کنفرانس بین المللی
مهندسی برق
۱۲ خرداد ۹۵، تهران، ایران
International Conference on Electrical Engineering

استفاده از مکانیزم مذاکره بین عامل‌ها برای مقابله با حمله جمینگ در بازار برق شبکه هوشمند

زهرا علوی کیا*، ناصر مزینی

دانشکده مهندسی کامپیوتر ـ دانشگاه علم و صنعت ایران

تهران ـ ایران

خلاصه

همزمان با ارتقاء شبکه برق فعلی به شبکه هوشمند، شبکه برق در ارتباطات سیستم‌های خود نسبت به حملات امنیتی از جمله حمله جمینگ به عنوان نوعی حمله محروم‌سازی از سرویس آسیب‌پذیرتر می‌شود. در زمینه بازار برق شبکه هوشمند برق، مهاجم طی حمله جمینگ سعی می‌کند مانع ارسال اطّلاعات اندازه‌گیری شده توسط حس‌گرهای از راه دور به مرکز کنترل شود و با سوء استفاده از استقرار قیمت کاذب به دلیل محاسبه غیرواقعی قیمت برق توسط مرکز کنترل، از شکاف قیمت در بازار برق به سود برسد. از این رو، اطمینان از مقاومت سیستم شبکه برق در برابر حمله جمینگ امری حیاتی است. در این مقاله، به دلیل مزایای فن‌آوری سیستم‌های چند عامله، شبکه هوشمند برق به عنوان یک سیستم چند عامله در نظر گرفته می‌شود و سپس برای مقابله با بروز حمله جمینگ در لایه فیزیکی شبکه ارتباطات آن در زمینه بازار برق راهکاری بر اساس پروتکل مذاکره قراردادی ارائه می‌گردد. در این روش پارامتر اعتماد به عنوان عاملی برای مقابله با محدودیت کارآمدی این پروتکل در مقیاس بزرگ و محیط باز نیز به‌کار گرفته می‌شود. قیمت برق بازار در زمان وقوع حمله از طریق نظارت مستقیم مرکز کنترل از طریق این پروتکل تعیین می‌گردد. نتایج پیاده سازی روش ارئه شده نشان می‌دهد می‌توان حتی با در نظر گرفتن وجود کاربران اخلال‌گر در محیط بازار، با اعمال این پروتکل در زمان بروز حمله جمینگ تا رسیدن به تعادل در بازار برق شبکه هوشمند تا حد زیادی از سود مهاجم کاسته و در نتیجه انگیزه آن را برای حمله از بین برد.

کلمات کلیدی: شبکه هوشمند، بازار برق، حمله جمینگ، سیستم چند عامله، پروتکل مذاکره قراردادی، اعتماد، امنیت

۱. مقدمه

شبکه هوشمند برق به عنوان نسل آینده شبکه برق شناخته می‌شود و اساساً شبکه الکترونیکی مدرنی است که با استفاده از فن‌آوری اطّلاعات و ارتباطات، انرژی را از تولیدکنندگان به مصرف کنندگان منتقل می‌کند و اطّلاعاتی چون چگونگی رفتار

* **Email: alavikia_z@com.iust.ac.ir**

تولیدکنندگان و مصرف‌کنندگان را به‌صورت خودکار جمع‌آوری و دنبال می‌کند تا با کنترل وسایل منازل مصرف‌کنندگان در مصرف انرژی صرفه جویی شود، هزینه کاهش یابد و همچنین کارایی، قابلیت اطمینان و پایداری و ثبات تولید و توزیع برق بهبود یابد[۱]. شبکه هوشمند برق با به‌کارگیری فن‌آوری بروز در تولید، انتقال و مصرف برق باعث انقلابی در اقتصاد، محیط زیست و امنیت ملّی می‌شود[۲]. شبکه هوشمند برق در برگیرنده نهادهای واقع در سراسر شبکه برق از تولیدکننده انرژی گرفته تا وسایل خانگی خانه یا محل کار است و به‌منظور مدیریت هوشمندانه برق، حامی همکاری بین این نهادها در زمان واقعی[1] است[۳].

اگرچه طراحی و اجرای شبکه هوشمند برق کمک شایانی به حفظ منابع می‌کند امّا از طرفی افزایش مسائل جدید و چالش‌هایی در مورد عملکرد مؤثر سیستم برق و قدرت، آسیب‌پذیری‌هایی در مقابل شکاف‌های امنیتی برای شبکه به‌وجود می‌آورد. حمله جمینگ[2] یکی از حملات محروم‌سازی از سرویس[3] است که بر روی لایه فیزیکی شبکه ارتباطات در بازار برق شبکه هوشمند برق رخ می‌دهد [۲]. حمله جمینگ جدّی‌ترین تهدید امنیتی در زمینه شبکه‌های حسگر بی‌سیم (WSN)[4] است چرا که می‌تواند به‌راحتی حتّی شبکه‌ای که از مکانیزم‌های امنیتی لایه بالای قوی استفاده می‌کند را از کار بیاندازد. و دلیل آن این است که اغلب در طراحی اولیه شبکه‌های حسگر بی‌سیم نادیده گرفته می‌شود[۴].

در زمینه بازار برق شبکه هوشمند برق، طی حمله جمینگ مهاجم سعی می‌کند مانع ارسال اطّلاعات اندازه‌گیری شده توسط حسگرهای از راه دور به مرکز کنترل شود که این باعث بی‌ثباتی سیستم برق و یا حتی خاموشی منطقه‌ای می‌شود[۵]. در حین این حمله، مهاجم سیگنال‌های نامطلوبی در کانال ارتباطات منتشر می‌کند تا در انتقال داده‌های اندازه گیری شده مداخله نماید، که این منجر به دریافت اطّلاعات اندازه‌گیری شده ناقص در زمان واقعی در مرکز کنترل می‌شود. به دنبال این حمله، نظارت برخط و برآورد وضعیت ممکن است قادر به انعکاس وضعیت عملیاتی واقعی از سیستم نباشند، و بنابراین قیمت برق در آن مورد به اشتباه محاسبه شود و در نتیجه، عموم مصرف‌کنندگان و تأمین‌کنندگان برق به‌لحاظ اقتصادی متضرّر شوند، و این در حالی است که مهاجم می‌تواند از شکاف قیمت در بازار برق به سود برسد [۶]، [۷]. بنابراین، به‌کارگیری اقدامات متقابل در برابر حمله جمینگ در محیط‌های WSN به‌ویژه با توجه به این که شبکه هوشمند برق به‌دلیل زیادی تعداد دستگاه‌های هوشمند و مکان‌های فیزیکی به دور از شرکت تأمین برق مستعد ضبط و تسخیر فیزیکی و استفاده از کانال‌های ارتباطی بی‌سیم ناامن است از اهمیت بسیار زیادی برخوردار است [۶]، [۸].

۲. شبکه هوشمند برق

افزایش منابع تولید پراکنده، و نیاز به ارائه منبع تولید انرژی قابل اعتماد و امن برای مصرف‌کنندگان منجر به ظهور نوع جدیدی از سامانه کنترل نیرو به نام شبکه هوشمند برق شده است. هدف از کنترل نیرو، تولید و انتقال برق در یک سیستم به‌هم‌پیوسته است به‌طوری که تا حد امکان اقتصادی و قابل اعتماد بوده و همزمان با آن تغییرات ولتاژ و فرکانس در یک محدوده مجاز نگاه داشته شود [۸].

[1] Real Time
[2] Jamming Attack
[3] Denial of Service
[4] Wireless Sensor Networks

اساساً شبکه هوشمند برق ترکیبی از کاربردهای اطّلاعات و ارتباطات است که فن‌آوری‌های تولید، انتقال، توزیع، و استفاده نهایی مشتریان را به‌هم مربوط می‌سازد[۹]. شبکه خودکار و به‌طور گسترده توزیع‌شده انتقال انرژی، یا همان شبکه هوشمند برق، به‌وسیله یک جریان دو طرفه برق و اطّلاعات شناخته می‌شود و قادر است همه چیز را از نیروگاه‌های برق گرفته تا ترجیحات مشتری در مورد وسایل خانگی برقی رصد نماید. شبکه هوشمند برق از مزیّت‌های محاسبات توزیع‌شده و ارتباطات در درون شبکه بهره می‌گیرد تا اطّلاعات را در زمان واقعی منتقل کند و تعادل تقریباً آنی عرضه و تقاضا را در سطح دستگاه فراهم سازد [۱۰].

۳. شبکه هوشمند برق و انطباق آن با سیستم‌های چند عامله

شاکله این شبکه برق نو که تحت عنوان شبکه هوشمند شناخته شده است مفهوم گسترده‌ای دارد و در آن شبکه مدرن برق با بخش بزرگی از منابع انرژی بدون کربن به‌وسیله یک شبکه ارتباطی و نظارتی تعامل خواهد داشت. با وجود یک ساختار غیر متمرکز جدید، تولید برق از لحاظ قدرت در مقیاس بسیار پایین تر و از نظر تعداد ژنراتور یا مولد برق در مقیاس بسیار بالاتری صورت می‌گیرد. به‌عبارت دیگر، ما باید تعداد خیلی بیشتری ژنراتور با میزان قدرت پایین را مدیریت کنیم؛ مثلاً یک نیروگاه بزرگ با سوخت زغال سنگ می‌تواند با صدها توربین بادی جایگزین شود. این تکامل باعث بروز یک مشکل عمده می‌گردد: چگونه انرژی تعداد زیادی ژنراتور را مدیریت و به‌طور مؤثر و قابل اطمینان حتی با بار الکتریکی بیشتر مورد بهره‌برداری قرار دهیم؟ روش‌های کنترل کلاسیک برای سیستم‌های در این مقیاس مناسب نیستند، و به این ترتیب باید سیستم کنترل و نظارت دیگری را یافت.

سیستم‌های چند عامله، مفهومی که به‌طور عمده تا همین اواخر در علوم کامپیوتر استفاده می‌شود، یک راه حل جایگزین بسیار امیدبخش است. سیستم‌های چند عامله راه نسبتاً جدیدی برای حل مشکلات هستند که از مزایای هوش مصنوعی و محاسبات توزیع‌شده بهره می‌برند. اساساً سیستم‌های چند عامله سیستمی هستند که در آن چندین عامل تعاملی و هوشمند به‌منظور دستیابی به اهداف خود (اهداف صاحبان خود) در یک محیط مشاهده و عمل می‌کنند. بنابراین، هسته اصلی سیستم‌های چند عامله موجودیت‌های نرم‌افزاری به نام عامل هستند[۶]. قدرت درونی سیستم‌های چند عامله، حداقل در زمینه مدیریت انرژی، عبارت است از توانایی تعامل عامل‌ها با یکدیگر[۱۱]. شبکه هوشمند برق متشکّل از موجودیت‌هایی به نام عامل هوشمند در نظر گرفته می‌شود که وظیفه کنترل و پایش شبکه توزیع و انتقال برق را بر عهده دارند که این به شبکه طبیعت توزیع‌شده می‌بخشد [۱۲].

۴. امنیت در شبکه هوشمند برق

تقاضای بیشتر برای به‌کارگیری شبکه حسگر بی‌سیم در برنامه‌های کاربردی با مأموریت حیاتی چون شبکه هوشمند برق آن را بیشتر در معرض کاربران خرابکاری که در تلاش برای حمله به سیستم هستند قرار می‌دهد [۱]. شبکه هوشمند برق یک سیستم سایبری فیزیکی است و حمله به آن می‌تواند در عملکرد بازار برق یا سیستم قدرت اختلال ایجاد کند [۲]. انواع مهاجمانی هستند که وجود آن‌ها احتمالاً بدیهی به شمار می‌رود. برخی از مشتریان شرکت تأمین برق ممکن است با هدف کاهش صورت حساب برق خود به سیستم حمله کنند. برخی از مهاجمان ممکن است با دسترسی به سیستم صدور صورت

حساب برق یا با باج‌خواهی و تهدید مایل به درآمدزایی برای خود باشند. دیگر تهدیدات ممکن است با انگیزه شرورانه‌تری باشد و به دنبال خاموش کردن و از کار انداختن کل شبکه باشد [۱۳]. حملاتی که علیه در دسترس بودن شبکه رخ می‌دهد معمولاً تحت عنوان حمله محروم‌سازی از سرویس شناخته می‌شوند و هدف آن‌ها از دسترس خارج کردن شبکه‌های بی‌سیم، خراب کردن و یا ایجاد اختلال در عملکرد شبکه است[۱۴]. این حملات امنیتی عملکرد شبکه هوشمند برق به عنوان یک WSN را به لحاظ مصرف انرژی و توان در حد زیادی وخیم تر می‌کند[۱]. یکی از حملات محروم‌سازی از سرویس جمینگ است که نوع شایعی از حمله به لایه فیزیکی شبکه ارتباطات شبکه هوشمند برق است[۵]، [۱۴].

۱.۴ حمله جمینگ در بازار برق شبکه هوشمند

به‌طور کلی، جمینگ به‌صورت عملی تعریف می‌شود که عامدانه انرژی الکترومغناطیس را با هدف منقطع کردن و یا جلوگیری از انتقال سیگنال به سمت یک سامانه ارتباطی هدایت می‌کند. حملات محروم‌سازی از سرویس به‌وسیله پرکردن شبکه با اطّلاعات "بی‌فایده" مانع به‌کارگیری نرمال یا مدیریت ارتباطات می‌شود. در حمله جمینگ نیز فرکانس رادیویی[1] که توسط مهاجم منتشر می‌شود معادل اطّلاعات "بی‌فایده" ای است که توسط گره[2] همه حسگرها دریافت می‌شود [۱۵].

در زمینه بازار برق شبکه هوشمند برق، طی حمله جمینگ مهاجم سعی می‌کند مانع ارسال اطّلاعات اندازه‌گیری شده توسط حسگرهای از راه دور به مرکز کنترل شود که این باعث بی‌ثباتی سیستم برق و یا حتی خاموشی منطقه‌ای می‌شود[۲]. در حین این حمله، مهاجم از طریق نقاط ناامن شبکه سیگنال‌های نامطلوبی در کانال ارتباطات منتشر می‌کند تا در انتقال داده‌های اندازه گیری شده مداخله نماید، که این منجر به دریافت اطّلاعات اندازه‌گیری شده ناقص در زمان واقعی در مرکز کنترل می‌شود. به‌دنبال این حمله، نظارت برخط و برآورد وضعیت ممکن است قادر به انعکاس وضعیت عملیاتی واقعی از سیستم نباشد، و بنابراین قیمت برق در آن مورد به اشتباه محاسبه شود و در نتیجه، عموم مصرف‌کنندگان و تأمین‌کنندگان برق به‌لحاظ اقتصادی متضرّر شوند، و این در حالی است که مهاجم می‌تواند از شکاف قیمت در بازار برق به سود برسد [۶]. انگیزه مهاجم از حمله جمینگ، تغییر قیمت بازار برق است. مکانیزم قیمت‌گذاری به تخمین از وضعیت حسگرها بستگی دارد. امّا هنگامی‌که حسگرها مورد حمله جمینگ قرار می‌گیرند، سنجش و اندازه گیری‌های تخمین زننده-های وضعیت از دسترس مرکز کنترل خارج می‌شوند. عمدتاً به دلایل زیر مهاجم از میان تمام حسگرهای شبکه هوشمند برق تنها به تعداد محدودی حمله خواهد نمود:

۱- حملات بیش از حد ممکن است منجر به خاموشی شده و در نتیجه مانع تغییر قیمت می‌شود.
۲- حمله جمینگ در وسعت زیاد ممکن است جداً احتمال خطر شناسایی شدن را افزایش دهد.

فرایند حمله جمینگ در بازار برق شبکه هوشمند برق به‌شرح زیر است:

۱- مهاجم در ابتدای یک شکاف زمانی کانال‌هایی را در شبکه مورد حمله جمینگ قرار می‌دهد تا مقادیر سنجش‌شده را از دسترس خارج نماید و باعث شود قیمت‌های زمان واقعی در شین‌های متناظر نامعلوم گردد.

[1] Radio Frequency
[2] Node

۲- مرکز کنترل برای مدل dc OPF [1] قیمت‌های پیش فرض[2] را جایگزین مقادیر سنجش‌شده از دست‌رفته می‌کند.

۳- مهاجم به رصد بازار برق و ارسال جمینگ به مکان‌های اندازه‌گیری ناامن در کل شکاف زمانی ادامه می‌دهد.

۴- مهاجم می‌تواند با دسترسی به مقادیر سنجش‌شده در زمان واقعی، قیمت زمان واقعی را پس از دست کشیدن از حمله تخمین بزند.

با مقایسه قیمت زمان واقعی در حین و پس از حمله، مهاجم برق را به قیمت پایین‌تر خریداری می‌کند و به قیمت بالاتر به فروش می‌رساند تا از تفاوت میان دو قیمت به سود برسد [۵].

۵. مروری بر راهکارهای مقابله با حمله جمینگ

۱.۵ راهکارهای مقابله با حمله جمینگ در شبکه‌های حسگر بی‌سیم

کارهای تحقیقاتی زیادی استفاده از سخت‌افزارهای موجود در شبکه‌های حسگر بی‌سیم فعلی را برای مقابله با حمله جمینگ پیشنهاد می‌دهند، در حالی‌که برخی دیگر الزامات طراحی جدید گره‌ها را پیشنهاد می‌کنند که می‌تواند به‌طور مؤثر با این حمله مقابله کند. مزیت اصلی روش ابتدایی در این است که پیاده سازی آن بسیار ارزان‌تر و آسان‌تر بوده و با سخت افزارهای در دسترس موجود سازگارتر است؛ امّا با این وجود هنوز نمی‌تواند به آسانی با حملات سنگین جمینگ مقابله نماید. از طرفی پیشنهاد الزامات طراحی جدید گره‌ها می‌تواند به‌طور مؤثرتر با جمینگ مقابله نماید. امّا پیاده سازی این گره‌ها نیازمند حجم قابل توجهی تحقیقات است که هزینه مربوط به آن به‌شدّت افزایش می‌یابد. علاوه بر این، این روش هیچ سازگاری با سخت‌افزارهای موجود ارائه نمی‌دهد [۵]. لی[3] و همکارانش یک تکنیک ضد جمینگ با پهنای باند محدود پیشنهاد دادند که حسگرهای راه دور می‌توانند جهت تحویل اطّلاعات و جلوگیری از مداخله جمینگ از چندین کانال استفاده کنند. کاگالی[4] و همکارانش پایداری شبکه را با پیچیدگی و هزینه معاوضه کرده و برای گره حسگرها جفت اختصاص دادند به‌طوری که یکی از آن‌ها بیرون از منطقه تحت جمینگ قرار می‌گیرد تا یک اتصال ارتباطی فرضی بین دو منطقه به منظور عبور اطّلاعات از خارج از منطقه تحت جمینگ ایجاد نماید. ژو[5] و همکارانش به امید مقابله با حمله جمینگ از روش گشت‌زنی[6] در کانال که با فرکانس بنا به تقاضا[7] سروکار دارد استفاده می‌کند و دو روش متفاوت گشت‌زنی در کانال را مورد مطالعه قرار داده است [۱۵].

همان‌طور که پیش‌تر نیز اشاره شد، قابلیّت‌های شبکه هوشمند، پویایی و پیچیدگی‌های بسیاری به‌وجود می‌آورد و یکی از رویکردها برای مقابله با این پیچیدگی، به‌کار گرفتن راه‌حل‌های توزیع‌شده از جمله سیستم‌های چند عامله است. استفاده از بستر سیستم‌های چند عامله به‌منظور ساخت شبکه خود بازیاب هوشمند، می‌تواند به‌عنوان یک راه کار نوین برای ساخت شبکه هوشمند با قابلیّت اطمینان و امنیّت بالاتر محسوب شود. در توسعه سیستم‌های هوشمند، الگوی عامل به دلیل دارا بودن ویژگی‌هایی چون خود مختاری، انعطاف پذیری و رفتار حل مسئله به‌وسیله همکاری با عامل‌های دیگر یک دستاورد

[1] Direct Current Optimal Power Flow (DCOPF)
[2] Default
[3] Li
[4] Cagali
[5] Xu
[6] Surfing
[7] On-demand

نویدبخش به‌شمار می‌رود [۲]. چنانچه شبکه هوشمند برق را به‌عنوان یک سیستم چند عامله در نظر بگیریم که متشکّل از چندین عامل خودمختار است، دو نوع روش تشخیص و مقابله با حمله جمینگ تحت عنوان راه‌حل‌های مبتنی بر عامل در مقاله [۴] ارائه شده است. در این گروه از رویکردهای مقابله با حمله جمینگ، عامل‌های متحرک قادرند بقای شبکه حسگر بی‌سیم را ارتقاء بخشند.

۱- سیستم مورچه: میورالیدهارن[1] و اوزادشیو[2] پیشنهاد استفاده از الگوریتم مورچه به عنوان یک اقدام متقابل کارآمد در برابر حملات جمینگ در یک شبکه حسگر بی‌سیم را مطرح کردند. در واقع، مورچه‌ها به عنوان یک نوع عامل متحرک در نظر گرفته می‌شوند. اولین مجموعه مورچه‌ها از میان گره‌ها به‌صورت تصادفی عبور می‌کنند و زمانی که به مقصد خود رسیدند به‌عنوان یک وسیله ارتباطی غیرمستقیم با دیگر مورچه‌ها در مسیرهای پیمایش شده فرمون[3] به جای می‌گذارند. مقدار فرمونی که توسط عامل‌های مورچه قبلی باقی می‌ماند این احتمال را که همان مسیر در دور جاری تکرار شود افزایش می‌دهد. پارامترهایی چون هاپس[4]، انرژی، فاصله، از دست دادن بسته، نسبت سیگنال به نویز[5]، نرخ خطای بیت[6] و تحویل بسته احتمال انتخاب یک مسیر یا راه‌حل خاص را تحت تأثیر قرار می‌دهد. همچنین تبخیر فرمون در طول زمان مانع از غالب شدن راه‌حل‌های شبه بهینه[7] در ابتدا می‌شود.

مزیت اصلی راه‌حل مورچه این است که عامل‌های مورچه در شبکه پخش می‌شوند و پیوسته برای یافتن مسیرهای بهینه و بدون جمینگ برای انتقال داده‌ها با در نظر داشتن گره‌ها و پارامترهای حیاتی شبکه (مانند انرژی باقی‌مانده گره، ازدست دادن بسته، نسبت سیگنال به نویز) در تلاش‌اند. در شبکه‌های حسگر بی‌سیم بزرگ این روش یک مزیت روشن نسبت به روش‌های دیگر دارد چرا که می‌تواند بیشتر با محیط انطباق پیدا کند. یک عامل مورچه می‌تواند در گره‌ای که مورد حمله قرار گرفته باقی بماند و پس از تشخیص کانال ارتباطی "پاک" و بدون خطر به یک گره مجاور حرکت نماید (مکث جمینگ).

متاسفانه این سیستم در شبکه‌های حسگر بی‌سیم شبیه سازی در مقیاس وسیع آزمایش نشده است (شبیه سازی در توپولوژی متشکل از ۱۶ گره انجام شده است)، از این رو مقیاس پذیری آن سؤال برانگیز است. همچنین هزینه اضافی محاسباتی و انرژی مورد نیاز مورچه‌ها ارزیابی نشده است. شایان ذکر است نویسندگان اطّلاعات مربوط به اینکه با چه سرعتی مسیرهای پیمایش شده فرمونی قادر به واکنش نشان‌دادن در برابر مهاجمان زیرک هستند را هم حذف کرده‌اند. در نهایت، در صورتی که بخش قابل توجهی از گره‌های شبکه مورد حمله جمینگ قرار بگیرند، احتمالاً مورچه‌ها موفق به تضمین عملکرد بی وقفه شبکه نمی‌شوند.

۲- طراحی خط سیر مقابله با جمینگ[8]: الگوریتم طراحی خط سیر جهت جلوگیری از جمینگ الگوریتمی برای همجوشی داده‌ها و مقابله با جمینگ در شبکه‌های حسگر بی‌سیم بوده و مبتنی بر این باور است که عامل‌های متحرک به همراه همجوشی داده‌ها می‌توانند نقش حیاتی در زمینه امنیت و پایداری یک شبکه حسگر بی‌سیم داشته باشند. هدف طراحی این الگوریتم دوگانه است:

---

[1] Muraleedharan
[2] Osadciw
[3] Pheromone
[4] Hops
[5] Signal to Noise Ratio
[6] Bit Error Rate
[7] Suboptimal
[8] Jam Avoidance Itinerary Design (JAID)

۱) مسیرهای نزدیک به بهینه[1] را برای عامل‌های متحرکی که به‌صورت تدریجی همزمان با بازدید گره، داده را ترکیب می‌کند محاسبه می‌نماید؛

۲) در مواجهه با حملات جمینگ علیه شبکه، خط سیر عامل متحرک را با حذف گره تحت جمینگ از فرایند همجوشی داده‌ها جهت ممانعت از ورود آن به مناطق تحت جمینگ از طریق بروز رسانی با پیچیدگی کم تغییر می‌دهد در حالی که اخلالی در در انتشار داده کارآمد توسط حسگرهای در حال کار ایجاد نمی‌کند.

برای تحقق هدف دوم، عنصر پردازشگر[2] الگوریتم جَم[3] را به‌منظور نگاشت منطقه تحت جمینگ استفاده می‌کند و گره‌های مشکل دار را شناسایی می‌کند. علاوه بر این، در فواصل زمانی خاص جستجو و تحقیق انجام می‌دهد تا به‌محض آن که گره‌ها کار خود را از سر گرفتند و پاک شدند مطلع شود. با فرض این که کل شبکه تحت تأثیر قرار نگیرد، عامل‌های متحرک برنامه ریزی شدند که از گره‌های تحت جمینگ بازدید نکنند. در عوض، از گره‌های پیرامون منطقه یا مناطق تحت جمینگ که تحت تأثیر قرار نگرفتند بازدید کنند تا از خطر امنیتی و در نتیجه فروپاشی شبکه جلوگیری به‌عمل آید. اگر تعداد گره‌های تحت جمینگ پایین تر از حد آستانه خاصی باشد، JAID تنها خط سیر برنامه ریزی شده قبل از حمله جمینگ را تغییر می‌دهد (گره‌های قطع شده را به گره‌های عاری از جمینگ "وصل" می‌کند) تا سرعت عمل الگوریتم را افزایش دهد. در غیر این صورت، JAID خط سیر عامل‌ها را به استثنای منطقه تحت جمینگ بازسازی می‌کند.

نویسندگان این مقاله عملکرد JAID را در توپولوژی شبیه سازی شده با بررسی سناریویی که در آن چندین مهاجم به شبکه حسگر بی‌سیم متشکل از ۱۰۰ گره که به‌صورت تصادفی در میدانی مستقر شدند جمینگ ارسال می‌کنند مورد ارزیابی قرار دادند (شکل ۱۰). نویسندگان فرض کردند که مهاجمان محدوده جمینگ محدودی دارند که کل شبکه را پوشش نمی‌دهد چرا که همانطور که خود اذعان دارند، در مواقعی که کل شبکه مورد حمله جمینگ قرار بگیرد، هیچ راه حل الگوریتمیکی نمی‌تواند به‌طور مؤثر از شبکه دفاع نماید.

عامل‌های متحرک مورد استفاده در JAID مزیت مستثنی کردن گره مشکل دار از خط سیر خود را دارند و داده‌ها را به‌طور کارآمد از گره‌های در حال کار به عضو پردازشگر تحویل می‌دهند. علاوه بر این JAID مسیرهای نزدیک به بهینه را برای عامل‌های متحرک محاسبه می‌نماید که این هزینه انرژی مورد نیاز برای انتقال را به حداقل می‌رساند. امّا همانطور که پیش‌تر به آن اشاره شد، نقطه ضعف JAID این است که در موردی که مهاجم حمله کارآمدی را در برابر تمام گره‌ها به‌طور همزمان اجرا کند نمی‌تواند از شبکه دفاع نماید [۴].

۲.۵ راهکارهای مقابله با حمله جمینگ در بازار برق شبکه هوشمند

تا کنون کارهای بسیاری پیرامون حملات جمینگ بر روی شبکه‌های حسگر بی‌سیم انجام شده است، امّا تعداد کمی از آن‌ها به این حمله در شبکه هوشمند برق توجه داشته‌اند [۵]، [۱۳]. به منظور حل مشکلات امنیتی قدیمی و جدید مؤثر بر عملکرد شبکه هوشمند برق برخی از محقّقان پس از بررسی چالش‌های امنیتی آن پیشنهادات و راهکارهایی جهت ارتقاء

[1] near-optimal
[2] Processing Element (PE)
[3] A Jammed-Area Mapping Service for Sensor Networks (JAM)

امنیت آن ارائه داده‌اند که در این بین بعضی تنها طرح‌هایی را ارائه کرده‌اند و هیچ پیاده سازی از آن‌ها در دسترس نیست. مقاله[۵] با الهام از تئوری بازی ها، بر اساس مدل بازاریابی برق یک بازی چند نفره پویا بین مهاجم و مدافع پیشنهاد می‌دهد که در آن استراتژی‌های بهینه توسط دو طرف اجرا می‌شود تا سود خود را به حداکثر برسانند. برای تجزیه و تحلیل استراتژی مهاجم و مدافع، روش‌های مبتنی بر تئوری بازی‌ها در شبکه هوشمند برق در مقالات دیگر نیز به کار گرفته شده‌اند. شباهت این روش‌ها با روش‌های ارائه شده در حوزه سیستم‌های چند عامله بسیار زیاد است (هر دو توزیع‌شده‌اند) امّا با در نظر گرفتن شبکه هوشمند برق به عنوان یک سیستم چند عامله و سپس ارائه راهکار امنیتی جامع در این مورد، ما می‌توانیم با بهره‌برداری از مزایای ذاتی سیستم‌های چند عامله همچون انعطاف پذیری، توسعه پذیری، هوشمندی، خود مختاری، نیاز به نگهداری کمتر و غیره، در آینده برای رفع مشکلات و موانع دیگر اجزای شبکه از آن‌ها استفاده کنیم [۱۶].

۶. معرفی پروتکل شبکه قراردادی

سیستم‌های چند عامله به‌طور فزاینده‌ای به ابزار قدرتمندی برای توسعه سیستم‌های پیچیده بدل شده‌اند. دانشمندان علوم کامپیوتر از مفهوم سیستم‌های چند عامله برای توسعه سیستم‌های کنترل توزیع‌شده و نامتمرکز و از فرآیندهای استدلالی هوشمند همراه با تعامل و تبادل اطّلاعات میان عامل‌ها استفاده کرده‌اند. از آن جایی که مذاکره در اقتصاد نیز مطرح بوده است یک موضوع مورد توجه در سیستم‌های چند عامله نیز است. مذاکرات می‌تواند برای حل و فصل اختلافات در طیف گسترده‌ای از حوزه‌های چند عامله مورد استفاده قرار گیرد که نمونه ای از این‌ها عبارتند از اختلافات بین خریدار و فروشنده در تجارت الکترونیکی بازار برق [۸]. اگر شبکه هوشمند برق را به عنوان یک سیستم چند عامله که متشکّل از چندین عامل خودمختار است در نظر بگیریم، مذاکره شکل کلیدی تعامل است که گروهی از عامل‌ها را قادر به رسیدن به یک توافق دو طرفه در رابطه با یک هدف می‌سازد. هنگامی که یک عامل خودمختار و قادر به مذاکره انعطاف پذیر و پیچیده ساخته می‌شود، سؤال اصلی که باید در نظر گرفته شود این است که از چه پروتکل مذاکره‌ای استفاده شود؟ و عامل‌ها چه مدل استدلالی، روند تصمیم گیری و استراتژی‌هایی را به‌کار ببرند؟

پروتکل، اهداف هماهنگی، و مکانیزم رفتار یک عامل برای توازن بسیار لازم است. پروتکل مجموعه‌ای از قوانین جهت تعاملات و ارتباطات میان اعضای یک سیستم است که مورد توافق آن‌ها قرار گرفته است. هماهنگی متشکّل از مجموعه‌ای از مکانیزم‌هایی است که برای عملیات کارآمد سیستم‌های چند عامله ضروری است تا تقسیم وظایف به صورت متعادل صورت گیرد در حالی که روابط متقابل منطقی و وابستگی به منابع عامل‌ها کاهش یابد [۱۷]. یکی ازمهم‌ترین مکانیزم‌های هماهنگی پروتکل شبکه قراردادی است[۱] که به‌طور گسترده در حوزه‌های بسیاری مورد مطالعه قرار گرفته است[۱۸]. قرارداد میان یک کارفرمای مشخص و طرف قرارداد از طریق فرایند انتخاب دوجانبه مبتنی بر یک انتقال دو طرفه اطّلاعات ایجاد می‌شود. قرارداد یک توافق صریح میان کارفرما و طرف دیگر قرارداد است [۱۷].

در پروتکل شبکه قراردادی FIPA[۲]، یک عامل یعنی آغازگر می‌خواهد کاری را توسط عامل‌ها یا همان شرکت-کنندگان دیگر انجام دهد. و فرایند هماهنگی متشکّل از چهار گام اصلی است. اولین گام "اعلام کردن"[۳] است که در آن

[1] Contract Net Protocol (CNP)
[2] Foundation for Intelligent Physical Agents
[3] Announce

آغازگر یک وظیفه را با پیام cfp [1] به شرکت‌کنندگانی که احتمالاً تصور می‌شود کار فراخوانده شده را اجرا کنند اعلام می‌کند. گام دوم "پیشنهاد دادن"[2] است که در آن پیشنهاد کنندگان پیشنهادهای خود را بر اساس منابع، توانایی و نیروی خود به آغازگر ارسال می‌کنند. گام سوم "اعطا کردن"[3] است که در آن آغازگر تمام پیشنهادها را ارزیابی می‌کند و قرارداد[4] را به بهترین شرکت کننده می‌فرستد که این به معنی پذیرش پیشنهاد می‌باشد. آغازگر می‌خواهد تابعی که آن کار را مشخص می‌کند بهینه نماید تا سود حاصل از انجام آن را به حداکثر برساند. مشخصات این تابع معمولاً به عنوان قیمت، زمان اتمام کار، تقسیم عادلانه وظایف و ... بیان می‌شود[۱۸].

۱.۶ پروتکل شبکه قراردادی مبتنی بر اعتماد

پروتکل شبکه قراردادی یک روند رسمی و قراردادی در فرایند هماهنگی در سیستم شبکه‌ای عرضه می‌دارد و به‌طور گسترده در سیستم‌های چند عامله به‌کار گرفته شده است. اما توجه به این نکته ضروری است که تنها در مقیاس کوچک از محیط سیستم چند عامله محافظت می‌نماید [۱۷]. برای مقابله با محدودیت کارآمدی در مقیاس کوچک که CNP متداول با آن مواجه است، مقاله [۱۸] رویکرد جدیدی برای تعمیم CNP ارائه می‌دهد که مبتنی بر مکانیزم اعتماد[5] شکل می‌گیردو

اعتماد یک نگرانی بنیادی در سیستم‌های باز و مقیاس بزرگ است و در هسته تمام تعاملات میان موجودیت‌هایی که باید در محیط‌های ناامن یا مدام در حال تغییر فعالیت کنند قرار می‌گیرد. تعاریف متعددی در حوزه‌های گوناگون برای اعتماد ارائه شده است که با توجه به مبحث مورد مطالعه به این صورت بیان می‌شود. اعتماد باور یک عامل مبنی بر آن است که طرف‌های دیگر، همان کاری که بیان می‌دارند انجام می‌دهند (صادق و قابل اطمینان هستند) و یا معامله متقابل می‌کنند (رابطه متقابل در جهت منافع مشترک طرفین) که این فرصت ترک رابطه جهت سود بالاتر را می‌دهد. عامل‌ها از طریق مدل اعتماد می‌توانند در مورد قابل اطمینان بودن یا نبودن دیگر شرکا استدلال نمایند. در واقع، به وسیله مدل اعتماد می‌توانند میزان اعتماد خود به طرف مقابل را محاسبه نمایند. میزان بالای اعتماد به این معنی است که احتمالاً آن عامل می‌تواند به عنوان طرف تعامل انتخاب شود. و برعکس، چنانچه میزان اعتماد پایین باشد منجر به عدم انتخاب آن می‌شود (در صورت بودن طرف قابل اعتمادتر). به این صورت، مدل اعتماد قصد هدایت عامل‌ها به تصمیم‌گیری در این که چگونه، چه زمانی و با چه کسی تعامل کنند دارد [۱۹].

۷. روش پیشنهادی

راه حل پیشنهادی به این صورت است که در هنگام وقوع حمله، پروتکل شبکه قراردادی مبتنی بر اعتماد برای تعیین قیمت اجرا می‌شود. به دلیل تغییراتی که بر روی CNP متداول ایجاد کردیم، روش پیشنهادی را TB-CNP [6] می‌نامیم. در این روش مرکز کنترل با آگاهی از وجود حمله به دلیل از دست رفتن اطّلاعات واقعی حسگرها، قیمت نهایی برق را با نظارت

[1] call for proposals
[2] Bid
[3] Award
[4] Contract
[5] Trust
[6] Trust Based - CNP

مستقیم خود تعیین می‌کند. در واقع، به جای اینکه قیمت بر مبنای پخش بار بهینه تعیین شود، با نظارت مستقیم مرکز کنترل به عنوان کارفرما در پروتکل شبکه قراردادی مشخص می‌شود. از آن جا که اطّلاعات حسگرها در زمان وقوع حمله غیرواقعی و نامعتبر است، آخرین قیمت معتبر ذخیره شده در حافظه مرکز کنترل به عنوان قیمت پیشنهادی هر عامل و همچنین تخمینی از میزان تولید هر کاربر پیش از وقوع حمله و میانگین انرژی تولیدی در زمان‌های مشابه به عنوان انرژی تولیدی هر کاربر درنظر گرفته می‌شود. همان‌طور که پیش‌تر اشاره شد، برای در نظر گرفتن احتمال وجود کاربران اخلال‌گر به عنوان جمر در میان کاربران، برای هر کاربر یا عامل با توزیع احتمالی یک میزان اعتماد در نظر گرفته می‌شود. هنگام اجرای پروتکل، برای هر عامل، با توجه به مقدار انرژی تولیدی و قیمت پیشنهادی آن امتیازی تعیین می‌شود. مقدار این امتیاز به‌وسیله رابطه ۱ محاسبه می‌شود.

$$point\ (Agent) = W1 * Trust\ (Agent) - W2 * LMP(Agent) \qquad (1)$$

که در آن مقادیر W_1 و W_2 هر کدام وزن متناظر با پارامترهای مؤثر در انعقاد قرارداد در بازار شبکه هوشمند برق یعنی قیمت و اعتماد است. مقدار وزن‌ها نشان‌گر نقش هر پارامتر در امتیاز نهایی دارد. در پایان این مرحله، کاربران بر مبنای امتیازی که دارند به‌صورت نزولی مرتب می‌شوند.

تا زمانی که میزان بار توسط مقدار انرژی تولیدی ژنراتورها تأمین شود خرید انرژی از آن‌ها ادامه می‌یابد و به این ترتیب فروشندگان نهایی مشخص می‌شوند. هنگامی‌که میزان بار با میزان انرژی تولیدی برابر باشد، تمام ژنراتورها در لیست فروشندگان نهایی قرار می‌گیرند. در پایان، مرکز کنترل هزینه متناظر به ازای یک واحد افزایش انرژی را به عنوان قیمت نهایی تمام شین‌ها تعیین می‌کند.

پس از اتمام حمله و بازگشتن بازار به وضعیت پایدار، مرکز کنترل با بررسی میزان مصرف و تولید هر کاربر، از میزان اعتماد کاربرانی که الگوی مصرف و تولید آن‌ها از حالت نرمال خارج شده می‌کاهد. به موجب این عمل، از میزان تأثیر کاربران اخلال‌گر در معاملات آینده بازار برق کاسته می‌شود و در نتیجه، برای انتخاب به‌عنوان طرف قرارداد در اولویت پایین‌تری قرار می‌گیرند.

۷. طرح مسئله

۱.۷ روش پیشنهاد قیمت در بازار برق

برای محاسبه قیمت برق تولیدکننده‌ها از روش ارائه شده در مقاله [۵] استفاده میشود. در هر شین، دریافت از بار و پرداخت به ژنراتور، براساس قیمت نهایی مکانی[1] انجام می‌شود. قیمت نهایی مکانی بازار بر مبنای پخش بار بهینه تعیین می‌شود. در این مسأله، هدف بیشینه کردن رفاه اجتماعی، ضمن برآوردن توازن توان و محدودیت‌های شبکه است.
مدل کلی توزیع توان بر اساس معادلات خطی در رابطه ۲ آمده است.

$$\min_{G_i} \quad \sum_{i=1}^{n} C_i \times G_i \qquad (2)$$

مشروط به این‌که:

[1] Locational Marginal Price (LMP)

$$s.t.\begin{cases}\sum_{i=1}^{N} G_i - \sum_{i=1}^{N} D_i = 0 \\ \sum_{i=1}^{N} GSF_{k-1} \times (G_i - D_i) \le Limit_k^{max}, k \in \kappa \\ G_i^{min} \le G_i \le G_i^{max}, i \in \Im \end{cases}$$

که در این روابط n تعداد شین‌های سیستم قدرت، C_i هزینه تولید در شین i، G_i تولید توان در شین i، D_i مصرف توان در شین i، GSF_{k-i} ضریب جابجایی تولید خط k از شین i، $Limit^{max}_k$ محدودیت انتقال در خط k، و $\Im$ مجموعه ژنراتورها است.

فرمول کلی محاسبه LMP در شین i متشکّل از سه مؤلفه قیمت نهایی مکانی انرژی، قیمت نهایی مکانی گرفتگی[1]، و قیمت نهایی مکانی تلفات[2] به‌شرح زیر است:

$$LMP_i = LMP_i^{energy} + LMP_i^{cong} + LMP_i^{loss} \quad (3)$$

$$LMP^{energy} = \lambda \quad (4)$$

$$LMP_i^{cong} = \sum_{k=1}^{L} GSF_{k-1} \times \mu_k \quad (5)$$

$$LMP_i^{loss} = \lambda \times (DF_i - 1) \quad (6)$$

که در آن L تعداد خطوط، λ ضریب لاگرانژ قیود تساوی، و μ ضریب لاگرانژ قیود نامساوی یا انتقال kام، و DF_i ضریب تحویل در شین i است که در این مقاله برای تأکید بر روی قسمت اصلی LMP برابر با ۱ در نظر گرفته می‌شود. بنابراین داریم:

$$LMP_i = \lambda + \sum_{k=1}^{L} GSF_{k-1} \times \mu_k . \quad (7)$$

در صورتی‌که محدودیت تولید الزام آور نشود، در هر شین LMP با هزینه نهایی ژنراتور برابر است. درغیر این صورت، بسته به اینکه حد بالا یا حد پایین تولید در یک شین الزام آور شود، LMP می‌تواند از هزینه نهایی ژنراتور بیشتر یا کمتر باشد.

۲.۷ مجموعه داده‌ها

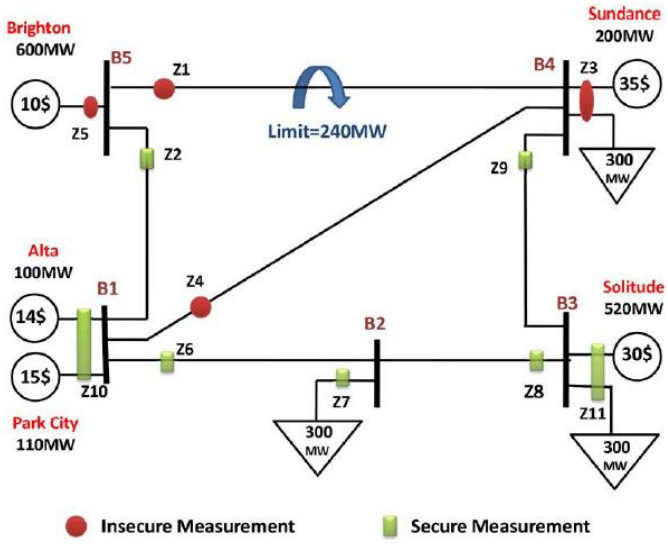
برای تست روش پیشنهادی از داده‌های مصرف موجود در مقاله [۲۰] استفاده شده است.

۸. مطالعه موردی

برای اعتبارسنجی روش پیشنهادی، راه حل ارائه شده بر روی شبکه PJM ۵ شین مورد مطالعه مقاله [۵] اعمال شده است.

[1] Congestion
[2] Loss

پیکربندی شبکه تست PJM ۵ شین به همراه نقاط اندازه‌گیری مطمئن و نامطمئن در شکل ۱ قابل مشاهده است.



شکل ۱ _ پیکربندی سیستم تست PJM ۵ شین [۵]

این شبکه دارای ۴ ژنراتور، ۴ بار و ۶ خط انتقال می باشد. اطّلاعات مربوط به هر یک از شین ها، به‌علاوه راکتانس[1] و محدودیت حرارتی[2] خطوط و ماتریس ضریب جابجایی تولید[3] بر اساس اطّلاعات مقاله [۵] به ترتیب ذیل جداول ۱، ۲ و ۳ قرار گرفتند. جهت سهولت در امر پیاده‌سازی مسئله، قیمت در شین ۱، میانگین قیمت پیشنهادی دو ژنراتور آن در نظر گرفته می‌شود.

جدول۱. اطّلاعات ژنراتورها و بارهای سیستم PJM

شماره شین	حداکثر تولید (MW)	هزینه نهایی ($/MW)	مصرف (MW)
۱	۲۱۰	۱۴,۵	۰
۲	۰	--	۳۰۰
۳	۵۲۰	۳۰	۳۰۰
۴	۲۰۰	۳۵	۳۰۰
۵	۶۰۰	۱۰	۰

جدول۲. راکتانس و محدودیت حرارتی خطوط سیستم PJM

خط	L12	L14	L15	L23	L34	L45
راکتانس X(%)	۲,۸۱	۳,۰۴	۰,۶۴	۱,۰۸	۲,۹۷	۲,۹۷
محدودیت حرارتی (MW)	۹۹۹	۹۹۹	۹۹۹	۹۹۹	۹۹۹	۲۴۰

[1] Reactance
[2] Thermal Limit
[3] Generation Shift Factor

جدول۳. ضریب جابجایی تولید سیستم PJM

خط / شین	B1	B2	B3	B4	B5
L12	۰,۱۰۳۹	-۰,۴۷۶	-۰,۳۴۹	۰	۰,۱۵۹۵
L14	۰,۴۳۷۶	۰,۲۵۸	۰,۱۸۹۵	۰	۰,۳۶
L15	۰,۳۶۸۵	۰,۲۱۷۶	۰,۱۵۹۵	۰	-۰,۵۱۹۵
L23	۰,۱۹۳۹	۰,۵۲۴۱	-۰,۳۴۹	۰	۰,۱۵۹۵
L34	۰,۱۹۳۹	۰,۵۲۴۱	۰,۶۵۱۰	۰	۰,۱۵۹۵
L45	۰,۳۶۸۵	۰,۲۱۷۶	۰,۱۵۹۵	۰	۰,۴۸۰۵

در این آزمایش پارامتر اعتماد که نشان دهنده عملکرد کاربران در بازار برق است، به‌صورت رندوم و بر اساس فرضیات موجود در مقاله[۱۸] محاسبه شده است. این مشخصات ذیل جدول ۴ قرار دارند.

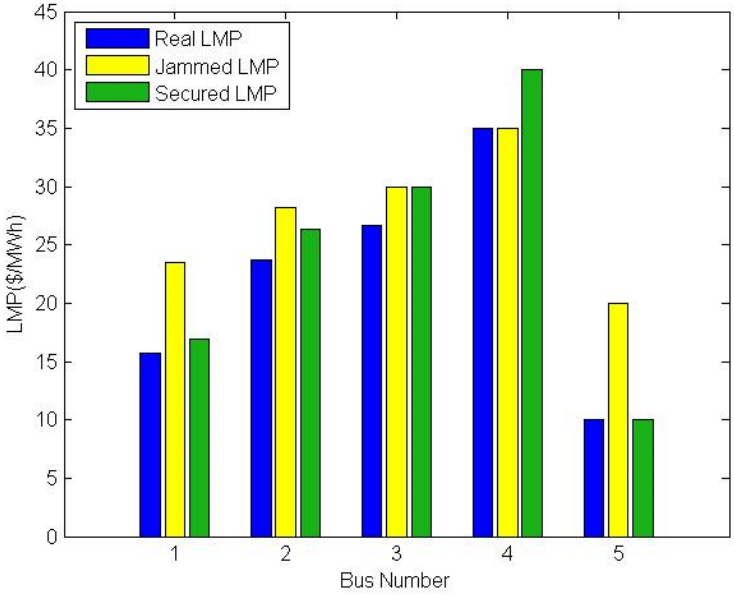
جدول۴. عملکرد کاربران در بازار برق شبکه هوشمند

نوع کاربر	احتمال ظهور	انحراف از معیار
خوب	۰,۲	۰,۱
نرمال	۰,۴	۰,۲
بد	۰,۴	۰,۲

۹. ارزیابی عملکرد روش پیشنهادی

پس از مدل سازی مسئله، روش پیشنهادی به منظور راستی‌آزمایی بر روی محیط MATLAB پیاده سازی شد. بر مبنای آزمایش‌های انجام گرفته، مقادیر وزن روش ارائه شده یعنی W_1 و W_2 به ترتیب برابر با ۱ و ۰,۱ قرار داده شد. در محیط تست برای هر شین سه کاربر در نظر گرفته شده است که هر کدام می‌توانند تولید کننده، مصرف کننده و یا هر دو باشند.

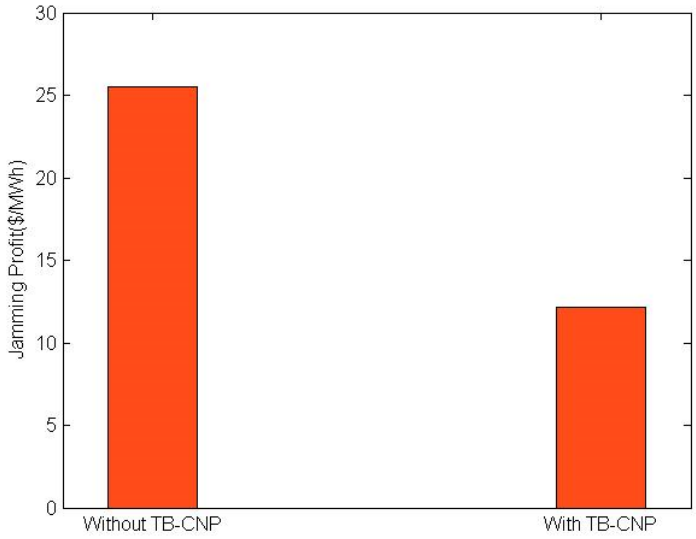
شکل ۲ میزان تعیین شده LMP در هر شین به ازای اجرای برنامه در سه حالت بدون حمله، تحت حمله جمینگ، و اعمال پروتکل شبکه قراردادی مبتنی بر اعتماد در شرایط حمله جمینگ است.



شکل ۲ _ مقایسه قیمت نهایی شین‌ها در حالت واقعی، حمله و ایمن شده بوسیله اعمال روش پیشنهادی

همان‌طور که در شکل ۲ قابل مشاهده است، روش ارائه شده توانسته در شین‌های ۱، ۲، و ۵ مقدار سود جمر را کاهش دهد. این مقدار در شین ۳ تغییر محسوسی نداشته و در شین ۴ افزایش یافته است. واضح است هنگامی‌که پروتکل شبکه قراردادی فراخوانده می‌شود، مقدار LMP تعیین شده در شین‌ها یکسان تعیین می‌شود. همین امر ناگزیر باعث می‌شود کاربرانی متضرّر گردند که با این با توجه به نتایج کلی بدست آمده روش پیشنهادی که در ادامه به آن اشاره می‌شود قابل توجیح است.

شکل ۳ نمودار سود کلی جمر طی حمله به بازار برق شبکه هوشمند را نشان می‌دهد که در دو حالت اجرای روش پیشنهادی هنگام حمله و عدم اجرای آن در همان شرایط حمله محاسبه شده است. همانطور که نمایان است، اجرای روش پیشنهادی توانسته است سود جمر را به کمتر از نصف کاهش دهد. بر این اساس، مهاجم کم کم انگیزه خود را برای حمله از دست می‌دهد چرا که اگر خواهان سود بیشتری باشد باید به مکان‌های بیشتری حمله کند که این خود با ریسک شناسایی او همراه است.



شکل ۳ _ مقایسه سود نهایی جمر در دو حالت اجرای TB-CNP و عدم اجرای آن در شرایط حمله

۱۰. نتیجه‌گیری

در این مقاله، برای مقابله با حمله جمینگ در بازار برق راهکاری بر مبنای پروتکل مذاکره در سیستم‌های چند عامله ارائه شد و مورد تجزیه و تحلیل قرار گرفت. روش پیشنهادی ارائه شده بر اساس پروتکل شبکه قراردادی مبتنی بر پارامتر اعتماد است که TB-CNP نامیده شد. این روش در زمانی که جمر مقادیر واقعی اطّلاعات حسگرها را از دسترس خارج می‌کند، با استفاده از مقادیر معتبر پیش از وقوع حمله و همچنین تخمینی از نمونه‌های گذشته، مقادیر قیمت را طی اجرای این پروتکل تعیین می‌کند. نتایج حاصل از شبیه سازی این روش بر روی شبکه PJM ۵ شینه نشان می‌دهد این رویکرد می‌تواند به میزان قابل توجهی از سود جمر بکاهد و در نتیجه انگیزه او را در حملات بعدی از بین ببرد تا در نهایت امنیت شبکه ارتقا یابد. پیشنهاد قیمت در روش پیشنهادی بر اساس مدل DC است. در تحقیقات آینده روش ارائه شده می‌تواند بر روی مدل AC[1] مورد مطالعه قرار گیرد.

۱۱. تشکر و قدردانی

نویسندگان مقاله لازم می‌دانند از جناب آقای دکتر علی اخوین، مشاور پروژه در مباحث مربوط به تعیین قیمت در بازار برق شبکه تشکر نمایند.

[1] Alternating Current

۱۲. مراجع

[1] "Smart Grid / Department of Energy,"
http://energy.gov/oe/services/technology-development/smart-grid,
U.S. Department of Energy. Retrieved 2012-06-18. Visited: 2015-04-27.

[2] Tony, F. and Morehouse, J. T. (2011), "Securing the Smart Grid: Next Generation Power Grid Security", Elsevier.

[3] Hardy, A., Bouhafs, F. and Merabti, M. (2011), "A Survey of Communication and Sensing for Energy Management of Appliances", International Journal of Advanced Engineering and sciences and Techmology (IJAEST), vol no. 3, Issue no. 2, pp.061-077.

[4] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou G. (2009), "A Survey on Jamming Attacks and Countermeasures in WSNs", IEEE Communication & Survey Tutorials, vol. 11, no. 4, pp. 42–56.

[5] Ma, J., Liu, Y., Song, L., and Han, Z. (2015), "Multiact Dynamic Game Strategy for Jamming Attack in Electricity Market", IEEE Transactions on Smart Grid, vol. 6, no. 5.

[6] Orfanogianni T. and Gross, G. (2007), "A General Formulation for LMP Evaluation", IEEE Transactions on Power Systems, vol. 22, no. 3, pp. 1163–1173.

[7] Frowd R. and Papalexopoulos, A. (2009), "Market simulation for LMP forcasting", in Proc. IEEE Power Energy Soc. Gen. Meeting, Calgary, AB, Canada, pp.1- 6.

[8] Aloula, F., Al-Alia, Al-Dalkya, A.R. R., Al-Mardinia, M. and El-Hajjb, W. (2012), "Smart grid security-Threats vulnerabilities and solutions", International Journal of Smart Grid and Clean Energy, vol. 1, no. 1.

[9] Goldman, C. (2011), "*An Introduction – Smart Grid 101*", Lawrence Berkeley National Laboratory, Smart Grid Technical Advisory Project.

[10] Litos Strategic Communication (2014), "*The Smart Grid: An Introduction*", U.S. Department of Energy Office of Energy Efficiency and Renewable Energy.

[11] Roche, R., Blunier, B., Miraoui, A., Hilaire, V. and Koukam, A. (2010), "Multi-Agent Systems for Grid Energy Management: A Short Review", IECON - 36th Annual Conference on IEEE Industrial Electronics Society, pp.3341-3346, 7-10.

[12] Yilmaz, C., Albayrak, S. and L¨utzenberger, M., (2014) "*Smart Grid Architectures and the Multi-Agent System Paradigm*", The Fourth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, DAI-Labor ,Technical University of Berlin .Berlin, Germany. ENERGY.

[13] Lu, Z., Wang, W. and Wang, C. (2014), "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications", IEEE Transactions on Mobile Computing, vol. 13, no. 8.

[14] Abdulqader Hussein, A., Rahman, T. A. and Yen Leowa, C. (2015), "Survey and Open Issues Of Jammer Localization Techniques In Wireless Sensor Networks," Journal of Theoretical and Applied Information Technology (JATIT), Vol.71.

[15] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C. and Pantziou, G. (2009), "A Survey on Jamming Attacks and Countermeasures in WSNs", IEEE Communication Survey and Turorials, Vol. 11, No. 4.

[16] Kim, H., Lim, Y. and Kinoshita, T. (2012), "An Intelligent Multiagent System for Autonomous Microgrid Operation", Energies, vol.5, pp3347-3362.

[17] Wu, J. (2008), "Contract Net Protocol for Coordination in Multi-agent System," IEEE.

[18] Zhao, X., Hu, G., and Wu, Z. (2014), "The Smart grid scheduling based on Contract Net Protocol with Trust Model", IEEE.

[19] Ramchurn, S. D., Hyunh D. and Jenings, N. R. (2004), "*Trust in multi-agent systems*", School of Electronics and Computer Science, University of Southampton, The Knowledge Engineering Review, Vol. 19:1, 1-25. Cambridge University Press.

[20] Li, H. and Han, Z. (2011), "Manipulating the Electricity Power Market via Jamming the Price Signaling in Smart Grid", IEEE International Workshop on Smart Grid Communications and Networks.