مدیریت امن انرژی در ریزشبکه‌های هیبریدی با به‌کارگیری تکنولوژی بلاکچن

ستار شجاعیان[۱]، طاهر نیکنام*[۲]، مهدی نفر[۳]

۱- دانشجوی دکتری، گروه برق، دانشکده برق، واحد مرودشت، دانشگاه آزاد اسلامی، مرودشت، ایران، shojaeiyan.mau@gmail.com

*۲- استاد، گروه برق، دانشکده برق، واحد مرودشت، دانشگاه آزاد اسلامی، مرودشت، ایران، taher_nik@yahoo.com

۳- استادیار، گروه برق، دانشکده برق، واحد مرودشت، دانشگاه آزاد اسلامی، مرودشت، ایران، mehdinafar@gmail.com

تاریخ دریافت: ۱۴۰۲/۹/۲۰ تاریخ پذیرش: ۱۴۰۲/۱۱/۲۵

چکیده: دستیابی به مدیریت و برنامه‌ریزی بهینه و امن انرژی با درنظر گرفتن کاهش هزینه‌های تولید، انتقال و توزیع برق و همچنین کاهش انتشار آلاینده‌های زیست محیطی، در بسیاری از شرکت‌های برق کشورهای در حال توسعه اهمیت فزاینده‌ای پیدا کرده است. با استفاده بهینه از منابع انرژی تجدیدپذیر و بکارگیری یک پلتفرم امن ازجمله تکنولوژی بلاکچن می‌توان به اهداف ذکر شده دست یافت. بمنظور حل مسئله بهینه‌سازی، پس از مدل‌سازی ریزشبکه هیبرید AC-DC و باتوجه به پیچیدگی بالای فرمول پیشنهادی، الگوریتم بهینه‌سازی گرگ خاکستری جهت حل مسئله پیشنهاد شده است. جهت بررسی کارایی سیستم تحت حملات سایبری، سیستم مورد نظر تحت حملات تزریق داده غلط در نقاط مختلف سیستم اعمال می‌شود و سپس بهره‌برداری در شرایط عادی و حملات سایبری صورت می‌گیرد. در این مقاله، بسته نرم افرازی متلب جهت حل مسئله بهینه‌سازی و مدل‌سازی حملات سایبری استفاده شده است. نتایج بهره‌برداری در سناریوهای مختلف بررسی شده است و با مقایسه با حالت نرمال اثرات منفی اینگونه حملات نشان داده می‌شود. سپس جهت تقویت امنیت سیستم و جلوگیری از بروز حملات، تکنولوژی بلاکچن جهت افزایش امنیت داده‌های مبادله شده در شبکه ارائه شده است.

واژه‌های کلیدی: ریز شبکه‌های هیبرید، الگوریتم گرگ خاکستری، حمله تزریق داده غلط، تکنولوژی بلاکچن.

۱- مقدمه

امروزه به خاطر پیشرفت‌های گسترده‌ی صنعت مخابرات و اطلاعات در شبکه‌های قدرت الکتریکی، بهره‌برداری به شکل سنتی از شبکه‌های برق تغییر یافته و به بهره‌برداری هوشمند از شبکه‌ها تبدیل شده است. براساس اطلاعات اساسی موجود در این شاخه، اهداف شبکه‌های هوشمند می‌تواند شامل اینگونه موارد باشد: ۱) کاهش خاموشی‌ها در سطح شبکه، ۲) توسعه استفاده از انرژی‌های تجدیدپذیر و ۳) ارائه راه‌کارهایی برای کنترل و مدیریت مصرف انرژی الکتریکی. لازم به ذکر است که تولید انرژی الکتریکی در شبکه‌های هوشمند بسیار متفاوت با شبکه‌های سنتی امروزی است که دلیل اصلی آن نفوذ بسیار گسترده منابع انرژی تجدیدپذیر در سطح شبکه‌های با ولتاژ پایین و یا متوسط (ریزشبکه‌ها) می‌باشد.

تجدید ساختار در صنعت برق، شرکت‌های الکتریکی را برآن داشته تا از تولیدات پراکنده در نزدیکی مصرف استفاده کنند. همچنین پیشرفت بسیار گسترده در ادوات الکترونیک قدرت باعث شده تا ذخیره‌کننده‌های انرژی الکتریکی نقش بسیار اساسی را در شبکه‌های قدرت پیدا کنند. با این تعاریف، می‌توان گفت که ریزشبکه یک شبکه با سطح ولتاژ پایین یا متوسط است که شامل منابع تولید پراکنده، ذخیره-کننده‌ها، بارهای کنترل پذیر، واحدهای تولید همزمان گرما و الکتریسیته و یک سیستم مدیریت و کنترل خودگردان انرژی است [۱]. نقش بسیار موثر و مفید ریزشبکه‌ها در صنعت الکتریسیته، محققان زیادی را مصمم کرده تا جنبه‌های مختلف ریزشبکه را به شکل موشکافانه‌ای مورد تجزیه و تحلیل قرار دهند. از جمله مهم‌ترین شاخه-های تحقیق در ریزشبکه‌ها، بهره‌برداری بهینه از آن‌ها می‌باشد. در این راستا بهره‌بردار ریزشبکه سعی برآن دارد تا یک ابزار کارآمد و قوی مدیریت را در دست گیرد و بار را به گونه‌ای بین منابع تولید پراکنده، ذخیره‌کننده‌ها و شبکه‌ی بالا دست پخش کند که هم از نظر اقتصادی و هم ازنظر آلودگی‌های زیست محیطی به صرفه باشد.

از دیدگاه مصرف‌کننده‌های انرژی، استفاده از ریزشبکه‌ها فواید بسیاری را به دنبال خواهد داشت که از آن جمله می‌توان به کاهش هزینه‌ها، افزایش قابلیت اطمینان سیستم، افزایش کیفیت توان، افزایش بازدهی، کاهش آلاینده‌های زیست محیطی، کاهش ریسک سرمایه گذاری، کاهش اتلاف انرژی در خطوط انتقال، کاهش وابستگی به سوخت وارداتی وایجاد شغل اشاره کرد. واضح است که برای رسیدن به فواید ذکر شده، بهره‌برداری بهینه از ریزشبکه‌ها در جهت بهترین استفاده از واحدهای تولیدی، ذخیره کننده‌ها و شبکه بالادست امری ضروری است [۲].

یکی از مهمترین مباحث ذکر شده در شبکه هوشمند امنیت سایبری در این سیستم‌های مدرن می‌باشد. با توجه به گستردگی جغرافیایی شبکه‌های هوشمند و تجهیزات متنوع بکاربرده شده در این سیستم‌ها از جمله سنسورهای هوشمند، تجهیزهای کنترلی، مخابراتی، تعداد بارها و منابع تولیدی، گسترش آسیب‌پذیری‌های امنیت سایبری امری اجتناب ناپذیر و یک موضوع مهم و کلیدی می‌باشد. علاوه بر این، نقض امنیت سایبری در چنین زیرساخت‌های حیاتی، عواقب و ضررهای قابل توجه و جبران‌ناپذیری را به دنبال خواهد داشت. در مرجع [۳]، شبکه هوشمند را یک سیستم الکتریکی تعریف می‌کنند که از فناوری اطلاعات و ارتباطات ایمن سایبری استفاده می‌کنند. می‌توان امنیت سایبری شبکه‌های هوشمند را به سه دسته در زیر ساخت سیستم هوشمند طبقه‌بندی کرد: ۱) انرژی هوشمند، ۲) اطلاعات هوشمند و ۳) ارتباطات هوشمند. راه‌حل‌های موجود امنیت سایبری در تأمین نیازهای سیستم‌های ارتباطی شبکه هوشمند مشکل دارند. اگر سیستم‌های حیاتی مانند زیرساخت ارتباطی سیستم قدرت ازنظر امنیت سایبری در معرض خطر حمله باشند، عواقب شدیدی می‌تواند رخ دهد، در حالی که در بیشتر تحقیق‌ها خطرهای سنتی در ارزیابی ریسک درنظر گرفته شده است. امنیت سیستم‌های شبکه هوشمند موضوعی نسبتاً جدید است و تحقیق‌های آکادمیک و تجربی کمی در این راستا صورت گرفته است و باتوجه به پیشرفت روزافزون سیستم‌های قدرت و سوق پیدا کردن به سمت هوشمند شدن، بایستی این مسئله بطور کامل مورد بررسی و مطالعه قرار گیرد [۴, ۵]. امنیت سایبری در شبکه‌های هوشمند یک زمینه در حال ظهور است [۶]. بنابراین، هر مولفه امنیتی بایستی امنیت سایبری آن مورد بررسی قرار گیرد.

بهره‌برداری و مدیریت انرژی در شبکه‌های هیبریدی موضوع مطالعات بسیاری در سال های اخیر بوده است. در ادامه به برخی از مهمترین تحقیقات انجام شده اشاره می‌شود. در [۷] دکتر تیمورزاده و همکارانش روشی را برای بهره‌برداری از شبکه‌های ترکیبی ارائه کردند. مقاله [۸] به بررسی بهره‌برداری از یک شبکه هایبرید در حالت اتصال به شبکه و حالت جزیره‌ای پرداخته شده است. در این مقاله، عناصر مختلف بخش AC و DC شبکه هایبرید، مانند توربین‌های بادی، سلول‌های خورشیدی و باتری‌ها، مورد بررسی قرار گرفته است. در [۹]، نرخ مصرف سوخت را در حضور قیود تامین بار الکتریکی و حرارتی و قیود فنی ریزشبکه کمینه می‌کنند. همچنین، آن‌ها یک مقدار حداقل ذخیره برای بهره‌برداری بهینه‌ی تک هدفه خود درنظر گرفته‌اند. نویسندگان در [۱۰]، بهینه‌سازی ریزشبکه شامل توربین‌های بادی و سلول‌های خورشیدی بر اساس احتمال از دست رفتن بار و هزینه را تجزیه و تحلیل کرده‌اند.

در [۱۱] بلاکچن برای ذخیره‌سازی به روش غیرقابل دستکاری استفاده کرده است، در این مقاله، اطلاعات از کنتورهای هوشمند جمع‌آوری می‌شود و سپس مورد استفاده قرار می‌گیرد. در [۱۲]، یک سیستم کنترل کاملاً غیرمتمرکز، با استفاده از مفهوم فناوری ارتباطات و اطلاعات پوشش شبکه و شبکه‌های P2P[1] برای ریزشبکه‌ها ارائه شده است. این کار نشان می‌دهد که چگونه می‌توان با استفاده از چارچوب-های P2P بعنوان ساختارهای کنترل اساسی، به تمرکززدایی دست یافت. در [۱۳]، DSO[2] مشخصات برق مورد نظر خود را به واحدهای تولیدکننده ارسال می‌کند که آن‌ها به روش‌های مشارکتی و رقابتی، مصرف برق یا تولید خود را تغییر می‌دهند تا انعطاف‌پذیری مطلوب را با بهترین قیمت برای DSO و حداکثر درآمد برای همه فراهم کنند. در [۱۴] نویسنده‌ها یک سیستم DR[3] غیرمتمرکز مبتنی بر قیمت را با در نظر گرفتن تمایل مشتری بمنظور انعطاف‌پذیری خود، به شبکه پیشنهاد داده است. در مقاله [۱۵]، یک طرح مبتنی بر اعتبار برای پرداخت‌های مطمئن در معاملات انرژی در نظر گرفته شده است. با این‌حال، ویژگی‌های یک سیستم قدرت بطور کامل درنظر گرفته نشده است، زیرا به نقش اصلی DSOها در سیستم قدرت پرداخته نشده است. مقاله [۱۶] برای اطمینان از شفافیت و امنیت مصرف انرژی، یک سیستم نظارت بر بلاکچن و هوشمند مبتنی بر قرارداد برروی شبکه هوشمند را ارائه می‌دهد. در [۱۷]، نویسنده‌ها برای پرداختن به مباحث

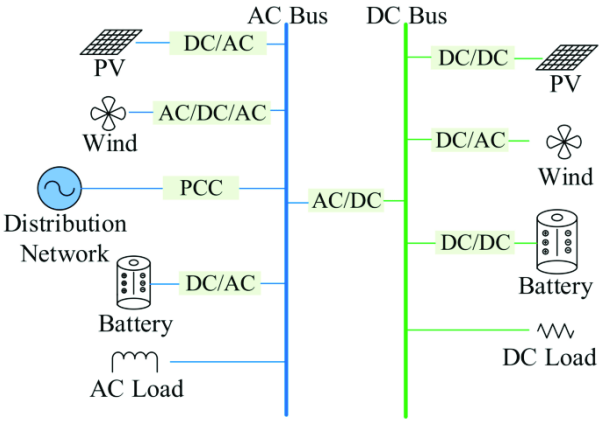
معماری مبتنی بر ابر سنتی، معماری سیستم سایبری-فیزیکی غیرمتمرکز را با کمک بلاکچن معرفی کردند.

از آنجایی که با رمزنگاری داده‌های مبادله شده بین مرکز کنترل، واحدهای تولید پراکنده، واحدهای کنترل و داده‌های اندازه گیری شده توسط سنسورهای هوشمند، می‌توان امنیت داده‌های مبادله شده در یک سیستم هوشمند را افزایش داد، در این مقاله از تکنولوژی بلاکچن جهت رمزنگاری اطلاعات و داده‌های مبادله شده در شبکه هوشمند استفاده می‌شود, که رمزنگاری داده‌ها سبب می‌شود هکرها به آسانی به داده‌ها دسترسی پیدا نکنند، و یا در صورت دسترسی و تغییر در بلوک‌های هش شده، واحد دریافتی بلوک، صحت داده را تایید نمی‌کند، که این امر سبب افزایش امنیت اطلاعات مبادله شده در سیستم می‌شود. بطور خلاصه در این طرح از تکنولوژی بلاکچن جهت افزایش امنیت سایبری داده‌های مبادله شده بین واحدها در یک شبکه هوشمند استفاده می‌شود.

نوآوری های این مقاله بشرح زیر خلاصه می شود:

- ارائه یک معماری امن و هوشمند برای بهره‌برداری بهینه از ریزشبکه‌های برق هایبرید بر اساس تکنولوژی بلاکچن
- استفاده از الگوریتم گرگ خاکستری در حل مساله برنامه‌ریزی بهینه مدیریت ریزشبکه هیبرید
- مدل‌سازی دقیق سیستم خورشیدی در فرمول‌بندی مسئله
- مدل‌سازی دقیق شارژ و دشارژ باطری در فرمول‌بندی مسئله

ادامه این مقاله بدین ترتیب می‌باشد: بخش دوم مقاله به فرمول‌بندی مسئله ریزشبکه هیبرید AC-DC به همراه نظریه ابر فازی برای مدل‌سازی عدم قطعیت می‌پردازد. الگوریتم بهینه سازی گرگ خاکستری و همچنین تکنولوژی بلاکچن جهت تبادل داده بترتیب در بخش های سوم و چهارم ارائه شده است. در بخش پنجم نتایج شبیه سازی در سناریوهای مختلف بررسی شده است. نتیجه گیری نهایی در بخش ششم بیان شده است.



شکل (۱): ساختار یک ریزشبکه هیبریدی.

۲- فرمول‌بندی مسئله ریزشبکه هیبرید AC-DC

این بخش به مدیریت انرژی بهینه ریزشبکه‌های هیبریدی AC-DC با ترکیب منابع تجدیدپذیر اختصاص داده شده است. ایده هیبریدیزاسیون منابع برق از نوع AC و DC تنها نمی‌تواند هزینه‌ها و تلفات توان را کاهش دهد، بلکه می‌تواند با تطبیق بهترین تولید و نوع بار، کیفیت توان را بهبود بخشد و پایداری سیستم را افزایش دهد. از طریق چنین فرآیندی، مبدل ها حذف می‌شوند که می‌تواند کیفیت توان و مشخصات ولتاژ را بهبود بخشد. بنابراین واحدهای AC و واحدهای DC به ترتیب مستقیماً به بارهای AC و DC متصل می‌شوند. ایده ریزشبکه هیبریدی در شکل (۱) نشان داده شده است.

در ابتدا فرمول‌های مورد نظر بیان می‌شود و به دنبال آن محدودیت‌های مربوط به ریزشبکه های هیبریدی و همچنین محدودیت‌های مربوط به سایر قسمت های شبکه بیان می‌شود.

تابع هدف درنظر گرفته شده نشان‌دهنده هزینه برق تولید شده توسط منابع تولیدپراکنده، سیستم‌های ذخیره انرژی، منابع انرژی تجدیدپذیر و شبکه اصلی است که ریزشبکه هیبریدی به آن متصل است. تابع هدف بدین صورت بیان است.

$$
\begin{aligned}
&f(x)\\
&=\sum_{t=1}^{N_t}\{\sum_{i=1}^{N_g}\big[{u_i}^t {P_{Gi}}^t {B_{Gi}}^t\\
&+ {S_{Gi}}^{on}\, max\{0, u_i^t - u_i^{t-1}\}\\
&+ S_{Gi}^{Off}\, max\{0, u_i^{t-1} - u_i^t\}\big] +\\
&\sum_{j=1}^{N_S}\big[u_j^t P_{sj}^t B_{sj}^T\\
&+ {S_{Si}}^{on}\, max\{0, u_i^t - u_i^{t-1}\}\\
&+ S_{Si}^{Off}\, max\{0, u_i^{t-1} - u_i^t\}\big]\\
&+ P_{Grid}^t B_{Grid}^T\}
\end{aligned}
\qquad (۱)
$$

در رابطه (۱) f(x)، تمام هزینه‌های یک ریزشبکه هیبرید می‌باشد و علاوه بر این در رابطه (۲) X نشان‌دهنده مقدار توان خروجی واحدهای تولیدپراکنده، ذخیره‌کننده انرژی و شبکه ی اصلی است که ریزشبکه هیبرید به ان متصل می‌باشد.

$$
\begin{aligned}
&X = [P_g, U_g]_{1\times(2\times n\times N_T)}\\
&P_g^t = [P_G^t, P_S^t, P_{Grid}^t]\\
&P_G^t = \left[P_{G1}^t, P_{G2}^t, \dots., P_{G,N_g}^t\right]\\
&P_S^t = \left[P_{S1}^t, P_{S2}^t, \dots., P_{S,N_S}^t\right]\\
&P_{Grid}^t = [P_{Grid}^t]\\
&\mathrm{n=N_g+N_s+1}
\end{aligned}
\qquad (۲)
$$

علاوه بر این در رابطه زیر مقدار 0 نشان‌دهنده وضعیت حالت خاموش می‌باشد و ۱ بیان‌کننده وضعیت روشن واحد است.

$$U_g^t = [u_1^t, u_2^t, \dots., u_N^t\ ]\ \ u_k^t \in \{0,1\} \qquad (۳)$$

قیود در این مسئله شامل قیود بخش‌های AC و DC است،

همچنین بار بایستی در بخش‌های AC و SC تامین شوند. قید تولید و تقاضا در قسمت DC ریز شبکه بشرح زیر تعریف می‌شود.

$$\sum_{i=1}^{N_g} P_{Gi}^t + \sum_{j=1}^{N} P_{Sj}^t + P_{Grid}^t = \sum_{k=1}^{N_{load}} P_{Load,k}^t \quad (۴)$$

قیود پخش بار در بخش AC ریز شبکه هیبرید در پایین ارائه شده است.

$$P_m^{Inj,t} = \sum_{n=1}^{N_B} V_m^t Y_{mn} \cos(\theta_{mn} + \delta_m^t - \delta_n^t) \quad (۵)$$

$$Q_m^{Inj,t} = \sum_{n=1}^{N_B} V_m^t Y_{mn} \sin(\theta_{mn} + \delta_m^t - \delta_n^t) \quad (۶)$$

هر واحد تولیدی ریزشبکه قادر به تولید برق در محدوده معینی است که در زیر به آن اشاره شده است. این عملکرد پایدار ریزشبکه را تضمین می کند.

$$\begin{aligned} P_{Gi,\min}^t \le P_{Gi}^t \le P_{Gi,\max}^t \\ P_{Sj,\min}^t \le P_{Sj}^t \le P_{Sj,\max}^t \\ P_{Grid,\min}^t \le P_{Grid}^t \le P_{Grid,\max}^t \end{aligned} \quad (۷)$$

علاوه بر این قیود باطری بشرح زیر بیان شده است.

$$\begin{aligned} W_{ess}^t = W_{ess}^{t-1} + \eta P_{charge} \Delta t - \frac{1}{\eta_{charge}} P_{discharge} \Delta t \\ W_{ess,\min} \le W_{ess}^t \le W_{ess,\max} \\ P_{charge,t} \le P_{charge,\max} \\ P_{discharge,t} \le P_{discharge,\max} \end{aligned} \quad (۸)$$

همچنین قید رزرو چرخان نیز در زیر مدل شده است.

$$\sum_{i=1}^{N_g} \left\{ u_i^t P_{Gi,\max}{}^t \right\} + \sum_{j=1}^{N_S} \left\{ u_j^t P_{sj,\max}^t \right\} + P_{Grid,\max}^t \ge \sum_{k=1}^{N_{load}} P_{load,k}^t + P_{loss}^t \quad (۹)$$

در ادامه محدودیت‌های مربوط به ظرفیت خط و محدودیت‌های ولتاژ مجاز آورده شده است.

$$P_i^{line.t} < P_{i,max}^{Line} \quad (۱۰)$$

$$V_m^{\min} \le V_m^t \le V_m^{\max} \quad (۱۱)$$

۳- الگوریتم بهینه‌سازی گرگ خاکستری

بهینه‌ساز گرگ خاکستری (GWO[4]) یکی از الگوریتم‌های فرابتکاری قدرتمند است که توسط میرجلالی [۱۸] پیشنهاد شده است. این الگوریتم از اعضای خانواده گرگ‌های خاکستری، که شکارچیان پیشرو در بالای زنجیره غذایی هستند، الهام گرفته شده است .این نوع گرگ‌ها در گروه‌های ۵ تا ۱۲ نفره زندگی می‌کنند که رهبر دسته گرگ آلفا نام دارد و مسئولیت گله را بر عهده دارد. بتا دومین سطح بعد از آلفا است که دستورالعمل‌های آلفا را در سراسر دسته تقویت می‌کند و بازخورد را به آلفا ارائه می‌دهد. سطح پایین سلسله مراتب گرگ خاکستری امگا نامیده می‌شود. علاوه بر این، اگر گرگ آلفا، بتا یا امگا نباشد، به او دلتا می‌گویند. وظایف گرگ دلتا به عنوان پیشاهنگ، نگهبان، بزرگتر، شکارچی و مراقب است. مراحل GWO برای شکار طعمه در بخش بعدی ارائه شده است.

۳-۱- فرمول‌بندی ریاضی الگوریتم گرگ خاکستری

رفتار GWO را می‌توان به صورت ریاضی فرمول‌بندی کرد، که در آن موقعیت گرگ آلفا (a) بهترین پاسخ در الگوریتم GWO پیشنهادی فرض می‌شود، در حالی که موقعیت‌های بتا (b) و دلتا (d) دومین و سومین بهترین پاسخ ها هستند. امگا (w) نشان‌دهنده بقیه پاسخ‌های است. شکار در الگوریتم GWO توسط a، b و d هدایت می‌شود، در حالی که امگا آنها را دنبال می‌کند. روند حمله گرگ‌های خاکستری شامل چندین مرحله قبل از گرفتن طعمه است. در مرحله اول، گرگ‌ها تمایل دارند طعمه را محاصره کنند تا مانع حرکت او شوند، این رفتار محاصره‌ای را می توان با مجموعه معادلات زیر نشان داد:

$$\vec{D} = \left| \vec{C}.\overrightarrow{X_p}(t) - \vec{X}(t) \right| \quad (۱۲)$$

$$\vec{X}(t+1) = \overrightarrow{X_p}(t) - \vec{A}.\vec{D} \quad (۱۳)$$

که در آن $\vec{A}$ و $\vec{D}$ ضرایب بردار هستند، $\overrightarrow{X_p}(t)$ مکان بردار طعمه است، t تکرار فعلی را نشان می‌دهد، و $\vec{X}$ بردار مکان یک گرگ خاکستری است. با یافتن بردارهای $\vec{A}$ و $\vec{C}$ می‌توان معادلات دایره‌ای را به دست آورد.

$$\vec{A} = 2\vec{a}.\overrightarrow{r_1} - \vec{a} \quad (۱۴)$$

$$\vec{C} = 2.\overrightarrow{r_2} \quad (۱۵)$$

$$a = 2 - t * \frac{2}{maximum\ iteration} \quad (۱۶)$$

که در آن $\vec{a}$ به صورت خطی از ۲ به ۰ در طول تکرارهای الگوریتم تغییر می‌کند و r_1 و r_2 مقادیر تصادفی بین (۰، ۱) هستند. در هر تکرار، بهترین راه حل‌ها از آلفا، بتا و دلتا ذخیره می‌شوند و سایر گرگ‌ها (امگا) موقعیت خود را بر اساس بهترین راه‌حل‌ها بروز می‌کنند. این مراحل با معادلات زیر نشان داده می‌شوند:

$$\overrightarrow{D_{Alpha}} = \left| \overrightarrow{C_1}.\overrightarrow{X_{Alpha}} - \vec{X} \right| \quad (۱۷)$$

$$\overrightarrow{D_{Beta}} = \left| \overrightarrow{C_2}.\overrightarrow{X_{Beta}} - \vec{X} \right| \quad (۱۸)$$

$$\overrightarrow{D_{Delta}} = \left| \overrightarrow{C_3}.\overrightarrow{X_{Delta}} - \vec{X} \right| \quad (۱۹)$$

موقعیت‌های برداری طعمه را می‌توان بر اساس موقعیت‌های آلفا، بتا و دلتا با استفاده از معادلات زیر تعیین کرد:

$$\overrightarrow{X_1} = \left| \overrightarrow{X_{Alpha}} - \overrightarrow{A_1}.\overrightarrow{D_{Alpha}} \right| \quad (۲۰)$$

$$\overrightarrow{X_2} = \left| \overrightarrow{X_{Beta}} - \overrightarrow{A_2}.\overrightarrow{D_{Beta}} \right| \quad (۲۱)$$

$$\overrightarrow{X_3} = \left| \overrightarrow{X_{Delta}} - \overrightarrow{A_3}.\overrightarrow{D_{Delta}} \right| \quad (۲۲)$$

$$\vec{X}(t+1) = \frac{\overrightarrow{X_1} + \overrightarrow{X_2} + \overrightarrow{X_3}}{3} \quad (۲۳)$$

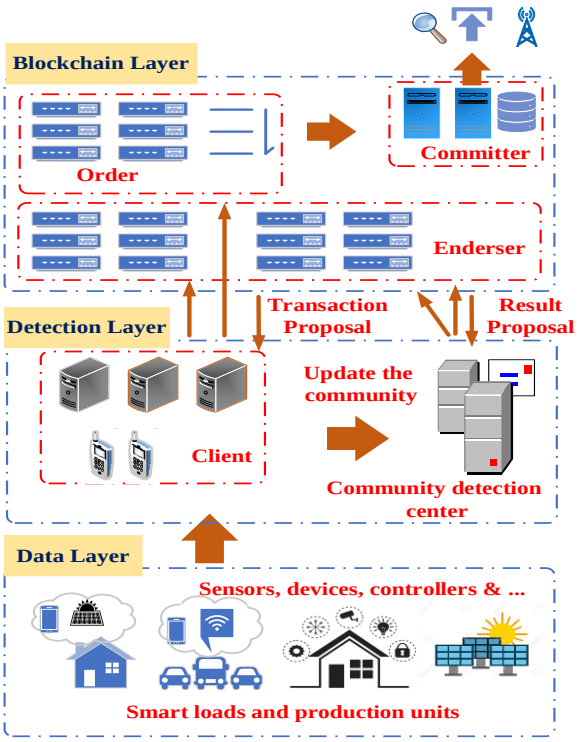
اکتشاف و بهره‌برداری از عوامل گرگ خاکستری به پارامتر A بستگی دارد، با کاهش نیمی از تکرارها ($|A| \geq 1$) به اکتشاف اختصاص داده می‌شود. در همین حال، ($|A| < 1$) به نیمی دیگر از تکرارها در بهره‌برداری اختصاص داده می‌شود.

۴- تکنولوژی بلاکچن

بلاکچن را می‌توان بعنوان اصلی‌ترین فناوری بیت‌کوین و برخی دیگر از انواع ارزهای رمزپایه درنظر گرفت، که به یکی از فنآوری‌های جهان در سال ۲۰۱۰ تبدیل شده است. مشکل اتصال شبکه انتقال همیشه یکی از موانع جدی در برابر اجرای کامل بازسازی سیستم‌های قدرت، ارتباط صحیح و آزاد تولیدکنندگان و مصرف‌کنندگان و چالش اصلی اپراتورهای مستقل سیستم بوده است. بنابراین، سیاست استفاده از منابع تولید توزیع شده برای مدیریت اتصال خطوط انتقال از اهمیت ویژه‌ای برخوردار است. سیاست استفاده از فناوری شفاف بلاکچن به کاهش خطرات کمک می‌کند و امنیت بالاتری را در شبکه ایجاد می‌کند، از این رو تقلب مالی حذف شده و کل هزینه عملیاتی کاهش می‌یابد. بمنظور نشان دادن مواردی که در طرح‌های معمول بلاکچن اتفاق می افتد، عمدتا به دلیل ذخیره‌سازی و سطح بالایی از محاسبات آدرس هش، فناوری بلاکچن بیان شده است. بعلاوه، یک روش بازیابی اطلاعات جدید با هدف ارائه رویکردی برای بازیابی داده‌های مناسب و دقیق گسترش یافته است.

۴-۱- ساختار تبادل اطلاعات بر اساس تکنولوژی بلاکچن

به منظور ارائه خدمات مبتنی بر ساختار ریزشبکه و به اشتراک‌گذاری داده‌ها، تراکنش‌های ذخیره‌شده در پایگاه داده بلاکچن براساس سطح حریم خصوصی طبقه‌بندی شده‌اند. سطح حریم خصوصی شامل داده‌های انجمن، داده‌های رمزگذاری شده و داده‌های عمومی است. داده‌های عمومی، در اینجا، به داده‌ای اشاره دارند که می‌تواند از طریق کل گره‌ها مشاهده شود. علاوه بر این، داده‌های عمومی جامعه اطلاعاتی را ارائه می‌دهند که می‌تواند از طریق کل گره‌های مربوط به یک جامعه مشابه شناخته شود، و اطلاعات رمزگذاری شده اساساً به داده‌های خصوصی و آن‌هایی که کاربران تمایل به خرید/فروش دارند، اشاره دارد. بطور کلی، هنگامی که کاربران اطلاعات حرفه‌ای را به اشتراک می‌گذارند، پیشنهاد می‌شود که آنها میزان حریم خصوصی اطلاعات را بر روی داده‌های عمومی موجود در جامعه تنظیم کنند تا این اطلاعات توسط کاربران بیشتری که واقعاً به آن دسترسی دارند، به اشتراک گذاشته شود و نیاز به قابل مشاهده بودن آنها دارد. در نتیجه، هدف اصلی می‌تواند تقسیم منطقی جامعه از طریق بدست آوردن یک روش تشخیص جامعه باشد تا اطلاعات عمومی جامعه بتواند بین کاربران بیشتری که واقعاً به آن نیاز دارند تقسیم شود. شکل (۲) ساختار اشتراک داده را مطابق با روش بلاکچن نشان می‌دهد. در استراتژی ارائه داده اشتراک سه لایه مختلف وجود دارد: لایه داده، لایه بلاکچن و لایه تشخیص. اطلاعات توسط لایه داده جمع آوری شده و به لایه شناسایی ارسال می‌شود. لایه تشخیص یک روش شناسایی جامعه را پیاده‌سازی می‌کند که مشتریان را به جوامع مختلف تقسیم می‌کند و دامنه اشتراک اطلاعات را محدود می‌کند. لایه بلاکچن همچنین مسئولیت ایمن نگه داشتن نتیجه شناسایی جامعه و سوابق معاملات را دارد.



شکل (۲): ساختار اشتراک داده با توجه به فناوری بلاکچن.

۴-۲- لایه داده

لایه داده شامل داده‌هایی است که از طریق سنسورهای مقیاس بزرگ [۱۹] مانند نوع محصول و مقدار محصول ، وضعیت عملکرد دستگاه و سایر داده های چندین پارامتر قابل درک هستند. داده‌های ادراک توسط حسگرها بدست می‌آید و برای تجزیه و تحلیل و به اشتراک‌گذاری جامع در سرویس دهنده مشتری بارگذاری می‌شود. اطلاعات، پس از دریافت از حسگرها، برای تجزیه و تحلیل در سرور مشتری ارسال و به اشتراک گذاشته می‌شود.

۴-۳- لایه تشخیص

لایه تشخیص شامل سرویس گیرنده‌ها، سرور مشتری و همچنین سرور شناسایی جامعه است. سرور مشتری اساساً وظیفه دارد داده ها را بدست آورد و سپس آنها را به شبکه بلاکچن ارسال کند و همچنین به سرور شناسایی جامعه بفرستد. علاوه بر این، داده‌های برچسب نیز هنگامی تولید می‌شوند که کاربر زنجیره وابستگی را پیوند دهد. سرور تشخیص جامعه وظیفه جمع‌آوری کل داده‌های برچسب و انجام تکنیک تشخیص جامعه و همچنین تولید نتایج شناسایی جامعه و همچنین ارسال این داده‌ها به شبکه بلاکچن را دارد. هنگامی که نتایج شناسایی جامعه با

موفقیت در پایگاه داده بلاکچن ذخیره می شود، مشتری قرارداد هوشمند را برای جستجوی اطلاعات تقسیم شده از انجمن اجرا می کند.

۴-۴- لایه بلاکچن

از آنجا که لایه بلاکچن بر اساس ساختارهای ساخته شده، از گره‌های تأیید، سفارش و همچنین متعهد تشکیل شده است. گره تأیید مسئولیت اطمینان از ارائه معامله از طریق سرور مشتری را دارد. گره سفارش وظیفه طبقه‌بندی و بسته بندی معاملات را در بلاک‌ها دارد. گره متعهد همچنین وظیفه تأیید اعتبار و افزودن بلوک به بلاکچن پایگاه داده را دارد. روش معامله معمول به صورت مراحل زیر طراحی شده است:

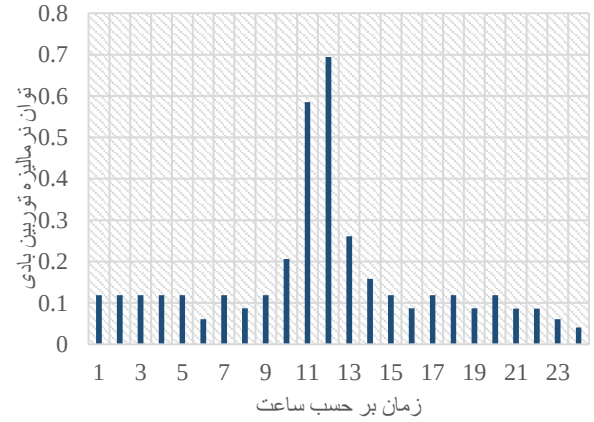
- طرف مشتری پیشنهاد معامله را انجام می‌دهد.
- اجرای معامله توسط گره شبیه سازی می‌شود.
- مشتری معامله را به سرویس اجماع منتقل می‌کند.
- مشتری سفارش معاملات را با اجماع ایجاد بلوک‌های جدید می‌کند و معاملات را انجام می‌دهد.

۵- شبیه‌سازی و نتایج

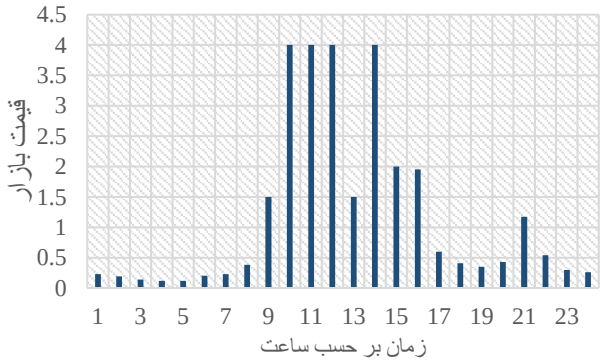
این بخش عملکرد چارچوب و مدل پیشنهادی را برای مدیریت انرژی بهینه ریزشبکه‌های هیبریدی AC-DC ارزیابی می‌کند. شکل (۱) ساختار ریزشبکه هیبریدی AC-DC را ارائه می‌دهد. در واقع، از آنجایی که هیچ سیستم تست استاندارد IEEE برای ریزشبکه‌های هیبریدی AC-DCوجود ندارد، این مقاله دو سیستم آزمایشی را برای انجام یک مطالعه موردی ترکیب کرد. تمام داده‌های سیستم AC و DC از مقالات [۲۰] و [۲۱] گرفته شده است. برای اثبات توانایی جستجوی مناسب GWOپیشنهادی، بخش اول نتیجه شبیه‌سازی بدون حمله سایبری متمرکز است. و سپس در مرحله بعدی سیستم تحت حملات سایبری بررسی می‌شود.

در این قسمت مقادیر پیش‌بینی واحد خورشیدی، توربین بادی، قیمت بازار و ضریب بار بعنوان ورودی الگوریتم ارائه شده است. شکل (۳) این مقادیر را در سیستم تست DC نشان می‌دهد. جدول (۱) مشخصات واحدها از جمله قیمت، ظرفیت و غیره را ارائه می‌دهد. دو حالت عملیات (SoP^5) در این تحلیل در نظر گرفته شده است. در SoP1، واحدها روشن هستند و باتری به اندازه کافی بزرگ و کاملا شارژ شده است، بنابراین در ابتدا نیازی به شارژ شدن ندارد. درSoP2 ، واحدها می‌توانند روشن یا خاموش شوند و انرژی اولیه باتری صفر است.

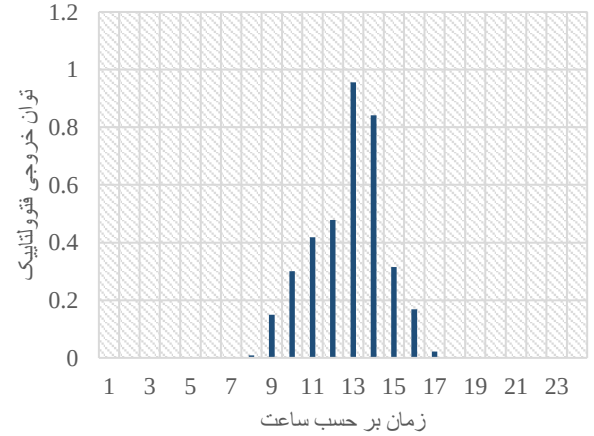
برای SoP1 وSoP2 ، نتایج شبیه‌سازی با استفاده از الگوریتم بهینه‌سازی پیشنهادی در شرایط عادی و حمله تزریق داده غلط در جدول (۲) ارائه شده است. برای مقایسه خوب، از روش‌های بهینه‌سازی مختلف شامل GA^6، PSO^7 مقایسه استفاده شده است. برای نشان دادن پایداری بالای مدل، بهینه‌سازی ۴۰ بار اجرا شده و نتایج برای میانگین بهترین راه‌حل، بدترین راه‌حل، بهترین راه‌حل در بین تمام مسیرها و مقدار انحراف استاندارد نشان داده شده است.



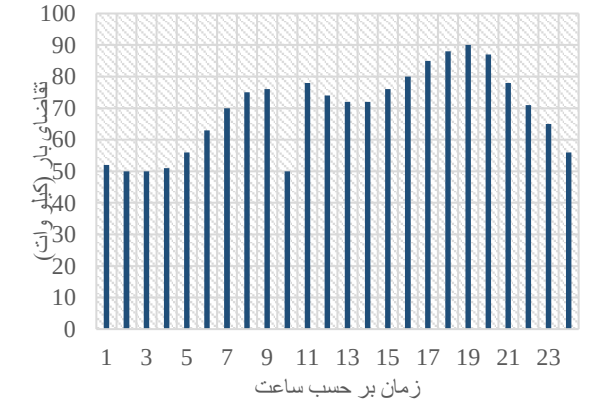
(الف) توان خروجی واحد باد



(ب) پیشنهاد قیمت اصلی برق شهری



(ج) توان خروجی پنل خورشیدی



(د) تقاضای بار منطقهDC

شکل (۳): ویژگی‌های ورودی ریزشبکه DC [۲۰]

جدول (۱): ظرفیت و قیمت منابع تولیدپراکنده و شبکه اصلی

حالت	باتری	توربین بادی	فتوولتاییک	پیل سوختی	میکروتوربین	شبکه
حداقل توان (کیلو وات)	-۳۰	۰	۰	۳	۶	-۳۰
حداکثر توان (کیلو وات)	۳۰	۱۵	۲۵	۳۰	۳۰	۳۰
قیمت (سنت/کیلو وات ساعت)	۰,۳۸	۱,۰۷۳	۲,۵۸۴	۰,۲۹۴	۰,۴۵۷	-
هزینه راه‌اندازی/خاموشی (سنت)	۰	۰	۰	۱,۶۵	۱,۹۶	-

با توجه به این نتایج، GWO پیشنهادی با یافتن راه‌حل بهینه‌تر از سایر روش‌ها، توانایی جستجوی بهتری را از خود نشان داده است. همچنین با توجه به پایین بودن مقدار انحراف استاندارد، پایداری بالای مدل نسبت به سایر الگوریتم‌ها اثبات می‌شود. دلیل یکسان بودن بهترین مقدار، بدترین مقدار و مقدار متوسط روش پیشنهادی این است که می‌تواند در تمام ۲۵ مسیر به راحتی به راه حل بهینه وارد شود، این منجر به یک مقدار انحراف استاندارد صفر می‌شود که استحکام بالا و توانایی جستجوی بالای الگوریتم پیشنهادی را نشان می‌دهد. با مقایسه SoP1 و SoP2، در حالت نرمال مشاهده می‌شود که هزینه ریزشبکه در SoP2 بیشتر از SoP1 است، که این نشان‌دهنده هزینه اضافی ناشی از انرژی اولیه باتری است. شکل (۴) انتقال توان بهینه واحدها را برای SoP1 و SoP2 نشان می‌دهد.

جدول (۲): مقایسه تابع هزینه برای سناریوهای مختلف با استفاده از روش‌های مختلف [۲۲].

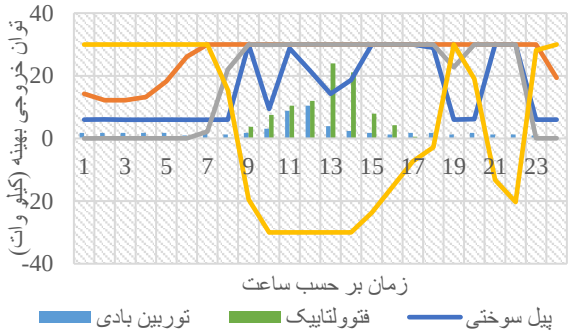
		رو ش	بهترین جواب (سنت)	بدترین جواب (سنت)	میانگین (سنت)	انحراف استاندارد (سنت)
حالت عادی	SoP1	GA	۲۷۷,۷۴۴۴	۳۰۴,۵۸۸۹	۲۹۰,۴۳۲۱	۱۳,۴۴۲۱
		PSO	۲۷۷,۳۲۳۷	۳۰۳,۳۷۹۱	۲۸۸,۸۷۶۱	۱۰,۱۸۲۱
		GWO	۲۵۵,۷۹۱۹	۲۵۵,۸۰۸۴	۲۵۵,۸۰۶۴	۰,۰۱۳۲
	SoP2	GWO	۳۶۱,۳۶۵۰	۳۶۱,۹۹۰۶	۳۶۱,۹۱۳۸	۰,۶۵۸۸

در ادامه جهت بررسی تاثیر حمله تزریق داده غلط حالت‌ها تحت حملات مختلف بررسی می‌شود. شبیه‌سازی در حملات مختلف از جمله افزایش ۱۰ درصدی بار، کاهش ۱۰ درصدی بار و... بررسی شده است. در زمانی که بدلیل یک حمله تزریق داده غلط، مقدار بار ۱۰ درصد افزایش می‌یابد، سبب می‌شود که تمامی برنامه‌ریزی‌های شبکه بر اساس این مقدار صورت گیرد و مقدار تعادل تولید و بار به هم بریزد و در نتیجه آن قیمت نهایی افزایش یابد و تلفات در شبکه بالا رود، که این در هر دو سناریو در جدول (۳) و شکل (۴) قابل مشاهده است.

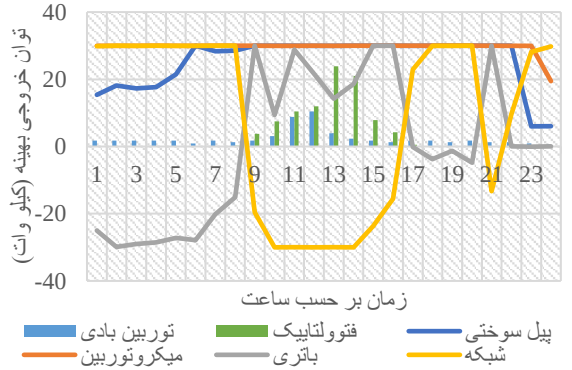
همانگونه که مشاهده می‌شود، هنگامی که در پی یک حمله سایبری ۹۰ درصد بار در برنامه ریزی درنظر گرفته شود, سبب می‌شود که توان لازم جهت تامین تمامی بارها در شبکه موجود نباشد و در پی آن خاموشی در شبکه ایجاد می‌شود و همچنین تولید منابع در حالت بهینه نمی‌باشد. دلیل پایین بودن هزینه در این شرایط عدم صحیح بودن اطلاعات و درنظر نگرفتن تمامی بارهای شبکه می‌باشد که بدلیل حمله در برنامه‌ریزی شبکه درنظر گرفته نشده است. نتایج برای هر دو سناریو تحت این حمله در جدول (۳) و شکل (۵) قابل مشاهده است.

جدول (۳): مقایسه تابع هزینه برای سناریوهای مختلف تحت حملات سایبری

رخداد حمله سایبری در SoP1			
نرمال	افزایش ۱۰ درصدی بار	کاهش ۱۰ درصدی بار	افزایش ۱۰ درصدی در توان فتوولتاییک
۲۵۵,۷۹۱۹	۳۸۵,۱۸۸۸	۱۵۲,۸۸۶۲	۲۷۶,۱۲۶۸
رخداد حمله سایبری در SoP2			
نرمال	افزایش ۱۰ درصدی بار	کاهش ۱۰ درصدی بار	افزایش ۵ درصدی در توان توربین بادی
۳۶۱,۳۶۵۰	۵۲۱,۳۴۷۱	۲۳۶,۷۷۴۱	۳۶۳,۵۲۶۷



(الف)



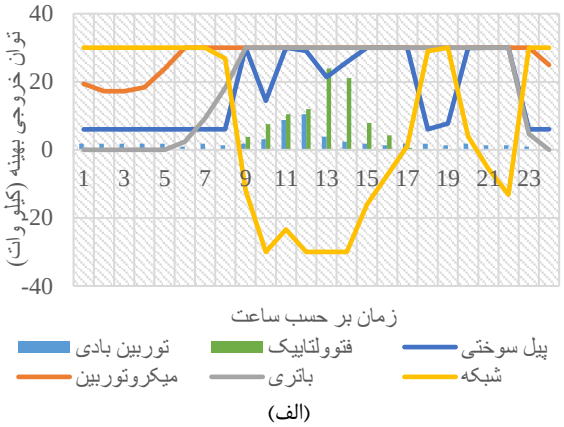
(ب)

شکل (۴): بدست آوردن توزیع توان بهینه منابع تولیدات‌پراکنده با استفاده از GW[8] پیشنهادی الف) سناریوی اول، ب) سناریو دوم.

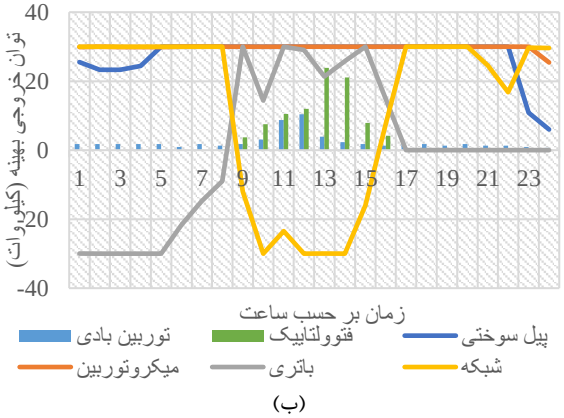
جدول (۴) شرح بلاکچن تراکنش

	بلوک اطلاعات			بلوک شاخص ها
توضیحات	۱			شاخص
	۱			زمان
	توان (kW)	دریافت کننده	ارسال کننده	تراکنش داده
	۶،۵	توربین بادی	اپراتور مستقل	
	6ace5c77c9f1abba4f25f81f5557ca3d			هش قبلی
	7ab52efec4674cbf34f97e2a72d5e753			هش فعلی
توضیحات	۲			شاخص
	۲			زمان
	توان (kW)	دریافت کننده	ارسال کننده	تراکنش داده
	۴،۲	سلول خورشیدی	اپراتور مستقل	
	7ab52efec4674cbf34f97e2a72d5e753			هش قبلی
	266477dd8561492cfa2bef961485b8a4			هش فعلی
توضیحات	۴			شاخص
	۴			زمان
	توان (kW)	دریافت کننده	ارسال کننده	تراکنش داده
	۱۱۵،۳	شبکه	اپراتور مستقل	
	098e81b5609be3f39bdb61c2e6d2c67d			هش قبلی
	de3a8a139ecee8aaf023fc914417d748			هش فعلی
توضیحات	۵			شاخص
	۴			زمان
رخ دادن حمله سایبری	توان (kW)	دریافت کننده	ارسال کننده	تراکنش داده
	۸۰	شبکه	اپراتور مستقل	
	098e81b5609be3f39bdb61c2e6d2c67d			هش قبلی
	029e6f1af9dacfe2f3e01fda58634a00			هش فعلی
توضیحات	۶			شاخص
	۵			زمان
	قیمت ($/kWh)	دریافت کننده	ارسال کننده	تراکنش داده
	۴۰	اپراتور مستقل	میکروتوربین	
	de3a8a139ecee8aaf023fc914417d748			هش قبلی
	3490acda48423d504c295da91fa2aa92			هش فعلی
توضیحات	۷			شاخص
	۵			زمان
رخ دادن حمله سایبری	قیمت ($/kWh)	دریافت کننده	ارسال کننده	تراکنش داده
	۲۰	اپراتور مستقل	میکروتوربین	
	de3a8a139ecee8aaf023fc914417d748			هش قبلی
	706ef584b4a6529f9af410c950fcecc9			هش فعلی

با توجه به جدول (۴)، بلاکچن خصوصی شامل داده‌های ارسالی در معماری می‌باشد. داده‌های موجود در بلاکچن قادر هستند که به داده‌های اپراتورها توجه ویژه‌ای داشته باشند. در بلاکچن، بلوک متشکل از هش قبلی و هش خود می‌باشد که در آنها هش قبلی آن بلوک را به بلوک قبلی متصل می‌کند. همچنین با توجه به جدول، در هر شاخص زمانی، هش تغییر کرده است که این امر منجر به امنیت سایبری بالاتر شبکه و ارائه یک زنجیره پیوسته می‌شود. ذکر این نکته قابل توجه است که کل عوامل دیگر در تمام مدت دارای بلاکچن خصوصی خود در حالت مشابه می‌باشند. جدول (۴) زنجیره بلوکی عمومی مرتبط با عواملی را نشان می‌دهند که در آن داده و بلاکچن خصوصی عامل‌ها با یکدیگر مشابه هستند. روش پیشنهادی می‌تواند به بازیابی داده‌ها با وجود حمله‌های سایبری یا کاهش بسته در بلاکچن کمک کند.



(الف)



(ب)

شکل (۵): بدست آوردن توزیع توان بهینه منابع تولیدات پراکنده با استفاده از GW پیشنهادی در زمان حمله سایبری و افزایش ۱۰ درصدی بار الف) سناریوی اول، ب) سناریو دوم

۶- نتیجه گیری

در این مقاله سعی شده است تا مدیریت بهینه انرژی ریزشبکه‌های هیبریدی AC-DC شامل انواع واحدها مانند توربین‌های خورشیدی، باد، پیل سوختی و میکروتوربین‌ها در یک چارچوب امن مورد بررسی قرار گیرد. در این پژوهش جهت حل مسئله بهینه سازی از الگوریتم گرگ خاکستری استفاده شده است. دو وضعیت عملکرد متفاوت به نام‌های SoP1 و SoP2 شبیه‌سازی شدند که می‌توانند نقش باتری، مبدل‌های AC-DC بین مناطق AC و DC و منابع تجدیدپذیر در ریزشبکه را برجسته کنند. از نظر روش بهینه‌سازی، توانایی جستجوی بالا و پایداری الگوریتم نسبت به الگوریتم‌های سنتی و معروف نیز ثابت شد. همچنین در ادامه اثرات حملات سایبری در سیستم پیاده‌سازی و اجرا شده است و نتایج در حالت نرمال و در شرایط حمله بررسی و مقایسه شده است. معماری بلاکچن برای ارتباط بین تجهیزات و ارتباط بین منابع انرژی استفاده شده است. همچنین، شبکه هوشمند میزبان بازار انرژی تراکنش مبتنی بر بلاکچن می‌تواند بطور مداوم اطلاعات را مبادله کنند تا ثبات سیستم تضمین گردد. ارتقای امنیت سایبری را می‌توان بعنوان مزیت این مدل پیشنهادی درنظر گرفت، از دیگر مزایای آن می‌توان ایمن و شفاف بودن آن اشاره کرد که توانایی کمک بحداقل رساندن خطرهای موجود در شبکه را دارد.

ضمایم

t	زمان
V	ولتاژ
P	توان
P_{Gi}^{t}	توان تولیدی توسط واحد های تولید پراکنده i در ساعت t
B_{Gi}	هزینه تولید توان واحد i
P_{sj}^{t}	توان تبادلی واحد ذخیره کننده j در ساعت t
B_{sj}^{T}	هزینه تولید توان ذخیره کننده انرژیj در ساعت t
P_{Grid}^{t}	توان گرفته شده از شبکه اصلی در ساعت t
B_{Grid}^{T}	هزینه توان خریداری شده از شبکه در ساعت t
$P_{Gi,min}^{t}$	حداقل توان تولیدی واحد تولید توان i
$P_{Gi,max}^{t}$	حداقل توان تولیدی واحد تولید توان i
$P_{Sj,min}^{t}$	حداقل توان ذخیره ساز انرژی j
$P_{Sj,max}^{t}$	حداکثر توان ذخیره ساز انرژی j
$P_{Grid,min}^{t}$	حداقل توان دریافتی از شبکه اصلی
$P_{Grid,max}^{t}$	حداقل توان دریافتی از شبکه اصلی
$W_{ess,min}$	حداقل انرژی باتری
$W_{ess,max}$	حداکثر انرژی باتری
$P_{charge,max}$	حداکثر توان شارژ
$P_{discharge,max}$	حداقل توان دشارژ
η_{charge}	ضریب شارژ باتری

مراجع

[1] Wang P, Wang D, Zhu C, Yang Y, Abdullah HM, Mohamed MA. Stochastic management of hybrid AC/DC microgrids considering electric vehicles charging demands. Energy Reports. 2020 Nov 1;6:1338-52.

[2] Li S, Li Y, Chen X, Li T, Zhang W. A novel flexible power support control with voltage fluctuation suppression for islanded hybrid AC/DC microgrid involving distributed energy storage units. International Journal of Electrical Power & Energy Systems. 2020 Dec 1;123:106265.

[3] Jaradat M, Jarrah M, Bousselham A, Jararweh Y, Al-Ayyoub M. The internet of energy: smart sensor networks and big data management for smart grid. Procedia Computer Science. 2015 Jan 1;56:592-7.

[4] Ustun TS, Ozansoy C, Zayegh A. Recent developments in microgrids and example cases around the world—A review. Renewable and Sustainable Energy Reviews. 2011 Oct 1;15(8):4030-41.

[5] Chhaya L, Sharma P, Kumar A, Bhagwatikar G. Cybersecurity for smart grid: threats, solutions and standardization. Advances in Greener Energy Technologies. 2020:17-29.

[6] Unsal DB, Ustun TS, Hussain SS, Onen A. Enhancing cybersecurity in smart grids: false data injection and its mitigation. Energies. 2021 May 6;14(9):2657.

[7] Teimourzadeh Baboli P, Shahparasti M, Parsa Moghaddam M, Haghifam MR, Mohamadian M. Energy management and operation modelling of hybrid AC–DC

microgrid. IET Generation, Transmission & Distribution. 2014 Oct;8(10):1700-11.
[8] Qachchachi N, Mahmoudi H, El Hasnaoui A. Optimal power flow for a hybrid AC/DC microgrid. In2014 International Renewable and Sustainable Energy Conference (IRSEC) 2014 Oct 17 (pp. 559-564). IEEE.
[9] Hernandez-Aramburo CA, Green TC, Mugniot N. Fuel consumption minimization of a microgrid. IEEE Trans Ind Appl, 41, (2005), 673-681.
[10] Khatiba T., Mohameda A., Sopianb K., "Optimization of a PV/wind micro-grid for rural housing electrification using a hybrid iterative/genetic algorithm: Case study of Kuala Terengganu," Malaysia, *Energy and Buildings*, vol. 47, pp. 321–331, 2012.
[11] Pop C, Cioara T, Antal M, Anghel I, Salomie I, Bertoncini M. Blockchain based decentralized management of demand response programs in smart energy grids. Sensors. 2018 Jan 9;18(1):162.
[12] Croce D, Giuliano F, Tinnirello I, Galatioto A, Bonomolo M, Beccali M, Zizzo G. Overgrid: A fully distributed demand response architecture based on overlay networks. IEEE transactions on automation science and engineering. 2016 Nov 21;14(2):471-81.
[13] Tang R, Wang S, Li H. Game theory based interactive demand side management responding to dynamic pricing in price-based demand response of smart grids. Applied Energy. 2019 Sep 15;250:118-30.
[14] Liu N, Yu X, Wang C, Li C, Ma L, Lei J. Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers. IEEE Transactions on Power Systems. 2017 Jan 9;32(5):3569-83.
[15] Ahl A, Yarime M, Tanaka K, Sagawa D. Review of blockchain-based distributed energy: Implications for institutional development. Renewable and Sustainable Energy Reviews. 2019 Jun 1;107:200-11.
[16] Gao J, Asamoah KO, Sifah EB, Smahi A, Xia Q, Xia H, Zhang X, Dong G. GridMonitoring: Secured sovereign blockchain based monitoring on smart grid. IEEE access. 2018 Feb 27;6:9917-25.
[17] Wan J, Li J, Imran M, Li D. A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Transactions on Industrial Informatics. 2019 Jan 22;15(6):3652-60.
[18] Mirjalili S, Mirjalili SM, Lewis A. Grey wolf optimizer. Advances in engineering software. 2014 Mar 1;69:46-61.
[19] Jiang H, Chen J, Dong G, Liu T, Chen G. Study on Hankel matrix-based SVD and its application in rolling element bearing fault diagnosis. Mechanical systems and signal processing. 2015 Feb 1;52:338-59.
[20] Baziar A, Kavousi-Fard A. Considering uncertainty in the optimal energy management of renewable micro-grids including storage devices. Renewable Energy. 2013 Nov 1;59:158-66.
[21] Kavousi-Fard A, Niknam T, Fotuhi-Firuzabad M. Stochastic reconfiguration and optimal coordination of V2G plug-in electric vehicles considering correlated wind power generation. IEEE Transactions on Sustainable Energy. 2015 Apr 15;6(3):822-30.
[22] Kavousi-Fard A, Niknam T, Fotuhi-Firuzabad M. A novel stochastic framework based on cloud theory and $\theta $-modified bat algorithm to solve the distribution feeder reconfiguration. IEEE Transactions on Smart Grid. 2015 Jun 12;7(2):740-50.

رزومه

ستار شجاعیان در نورآباد ممسنی متولد شده است. تحصیلات دانشگاهی خود را در مقطع کارشناسی و کارشناسی ارشد مهندسی برق- قدرت از دانشگاه آزاد اسلامی واحد نورآباد سپری کرده است. فعالیت‌های پژوهشی و علاقه‌مندی ایشان در زمینه الگوریتم های بهینه سازی، مدیریت انرژی، بهره‌برداری از سیستم‌های قدرت، حملات سایبری و تکنولوژی بلاکچن است و در حال حاضر دانشجو دکتری مهندسی برق قدرت در دانشگاه آزاد اسلامی واحد مرودشت می‌باشد.

طاهر نیکنام استاد تمام در رشته مهندسی برق دانشگاه صنعتی شیراز می باشد. فعالیت‌های پژوهشی و علاقه‌مندی ایشان در زمینه الگوریتم های بهینه سازی، مدیریت انرژی، بهره‌برداری از سیستم‌های قدرت، تولیدات پراکنده، بازار برق، شبکه هوشمند، حملات سایبری و تکنولوژی بلاکچن است.

مهدی نفر عضو هیئت علمی در رشته مهندسی برق دانشگاه آزاد اسلامی واحد مرودشت می باشد. فعالیت‌های پژوهشی و علاقه‌مندی ایشان در زمینه مدیریت انرژی، ریزشبکه، تولیدات پراکنده، برنامه‌ریزی و بهره‌برداری است.

زیرنویس‌ها

[1] Peer-to-Peer
[2] Distributed System Operator
[3] Demand Response
[4] Grey Wolf Optimizer
[5] States of Operations
[6] Genetic Algorithm
[7] Particle Swarm Optimization
[8] Grey Wolf

Secure Energy Management in Hybrid Microgrids Based on Blockchain Technology

Sattar Shojaeiyan[1], Taher Niknam[* 2], Mehdi Nafar[3]

1- PhD student, Department of Electrical Engineering, Marvdasht Branch, Islamic Azad University, Marvdasht, Iran,

*2- Professor, Department of Electrical Engineering, Marvdasht Branch, Islamic Azad University, Marvdasht, Iran, taher_nik@yahoo.com

3- Associate Professor, Department of Electrical Engineering, Marvdasht Branch, Islamic Azad University, Marvdasht, Iran

Abstract: Achieving optimal and safe energy management and planning, taking into account the reduction of electricity production, transmission and distribution costs, as well as the reduction of environmental pollutants, has become increasingly important in many power companies in developing countries. With the optimal use of renewable energy sources and the use of a secure platform, including blockchain technology, the aforementioned goals can be achieved. To solve optimization problem, after modeling the hybrid AC-DC microgrid and considering the high complexity of the proposed formulation, the grey wolf optimization algorithm is proposed to solve the problem. In order to check the efficiency of the system under cyber-attacks, the system is subjected to false data injection attacks in different parts of the system, and then the operation is done under normal conditions and cyber-attacks. In this paper, MATLAB software package is used to solve the optimization problem and modeling the cyber-attacks. The operation results have been examined in different scenarios and the negative effects of such attacks are shown by comparing with the normal state. Then, to enhance the security of the system and prevent attacks, blockchain technology is presented to increase the security of the data exchanged in the system.

Key-words: Hybrid microgrids, grey wolf algorithm, false data injection attack, blockchain technology.