\theta_i, \theta_{-i})) \qquad (۷)$$

برای محاسبه پرداختی، از مکانیسم VCG استفاده می‌کنیم [۲۹] تا غالب بودن استراتژی راستگو را ثابت کنیم. این مکانیسم به صورت رابطه (۸) تعریف می‌شود [۱۶].

$$p_i = R_i = \sum_{j \in n_{-i}} v_j(\theta_j, o(\theta_i, \theta_{-i})) \qquad (۸)$$

که در آن R_i اعتبار گره و $\sum_{j \in n_{-i}} v_j(\theta_j, o(\theta_i, \theta_{-i}))$ بهترین پیشنهاد به استثنای پیشنهاد n_i است (بهترین قیمت دوم مخفی[۶]) [۲۴].

۳-۲- مکانیسم انتخاب سر خوشه

برای انتخاب سرخوشه از الگوریتم (۱) استفاده می‌کنیم. در مرحله اول این الگوریتم، سرخوشه جاری یک پیغام مبنی بر شروع انتخاب سرخوشه برای برش زمانی بعدی، به همه گره‌ها می‌فرستد. در مرحله دوم، گره‌های خوشه بعد از دریافت پیغام مرحله اول، یک پیغام شامل شناسه ID_i گره n_i، رمز شده شناسه ID_i، هزینه آنالیز C_i و برچسب زمانی TS_j را به سرخوشه می‌فرستند. TS_j برای مشخص کردن زمان شروع انتخاب یا برش زمانی استفاده می‌شود. این پیغام با استفاده از تابع هش رمزنگاری شده است. این قسمت از الگوریتم، معادل پیشنهاد مخفی مبلغ در مزایده‌ها می‌باشد و به همین دلیل برای جلوگیری از آشکار شدن مقدار پیشنهادی گره‌ها از همدیگر، این مقدار را با الگوریتم هش رمزنگاری می‌کنیم این الگوریتم رمزنگاری برگشت ناپذیر می‌باشد.

(1) CH → CM : Start-Selecting

(2) CM → CH :Message (ID_i , Hash(ID_i, C_i, TS_j))

(3) CM → CH :Message (ID_i, C_i, TS_j)

(4) NewCH = Select (Min C)

(5) CH → CM : Selected(NewCH)

(6) CH → ADD (R_{NewCH}= R_{NewCH} + Best Second C)

(7) CH → CM : Update Reputation (NewCH)

الگوریتم (۱): الگوریتم انتخاب سر خوشه در هر برش زمانی

در مرحله سوم، همه گره‌ها یک پیغام شامل، شناسه ID_i، هزینه آنالیز و برچسب زمان TS_j را می‌فرستند. اگر گرهی این پیغام را نفرستد از سرویس‌های خوشه محروم می‌شود. گره‌های دریافت‌کننده، آن را با مقدار هش شده در مرحله اول، مقایسه می‌کنند و در صورت یکسان نبودن این مقادیر، آن را به عنوان یک گره بدرفتار شناسایی می‌کنند. در مرحله چهارم سرخوشه بر اساس تابع انتخاب جمع، کمترین مقدار هزینه آنالیز پیشنهادی را انتخاب می‌کند و در مرحله پنجم به آن گره اطلاع می‌دهد که به عنوان سرخوشه برای برش زمانی بعدی انتخاب شده است. در مرحله ششم، سرخوشه در جدول خودش، مقدار اعتبار گره انتخاب شده را به اندازه بهترین هزینه دوم اضافه می‌کند و در مرحله نهایی پیغام به‌روزرسانی این مقدار را، به همه گره‌ها اعلام می‌کند. کل این فرآیند در هر برش زمانی، یک بار اجرا می‌شود.

۳-۲-۱- مثال عددی

یک خوشه تشکیل شده از ۱۰ گره را در نظر می‌گیریم که ۲۰٪ آن‌ها گره‌های خودخواه - منطقی هستند. گره‌ها می‌خواهند با همکاری یکدیگر، یک سرخوشه مناسب را انتخاب کنند تا وظیفه تشخیص نفوذ را به آن بسپارند. فرض بر این است که، الگوریتم چهار بار تکرار شده و گره N_8 به عنوان سرخوشه جاری بوده و هزینه و اعتبار گره‌ها به صورت جدول ۱ در آمده است. با فرض اینکه بودجه نمونه‌گیری IDS، ۱۰۰ بسته بر ثانیه است توزیع نمونه‌گیری سرخوشه روی گره‌ها همانند ستون سوم جدول خواهد بود.

برای انتخاب سرخوشه جدید در تکرار پنجم، هر گره مقدار هزینه آنالیز خود را با کمک رابطه (۴) محاسبه می‌کند و نتایج در ستون چهارم جدول قرار می‌گیرد. با توجه به رابطه (۷)، گره N_6 بهترین و کمترین مقدار هزینه را دارد. گره‌ها مقدار پرداختی خود را برای گره انتخابی طبق رابطه (۸) محاسبه می‌کنند که نتیجه برابر ۹ واحد اعتبار است (با مکانیسم دومین قیمت، بعد از N_6 برنده خوشه N_{10} است که مقدار هزینه آن ۹ است). سپس همه گره‌ها اعتبار گره انتخابی یعنی N_6 را ۹ واحد افزایش می‌دهند و در نتیجه بهره‌وری گره N_6 عبارت خواهد بود از ۳ = ۶ - ۹، که همان سود حاصله برای آن است. به عبارت دیگر، سرخوشه وظیفه‌اش را با هزینه کردن ۶ واحد انجام می‌دهد و ۹ واحد پاداش می‌گیرد که این ۳ واحد افزایش، در تکرارهای بعدی باعث افزایش سرویس گرفتن این گره می‌شود چون سرویس‌دهی به گره‌ها، بر اساس اعتبار آنها است.

جدول ۱: مثال برای انتخاب سرخوشه

گره	اعتبار (R)	نمونه‌گیری (PS)	هزینه (Cost)
N_1	۸	٪۸	۱۴
N_2	۱۳	٪۱۳	۲۶
N_3	۱۱	٪۱۱	۱۲
N_4	۹	٪۹	۲۲
N_5	۱۵	٪۱۵	۳۰
N_6	۳	٪۳	۶
N_7	۱۲	٪۱۲	۲۰
N_8	۱۰	٪۱۰	۱۶
N_9	۱۴	٪۱۴	۲۸
N_{10}	۵	٪۵	۹

اگر یک سرخوشه بعد از انتخاب شدن، رفتار خودخواهانه از خود بروز دهد اعتبار آن کاهش می‌یابد که در این مثال در صورت خودخواه بودن سرخوشه، باعث کاهش ۹ واحدی اعتبار برای آن گره می‌شود.

۳-۳- اثبات درستی مکانیسم

در این بخش، ثابت می‌کنیم که چگونه گره‌های خودخواه را با این مکانیسم مجبور می‌کنیم صادقانه برخورد کنند [۵] به بیان دیگر نشان می‌دهیم که استراتژی راستگویی، استراتژی غالب است.

گره به دو صورت می‌تواند در مورد هزینه آنالیز، مقدار دروغ بدهد: یا از مقدار واقعی کمتر اعلام می‌کند یا بیشتر. اگر گره i، هزینه کمتر از مقدار واقعی تعریف کند ($v_i' < v_i$) حتماً تمایل دارد که در انتخاب برنده شده و سرخوشه باشد. کمتر از هزینه واقعی تعریف کردن هیچ کمکی به آن نخواهد کرد زیرا دو حالت پیش می‌آید. حالت اول این است که مقدار واقعی هزینه‌اش شاید کمترین هزینه در خوشه باشد و حتی با مقدار واقعی نیز بتواند برنده شود در این صورت کمتر از هزینه واقعی تعریف کردن برای او سودی نخواهد داشت زیرا مقدار پرداختی همان بهترین مقدار دوم (برنده بعد از آن) است که در هر صورت ثابت است. از این رو بهره‌وری آن گره همان مقدار می‌ماند که با هزینه واقعی به دست می‌آید. حالت دوم نیز، این است که مقدار واقعی هزینه‌اش کمترین در خوشه نباشد و با مقدار واقعی v_i برنده خوشه نباشد که با این کار باعث می‌شود تابع بهره‌وری‌اش (u_i) منفی باشد چون که پرداخت‌های انجام شده کمتر از مقدار واقعی هزینه‌اش خواهد بود.

اگر گره i، هزینه‌ای بیشتر از هزینه واقعی‌اش تعریف کند ($v_i' > v_i$)، به دو دلیل هیچ وقت برای او سودی نخواهد داشت اول اینکه اگر مقدار واقعی‌اش کمترین مقدار در خوشه باشد این کار باعث خواهد شد برنده نشود و در نتیجه مقدار پرداختی مثبت را از دست خواهد داد. اگر با مقدار هزینه دروغین (v_i') هم برنده شود باز هم در مقدار پرداختی او تاثیری نخواهد داشت. دوم اینکه اگر مقدار واقعی‌اش کمترین مقدار در خوشه نباشد باز این استراتژی برای او هیچ سودی نخواهد داشت. پس نتیجه می‌گیریم که مکانیسم ارائه شده، یک مکانیسم قابل اعتماد و راستگو است [۳۲].

۴- ارائه یک بازی بیزی بین سرخوشه و گره‌ها

برای یک گره حسگر مخرب، سود حمله را با g_A و هزینه حمله را با C_A نشان می‌دهیم. وقتی یک گره استراتژی همکاری را انتخاب می‌کند به این معنی است که گره برای ارتباط در دسترس است و بسته‌ها می‌توانند از طریق آن با موفقیت ارسال شوند. درست کار کردن شبکه برای گره‌های نرمال سود دارد هر چند که دریافت و ارسال بسته‌ها نیازمند مصرف انرژی برای گره‌ها است. فرض می‌کنیم که این سود و هزینه مصرف انرژی برای هر دو گره نرمال و مخرب یکسان باشد. برای نشان دادن سود همکاری از پارامتر g_C و برای هزینه همکاری از c_C استفاده می‌کنیم. وقتی CH-IDS استراتژی دفاع را انتخاب می‌کند سود حاصل از تشخیص درست را با g_D و هزینه انرژی مصرفی آن را با c_D نشان می‌دهیم.

همچنین نرخ تشخیص را با α و نرخ خطای اشتباه را با β استفاده می‌کنیم. منظور از خطای اشتباه تشخیص نادرست گره‌های نرمال به عنوان گره مخرب می‌باشد که این تشخیص غلط باعث جریمه IDS به اندازه L_f می‌شود.

در این بازی دو بازیکن داریم، گره حسگر بی‌سیم S (فرستنده) که با θ_S نشان می‌دهیم و CH-IDS (گیرنده R) که با θ_R نشان می‌دهیم. عامل S یعنی گره فرستنده ممکن است نرمال باشد ($\theta_S=0$) یا مخرب باشد ($\theta_S=1$) و نوع آن قبل از بازی داده خصوصی است که CH-IDS از آن اطلاعی ندارد. اگر نوع آن مخرب باشد می‌تواند دو کنش[۱۷] حمله و همکاری داشته باشد این کنش را با $a_s(\theta_s=1)$ و فضای کنش را با $A_s(\theta_s=1)=\{Cooperate, Attack\}$ نشان می‌دهیم. اگر نوع آن نرمال باشد همیشه کنش همکاری $a_s(\theta_s=0)$ را در برابر سایر گره‌ها انتخاب می‌کند و فضای کنش آن به صورت $A_s(\theta_s=0)=\{Cooperate\}$ خواهد بود.

کنش عامل R یا گره گیرنده را با $a_R(\theta_R)$ نشان می‌دهیم. به منظور ذخیره بیشتر انرژی برای افزایش عمر CH، عامل CH-IDS نباید به طور مداوم در حال دفاع باشد و باید به فکر راه حلی باشد تا در برش‌های زمانی که نیازی به روشن بودن IDS آن نیست در حالت بیکار باشد. بنابراین فضای کنش آن شامل دو حالت دفاع[۱۸] و بیکار[۱۹] می‌باشد. شکل ۱، شکل گسترده بازی [۳۳] را نشان می‌دهد.

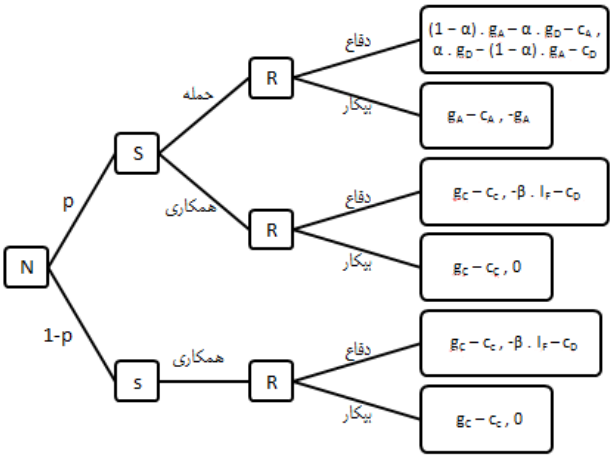
بهره‌وری‌های این بازی در جدول ۲ و جدول ۳ نمایش داده شده است. همه کنش‌ها به استثنای بیکاری IDS، متحمل هزینه هستند.

جدول ۲: بهره‌وری بازی بین IDS و گره مخرب

		بازیکن R	
		دفاع	بیکار
بازیکن S	حمله	$(1-\alpha).g_A-\alpha.g_D-c_A$, $\alpha.g_D-(1-\alpha).g_A-c_D$	g_A-c_A , $-g_A$
	همکاری	g_C-c_c , $-\beta.l_F-c_D$	g_C-c_C , 0

جدول ۳: بهره‌وری بازی بین IDS و گره نرمال

		بازیکن R	
		دفاع	بیکار
بازیکن S	همکاری	g_C-c_c , $-\beta.l_F-c_D$	g_C-c_c , 0



شکل ۱: شکل گسترده بازی

تعریف: بازی تشخیص حملات، یک مجموعه ۵ تایی (N,Θ,A,P,U) است که:

N: بازیکنان شامل عامل‌های R و S.

$\Theta=\Theta_S\times\Theta_R$ که $\Theta_S=\{\theta_s=0,\theta_s=1\}$ فضای کنش بازیکن S و $\Theta_R=\{\theta_R\}$ فضای کنش بازیکن R است.

$A=A_S\times A_R$ که در آن A_S مجموعه کنش‌های بازیکن S است و به صورت رابطه (۹) تعریف می‌شود.

$$A_S=\{A_S(\theta_s=0),A_S(\theta_s=1)\}= \{\{a_S(\theta_s=0)\,|\,Cooperate\},\{a_S(\theta_s=1)\,|\,Attack,Cooperate\}\} \quad (۹)$$

و همچنین A_R مجموعه کنش‌های بازیکن R است که به صورت رابطه (۱۰) تعریف می‌شود.

$$A_R=\{a_R\,|\,Defend,Idle\} \quad (۱۰)$$

P={p,1-p} یک توزیع احتمال پیشین، بین ۰ و ۱ روی گره‌ها است که P احتمال مخرب بودن گره حسگر و 1-p هم احتمال نرمال بودن آن را نشان می‌دهد.

U=(u_S,u_R) که در آن تابع بهره‌وری برای بازیکن S را با $u_S=A\times\Theta$ و تابع بهره‌وری بازیکن R را با $u_R=A\times\Theta$ نشان می‌دهیم. این مقادیر همان مقادیر محاسبه شده در جدول‌های ۱ و ۲ است.

۴-۱- تعادل بازی

در این بازی هر گره فقط از نوع خودش آگاه است پس نوع بازی ، بازی با اطلاعات ناقص است [۲۷، ۳۴]. بنابراین می‌توان از این بازی یک تعادل نش بیزی (BNE) به دست آورد.

اگر گره S، استراتژی $(a_S(\theta_s=1)=Attack,a_S(\theta_s=0)=Cooperate)$ را انتخاب می‌کند یعنی گره S اگر مخرب باشد همیشه حمله می‌کند و اگر نرمال باشد همکاری می‌کند در این صورت بهره‌وری مورد انتظار برای عامل R یا همان CH-IDS، در دو حالت دفاع و بیکاری به صورت رابطه (۱۱) خواهد بود.

$$Eu_R(Defend)=p.(\alpha.g_D-(1-\alpha).g_A-c_D)+(1-p).(-\beta.l_F-c_D)$$
$$Eu_R(Idle)=-p.g_A+(1-p).0=-p.g_A \quad (۱۱)$$

اگر $Eu_R(Defend)\geq Eu_R(Idle)$ باشد داریم:

$$p.(\alpha.g_D-(1-\alpha).g_A-c_D)+(1-p).(-\beta.l_F-c_D)\geq -p.g_A$$
$$p\geq(\beta.l_F+c_D)/(\alpha.g_D+\alpha.g_A+\beta.l_F) \quad (۱۲)$$

در این حالت استراتژی غالب برای CH-IDS، استراتژی دفاع است. بنابراین اگر CH-IDS، استراتژی دفاع را انتخاب کند برای گره S، حمله استراتژی غالب نخواهد بود زیرا رابطه (۱۳) برای بهره‌وریهای آن بدیهی است.

$$(1-\alpha).g_A-\alpha.g_D-c_A<g_C-c_C \quad (۱۳)$$

بنابراین رابطه (۱۴) یک BNE استراتژی خالص نیست.

$$\{(a_S(\theta_S=1)=Attack,a_S(\theta_S=0)=Cooperate), a_R(\theta_R)=Defend\} \quad (۱۴)$$

اگر $Eu_R(Defend)<Eu_R(Idle)$ باشد داریم:

$$p<(\beta.l_F+c_D)/(\alpha.g_D+\alpha.g_A+\beta.l_F) \quad (۱۵)$$

در این حالت نیز استراتژی غالب برای CH-IDS، استراتژی بیکاری است و همچنین برای گره S استراتژی حمله، استراتژی غالب خواهد بود زیرا رابطه (۱۶) نیز برای بهره‌وری‌های گره منطقی است.

$$g_A-g_C>(1-\alpha).g_A-\alpha.g_D-c_A \quad (۱۶)$$

بنابراین رابطه (۱۷) یک BNE استراتژی خالص نیست.

$$\{(a_S(\theta_S=1)=Attack,a_S(\theta_S=0)=Cooperate), a_R(\theta_R)=Idle\} \quad (۱۷)$$

وقتی گره S، استراتژی $(a_S(\theta_S=1)=Cooperate,a_S(\theta_S=0)=Cooperate)$ را انتخاب می‌کند به این معنی است که صرف‌نظر از نوع گره همیشه می‌خواهد استراتژی همکاری را بازی کند. برای CH-IDS بهترین پاسخ برای استراتژی بیکاری S، استراتژی بیکاری است و برای گره مخرب $\theta_S=1$، بهترین پاسخ برای استراتژی بیکاری R ، استراتژی حمله است. در نتیجه یک تناقض با استراتژی خالص $(a_S(\theta_S=1)=Cooperate,a_S(\theta_S=0)=Cooperate)$ به وجود می‌آید. بنابراین رابطه (۱۸) نیز یک BNE استراتژی خالص نخواهد بود.

$$\{(a_S(\theta_S=1)=Cooperate, a_S(\theta_S=0)=Cooperate), \quad a_R(\theta_R)=Idle\} \tag{۱۸}$$

به طور خلاصه وقتی $p<(\beta.l_F+c_D)/(\alpha.g_D+\alpha.g_A+\beta.l_F)$ باشد یک BNE به صورت رابطه (۱۹) وجود خواهد داشت به این معنی که وقتی عامل R یا $CH\text{-}IDS$، همیشه استراتژی بیکاری را انتخاب می‌کند گره مخرب همیشه استراتژی حمله و گره نرمال استراتژی همکاری را بازی می‌کنند.

$$\{(a_S(\theta_S=1)=Attack, a_S(\theta_S=0)=Cooperate), \quad a_R(\theta_R)=Idle\} \tag{۱۹}$$

هر چند که یک BNE در این مورد وجود دارد اما این استراتژی عملی نیست زیرا همان‌گونه که اثبات کردیم CH-IDS باید به صورت مداوم کنش بیکاری را انتخاب کند و در نتیجه، گره‌های مخرب هیچ موقع توسط CH-IDS تشخیص داده نخواهند شد. بنابراین تنها به دست آوردن BNE استراتژی خالص برای بازی تشخیص حمله کافی نیست و نیاز به پیدا کردن BNE استراتژی مخلوط[۲۰] داریم.

برای گره مخرب $\theta_S=1$، استراتژی مخلوط با احتمالات $\sigma_S=(\rho,1-\rho)$ را در نظر می‌گیریم سپس برای CH-IDS بهره‌وری مورد انتظار استراتژی دفاع و بیکاری به صورت رابطه (۲۰) خواهد بود.

$$\begin{aligned} &Eu_R(Defend)=\rho.p.(\alpha.g_D-(1-\alpha).g_A-c_D)\\ &+(1-\rho).p.(-\beta.l_F-c_D)+(1-p).(-\beta.l_F-c_D)\\ &Eu_R(Idle)=\rho.p.(-g_A)+(1-\rho).p.0+(1-p).0=-\rho.p.g_A \end{aligned} \tag{۲۰}$$

با توجه به بی‌تفاوت بودن استراتژی دفاع یا بیکاری تحت استراتژی مخلوط σ_S داریم:

$$\begin{aligned} &Eu_R(Defend)=Eu_R(Idle)\\ &\rho^*=(\beta.l_F+c_D)/(p.\alpha.g_D+p.\alpha.g_A+p.\beta.l_F) \end{aligned} \tag{۲۱}$$

برای CH-IDS عامل R استراتژی مخلوط $\sigma_R=(\delta,1-\delta)$ را در نظر می‌گیریم پس برای گره S بهره‌وری مورد انتظار از دو حالت حمله و همکاری به صورت رابطه (۲۲) خواهد بود.

$$\begin{aligned} &Eu_S(Attack)=\delta.p.((1-\alpha).g_A-\alpha.g_D-c_A)+(1-\delta).p.(g_A-c_A)\\ &Eu_S(Cooperate)=\delta.p.(g_C-c_C)+(1-\delta).p.(g_C-c_C)\\ &+\delta.(1-p).(g_C-c_C)+(1-\delta).(1-p).(g_C-c_C) \end{aligned} \tag{۲۲}$$

با توجه به بی‌تفاوت بودن استراتژی حمله و همکاری تحت استراتژی مخلوط σ_R داریم:

$$\begin{aligned} &Eu_S(Attack)=Eu_S(Cooperate)\\ &\delta^*=(p.g_A-p.c_A-g_C+c_C)/(p.(\alpha.g_A+\alpha.g_D)) \end{aligned} \tag{۲۳}$$

به طور خلاصه وقتی رابطه (۲۴) برقرار است

$$p\geq(\beta.l_F+c_D)/(\alpha.g_D+\alpha.g_A+\beta.l_F) \tag{۲۴}$$

یک استراتژی مخلوط BNE به صورت رابطه (۲۵) وجود دارد.

$$\{(\sigma_S^*(a_S(\theta_S=1)=A\ ttack), a_S(\theta_S=0)=Cooperate), \quad \sigma_R^*(a_R(\theta_R)=Defend)\} \tag{۲۵}$$

به این معنی که وقتی CH-IDS عامل R، با احتمال δ^* استراتژی دفاع را بازی می‌کند، گره مخرب با احتمال ρ^*، استراتژی حمله و گره نرمال همیشه، استراتژی همکاری را بازی می‌کنند.

مزیت استفاده از بازی تشخیص حملات تک مرحله‌ای بالا، این است که CH-IDS عامل R، به صورت مداوم در هر مرحله زمانی در حال دفاع نمی‌باشد در نتیجه مصرف انرژی آن کاهش یافته و باعث بیشتر زنده ماندن گره می‌شود. هر چند یک احتمال پیشین p برای کنش‌ها در ابتدای مرحله در نظر گرفته شد اما مشکلی که هست این است که این مقدار باید در ابتدای هر مرحله زمانی محاسبه و به صورت پویا به‌روزرسانی شود چون برای هر مرحله مقدار متفاوتی دارد به همین منظور در قسمت بعدی، این بازی تک مرحله‌ای استاتیک را به بازی تشخیص حملات چند مرحله‌ای پویا گسترش می‌دهیم.

۴-۲- بازی تشخیص حملات چند مرحله‌ای

بازی زیر، بین گره S و CH-IDS عامل R است که به صورت تکراری در مرحله‌های زمانی t_k به‌طوری که $(k=1,2,\ldots,n)$ انجام می‌گردد. فرض می‌کنیم که بهره‌وری گره S و عامل R در مرحله t_k بازی با مرحله t_{k-1} آن یکسان است به عبارت دیگر گسستگی در آن نیست.

هم چنین فرض می‌کنیم که $h_s(t_k)$ تاریخچه[۲۱] کنش‌های گره s و $q_s(t_k)$، کنش گره s در مرحله t_k و $p(\theta_s=1|a_s(t_k),h_s(t_k))$ احتمال گره‌های مخرب در پایان مرحله t_k ام بازی باشد.

احتمال پسین CH-IDS عامل R را می‌توان با رابطه (۲۶) محاسبه کرد [۱۶، ۲۲].

$$p(\theta_s=1|a_s(t_k),h_s(t_k))=\frac{p(\theta_S=1|h_S(t_K)).p(a_S(t_K)|\theta_S=1,h_S(t_K))}{\sum_{\theta_S'\in\Theta_S}p(\theta_S'|h_S(t_K)).p(a_S(t_K)|\theta_S',h_S(t_K))} \tag{۲۶}$$

که $p(\theta_s|h_s(t_k))$ احتمال پسین به شرط $h_s(t_k)$ را نشان می‌دهد و هم چنین $p(a_s(t_k)|\theta,h_s(t_k))$ احتمال کنش $a_s(t_k)$ توسط گره S به شرط $h_s(t_k)$ در مرحله t_k ام بازی را نشان می‌دهد.

برای اینکه کنش‌ها و محاسبات CH-IDS واقعی باشد تأثیر نرخ تشخیص درست[۲۲] و تشخیص‌های اشتباه[۲۳] را نیز در محاسبه احتمال پسین در نظر می‌گیریم.

$$\begin{aligned} &p(\text{Attack}|\theta_s=1,h_s(t_k))=\alpha.\rho+\beta.(1-\rho)\\ &p(\text{Cooperate}|\theta_s=1,h_s(t_k))=(1-\alpha).\rho+(1-\beta).(1-\rho)\\ &p(\text{Attack}|\theta_s=0,h_s(t_k))=\beta\\ &p(\text{Cooperate}|\theta_s=0,h_s(t_k))=1-\beta \end{aligned} \tag{۲۷}$$

که $1-\alpha$ نرخ منفی تشخیص اشتباه و $1-\beta$ نرخ منفی تشخیص صحیح است.

بازی تشخیص حمله پویای چند مرحله‌ای یک مجموعه ۵ تایی $(N,\Theta,A,P(D),U)$ دارد که در آن:

- N ,Θ,A و U در تعریف قبلی آمده‌اند.

- $P(\mathrm{D}) = (p(\theta_s = 1 | h_s(t_k)), 1 - \mathrm{p}(\theta_s = 1 | h_s(t_k)))$ کـــــــــــــه $p(\theta_s = 1 | h_s(t_k))$ احتمال مخرب بودن گره‌های حسگر به شرط کنش‌های قبلی آن ($hs(t_k)$) در مرحله t_k را نشان می‌دهـد، کـه از طریق محاسبه $p(\theta_s = 1 | a_s(t_k), h_s(t_k))$ در آخر هر مرحله زمانی t_k به‌روزرسانی می‌شود.

از تعادل بیزی کامل[۲۴] (PBE) برای توصیف بازی تشـخیص حملـه پویای چند مرحله‌ای استفاده مـی‌کنـیم. بـا بـه‌روزرسـانی بـاور[۲۵]، گـره حسگر S و گـره CH-IDS در هـر مرحلـه بـازی اسـتراتژی یکسـانی را انتخاب نمی‌کنند و این استراتژی، به باور آنها در آن مرحله نسـبت بـه بازیگر مقابلش وابستگی دارد. بنابراین بر اساس PBE، سیستم کاملی از باورها در مورد نوع بازیگران مقابل به دست مـی‌آیـد و بهتـرین عکـس العمل‌ها از گره حسگر S و CH-IDS دریافت می‌شود.

در بازی تشخیص حمله پویای چند مرحلـه‌ای حتمـاً یـک تعـادل بیزی کامل مخلوط وجود دارد. برای اثبات ، فرض‌های زیر را داریم:

$\sigma_{S_K} = (\rho_K, 1-\rho_K)$: که در آن ρ_k نشانگر احتمال انتخاب کنش حملـه به وسیله گره حسگر مخرب ($\theta_S=1$) است.

$\sigma_{R_K} = (\delta_K, 1-\delta_K)$: که در آن δ_k نشانگر احتمـال کـنش دفـاع توسـط CH-IDS عامل R می‌باشد.

برای CH-IDS عامل R، سود مورد انتظار از کنش دفاع یا بیکـاری در مرحله زمانی t_k ، با رابطه‌های (۲۸) و (۲۹) محاسبه می‌شود.

$$\begin{aligned} &Eu_R(Defend) = \rho_K . p(\theta_S = 1 | h_S(t_K)).(\alpha.g_D - (1-\alpha).g_A - c_D) + \\ &(1-\rho_K).p(\theta_S = 1 | h_S(t_K)).(-\beta.l_F - c_D) + \\ &(1-p(\theta_S = 1 | h_S(t_K))).(-\beta.l_F - c_D) \end{aligned} \quad (۲۸)$$

$$\begin{aligned} &Eu_R(Idle) = \rho_K . p(\theta_S = 1 | h_S(t_K)).(-g_A) + \\ &(1-\rho_K).p(\theta_S = 1 | h_S(t_K)).0 + (1-p(\theta_S = 1 | h_S(t_K))).0 \\ &= -\rho_K . p(\theta_S = 1 | h_S(t_K)).g_A \end{aligned} \quad (۲۹)$$

با برقراری رابطه تساوی در رابطه‌های (۲۸) و (۲۹) داریم.

$$\begin{aligned} &Eu_R(Defend) = Eu_R(Idle) \\ &\rho_K^* = (\beta.l_F + c_D) / (p(\theta_S = 1 | h_S(t_K)).(\alpha.g_D + \alpha.g_A + \beta.l_F)) \end{aligned} \quad (۳۰)$$

برای گره حسـگر مخـرب $\theta_S = 1$ سـود مـورد انتظـار از کـنش حملـه و همکاری عبارت است از:

$$\begin{aligned} &Eu_S(Attack) = \delta_K . p(\theta_S = 1 | h_S(t_K)).((1-\alpha).g_A - \alpha.g_D - c_A) + \\ &(1-\delta_K).p(\theta_S = 1 | h_S(t_K)).(g_A - c_A) \end{aligned} \quad (۳۱)$$

$$\begin{aligned} &Eu_S(Cooperate) = \delta_K . p(\theta_S = 1 | h_S(t_K)).(g_C - c_C) + \\ &(1-\delta_K).p(\theta_S = 1 | h_S(t_K)).(g_C - c_C) + \\ &\delta_K .(1 - p(\theta_S = 1 | h_S(t_K))).(g_C - c_C) + \\ &(1-\delta_K).(1 - p(\theta_S = 1 | h_S(t_K))).(g_C - c_C) \end{aligned} \quad (۳۲)$$

با برقراری رابطه تساوی در رابطه‌های (۳۱) و (۳۲) داریم:

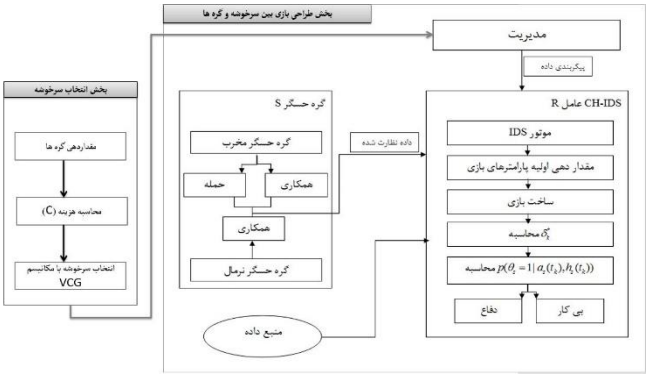
$$\begin{aligned} &Eu_S(Cooperate) = Eu_S(Attack) \\ &\delta_K^* = (p(\theta_S = 1 | h_S(t_K)).g_A - \\ &p(\theta_S = 1 | h_S(t_K)).c_A - g_C + c_C) \\ &/(p(\theta_S = 1 | h_S(t_K)).(\alpha.g_A + \alpha.g_D)) \end{aligned} \quad (۳۳)$$

به طور خلاصه ، یک استراتژی مخلـوط[۲۶] PBE وجـود دارد کـه از نمایه $(\sigma_{S_K}^*, \sigma_{R_K}^*)$ در مرحله زمـانی t_k بـه دسـت مـی‌آیـد، کـه $\sigma_{S_K}^*$ و $\sigma_{R_K}^*$ با پارامترهای α و β به دست می‌آینـد و بـا $p(\theta_S = 1 | h_S(t_K))$ به‌روزرسانی می‌شوند.

۴-۳- طراحی مکانیسم تشخیص بر اساس PBE

تعاملات بین گره حسگر S و CH-IDS عامل R در شکل ۲ نمایش داده شده است که در آن چهار موجودیت دیده می‌شود:

۱) منبع داده : شامل مقادیر مربوط به پارامترهای $g_D, g_A, c_A, \beta, \alpha, l_F, c_D, c_C$ و $p(\theta_S = 1 | h_S(t_K))$.
۲) مدیریت
۳) گره حسگر S
۴) CH-IDS عامل R



شکل ۲: مکانیسم تشخیص IDS بر اساس PBE

قبل از اینکه CH-IDS عامل R شروع به کار کند بخـش مـدیریت، CH-IDS را جهت کار کردن مطمئن و دقیـق پیکربنـدی مـی‌کنـد. در CH-IDS عامل R، موتور IDS که شامل روش‌هـای تشـخیص حمـلات است می‌تواند تصمیم بگیرد که آیا داده‌های نظارت شده مخرب هستند یا نرمال. سپس CH-IDS جهت شروع بازی پارامترهـای $g_D, g_A, c_A, c_C, \beta, \alpha, l_F, c_D$ و $p(\theta_S = 1 | h_S(t_K))$ را از منبـع داده مقـداردهی اولیـه می‌کند. بر اساس این پارامترها، تشخیص حمله یک مرحلـه‌ای سـاخته می‌شود. این بخـش خروجـی موتـور IDS را دریافـت کـرده و بـازی را تشکیل می‌دهـد کـه سـودهای آن از قبـل بـه صـورت دسـتی توسـط مدیریت تعریف شده است. فرآیند محاسبه δ_k^* نیاز به داده‌های ورودی

از بازی و همچنین پیاده‌سازی یک الگوریتم برای محاسبه احتمال دفاع با توجه به قضیه ارائه شده می‌باشد. بنابراین CH-IDS عامل R، با توجه به مقدار δ_k^* می‌تواند تصمیم بگیرد که با چه احتمالی دفاع کند یا بیکار بماند. در مرحله آخر CH-IDS، مقدار $p(\theta_s=1|a_s(t_k),h_s(t_k))$ را محاسبه کرده و مقدار $p(\theta_s=1|h_s(t_k))$ را با کمک عبارت $p(\theta_s=1|a_s(t_k),h_s(t_k))$ به‌روزرسانی کرده و مقدار $p(\theta_s=1|h_s(t_k))$ را برای استفاده در مرحله بعدی بازی در منبع داده ذخیره می‌کند.

Select Idle;
Do while
Compute δ_k^*;
Compute $p(\theta_s=1|a_s(t_k),h_s(t_k))$;
Update $p(\theta_s=1|h_s(t_k))$ with $p(\theta_s=1|a_s(t_k),h_s(t_k))$;
Store $p(\theta_s=1|h_s(t_k))$ into the Stored d ÷ata;
Select Defend with probability δ_k^*
END DO

الگوریتم (۲): تشخیص حمله بر اساس PBE برای CH-IDS عامل R

۵- ارزیابی نتایج حاصل از شبیه‌سازی

در این بخش می‌خواهیم نتایج حاصل از شبیه‌سازی انجام شده در محیط متلب ۲۰۱۵ را به نمایش در آوریم. در جدول ۴، پارامترها به همراه مقادیری که در نظر گرفته‌ایم آمده است.

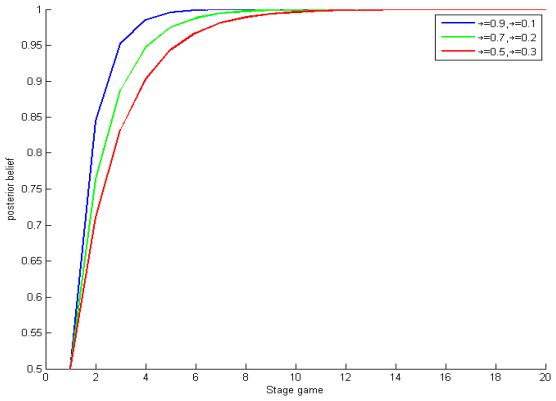
جدول ۴: پارامترهای شبیه‌سازی

پارامترها	مقادیر
تعداد گره‌های حسگر	۲۰ گره
تعداد گره‌های خودخواه	۲۰ درصد (۴ گره)
محل گره‌ها	تصادفی (۱۰۰×۱۰۰)
محل ایستگاه مرکزی	۱۵۰ × ۱۵۰
اندازه بسته	۴۰۰۰ بایت
انرژی آنالیز بسته‌ها	۰،۰۱ نانو ژول
اعتبار اولیه گره‌ها	۵ واحد
انرژی اولیه گره‌ها	۱ نانو ژول

در این بخش مقادیر مختلف باورهای پسین $p(\theta_s=1|a_s(t_k),h_s(t_k))$، را بر اساس ضرایب مختلف α و β در گره‌های مخرب مورد بررسی و مقایسه قرار می‌دهیم. همچنین تغییرات روند ρ_K^* و δ_K^* را با توجه به مقادیر مختلف α و β مورد بررسی قرار می‌دهیم و سپس عبارت $p(\theta_s=1|a_s(t_k),h_s(t_k))$ را با جایگزینی عبارت $p(\theta_s=1|h_s(t_k))$، بروز می‌کنیم. فرض می‌کنیم که پارامترهای توضیح داده شده بازی عبارتند از مقادیر زیر:

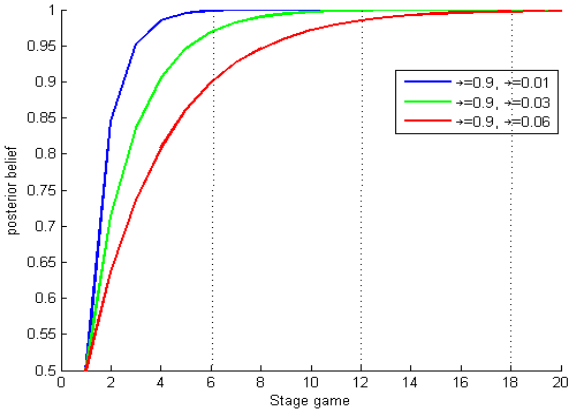
$$g_A=250, g_C=5, g_D=200, c_A=20, c_C=5, c_D=10, l_F=15$$

با دقت در شکل ۳ متوجه می‌شویم که در نرخ‌های تشخیص (α) بالا، سرعت تغییرات باور پسین زیاد است و سریع‌تر به سمت احتمال یک حرکت می‌کند. اگر $\alpha=0.9$ باشد در مرحله ششم باور پسین به مقدار یک می‌رسد و اگر $\alpha=0.7$ باشد در مرحله نهم یک می‌شود و اگر $\alpha=0.5$ باشد در مرحله دوازدهم یک می‌شود.



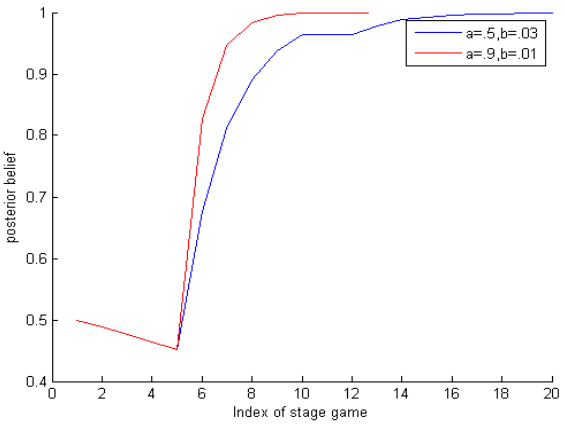
شکل ۳: نمودار باور پسین بازی بر حسب نرخ‌های تشخیص متفاوت

شکل ۴ نیز تغییرات باور پسین را بر حسب β متفاوت و α=0.9 ثابت نشان می‌دهد که در نتیجه آن با افزایش β، باور پسین با سرعت کمتری به مقدار یک نزدیک می‌شود. این باور با پارامتر β=0.01، در مرحله ششم و با پارامترβ=0.03 در مرحله دوازدهم و با پارامتر β=0.06 در مرحله هیجدهم به مقدار یک می‌رسد.



شکل ۴: نمودار باور پسین بازی بر حسب β متفاوت

در شکل ۵ فرض کرده‌ایم که $h_s(20)$ = [0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1 0 1 0] می‌باشد که در آن عدد یک نشان‌دهنده کنش حمله توسط و عدد صفر نشان‌دهنده کنش همکاری توسط گره در مرحله مربوطه بازی می‌باشد. یک‌های پیوسته نشان می‌دهند که گره به طور مداوم حمله می‌کند و صفرهای متوالی نشان می‌دهند که گره مخرب خودش را پنهان می‌کند یا به عبارت دیگر در این بازه زمانی به صورت نرمال عمل می‌کنند. در این قسمت ما شبیه‌سازی را طوری انجام داده‌ایم که تا زمانی که گره کنش صفر بوده یعنی نرمال بوده باور پسین به مخرب بودن آن کاهش می‌یابد اما تنها با یک بار کنش یک، یعنی کنش حمله، دیگر این باور نزولی نبوده و حتی اگر به صورت نرمال نیز عمل کند مقدار باور ثابت می‌ماند و اگر حمله کند مقدار باور به مخرب بودن افزایش پیدا می‌کند.



شکل ۵: نمودار باور پسین بر حسب α وβ متفاوت برحسب تاریخچه

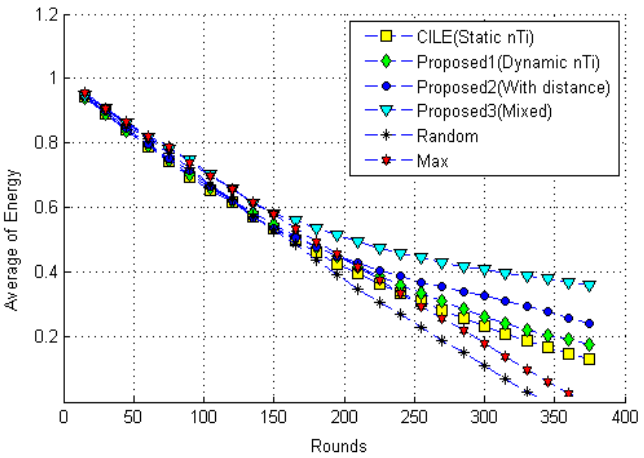
شکل ۵ نتایج $p(\theta_s=1|Attack,h_s(t_k))$ را با تاریخچه قبلی نشان می‌دهد. با دقت در آن متوجه می‌شویم که در نرخ‌های تشخیص بالا (α=0.9 و β=0.01) باور پسین گره‌های مخرب با سرعت بالایی به سمت یک می‌روند که در این شکل نمودار قرمز با نرخ تشخیص بالا و با تاریخچه اشاره شده در مرحله دهم بازی به مقدار یک می‌رسد یعنی از مخرب بودن گره اطمینان صددرصدی حاصل می‌کند در حالی که در نرخ‌های پایین تشخیص (α=0.5 و β=0.03) یعنی نمودار آبی رنگ دیرتر از قرمز و در مرحله هیجدهم به مقدار یک می‌رسد.

در بخش بعدی شبیه‌سازی که ترکیب دو بخش ۳ و ۴ است گره‌های خودخواه، به صورت تصادفی از بین گره‌ها انتخاب می‌شوند و رفتارشان در برش‌های زمانی تصادفی می‌باشد. با شروع به کار الگوریتم، گره‌ها هزینه خودشان را با توجه به رابطه‌های (۴) و (۵)، جهت سرخوشه شدن محاسبه می‌کنند و برای انتخاب سرخوشه جدید برای برش زمانی بعدی، هزینه را به سرخوشه جاری می‌فرستند. سرخوشه جاری بر طبق مکانیسم ارائه شده در بخش ۳، سرخوشه جدید را انتخاب می‌کند. همه بسته‌های خروجی گره‌ها از طریق سرخوشه به ایستگاه مرکزی ارسال می‌شوند. لازم به ذکر است که در برش زمانی اول، یکی از گره‌ها به صورت تصادفی به عنوان مجری رأی‌گیری، جهت انتخاب سرخوشه انتخاب می‌شود.

در شکل‌های ۶ و ۷، شش نمودار رسم شده و باهم مقایسه شده‌اند که در آنها:

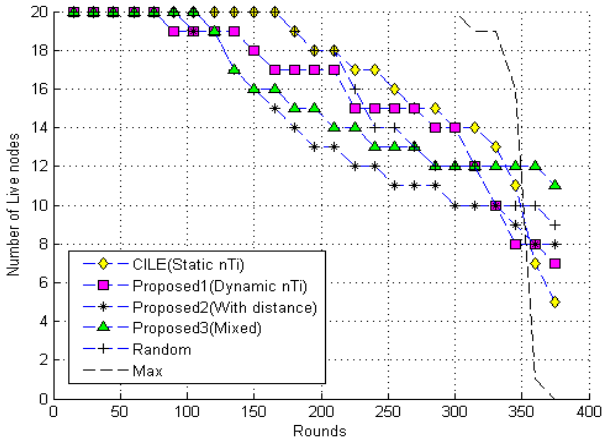
- نمودار اول (Max): در این نمودار گرهی که بیشترین انرژی باقی‌مانده را دارد به عنوان سرخوشه انتخاب می‌شود [۱۹، ۳۲].
- نمودار دوم (Random): در این نمودار سرخوشه به صورت تصادفی از بین گره‌ها انتخاب می‌شود [۱۵].
- نمودار سوم (CILE-Static nT_i): مربوط به کارهای قبلی انجام شده [۱۶، ۲۳] می‌باشد که در آن هزینه سرخوشه شدن با رابطه (۴) محاسبه می‌شود و nT_i در آنها به صورت ایستا در برش زمانی اول محاسبه می‌شود و فاصله گره تا ایستگاه مرکزی تاثیری در آن ندارد.
- نمودار چهارم (Dynamic nT_i): مربوط به روش اول ارائه شده در این کار می‌باشد که در آن nT_i به صورت پویا در هر برش زمانی محاسبه شده است و فاصله گره تا ایستگاه مرکزی تاثیری در آن ندارد (محاسبه هزینه با رابطه (۴)).
- نمودار پنجم (With Distance): در این نمودار هزینه سرخوشه شدن با رابطه (۵) محاسبه می‌شود و علاوه بر انرژی باقی‌مانده و اعتبار، فاصله گره از ایستگاه مرکزی نیز در محاسبه هزینه گره‌ها تأثیر داده شده است.
- نمودار ششم (Mixed): این نمودار حاصل ترکیب بخش ۳ و ۴ هست. در تمام پنج نمودار قبلی IDS سرخوشه به طور مداوم روشن است ولی در این نمودار سرخوشه با رابطه (۵) انتخاب می‌شود و پس از آن بازی طراحی شده بین سرخوشه و گره‌ها انجام می‌گیرد و IDS فقط در مواقعی تشخیص احتمال حمله، روشن می‌باشد.

با دقت در شکل ۶ متوجه می‌شویم که بعد از ۳۳۰ برش زمانی نمودار اول یا روش تصادفی بیشترین مصرف انرژی در کل خوشه را داشته و میانگین انرژی موجود در خوشه نزدیک ۰/۱ می‌باشد در همان فاصله زمانی روش ترکیبی یا نمودار ششم کمترین مصرف انرژی را داشته و میانگین انرژی کل خوشه حدود ۰/۴۵ می‌باشد. با گذشت زمان شیب نزولی این نمودار کمتر می‌شود و به دلیل بیرون کردن گره‌های مخرب از خوشه IDS کمتر روشن مانده و مصرف انرژی آن بهتر می‌شود و از سایر نمودارها فاصله باز می‌کند.



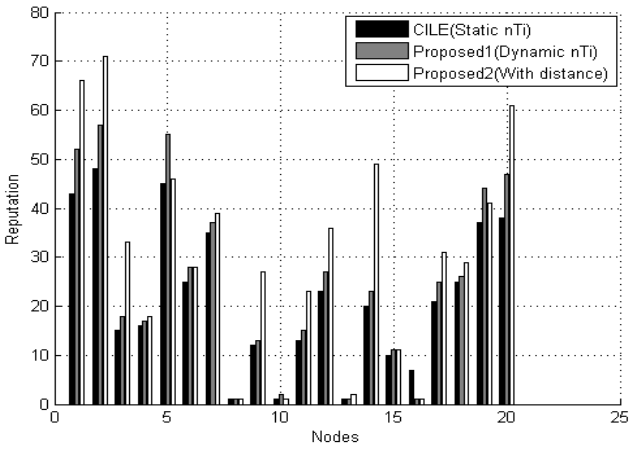
شکل ۶: میانگین انرژی باقی‌مانده گره‌ها در برش‌های مختلف زمانی

در شکل ۷ تعداد گره‌های زنده در خوشه، در برش‌های زمانی مختلف در سه نمودار نمایش داده شده است. که در انتهای برش زمانی ۳۳۰ ام روش ترکیبی بیشترین تعداد گره زنده را دارد. با توجه به شیب کاهشی نمودارها، تعادل مصرف انرژی گره‌ها، در نمودار ترکیبی بهتر از بقیه نمودارها می‌باشد و با شیب ملایمی کاهش می‌یابد. اگر میزان انرژی مصرفی در تمامی گره‌های موجود در خوشه متعادل باشد میانگین زمان خرابی هر گره افزایش یافته و به این ترتیب طول عمر شبکه افزایش خواهد یافت [۳۵].



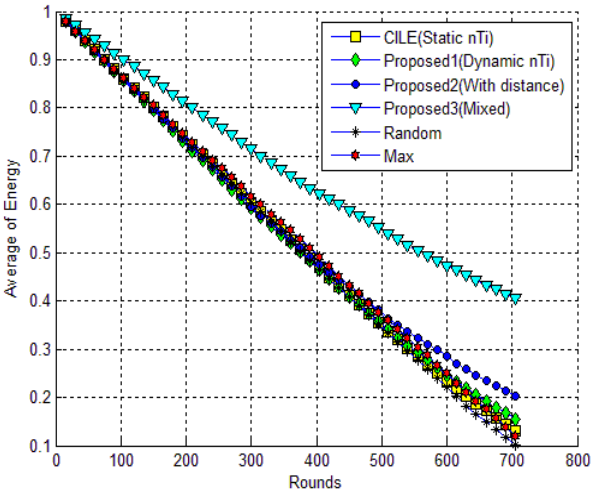
شکل ۷: تعداد گره‌های زنده در برش‌های زمانی مختلف

در شکل ۸ تعداد سرخوشه شدن هر گره در کل طول عمر خوشه، برای همه گره‌ها رسم شده است. هدف از این شکل نشان دادن این مطلب است که گره‌های مخرب و خودخواه، سرخوشه نمی‌شوند و از سرویس‌گیری محروم می‌شوند. با توجه به این که در روش‌های Max و Random رفتار گره‌ها در نظر گرفته نشده است در این نمودار رسم نشده‌اند. همچنین الگوریتم انتخاب سرخوشه در روش With distance با روش Mixed یکسان است و تعداد سرخوشه شدن گره‌ها در هر دو مقدار برابری دارند. با توجه به شکل می‌توان دریافت که گره‌های خودخواهی که در شبکه همکاری نداشتند (گره‌های ۸ و ۱۰ و ۱۳ و ۱۶) به تعداد کمتری سرخوشه شده‌اند.



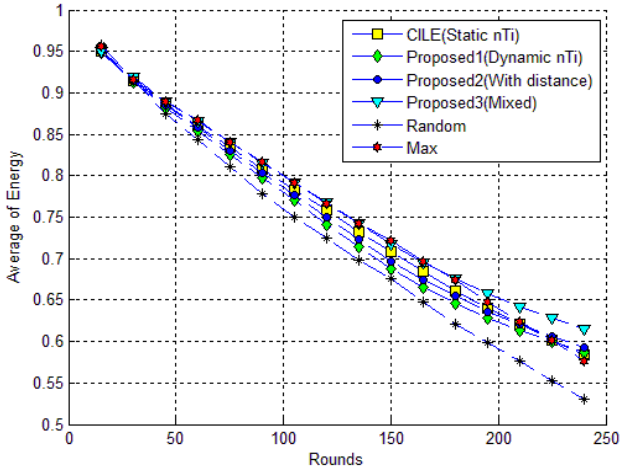
شکل ۸: تعداد سرخوشه شدن گره‌ها در طول عمر شبکه

اگر محل ایستگاه مرکزی را تغییر بدهیم با توجه به دور و یا نزدیک شدن ایستگاه به خوشه، نتایج فرق می‌کند. در صورت نزدیک شدن ایستگاه مرکزی به خوشه، به دلیل فاصله کمتر مصرف انرژی کمتر می‌شود و در نتیجه تعداد دوره‌های زمانی خوشه افزایش می‌یابد. به دلیل اینکه در روش سوم (Mixed-Proposed3) ارائه شده در برخی دوره‌ها IDS به حالت خواب می‌رود و مصرف آن کمتر می‌شود در نتیجه با بالا رفتن تعداد دوره‌های زمانی، از نمودار دیگر روش‌های ارائه شده و کارهای قبلی فاصله باز می‌کند و شیب نزولی کمتری پیدا می‌کند. در شکل ۶ فرض بر این بود که ایستگاه مرکزی در موقعیت (۱۵۰و۱۵۰) قرار دارد و در شکل ۹، فرض شده است که ایستگاه در موقعیت (۱۰۰و۱۰۰) قرار دارد. با دقت در شکل ۶ و ۹ مشاهده می‌شود که با افزایش تعداد دوره زمانی فاصله الگوریتم Proposed3 (Mixed) و الگوریتم Proposed (With distance)، از نمودار دیگر الگوریتم‌ها فاصله باز می‌کند.



شکل ۹: میانگین انرژی باقی‌مانده گره‌ها در برش‌های مختلف زمانی با موقعیت محلی (۱۰۰و۱۰۰) برای ایستگاه مرکزی

همچنین اگر تعداد گره‌های خودخواه را افزایش و یا کاهش بدهیم فاصله این نمودارها از همدیگر، به ترتیب کاهش و یا افزایش می‌یابد یعنی رابطه معکوس دارند این نتیجه در مقایسه شکل ۶ (۲۰ درصد گره‌ها خودخواه فرض شده است) با شکل ۱۰ (۶۰ درصد گره‌ها خودخواه فرض شده است) قابل مشاهده است.



شکل ۱۰: میانگین انرژی باقی‌مانده گره‌ها در برش‌های زمانی مختلف، با فرض ۶۰ درصدی گره‌های خودخواه

۶- نتیجه‌گیری

در شبکه‌های حسگر بی‌سیم، سرخوشه باید بسته‌های سایر گره‌ها را دریافت، آنالیز و به ایستگاه مرکزی ارسال کند از این‌رو انرژی بیشتری نسبت به سایر گره‌ها مصرف می‌کند. در این شبکه‌ها گره‌های

خودخواهی وجود دارند که تمایلی به سرخوشه شدن و سرویس‌دهی به شبکه ندارند. ما در این مقاله، برای تحمیل همکاری در بین همه گره‌های شبکه از مکانیسمی مبتنی بر سیستم تشویق و اعتباردهی نظریه بازی‌ها استفاده کردیم تا گره‌های خودخواه برای افزایش سرویس‌گیری از سایر گره‌های خوشه، مجبور به همکاری با آنها و ارائه سرویس شوند. تابع هزینه‌ای که ما در این مکانیسم استفاده کرده‌ایم علاوه بر پارامترهای مقدار انرژی باقی‌مانده و اعتبار یا شهرت گره به فاصله آن نسبت به ایستگاه مرکزی نیز بستگی دارد و در آن برش زمانی مورد انتظار برای زنده ماندن گره به صورت پویا در هر برش زمانی محاسبه می‌شود. هم چنین برای کاهش مصرف انرژی و کاهش نفوذ یک بازی بین IDS سرخوشه و گره مخرب ارائه دادیم تا با توجه به سابقه عملکرد گره‌ها بتوانیم رفتار متقابل آنها را نسبت به همدیگر پیش‌بینی کنیم و IDS سرخوشه را فقط در برش‌های زمانی که احتمال کنش حمله از سوی گره مخرب هست فعال کنیم. شبیه‌سازی مکانیسم‌های ارائه شده، بیانگر این بود که طول عمر شبکه در این کار نسبت به کارهای قبلی بیشتر شده و مصرف انرژی گره‌ها متعادل و عادلانه بود و با توجه به تعادل‌های نش به دست آمده گره‌های مخرب برای افزایش سرویس‌گیری و همزیستی در خوشه مجبور بودند کنش همکاری و حمله نکردن را انتخاب کنند. برای کارهای آتی می‌توان نوع خوشه را چندجهشی در نظر گرفت و در محاسبه هزینه پارامترهای دیگری از جمله ترافیک را تأثیر داد.

مراجع

[۱] رضا رافع و فرشته خدادادی، «ارائه یک الگوریتم شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم به کمک انتشارات محلی و کانال‌های کرم چاله قانونی»، *مجله مهندسی برق دانشگاه تبریز*، دوره ۴۴، شماره ۴، صفحه ۲۳، ۱۳۹۳.

[2] R. Mahidhar and A. Raut, "A Survey on Scheduling Schemes with Security in Wireless Sensor Networks," *Procedia Computer Science journal*, vol. 78, pp. 756-762, 2016.

[3] M. J. Osborne, "An Introduction to Game Theory," *Oxford University Press*, New York, NY, 2004.

[4] A. Ahmed, K. A. Bakar and M. I. Channa, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Frontiers of Computer Science*, vol. 9, no. 2, pp. 280–296, April 2015.

[5] N. Samian, Z. A. Zukarnain, W. K. G. Seah, A. Abdullah and Z. MohdHanapi, "Cooperation stimulation mechanisms for wireless multihop networks:Asurvey," *Journal of Network and Computer Applications*, vol. 54, pp. 88–106, 2015.

[6] J. Robert, H. Otrok and A. Chriqi, "RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks," *Computer Communications*, vol. 35, no. 4, pp. 487–499, February 2012.

[7] A. Agah, S.K. Das, K. Basu and M. Asadi, "Intrusion detection in sensor networks: a non-cooperative game approach," *IEEE Third IEEE International Symposium on Network Computing and Applications*, pp. 343–346, November 2004.

[8] Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," *Game theory for communications and networks*, 2006.

[9] Q. Zhu, C. Fung, R. Boutaba, T. Basar, "A game-theoretical approach to incentive design in collaborative intrusion detection networks," *Proceedings of GameNets*, 2009.

[10] P. Liu, W. Zhang, M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp.1-41, February 2005.

[11] C. A. Kamhoua and N. Pissinou, "Mitigating Selfish Misbehavior in Multi-Hop Networks Using Stochastic Game Theory," *IEEE 35th Conference on Local Computer Networks (LCN)*, March 2011.

[12] A. Agah, S. K. Das and k. Basu, "Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145–153, September 2007.

[13] Sh. Patila and S. Chaudharib, "DoS attack prevention technique in Wireless Sensor Networks," *Procedia Computer Science journal*, vol. 79, pp. 715–721, 2016.

[14] A. Rachedi, A. Benslimane, H. Otrok, N. Mohammed and M. Debbabi, "A Secure Mechanism Design-Based and Game Theoretical Model for MANETs," *Mobile Networks and Applications journal*, vol. 15, no. 2, pp. 191–204, April 2010.

[15] K.Samad, E. Ahmed and W. Mahmood, "Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks," *13th International Conference on Software, Telecommunications and Computer Networks*, pp. 15-17, September 2005.

[16] N. Mohammed, H. Otrok, M. Debbabi and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 89-103, Jan-Feb 2011.

[17] K. Ramesh and K. Somasundaram, "A Comprative Study of Clusterhead Selection Alghorithms in Wireless Sensor Networks," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 2, no. 4, November 2011.

[18] E. DeniRaj, "An Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks –Edrleach," *IOSR Journal of Computer Engineering (IOSRJCE)*, vol. 2, no. 2, pp. 39-44, July-Aug 2012.

[19] W. Wang and A. Jantsch, "An algorithm for electing cluster heads based on maximum residual energy," *international conference on Wireless communications and mobile computing*, pp. 1465-1470, 2006.

[20] G. Murali, R. S. Prasad and K.V. Bhaskar, "Leader Election for Intrusion Detection in MANET," *Network and Complex Systems journal*, vol. 5, no. 1, pp. 9-15, 2015.

[21] H. Otrok, N. Mohammed, L. Wang, M. Debbabi and P.Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Computer*

Communications journal, vol. 31, no. 4, pp. 708–721, March 2008.

[22] W. Wanga, M. Chatterjee, K. Kwiat and Q. Li, "A game theoretic approach to detect and co-exist with malicious nodes in wireless networks," *Computer Networks journal*, vol. 71, pp. 63–83, October 2014.

[23] E. Swetha, K. Sangeethasupriya and K. V. Bhaskar, "Intrusion Detection System in MANET with Secure Leader Election Model," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 7, pp. 996-1004, July 2013.

[24] K. Sun, P. Peng, P. Ning and C. Wang, "Secure Distributed Cluster Formation in Wireless Sensor Networks," *IEEE International Conference Computer Security Applications*, 2006.

[25] V. Sucasas, A. Radwan, H. Marques and J. Rodriguez, "A survey on clustering techniques for cooperative wireless networks," *Ad Hoc Networks journal*, vol. 47, pp. 53–81, September 2016.

[26] Y. B. Reddy, "A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks," *Third International Conference on Sensor Technologies and Applications*, August 2009.

[27] L.Tom, "Game-Theoretic Approach Towards Network Security A Review," *IEEE Conference on Circuit, Power and Computing Technologies*, July 2015.

[28] N. Labraoui, M. Gueroui and L. Sekhri, "A Risk-Aware Reputation-Based Trust Management in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 87, no. 3, pp. 1037–1055, April 2016.

[29] V. Richhariya and P. Kaushik, "A Reputation-based Incentive Framework for Mobile Ad Hoc Networks," *International Journal of Computer Applications*, vol. 120, no. 12, June 2015.

[30] S. Sabat and S. Kadam, "Adaptive Energy Aware Reputation Based Leader election for IDS in MANET," *IEEE International Conference on Communication and Signal Processing*, India, April 2014.

[31] D. Sathian, R. Baskaran and P. Dhavachelvan, "A Trustworthy Energy Efficient MIMO Routing Algorithm Based on Game Theory for WSN," *IEEE-International Conference On Advances In Engineering Science And Management*, March 2012.

[32] O. A. Wahab, H. Otrok and A. Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles," *Computer Communications journal*, vol. 41, no. 15, pp. 43–54, March 2014.

[33] I. Kantzavelou and S. Katsikas, "A game-based intrusion detection mechanism to confront internal attackers," *Computers & security journal*, vol. 29, pp. 859-874, June 2010.

[34] S. Roy, Ch. Ellis, S. Shiva, D. Dasgupta, V.Shandilya, Q.Wu, "A Survey of Game Theory as Applied to Network Security," *IEEE 43rd Hawaii International Conference on System Sciences*, pp. 1-10, March 2010.

[۳۵] معصومه واعظی و محمدعلی جبرئیل جمالی، «پروتکل مسیریابی جدید مبتنی بر کیفیت خدمات در شبکه‌های حسگر بی‌سیم با تحلیل سلسله مراتبی»، *مجله مهندسی برق دانشگاه تبریز*، دوره ۴۶، شماره ۲، صفحه ۳۵۵، ۱۳۹۵.

زیرنویس‌ها

[1] Incentive
[2] Multi-hop
[3] Vickrey Clarke Groves
[4] Reputation
[5] Cluster-Independent Leader Election
[6] Perfect Bayes–Nash Equilibrium
[7] Post Detection
[8] Co-Exist
[9] TimeSlot (TS)
[10] One-hop
[11] Distributed
[12] Cenralized
[13] Threshold
[14] Sampling
[15] Period time
[16] Best second price
[17] Action
[18] Defend
[19] Idle
[20] Mixed strategy
[21] Historic
[22] Detection rate
[23] False alarm or False detection
[24] Perfect bayesian nash EQ
[25] Belief
[26] Mixed strategy