تحلیل حمله و دفاع سایبری در سطح پردازش پست‌های دیجیتال با روش تئوری بازی

نورالله فرداد[۱]، دانشجوی دکتری؛ سودابه سلیمانی[۲]، دانشیار؛ فرامرز فقیهی[۳]، استادیار

۱- دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، گروه برق- قدرت، تهران، ایران- n.fardad@srbiau.ac.ir
۲- دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، گروه برق- قدرت، تهران، ایران- s.soleymani@srbiau.ac.ir
۳- دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، گروه برق- قدرت، تهران، ایران- faramarz.faghihi@srbiau.ac.ir

چکیده: استفاده از پست‌های هوشمند مبتنی بر فناوری دیجیتال در شبکه قدرت در حال افزایش است. در این پست‌ها انتقال اطلاعات از تجهیزات هوشمند سطح پردازش با سطوح مختلف، آن‌ها را مستعد حملات سایبری نموده است. در این مقاله حملات سایبری به حسگرهای سطح پردازش پست‌های دیجیتال در سه تجهیز سخت‌افزاری سوئیچ، واحد جمع کننده و واحد کنترل هوشمند بررسی می شود. تجزیه و تحلیل میزان حملات مهاجمین و دفاع صورت گرفته توسط مدافعین با روش نظریه بازی‌ها انجام می شود. بر اساس تعیین نقطه تعادل نش در درخت بازی معرفی شده، استراتژی بهینه حمله و دفاع تعیین می شود. روش پیشنهادی، میزان خسارت به حسگرهای سطح پردازش پست دیجیتال را مشخص می‌کند. با ارزیابی استراتژی دفاع سایبری، بودجه دفاعی بهینه جهت تأمین امنیت سایبری برآورد می‌شود.

واژه‌های کلیدی: شبکه هوشمند، حملات سایبری، نظریه بازی، پست دیجیتال، سطح پردازش، حسگر.

Analysis of Cyber Attack and Defense in Process Bus of Digital Substation by Game Theory

N. Fardad[1], PhD Student; S. Soleymani[2], Associate Professor; F. Faghihi[3], Assistant Professor

1- Department of Electrical Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran.
Email: n.fardad@srbiau.ac.ir
2- Department of Electrical Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran.
Email: s.soleymani@srbiau.ac.ir
3- Department of Electrical Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran.
Email: faramarz.faghihi@srbiau.ac.ir

Abstract: The use of smart substations based on digital technology is increasing in the power system. In these substations, according to the data transmission from different levels to intelligent devices of process bus, makes them susceptible to the cyber-attacks. In this paper, cyber attacks are made to the sensors of process bus in three hardware equipment including switches, merging units and intelligent control units. Analysis of the attacks by attackers and created defense through defenders has been assessed with game theory. Regarding to the Nash Equilibrium point for the suggested game, the best attack and defense strategy is determined. According to the proposed method, the damage to the process bus sensors of digital substation can be specified. Optimal defense budget is estimated for cyber security through assessment of cyber defense strategy.

Keywords: Smart Grid, Cyber Attack, Game Theory, Digital Substation, Process Bus, Sensor.

تاریخ ارسال مقاله: ۱۳۹۵/۱۲/۰۸
تاریخ اصلاح مقاله: ۱۳۹۶/۰۶/۰۵ و ۱۳۹۶/۰۷/۱۵
تاریخ پذیرش مقاله: ۱۳۹۶/۰۹/۱۲
نام نویسنده مسئول: سودابه سلیمانی
نشانی نویسنده مسئول: ایران - تهران - دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران- دانشکده مهندسی برق و کامپیوتر -گروه برق- قدرت

۱- مقدمه

حملات سایبری به شبکه هوشمند برق و اتوماسیون پست‌های فشارقوی با به‌کارگیری گسترده کامپیوتر و فن‌آوری‌های ارتباطی رو به افزایش است. سیستم اسکادا (SCADA[۱]) به مفهوم جمع‌آوری داده‌ها، نظارت و کنترل همه‌جانبه در این زمینه مورد استفاده قرار گرفته شده است. این سیستم، کنترل متمرکز را بر روی یک تجهیز خاص برای تأیید عملکرد آن در جهت صحیح و برنامه‌ریزی از پیش تدارک دیده شده تعریف می‌کند و عموماً در مورد سیستم‌هایی به کار می‌رود که عمل "کنترل از راه دور" بر آن‌ها اعمال می‌شود. طبیعی است که کنترل یک تجهیز یا سیستم بدون داشتن اطلاعات دقیق از وضعیت آن ناممکن است، بنابراین کنترل متمرکز همیشه با یک سیستم جمع‌آوری اطلاعات توأم است. در اصطلاح هر جا یک مرکز از تعدادی پایانه راه دور یا RTU[۲] اطلاعات را دریافت و به آن‌ها فرمان‌هایی ارسال کند، یک سیستم اسکادا وجود خواهد داشت. هر پست مجهز به یک پایانه راه دور جهت جمع‌آوری و ارسال داده‌ها به مرکز است. وضعیت و فرامین کلیه کلیدها، مقادیر اندازه‌گیری ولتاژ و جریان خطوط و ترانس‌ها، آلارم‌ها و حوادث باید در محل پست پیاده‌سازی شده، در پایانه راه دور مجتمع و آماده شوند. اطلاعات پست‌ها از طریق تجهیزات مخابراتی عموماً روی بستر فیبر نوری به مرکز اسکادا انتقال می‌یابد. در این رابطه، پست های مبتنی بر پروتکل IEC61850 و دستگاه های الکترونیکی هوشمند (IED) و اترنت به‌طور گسترده‌تر به کار گرفته شده است. همه این تغییرات منجر به آسیب‌پذیری‌های سایبری مانند دسترسی‌های غیرمجاز از راه دور به IED ها و پروتکل‌های استاندارد ناامن می‌شود. مهاجمین سایبری ممکن است از طریق نفوذ اینترنتی یا سایبری به سیستم‌های مانیتورینگ یا تجهیزات حفاظت و کنترل و یا سیستم اسکادا دسترسی پیدا کنند[۱]. سپس آن‌ها ممکن است فرامین بهره‌برداری ساختگی را مستقیماً به دستگاه‌های الکتریکی ارسال کنند یا اندازه‌گیری‌های ساختگی را برای گمراه ساختن بهره‌بردار سیستم ارسال نمایند. این فعالیت‌ها می‌تواند نهایتاً بر بهره‌برداری و امنیت سیستم قدرت تأثیر بگذارد[۲].

علاوه بر روش های امنیتی کلاسیک، روش های دیگر مبتنی بر نظریه بازی برای مطالعه و تجزیه و تحلیل مسائل امنیتی شبکه هوشمند بکار می‌روند[۴، ۳]. نظریه بازی ابزاری است که اجازه می‌دهد تا تجزیه و تحلیل فعل‌وانفعالات پیچیده بین بازیکن های مختلف با منافع یکسان یا متضاد انجام شود. مفهوم تعادل نش(NE)[۳] در نظریه بازی‌ها اجازه می‌دهد تا استراتژی‌های بهینه بازیکنان-که در آن هیچ یک از آن‌ها انگیزه‌ای برای انحراف یک‌جانبه ندارد- تعریف شود. نظریه بازی با توجه به موضوع مورد کاربرد، در مدل‌های مختلفی ارائه می‌شود که از آن جمله می‌توان به بازی غیر ائتلافی در مدیریت بهینه انرژی ریز شبکه‌ها و به‌منظور حداکثر نمودن سود بازیگران اشاره کرد[۵]. مطالعات بسیاری برای درک امنیت سیستم با توجه به بازی-که در آن هر فرد می‌تواند خطر خود را توسط سرمایه‌گذاری امنیتی کاهش دهد- مورد استفاده قرار می‌گیرد. با کمک نظریه بازی‌ها می‌توان اقدامات امنیتی-که بهترین رابطه بین هزینه‌های متحمل شده و سطح امنیت است- را به دست آورد[۶]. مسئله امنیت سایبری می‌تواند توسط نظریه بازی و به‌صورت یک بازی بین مهاجم و مدافع سایبری تعریف شود.

در شبکه قدرت، هدف مهاجم نفوذ به سیستم برای دریافت اطلاعات به‌منظور ضربه‌زدن به شبکه است. درحالی‌که هدف مدافع محافظت از اطلاعات شبکه به‌منظور حداقل نمودن خساراتی است که احتمال وقوع آن‌ها وجود دارد. همچنین ارتباط بین مهاجم و مدافع می تواند با استفاده از نظریه بازی غیر مشارکتی، مدل سازی شود. نهایتاً حداقل منابع موردنیاز برای دفاع و استراتژی بهینه مدافع به‌منظور حداقل سازی ریسک سیستم قدرت، استخراج می‌شود[۱۰-۷].

مشکل عمده در پست‌ها و سیستم‌های کنترل معمولی، هزینه کابل‌کشی تجهیزات به شبکه ارتباطی است. استفاده از حسگر باسیم یا بی‌سیم به‌طور قابل‌توجهی توانایی بهبود سیستم‌های موجود را دارد. انگیزه‌های تشویقی سبب شده که شرکت‌ها سیستم‌های مبتنی بر حسگر را در شبکه‌های ارتباطی صنعتی بکار گیرند. امنیت این شبکه‌های ارتباطی به دلیل به‌کارگیری حسگرها و احتمال نفوذ توسط مهاجمین از اهمیت بیشتری برخوردار می‌باشد[۱۱]. یکی از اهدافی که ممکن است توسط مدافعین شبکه هوشمند برق یا در ریز شبکه‌های هوشمند کاملاً شناسایی نشود، سیستم اتوماسیون پست‌ها است که بر مدیریت انرژی شبکه هوشمند تأثیر خواهد داشت[۱۴-۱۲]. مهاجمین با یادگیری مداوم نقاط ضعف شبکه و متغیرهای کنترلی آن‌ها اقدامات مخرب خود را برای نفوذ به سیستم اتوماسیون پست‌ها و تجهیزات هوشمند آن ازجمله واحدهای اندازه‌گیری فازوری (PMU)[۴] به‌منظور قطعی گسترده شبکه برق انجام می‌دهند[۱۵].

استاندارد IEC61850 به‌عنوان یک استاندارد مبتنی بر اترنت در سیستم‌های اتوماسیون پست‌ها استفاده می‌شود. ازجمله پروتکل‌هایی که بر اساس این استاندارد تعریف می‌شود می‌توان به MMS[۵]، GOOSE[۶] و SMV[۷] اشاره نمود. آسیب‌پذیری‌های متعددی مربوط به این پروتکل‌ها شناسایی شده که منجر به حملات سایبری به شبکه‌های اتوماسیون دارای استاندارد IEC61850 شده است[۱۷، ۱۶]. به‌منظور شناسایی و کاهش تأثیر حملات ازجمله حملات سایبری تزریق اطلاعات غلط به سیستم حفاظتی پست‌ها، بایستی نیازمندی‌های امنیت سایبری و اقدامات پیشگیرانه مشخص شود[۱۸]. جهت تعیین آسیب‌پذیری، امنیت شبکه و تأثیر معیارهای کمی و کیفی متعدد، روش سلسله‌مراتبی می‌تواند مورد استفاده قرار گیرد[۱۹].

علیرغم مطالعات متعدد انجام شده در حوزه امنیت سایبری در شبکه قدرت و سیستم اتوماسیون پست‌های فشارقوی هوشمند[۲۳-۲۰]، تحقیقات اندکی در رابطه با تصمیم‌گیری با روش‌های جدید ازجمله تئوری بازی بین مهاجم و مدافع سایبری در پست‌های هوشمند دیجیتال انجام شده است. ضمناً مطالعات کاربردی در سطح پردازش این پست‌ها با سه تجهیز هوشمند یعنی سوئیچ، واحد ادغام و واحد

کنترل هوشمند- به‌عنوان بخشی که اطلاعات ولتاژ و جریان و وضعیت بریکر و سکسیونر را به تجهیزات کنترلی و حفاظتی منتقل می‌کند- صورت نگرفته است. همچنین برای ارزیابی کلی امنیت سیستم در مرجع[۲۴] از روش درخت حمله استفاده شده که استراتژی‌های دفاعی نیز می‌توانند به درخت حمله اضافه شود. در این روش تعیین آسیب‌پذیری مستلزم تحلیل مشخصات امنیتی و احتمال خطای اجزای تشکیل‌دهنده سیستم است که فاقد تصمیم‌گیری هم‌زمان بین مهاجم و مدافع می‌باشد. اما در تحلیل حاضر، با شناسایی مهم‌ترین حملات در سطح پردازش پست‌های هوشمند دیجیتال و استفاده از تکنیک‌های تئوری بازی، مدل‌سازی بر اساس تأثیر رفتار مهاجم و مدافع و هزینه‌های مربوطه انجام شده است. هدف اصلی این مقاله تجزیه و تحلیل میزان هزینه انجام شده توسط مهاجم در حمله به لایه حسگر پست‌های دیجیتال است که در این راستا بودجه‌ای که مدافع متحمل می‌شود محاسبه می‌شود. در ادامه این مقاله در بخش دوم، مبانی نظریه بازی مورد ارزیابی قرار می‌گیرد. بخش سوم مشخصات پست‌های هوشمند یا دیجیتال و تجهیزات مورداستفاده در آن‌ها را معرفی می نماید. بخش چهارم به بیان مدل بازی و تحلیل عملکرد مدافع و مهاجم می‌پردازد. نتیجه‌گیری مقاله در بخش پنجم ارائه می‌شود.

۲- مبانی نظریه بازی

با گذشت بیش از نیم‌قرن از معرفی مفاهیم پایه نظریه بازی یا تئوری بازی، هم‌اکنون نیز تحقیقات در زمینه کاربرد های این نظریه در حوزه‌های مختلف ازجمله پدافند غیرعامل، مسائل امنیتی و جلوگیری از حملات سایبری، شبکه‌های مخابراتی، تجارت، سیستم‌های قدرت شاهد رشد قابل‌توجه است. با توجه به پیچیدگی رفتارهای حمله مهاجم سایبری، نیاز به یک رویکرد سیستماتیک است که بتواند رفتارهای مهاجمین را برای تصمیم‌گیری در مدیریت امنیت، تجزیه و تحلیل نماید. به‌منظور بهینه‌سازی هزینه تشخیص، کاهش حادثه و بهبود، نیاز به دانستن و پیش‌بینی حرکت دشمن سایبری است. این وضعیت را می‌توان توسط بازی استراتژیک شبیه‌سازی نمود که در آن دو بازیکن A و B، با استراتژی‌های خود به ترتیب a و b انتخاب می شوند و دریافتی $L(a,b)$[۸] را به دست خواهند آورد. بازیکن A می‌خواهد حداقل درآمد خود را حداکثر کرده، بازیکن B می‌خواهد حداکثر ضرر خود را به حداقل برساند[۲۵]. در نظریه بازی بر اساس دریافتی هر بازیکن، بازی به دو دسته کلی بازی با دریافتی صفر و بازی با دریافتی غیر صفر تقسیم می شود. در بازی نوع نخست بازیکنان قادر به افزایش یا کاهش منابع موجود نیستند و سود کل برای همه بازیکنان برای هر ترکیب از استراتژی‌ها همیشه صفر است. لذا یک بازیکن دارای سود بوده؛ درحالی‌که به دیگری ضرر وارد می‌شود. اما در بازی با دریافتی غیر صفر نتیجه خالص بازی ممکن است بیشتر یا کمتر از صفر باشد. در این نوع بازی سود یک بازیکن ضرورتاً به معنی ضرر دیگری نیست. در این مقاله برای تحلیل امنیت سایبری از بازی با دریافتی غیر صفر با استراتژی مرکب استفاده می شود. در استراتژی مرکب به هر استراتژی خالص بازی یک احتمال تخصیص داده می‌شود که مجموعه همه احتمالات برابر یک است[۲۶].

درصورتی‌که استراتژی خالص به‌صورت $a \in A_1 \times A_2 \times ... \times A_n$ باشد، دریافتی بازیکنان تحت این استراتژی‌ها تعریف می‌شود. دریافتی یک بازیکن با استراتژی مرکب σ به‌صورت رابطه (۱) خواهد بود:

$$u_i(\sigma) = \sum_{\sigma \in A_1 \times ... \times A_n} p(a)u(a) = \sum_{\sigma \in A_1 \times ... \times A_n} \prod_{i \in N} \sigma_i(a_i)u(a) \qquad (۱)$$

که $p(a) = \prod_{i \in N} \sigma_i(a_i)$ برابر احتمال a در استراتژی مرکب بازیکنان می‌باشد.

برای تعیین دریافتی بازیکنان بایستی نقطه تعادل بازی را مشخص نمود. در نظریه بازی‌ها مفهوم " تسلط و تعادل " نقش محوری ایفا می کند. در استراتژی مرکب از تئوری نقطه تعادل نش (NE)، نقطه تعادل بازی به دست می‌آید. نقطه تعادل نش حالتی است که هیچ‌کدام از بازیکنان نمی‌توانند سود خود را به صورت یک‌جانبه از این نقطه تعادل منحرف نمایند[۲۹-۲۷]. نقطه تعادل نش در بازی غیر مشارکتی می تواند بر اساس محدودیت‌های محلی و کلی به دست آید[۳۰].

استراتژی مرکب σ^* یک نقطه تعادل نش می‌باشد اگر برای هر $i \in N$

$$\sigma_i^* \in \arg\max_{\sigma_i \in \Delta(A_i)} (u_i(\sigma_i, \sigma_{-i}^*))$$

در بازی امنیتی تئوری NE برای بررسی رفتار مهاجم نسبت به استراتژی حمله تحت مجموعه‌ای از شرایط ارزیابی می شود. به همین ترتیب استراتژی NE مدافع چگونگی تخصیص منابع محدود دفاعی در مواجهه با یک مهاجم را مشخص می‌نماید. در بازی امنیتی، بازیکن A یا p^A برای مهاجمین و بازیکن D یا P^D برای مدافعین تعریف می‌شود. فضای عملکرد مجموعه‌ای از حملات $A^A := (a_1,...,a_{NA})$ و اقدامات دفاعی $A^D := (d_1,...,d_{ND})$ هست. در این بازی $P^A := (p_1,...,p_{NA})$ به‌عنوان توزیع احتمال حمله در مجموعه A^A و $q^D := (q_1,...,q_{ND})$ توزیع احتمال دفاعی در مجموعه A^D تعریف می‌شود به‌نحوی که $0 \le p_i, q_i \le 1$ و $\forall i$ و $\sum_i p_i = \sum_i q_i = 1$ آنگاه نقطه تعادل نش در استراتژی مرکب با زوج احتمال (p^*,q^*) تعریف می‌شود[۳۱].

۳- پست‌های هوشمند یا دیجیتال

پست‌های دیجیتال از تجهیزات هوشمند برای اشتراک‌گذاری اطلاعات و عملکرد مبتنی بر پروتکل IEC61850 تشکیل شده‌اند. تجهیزات سیستم اتوماسیون پست را می‌توان در سه سطح دسته‌بندی نمود که عبارت از سطح ایستگاه، سطح بی(Bay) و سطح پردازش یا پروسس هستند. در سطح ایستگاه، یک سیستم تعاملی با کاربر با پایگاه داده، سرور، ایستگاه کاری(Workstation) و تجهیزات مهندسی نصب می شود. IED های حفاظتی و کنترلی و واحدهای اندازه‌گیری فازوری (PMU) در سطح بی نصب می شوند. تجهیزات سطح پردازش شامل سنسورها، دستگاه‌های اندازه‌گیری جریان (CT) و ولتاژ (VT) ، کلید

(CB)، سکسیونر (DS) ، واحدهای ادغام (MU)[۹] و واحدهای کنترل هوشمند (ICU)[۱۰] هستند. پروتکل‌های مبتنی بر IEC61850 نظیر G00SE ، SMV و MMS به‌وسیله تجهیزات اتوماسیون پست مورد استفاده قرار می‌گیرد. در این رابطه یادآوری تعاریف زیر الزامی است:

MMS: پیاده‌سازی تابع اتوماسیون بین IED ها و مرکز کنترل مبتنی بر شبکه،

G00SE: پیاده‌سازی عملکرد فی‌مابین IED ها برای برقراری اینترلاک و ورودی/خروجی مجازی مبتنی بر شبکه LAN و ارسال سیگنال‌های تریپ از IED ها به کلیدهای قدرت

SMV: پیاده سازی انتقال دیجیتال ولتاژ و جریان از تراز سفورماتورهای اندازه‌گیری

SNTP[۱۱]: همگام سازی ساعت مبتنی بر شبکه LAN. جهت هم‌زمانی اطلاعات می‌بایست کلیه تجهیزات از طریق سیگنال ساعت SNTP با GPS در نظر گرفته‌شده سنکرون شوند.

در مقایسه با پست‌های متعارف، اینترفیس‌های ارتباطی و همچنین پروتکل‌های ارتباطی در "سطح بی" و "سطح ایستگاه" متفاوت هستند. بااین‌حال، تفاوت عمده بین این دو در فنّاوری سطح پردازش یا پروسس است. در پست های دیجیتال تجهیزات "پروسس باس" نظیر ترانسفورماتورهای جریان و ولتاژ الکترونیکی، فیبر نوری، واحدهای ادغام، واحد کنترل هوشمند و تابلوهای کنترل محلی استفاده می‌شود. این پست‌ها همچنین شامل تجهیزات حفاظت و کنترل نظیر رله‌های حفاظتی، ثبات حادثه، سیستم‌های اتوماسیون و کنترل راه دور می باشند. واحد ادغام را می‌توان مستقیماً به CT/VT متعارف و CT/VT الکترونیکی و صل کرد. بهره‌برداری از یک پست دیجیتال متکی به یک مسیر ارتباطی مطمئن و معقول است. ارتباطات در داخل و مابین "پروسس باس"،"سطح بی" و "سطح ایستگاه" توسط شبکه اترنت با سرعت بالا انجام می‌شود.

پروتکل‌های ارتباطی در "سطح ایستگاه" و "پروسس باس" شبکه GOOSE و شبکه SMV هستند. شبکه MMS پل ارتباطی بین اسکادا، مراکز دیسپاچینگ و IED های در سطح بی است.

رله‌های کنترل و حفاظت، به‌طور کامل با پروتکل IEC61850 سازگار بوده و می‌توانند مستقیم به اسکادا و درگاه ارتباطی[۱۲] متصل شوند. با استفاده از پروتکل IEC61850 ارتباط بین IED ها از سازندگان مختلف با سرعت بالا فراهم می‌شود. با به‌کارگیری پست دیجیتال شبکه فیبر نوری به‌جای کابل‌کشی استفاده می‌شود که منجر به کاهش حجم کار و گسترش دوره بهره‌برداری پست می‌شود.

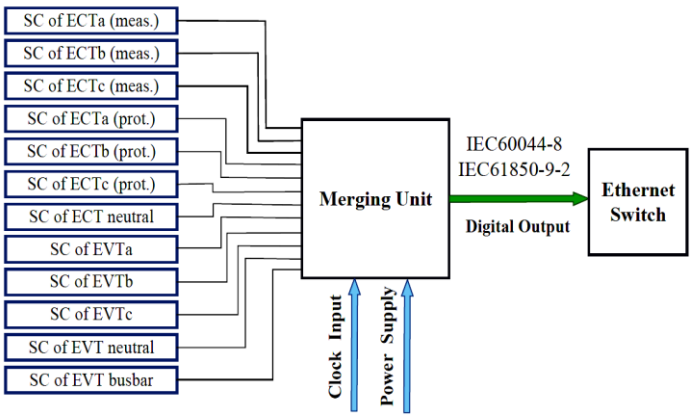
۳-۱- تجهیزات سطح پردازش پست‌های هوشمند

الف) واحد ادغام

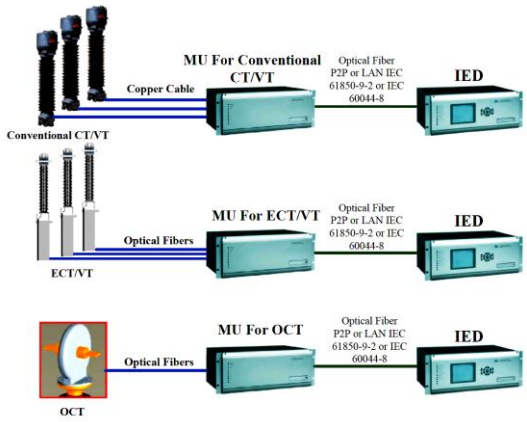
واحدهای ادغام به‌منظور الحاق و همگام‌سازی سیگنال‌های جریان و ولتاژ نمونه‌برداری شده و انتقال این داده‌ها به IED ها مورد استفاده قرار می‌گیرند. این تجهیز می‌تواند به‌عنوان یک مبدل آنالوگ به دیجیتال (A/D) و دیجیتال به آنالوگ (D/A) دریک پست بین CT/VT الکترونیکی و CT/VT متعارف قرار گیرد و سیگنال‌های همگام شده به رله‌های حفاظتی ارسال شود. این تجهیز پروتکل‌های IEC60044-8، IEC61850-9-1 و IEC61850-9-2 را پشتیبانی می‌نماید[۳۲]. ساختار یک واحد ادغام در شکل ۱ نشان داده شده است.

ب) ترانسفورماتورهای اندازه‌گیری جریان و ولتاژ الکترونیکی

ترانسفورماتورهای اندازه‌گیری جریان و ولتاژ الکترونیکی مقادیر ولتاژ و جریان را به‌صورت دیجیتال درآورده و آن‌ها را به IED های مختلف (تجهیزات حفاظت و کنترل، تجهیزات اندازه‌گیری و ثبات خطا) توسط فیبر نوری ارسال می‌نماید. این تجهیزات را می‌توان در پست‌های گازی (GIS)[۱۳] و (AIS)[۱۴] و پست‌های دیجیتال در سطوح مختلف ولتاژ بکار گرفت. توسط مبدل‌ها سیگنال‌های بزرگ جریان و ولتاژ به سیگنال‌های کوچک آنالوگ تبدیل شده و به ماژول‌های راه دور برای تبدیل A/D ارسال می‌شود. شکل ۲ نمایش استفاده از انواع ترانسفورماتورهای اندازه‌گیری را نشان می‌دهد.



شکل ۱: ساختار واحد ادغام (MU)



شکل ۲: ساختار ترانسفورماتورهای اندازه‌گیری و ارتباط با واحدهای ادغام و IED

ج) واحد کنترل هوشمند

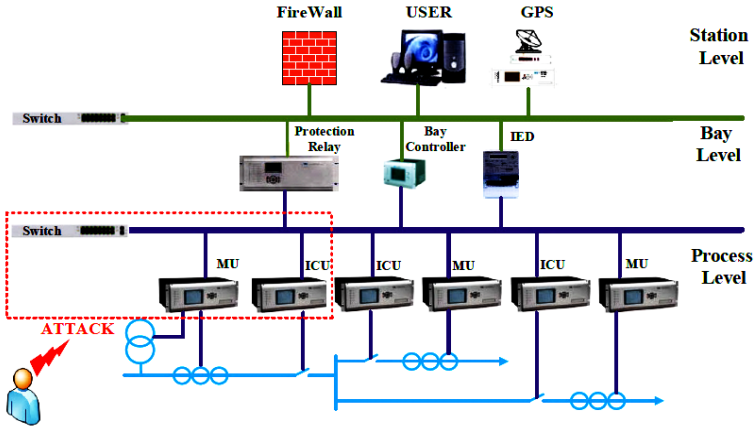
واحد کنترل هو شمند سیگنال‌های آنالوگ مربوط به اطلاعات و ضعیت تجهیزاتی نظیر کلیدها و سکسیونرها را به سیگنال‌های دیجیتال تبدیل و آن ها را به IED های مختلف از طریق "پروسس باس" و شبکه GOOSE منتقل می‌نماید. هم‌زمان فرامین تریپ و بستن را از تجهیزات حفاظتی و کنترلی و از طریق "پروسس باس" دریافت می‌کند. این فرمان‌ها پس از تبدیل به سیگنال‌های آنالوگ به تجهیزات اولیه پ ست ارسال می‌شوند.

۳-۲- *آسیب‌پذیری‌ها* در پست‌های هوشمند

تهدیدات سایبری بالقوه و محل مهاجمین در شبکه اتوما سیون پ ست هوشمند می‌تواند منجر به حملات سایبری از نقاط زیر شود. این تهدیدات به دلایل متعدد نظیر سی ستم کدینگ ضعیف، عدم توجه به مباحث سازگاری الکترومغناطیسی، عدم آگاهی کاربران از امنیت سایبری شبکه و آموزش ناکافی و ... امکان نفوذ را برای دشمن سایبری فراهم می‌سازد.

- به خطر انداختن نقاط دسترسی از راه دور (مثل VPN،dial-up و wireless)
- به خطر انداختن دیواره آتش[۱۵]
- دسترسی به شبکه پست
- وقفه در زمان همگام‌سازی GPS
- دسترسی به تجهیزات سطح بی یا تغییر تنظیمات تجهیزات حفاظتی
- دسترسی به رابط کاربر
- به خطر انداختن تجهیزات سطح پردازش
- تغییر وضعیت کلیدهای پست (مثل close به open یا برعکس)
- دسترسی به شبکه پست مجاور
- دسترسی به شبکه مرکز کنترل
- نفوذ از درون شبکه پست
- نفوذ از خارج شبکه پست از طریق شبکه پست مجاور

نفوذهای ممکن به شبکه ناحیه محلی می‌تواند از بیرون یا داخل شبکه یک پ ست سرچ شمه بگیرد. یکی از موارد فوق جهت نفوذ به پ ست به خطر انداختن سطح پردازش و تجهیزات مرتبط به آن ازجمله تجهیزاتی نظیر سنسورها، واحد کنترل هوشمند، واحد ادغام و سوئیچ‌های مرتبط با آن‌ها مطابق شکل ۳ است.



شکل ۳: تهدیدات سایبری در سطح پردازش پست هوشمند

مهاجم سایبری با استفاده از بسته‌های بدافزاری و نفوذ به سطح پردازش یک پست هوشمند، باعث تغییرات غیرمجاز در پیام‌های ارسالی GOOSE و SMV از تجهیزات سطح پردازش می‌شود. این تغییرات منجر به اختلال در عملکرد سیستم اتوماسیون و درنتیجه تریپ‌های غیرمجاز و بای‌پس نمودن اینترلاک‌های پست می‌شود. همچنین برخی از حملات می‌تواند بر زمان انتقال پیام‌ها تأثیر بگذارد و سبب تأخیر در انتقال سیگنال‌ها شود[۱۶].

۳-۳- انواع حملات به حسگرهای سطح پردازش پست دیجیتال

حملات سایبری مختلفی در سطح پردازش پست‌های دیجیتال می‌تواند صورت گیرد که در این مقاله برخی از آن‌ها که بیشتر علیه شبکه‌های G00SE و SMV به وقوع می‌پیوندد اشاره می‌شود. بخش زیادی از حملات در گزارشات معتبر ارائه‌شده و میزان اهمیت و درصد وقوع آن‌ها مشخص شده است[۳۳]. از مهم‌ترین این حملات، حمله به خطر انداختن حسگرها و شناسایی آن‌ها، حمله تکرار، حمله تزریق اطلاعات غلط، حمله نفوذ مرد میانی و حمله ممانعت از سرویس به‌صورت جدول ۱ می‌باشد[۳۴].

جدول ۱: انواع حملات به سوئیچ، G00SE و SMV سطح پردازش

	Cyber Attack Type	Results
Switch	Reconnaissance attack	Open CB
	Replay attack	Open CB
	Denial of Service attack	Lost availability of IED
	Man-in-the-Middle(MITM) attack	Lead Wrong Operation action
MU	Reconnaissance attack	Open CB
	Generate Fabricated SMV Packets	Open CB
	Denial of Service attack	Lost availability of IED
	False Data Injection	Warning occurred at CB
ICU	Reconnaissance attack	Open CB
	Replay attack	Open CB
	Denial of Service attack	Lost availability of IED
	Man-in-the-Middle(MITM) attack	Lead Wrong Operation action

- **حمله شناسایی (Reconnaissance)**

این حمله به مهاجم اجازه می‌دهد تا اهداف بالقوه را قبل از حمله شناسایی نماید. این حمله می‌تواند توسط مهاجم و به کمک یک لپ‌تاپ و تعیین IP تجهیزات صورت گیرد. مهاجم می‌تواند این اطلاعات را برای راه‌اندازی حملات مؤثرتر استفاده نماید.

- **حمله ممانعت از سرویس (Denial of Service(DoS))**

این نوع حملات با هدف خارج کردن منبع اطلاعاتی از سرویس به‌گونه‌ای که دیگر آن منبع قادر به ارائه سرویس به دیگران نبوده و نتواند تبادل اطلاعات درستی با کاربرانش داشته باشد، انجام می شود. وقتی نرم‌افزارهای سیستم اتوماسیون در معرض حملات DoS قرار گیرد، سبب جلوگیری از دسترسی مجاز به منابع سیستم یا به تعویق انداختن بهره‌برداری و توابع سیستم می شود. در این صورت مهاجمین می‌توانند فعالانه از اشکالات نرم‌افزار و سایر آسیب‌پذیری‌های موجود بهره‌برداری نمایند. درنتیجه به مکان‌هایی نظیر شبکه‌های مرکز کنترل، سیستم‌های اسکادا، ارتباطات و لینک‌های غیرمجاز دسترسی پیدا می کنند. حملات سایبری که مبتنی بر مکانیزم DoS هستند و آن‌هایی که به دلیل ویروس و کرم ها با ایجاد ترافیک در مدت زمان های کوتاه گسترش می‌یابند، می‌توانند بالقوه باعث به خطر انداختن سیستم و اختلال در خدمات شوند.

- **حمله نفوذ مرد میانی ((Man-in-the-Middle(MITM)**

این حمله به مهاجم اجازه می‌دهد تا ارتباط ترافیکی بین سیستم مانیتورینگ و IED ها تغییر کرده و ارتباط غیرمجاز و مخرب در شبکه سطح ایستگاه برقرار باشد. به‌عبارت‌دیگر مهاجم فرامین کنترلی مخرب و مقادیر تنظیم رله‌های حفاظتی دستکاری‌شده را ارسال می‌نماید[۳۵].

- **حمله تکرار (Replay)**

شکلی از حمله به شبکه است که در آن انتقال داده‌های معتبر به‌صورت مغرضانه یا متقلبانه تکرار شده یا با تأخیر صورت می‌گیرد. این نوع حمله زمانی رخ می‌دهد که مهاجم اطلاعاتی از قبیل نام کاربری و رمز عبور را یافته و همچنین پیام‌های قبلی سیستم را در خود ذخیره می کند. در هنگام قطع شدن اتصال مربوطه مجدداً اقدام به استفاده از این اطلاعات که قبلاً کپی آن توسط مهاجم انجام شده می‌کند و خود را به‌عنوان یکی از طرف‌های مورد اعتماد در ارتباط معرفی می‌کند. درواقع این کپی‌ها در اختیار مهاجم بوده و با سایر گره‌های شبکه تبادل اطلاعات می‌کند[۳۶].

- **تزریق اطلاعات غلط (False Data Injection)**

گره‌های حسگر به‌صورت ذاتی در برابر مداخلات مقاوم نبوده و به‌آسانی می‌توانند توسط دشمن به خطر بیفتند. در این نوع حمله، دشمن اطلاعات غلط را به گره‌های حسگر تزریق کرده و در مسیر اطلاعات قابل‌اعتماد خلل ایجاد می‌کند. این حمله زمانی صورت می‌گیرد که یک مهاجم از یک گره در معرض خطر با تزریق داده های کاذب به جای داده‌های ذخیره شده معتبر، یا کانال‌های ارتباطی استفاده می‌نماید. در صورت عدم تشخیص، داده معیوب می‌تواند منجر به اطلاعات نظارتی اشتباه در اسکادا شود، همچنین سبب اقدامات کنترلی شده که می تواند عملکرد شبکه‌های حسگر را مختل کرده و باعث گسترش خسارت به سطوح بالاتر کل سیستم شود[۳۷].

- **تولید بسته‌های ساختگی SMV (Generate Fabricated Packets Values)**

این حمله اقدام به در اختیار گرفتن، ویرایش و انتقال بسته های ساختگی به شبکه ICT پست هوشمند می‌نماید. این حمله بر اجرای توابع حفاظتی در رله‌ها و بازنمودن بریکرها اثر می‌گذارد[۳۸].

۴- ایجاد مدل بازی و تحلیل عملکرد مدافع و مهاجم

۴-۱- رابطه دریافتی در بازی مدافع و مهاجم

مهاجم دارای امکانات لازم جهت ضربه زدن به تجهیزات سطح پردازش پست‌های هوشمند بوده و مدافع نیز بودجه کافی برای دفاع در برابر حملات مهاجم را پیش‌بینی می‌نماید. لذا مثل دو بازیگر بوده که می توانند باهم رقابت کنند که یکی به دنبال ضرر رساندن به بازیگر دیگر و بازیگر بعدی به دنبال سود بیشتر می‌باشد. درنتیجه مهاجم و مدافع می توانند به‌صورت یک بازی با دو بازیگر عملکرد داشته باشند و بر اساس تئوری بازی سودمندی هرکدام برآورد می‌شود. برای تحلیل امنیت سایبری حسگرهای سطح پردازش شامل سوئیچ‌ها، ICU و MU، از تئوری بازی استفاده می‌شود.

در این بازی هر بازیگر تصمیم‌گیری یا استراتژی خود را به صورت هم‌زمان و بدون اطلاع از استراتژی اتخاذ شده توسط بازیگر دیگر انتخاب می‌کند و رفت و برگشت بین عملکرد بازیگران وجود ندارد، لذا این بازی از نوع استاتیک می‌باشد.

در این بازی هیچ‌گونه همکاری بین چند مهاجم و یا چند مدافع برقرار نبوده لذا بازی از نوع غیر اشتراکی می‌باشد. همچنین بازی بین مدافع و مهاجم از نوع بازی ترتیبی یا پی‌درپی و با مجموع دریافتی غیر صفر هست. لذا رفتار مهاجم و مدافع لایه حسگر سطح پردازش پست دیجیتال با دو بازیکن با مجموع دریافتی غیر صفر مدل سازی می شود. همچنین بازی نوع غیر مشارکتی، از نوع ترتیبی و با اطلاعات کامل است. حملات مهم که مهاجم می‌تواند به سه تجهیز بکار ببرد مشخص شده و مبتنی بر آن‌ها، دریافتی مهاجم تعیین می‌شود. همچنین دریافتی مدافع ناشی از دفاع سایبری محاسبه می‌شود.

دریافتی هر بازیکن در هر مرحله از بازی به شرح رابطه (۲) محاسبه می‌شود:

$$Payoff_s(p,a) = Payoff_{s-1}(p,a) + Interaction\ Function(p, Impact(a), s) \quad (۲)$$

در رابطه (۲) مقدار دریافتی جدید به دریافتی مرحله قبل، تابع عملکرد متقابل مدافع و مهاجم که متأثر از رفتار آن‌ها و میزان دریافتی آن‌ها که ناشی از پارامترهای امنیتی است، بستگی دارد.

۴-۲- تعیین عملکرد متقابل بین مدافع و مهاجم

به‌طورکلی، در بازی سطح پردازش پست دیجیتال، با اقدام صورت گرفته توسط مهاجم، مهاجم دارای مزایای بیشتری نسبت به مدافع در عملکرد حمله خود است. این کار باعث از دست دادن دریافتی بزرگ برای مدافع یا ضرر بیشتر برای او می‌شود که از طرف دیگر دربرگیرنده بهره بزرگ برای مهاجم خواهد بود[۲۳]. تابع عملکرد متقابل مهاجم و مدافع و درنتیجه دریافتی آن‌ها در صورت عملکرد مهاجم به‌صورت روابط(۳) و(۴) خواهد بود[۸].

$$Attacker's\ Payoff = s.Impact(a) \quad (۳)$$

$$Defender's\ Payoff = -s.e^{Impact(a)} \quad (۴)$$

با توجه به تعداد مراحل بازی در درخت بازی (s)، دریافتی عملکرد مهاجم به‌صورت خطی مثبت است، اما برای مدافع به‌صورت منفی نمایی است.

از سوی دیگر، با عملکرد مدافع پس از حمله، تنها مدافع دارای دریافتی با بهره کوچک مطابق رابطه (۵) است ولی تأثیری بر دریافتی حاصل از مهاجم ندارد.

$$Defender's\ Payoff = Impact(a) \quad (۵)$$

در روابط (۳) تا (۵) مهم‌ترین بخش تعیین میزان تأثیر (Impact) است که نشان‌دهنده جنبه‌های امنیتی است.

دسته‌بندی‌های امنیتی بر اساس تأثیر بالقوه حوادث در یک سیستم تعیین می‌شود. این حوادث، اطلاعات و سیستم‌های اطلاعاتی آن را که در جهت انجام وظایف تعریف‌شده، حفاظت از دستگاه‌ها، انجام مسئولیت‌های قانونی، حفظ کارکرد روزانه و حفاظت از اشخاص نیاز است به خطر می‌اندازد. برای شبکه‌های حسگر سطح پردازش پست‌های هوشمند، C(a)، I(a) و A(a) به ترتیب نشان‌دهنده مقادیر کیفی محرمانه بودن، صحت و در دسترس بودن اطلاعات برای هر نوع عملکرد، با وزن متناظر α_C، α_I و α_A است. در این رابطه فقدان محرمانگی به معنای افشای غیرقانونی اطلاعات، فقدان صحت به معنای تخریب یا ویرایش غیرقانونی اطلاعات و فقدان در دسترس بودن به معنای تخریب فرآیند دست‌یابی به اطلاعات است. این مقادیر را می‌توان بر اساس روش سلسله مراتبی مبتنی بر روش‌های تجربی و بر اساس نظرات کارشناسان و داده‌های تاریخی پیدا کرد[۳۹]. برای سیستم‌های امنیت اطلاعات معمولیIT پس از دسترس بودن اطلاعات، محرمانه بودن اطلاعات اهمیت دارد و صحت اطلاعات اولویت آخر خواهد بود درحالی که در شبکه‌های صنعتی و خصوصاً شبکه‌های حسگر که اطلاعات دقیق از حسگر به سیستم‌های ارتباطی و یا بالعکس ارسال می شود، بالاترین وزن را می‌توان برای صحت اطلاعات ارسالی و سپس در دسترس بودن آن‌ها و پس‌ازآن محرمانه بودن داده‌ها نسبت داد[۴۱، ۴۰]. میزان تأثیر به‌صورت رابطه(۶) تعریف می‌شود:

$$Impact(a) = a_C.C(a) + a_I.I(a) + a_A.A(a) \quad (۶)$$

که در آن مجموع وزن‌ها برابر یک است و محدوده مقدار هر یک از جنبه‌های امنیتی از صفر تا ۱۰ است. در این مقاله برای شبکه حسگر سطح پردازش پست‌های هوشمند مقادیر وزن‌ها به‌طور نمونه برای محرمانه بودن، صحت و در دسترس بودن اطلاعات به ترتیب برابر ۰/۱، ۰/۵ و ۰/۴ در نظر گرفته می‌شوند.

می‌توان ملاحظه کرد که با توجه به حملاتی که به GOOSE صورت می‌گیرد دو حسگر سوئیچ و واحد کنترل هوشمند را شامل می‌شود. دو حمله (حمله تکرار و حمله شناسایی) اقدام به قطع ارتباط ورودی به لایه حسگر نموده درحالی‌که دو حمله بعدی (یعنی حمله ممانعت از سرویس

و حمله نفوذ مردی در میان) می‌تواند به‌عنوان اقدامات نهایی مهاجم درنظرگرفته شود.

حملاتی که به SMV صورت می‌گیرد حسگر واحد ادغام را شامل می‌شود که دو حمله (حمله تولید بسته ساختگی و حمله شناسایی) اقدام به قطع ارتباط ورودی به لایه حسگر نموده درحالی‌که دو حمله بعدی (یعنی حمله ممانعت از سرویس و حمله تزریق اطلاعات غلط) می تواند به‌عنوان اقدامات نهایی مهاجم درنظرگرفته شود.

عملکرد مدافع لایه حسگر سطح پردازش و در پاسخ به حملات، با روش‌هایی نظیر تجهیزات سخت‌افزاری و نرم‌افزاری صورت می‌گیرد. روش‌های نرم‌افزاری شامل سیستم‌های تشخیص و ممانعت از نفوذ، تشخیص هویت در سطح تجهیزات مخابراتی و نرم‌افزارهایی از قبیل کدینگ و رمزنگاری است. انتخاب مسیر بهینه کابل‌های ارتباطی و شیلدینگ آن‌ها جهت ممانعت از تأثیر حملات از نوع میدانی مربوط به روش‌های سخت‌افزاری می‌شود.

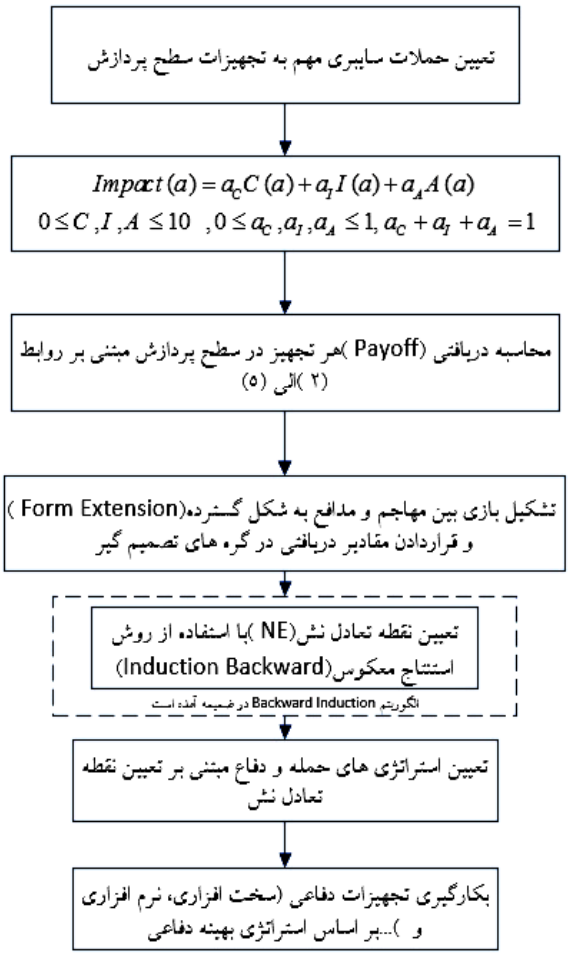
اقدامات مهاجم شامل چهار نوع حمله فوق بوده و در صورت عدم عملکرد مهاجم، وقتی‌که هیچ حمله‌ای صورت نگرفته است مقدار No attack لحاظ می‌شود. اقدامات دفاعی کلی با Defense و در صورت عدم عملکرد مدافع با No Defense در درخت بازی نشان داده می‌شود. با استفاده از وزن‌های فرض شده، اثرات هر عملکرد در جدول ۲ تعیین شده است. عملکرد No attack و No Defense هیچ تأثیری در جدول ندارد. اثرات سه مقدار نسبی ۱و ۵ و ۹ به ترتیب برای مقادیر کیفی کم، متوسط و بالا در نظر گرفته می‌شود.

همان‌طور که در جدول ۲ نشان داده شده است، مقدار نسبی بالا برای تأثیر بالقوه ناشی از فقدان محرمانه بودن در سوئیچ لحاظ می‌شود. همچنین در سوئیچ مقدار نسبی متوسط برای صحت و مقدار نسبی کم برای دردسترس‌بودن در نظر گرفته می‌شود. ولی برای واحد کنترل هوشمند و واحد ادغام که اطلاعات را منتقل می‌کنند علاوه بر محرمانه بودن، صحت اطلاعات دارای مقدار نسبی بالا و دردسترس‌بودن مقدار کم را دارا است. برای مهاجم، حمله تزریق داده‌های غلط برای سوئیچ و واحد کنترل هوشمند و همچنین حمله مردی در میان در واحد ادغام دارای بالاترین تأثیر ۶/۶ است که با صحت و در دسترس‌بودن امنیت اطلاعات به دست می‌آید.

مدل‌سازی مبتنی بر تئوری بازی مطابق شکل ۴ و با توضیحات به شرح زیر پیاده‌سازی می‌شود.

الف) حملات مهم سایبری که می‌تواند تجهیزات ا صلی سطح پردازش پست‌های هوشمند را مورد حمله قرار دهد تعیین می‌شود.

ب) بر اساس روابط (۲) الی(۵) مقاله و توجه به مقادیر محاسبه شده جدول۲، میزان دریافتی مدافع و مهاجم در سطح پردازش محاسبه می شود. این مقادیر در شکل ۴ و در نقاط تصمیم‌گیر نشان داده شده است. این مقادیر مبتنی بر مراحل بازی بین دو بازیگر می‌باشد.



شکل ۴: تشکیل مدل بازی در سطح پردازش پست هوشمند

جدول ۲: تعیین مقادیر دریافتی بر اساس عملکرد مهاجم و مدافع در حسگرهای موردمطالعه

	Defense/Attack	C(a)	I(a)	A(a)	Impact(a)
Switch	Defense	۹	۵	۱	۳/۸
	Replay attack	۵	۱	۱	۱/۴
	Reconnaissance attack	۵	۱	۱	۱/۴
	DOS attack	۹	۱	۱	۱/۸
	MITM attack	۱	۹	۵	۶/۶
MU	Defense	۹	۹	۱	۵/۸
	Generate Fabricated SMV Packets	۱	۵	۵	۴/۶
	Reconnaissance attack	۵	۵	۱	۳/۴
	DOS attack	۹	۱	۱	۱/۸
	False Data Injection attack	۱	۹	۵	۶/۶
ICU	Defense	۹	۹	۱	۵/۸
	Replay attack	۵	۱	۱	۱/۴
	Reconnaissance attack	۵	۵	۱	۳/۴
	DOS attack	۹	۱	۱	۱/۸
	MITM attack	۱	۹	۵	۶/۶

ج) پس از تعیین میزان دریافتی در هر مرحله از بازی مطابق بند(ج) با استفاده از روش استنتاج از عقب[۱۶]، نقطه تعادل نش بازی مشخص می شود که شرح دقیق با جزئیات مربوطه در بند(۴-۴) ارائه شده است.

د) پس از تعیین نقطه تعادل نش بازی، بهترین استراتژی حمله و دفاع مشخص شده و بر اساس آن اقدامات دفاعی مناسب برای دفاع مداوم در برابر حملات سایبری به سطح پردازش پست‌های هوشمند تعبیه می‌شود.

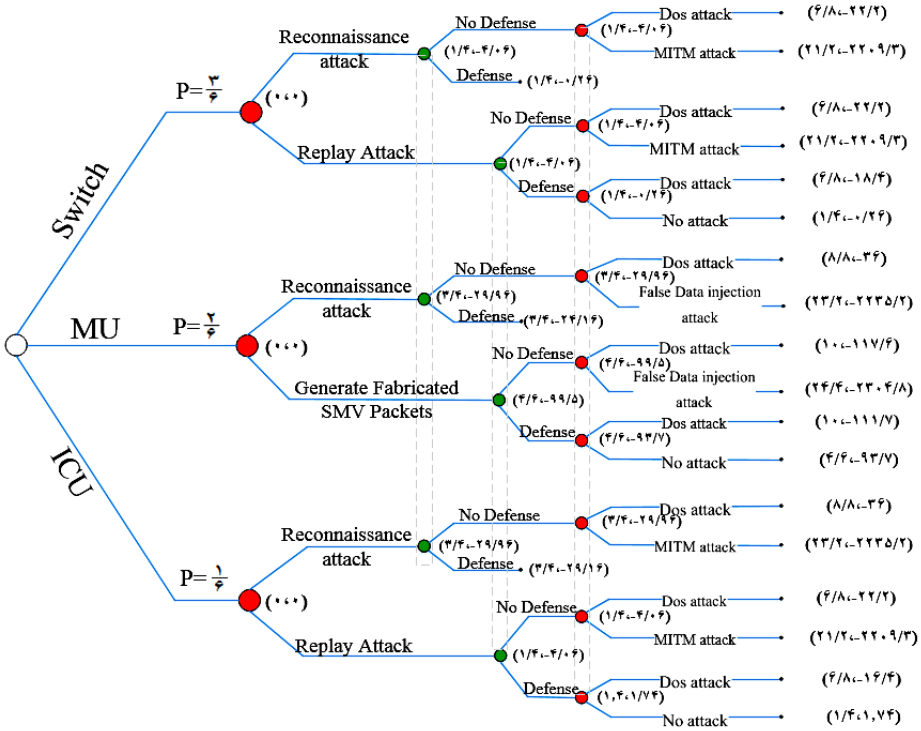
۴-۳- تعیین دریافتی مدافع و مهاجم در حمله به سطح پردازش

با استفاده از مقادیر جدول ۲ و روابط (۳) الی (۵) درخت بازی مبتنی بر مراحل بازی بین مدافع و مهاجم در سطح پردازش پست دیجیتال تشکیل می‌شود که در شکل ۵ نشان داده شده است. مطابق توضیحات و محاسبات صورت گرفته، نقطه تعادل نش برای هرکدام از سه تجهیز سوئیچ، ICU و MU تعیین و دریافتی مورد انتظار کل بازی نیز محاسبه می‌شود.

مرحله نخست بازی در هر تجهیز: با شروع بازی، دریافتی هر بازیکن یعنی مهاجم و مدافع صفر بوده و لذا زوج دریافتی به‌صورت (میزان دریافتی مدافع، میزان دریافتی مهاجم) برابر (۰، ۰) خواهد بود. اگر فرض شود که حمله توسط مهاجم از این نقطه شروع شود، مهاجم می تواند تنها اقدام به حمله نوع تکرار و یا حمله شناسایی برای صدمه به سوئیچ و واحد کنترل هوشمند کند. در واحد ادغام با حمله تولید بسته‌های ساختگی و حمله شناسایی، مهاجم اقدام به صدمه در سطح پردازش می‌نماید.

مرحله دوم بازی: در این مرحله و پس از وقوع حمله توسط مهاجم در مرحله قبل، مدافع بایستی اقدام به دفاع نماید، لذا مدافع می‌تواند توسط عملکرد دفاعی خود اقدام به دفاع در برابر حمله مهاجم نماید و یا هیچ دفاعی انجام ندهد. بر اساس نوع حمله صورت گرفته مهاجم از مرحله قبل، استراتژی دفاعی مدافع تعیین می‌شود و یا دفاعی توسط او صورت نمی‌گیرد. بر اساس هرکدام از این حالات میزان دریافتی مهاجم و مدافع مشخص می شود. مهم نیست که مهاجم چه مسیری را برای حمله انتخاب می‌کند، اگر مدافع دفاع نکند آنگاه مهاجم در سوئیچ یا واحد کنترل هوشمند می‌تواند اقدام به حمله ممانعت از سرویس یا حمله نفوذ مرد میانی نماید و در واحد ادغام نیز در صورت عدم دفاع از سوی مدافع، مهاجم باعث ممانعت از سرویس شده یا تزریق اطلاعات غلط می‌نماید. اگر دفاع در برابر حمله شناسایی صورت گیرد هیچ حمله‌ای نمی‌تواند توسط مهاجم انجام شده و عملاً بازی در این مرحله به اتمام خواهد رسید.

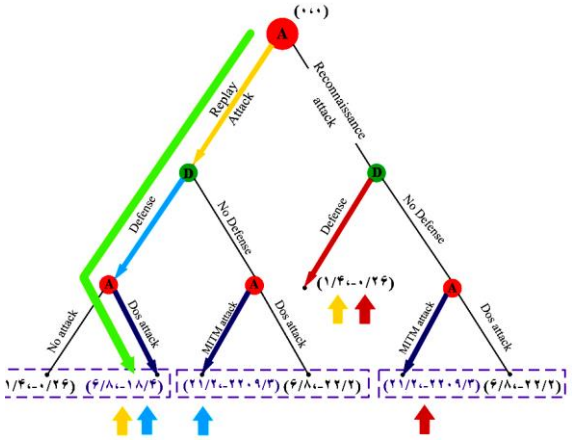
مرحله سوم بازی: با توجه به عملکرد مدافع در مرحله دوم و استراتژی های اتخاذشده توسط او، عکس‌العمل نهایی مهاجم صورت می‌گیرد. اگر دفاعی توسط مدافع پس از حمله نوع تکرار در سوئیچ و واحد کنترل هوشمند و واحد ادغام صورت گیرد، آنگاه مهاجم می‌تواند حمله نوع ممانعت از سرویس را صورت داده یا اقدامی نکند. بر این اساس دریافتی هرکدام از مدافع و مهاجم مشخص شده که در شکل ۵ نشان داده شده است. دریافتی‌ها را می‌توان با استفاده از روابط (۲) تا (۵) محاسبه نمود. ازآنجاکه محاسبه دریافتی‌ها دارای فرآیند مارکوف است، آن‌ها بر اساس تعداد مراحل بازی به شیوه از بالا به پایین و از نقطه شروع درخت بازی تا انتهای مسیر، محاسبه می‌شوند.



شکل ۵: مراحل بازی مدافع و مهاجم در سطح پردازش پست هوشمند

۴-۴- تعیین نقطه تعادل بازی

درخت بازی با استفاده از روش استنتاج از عقب برای پیدا کردن نقطه تعادل یا نقطه نش بازی یا SPNE[۱۷] تحلیل می‌شود. برای هرکدام از مسیرهای مشخص شده برای سوئیچ، MU و ICU نقطه تعادل تعیین می‌شود که در ادامه طریقه محاسبه نقطه تعادل نش برای درخت بازی سوئیچ به شرح زیر تحلیل شده و برای سایر مسیرها نیز بر این اساس نقطه تعادل محاسبه می‌شود. شکل ۶ درخت بازی مربوط به سوئیچ را نشان می‌دهد. این بازی دارای دو زیر بازی[۱۸] است.



شکل ۶: تعیین استراتژی تعادل در شبکه سوئیچ سطح پردازش پست هوشمند

الف) زیر بازی سمت چپ: با شروع حمله نوع Replay

با شروع تحلیل از انتهای درخت در این زیربازی، ازآنجاکه ریشه گره تصمیم‌گیری، مهاجم (A) است، اولین عنصر از دریافتی (۶/۸،-۱۸/۴) با اولین عنصر از دریافتی(۱/۴،-۰/۲۶) مقایسه می‌شود. ازآنجاکه ۶/۸>۱/۴ است، لذا بهترین حرکت A برابر حمله نوع DoS است که دریافتی نقطه نش NE از این زیر بازی برابر با (۶/۸،-۱۸/۴) می‌باشد. به‌طور مشابه، اولین عنصر از دریافتی (۶/۸،-۲۲/۲) با دریافتی (۲۱/۲،-۲۲۰۹/۳) مقایسه می شود. ازآنجاکه ۲۱/۲>۶/۸ است، لذا بهترین حرکت A برابر حمله نوع MITM است که دریافتی نقطه نش NE از این زیر بازی برابر با (۲۱/۲،-۲۲۰۹/۳) می‌باشد. با استنتاج به عقب، نتایج دریافتی حاصل از نقاط نش NE به سطح بالاتر برای تعیین بهترین حرکت مدافع (D) گسترش داده می شود. ازآنجاکه ریشه گره تصمیم‌گیری D است، با مقایسه عنصر دوم از چندتایی (۶/۸،-۱۸/۴) و (۲۱/۲،-۲۲۰۹/۳) ، ازآنجاکه۲۲۰۹/۳->۱۸/۴- است لذا بهترین حرکت D و نقطه نش این زیربازی برابر (۶/۸،-۱۸/۴) خواهد بود.

ب) زیر بازی سمت راست: با شروع حمله نوع Reconnaissance

به‌طور مشابه، ازآنجاکه ریشه گره تصمیم‌گیری A است، اولین عنصر از دریافتی (۶/۸،-۲۲/۲) با (۲۱/۲،-۲۲۰۹/۳) مقایسه می‌شود. ازآنجاکه 21.2>6.8 است لذا بهترین حرکت A برابر حمله نوع MITM است که دریافتی نقطه نش NE از این زیر بازی برابر با (۲۱/۲،-۲۲۰۹/۳) می باشد. با استنتاج به عقب، نتایج دریافتی حاصل از نقاط نش NE به سطح بالاتر برای تعیین بهترین حرکت D گسترش داده می‌شود. مقایسه عنصر دوم (۲۱/۲،-۲۲۰۹/۳) با (۱/۴،-۰/۲۶) از شاخه چپ، بهترین حرکت D برابر دفاع کردن بوده که دریافتی نقطه نش SPNE برابر با (۱/۴،-۰/۲۶) است.

ج) تعیین نقطه تعادل نش نهایی درخت بازی سوئیچ

با برگشت به عقب، دو نقطه دریافتی SPNE از زیربازی چپ برابر (۶/۸،-۱۸/۴) و از زیربازی راست برابر (۱/۴،-۰/۲۶) است. ازآنجاکه A گره تصمیم گیر است، مقایسه عنصر اول از دو مقدار چندتایی مذکور و چون۶/۸>۱/۴، لذا نقطه تعادل نش نهایی برابر (۶/۸،-۱۸/۴)می‌باشد. تفسیر فوق این است که برای مهاجم، بهترین استراتژی حمله Replay و سپس DoS است، درحالی‌که بهترین استراتژی برای مدافع انجام دفاع به‌صورت مداوم است.

به‌طور مشابه تحلیل فوق نقاط تعادل بازی برای درخت بازی MU و ICU به ترتیب برابر(۱۱۱/۷-،۱۰) و (۶/۸،-۱۶/۴) خواهد بود. بر اساس احتمال در نظر گرفته‌شده، احتمال حمله مهاجم به سوئیچ بیشتر بوده ولی دریافتی مورد انتظار کل بازی مبتنی بر استراتژی مرکب و براساس رابطه(۱)، به‌صورت زیر محاسبه می‌باشد.

$$Attacker's\ Payoff = \frac{3}{6}\times 6.8 + \frac{2}{6}\times 10 + \frac{1}{6}\times 6.8 = 7.87$$

$$Defender's\ Payoff = \frac{3}{6}\times(-18.4) + \frac{2}{6}\times(-111.7) + \frac{1}{6}\times(-16.4) = -49.17$$

۴-۵- تبیین مفهوم اقدامات دفاعی در بازی تحلیلی حملات سایبری

با افزایش تعداد حملات سایبری به تجهیزات در سطح پردازش پست‌های هوشمند و با توجه به استراتژی تعیین شده، دفاع مداوم در برابر این حملات ضروری می‌باشد. در تجهیزات مورد تحلیل در سطح پردازش پست‌های هوشمند، اقدامات دفاعی مناسب به شرح زیر از اهمیت زیادی برخوردار می‌باشد.

الف) شیلدنمودن تجهیزات سطح پردازش و مسیرهای ارتباطی

پالس‌های الکترومغناطیسی، میدان‌هایی از انرژی هستند که می‌توانند با القای ولتاژ و ایجاد خطر یا نویز یا تبدیل و تغییر در اطلاعات دیجیتال باعث صدمه به مدارات الکتریکی و الکترونیکی شوند. خطر عمدی یا غیرعمدی و ایجاد خسارات جبران‌ناپذیر و پیش‌بینی‌نشده، برای تداخل الکترومغناطیسی ازنقطه‌نظر منبع تولید، روش‌های حفاظت و تأثیر بر قطعات الکترونیکی دارای اهمیت زیادی می‌باشند. میدان‌های مغناطیسی ناخواسته ناشی از تجهیزات جریان بالا، سبب ایجاد اختلال در عملکرد تجهیزات حساس از طریق القا در هادی‌های حامل ولتاژهای پایین می‌نمایند. تولید عمدی و خرابکارانه انرژی الکترومغناطیسی به صورت اعمال نویز یا سیگنال به سیستم‌های الکتریکی و الکترونیکی منجر به اختلال، اغتشاش یا آسیب به این سیستم‌ها برای اهداف تبهکارانه یا تروریستی می‌شود. ازآنجاکه یکی از روش‌های اختلال از

طریق محیط انتقال ا ست، روش‌های ایجاد ایمن سازی انتقال در مقابل میدان‌های تداخلی مورد توجه قرار می‌گیرد. لذا شـــیلدینگ محفظه فلزی تجهیزات الکتریکی و الکترونیکی و مســـیر های ارتباطی حتماً بایستی انجام شود.

ب) به‌کارگیری نرم‌افزارهای امنیتی مناسب

نرم‌افزارهای بکار رفته در ســیســتم اتوماســیون پســت‌های فشــارقوی هوشمند به‌منظور افزایش میزان دفاع سایبری، مشتمل بر آنتی‌ویروس، ســیســتم تشــخیص و ممانعت از نفوذ، نرم‌افزار دائمی[۱۹]، کدینگ، رمزنگاری مثل توابع درهم[۲۰] و احراز هویت و غیره اســت. همچنین جهت مقابله با حملات به سطح پردازش پست‌های هوشمند استفاده از تجهیزاتی نظیر سوئیچ‌هایی که دارای سیستم تشخیص نفوذ و دیواره آتش هستند، توصیه می‌شود.

۵- نتیجه

با ایجاد خطا در زیرساخت‌های سایبری پست‌های دیجیتال یا هوشمند ازجمله شبکه حسگر سطح پردازش، می‌تواند باعث تریپ یک بخش با عملکرد درســت شــود و شــبکه قدرت موردنظر و همچنین شــبکه‌های مجاور را تحت تأثیر قرار دهد. نســبت به ســایر روش‌ها نظیر درخت حمله، روش‌های ســلســله مراتبی و تحلیل قابلیت اطمینان، ازآنجاکه مهاجمین ســایبری اغلب آموزش خود را بر اســاس اقدامات در طول حملات تغییر می‌دهند، نیاز به یک رویکرد ســیســتماتیک نظیر تئوری بازی با تصــمیم‌گیری آگاهانه اســت که بتواند رفتارهای مهاجمین را تحلیل نماید. در این مقاله، توسط روش نظریه بازی در سطح پردازش پســت هوشــمند برق و بر اســاس حملات صــورت گرفته به آن، نقطه تعادل بین مدافعین و مهاجمین ســایری مشــخص می‌شــود. با توجه به محاســبات به‌عمل‌آمده که منتج به تعیین نقطه تعادل نش و تعیین بهترین اســتراتژی برای مهاجم و مدافع شــد، ملاحظه می‌شــود که استراتژی مهاجم برای حمله به تجهیزات سطح پردازش پست هوشمند برق به ترتیب حمله نوع تکرار و حمله نوع ممانعت از ســرویس برای سوئیچ و واحد کنترل هوشمند و حملات تولید بسته‌های اندازه‌گیری ساختگی و ممانعت از سرویس برای واحد ادغام است. مدافع بایستی همواره اقدامات دفاعی مناســب و همچنین تعمیر مداوم و همیشــگی تجهیزات در معرض خطر و پوشــش لازم در برابر حملات را انجام دهد. افزایش هزینه دفاعی تا دو الی سه برابر نسبت به روتین فعلی مبتنی بر زیرســاخت‌های شــبکه از قبیل شــیلدینگ و کدینگ نرم‌افزاری و سخت‌افزاری می‌تواند میزان حملات موفقیت‌آمیز مهاجم به لایه حسگر سطح پردازش پست هوشمند برق را به‌طور چشمگیری کاهش دهد. درعین‌حال بایســتی توجه کرد که مقادیر بهینه برای بودجه دفاعی در آســیب‌پذیرترین نقطه از شــبکه تعیین شــود تا تأخیر ارســال داده به حداقل برسد. در تحقیقات آینده، این حملات می‌تواند با در نظر گرفتن هزینه های مربوط به تجهیزات و تأثیر آن ها در درخت بازی در نظر گرفته شــود به‌صــورتی که یک مدل پیچیده‌تر با تحلیل واقعی اثرات حملات سایبری به دست آید. همچنین بازی با بازیگران بیشتر یعنی مهاجمین و مدافعین و ائتلاف احتمالی آن ها در تحقیقات آینده می تواند لحاظ شود.

پیوست ۱- الگوریتم استنتاج از عقب

به‌منظور حل بازی با اطلاعات کامل توسط استنتاج از عقب یا معکوس، نخست مجموعه‌ای از گره‌های تصمیم‌گیری یکی مانده به آخر شناسایی می‌شــوند. یک گره از نوع گره تصــمیم‌گیر ماقبل آخر اســت اگر همه گره‌های بعدی گره‌های ترمینال باشــند. یک زیر بازی که دارای گره تصمیم‌گیر یکی مانده به آخر x به‌عنوان گره اولیه و عملکرد تصمیم‌گیر بازیگر در آن گره $l(x)$ است در نظر گرفته می شود. بازیگر عملکردهایی را انتخاب می‌کند که آن گره دریافتی‌اش نســبت به دیگر گره های ترمینالی حداکثر شود. بعد از آن عملکرد بازیگر در گره x تعیین شده و گره‌های بعدی حذف می‌شــود. ســپس x از گره تصــمیم گیر به گره ترمینال تغییریافته و با اختصــاص گره ترمینال جدید x، بردار دریافتی مربوط مشخص می‌شود که این روند سبب کوچک‌سازی بازی می‌شود. مجموعه جدید از گره‌های تصمیم‌گیری یکی مانده به آخر در این بازی کوچک شده شناسایی شده و روند فوق تکرار می شود. سرانجام بازی کاهش می‌یابد تا تنها یک گره تصــمیم گیر باقی بماند که گره اولیه O اســت. آنگاه بازیگر گره اولیه دریافتی خود را ماکزیمم کرده و جواب استنتاج معکوس بازی کامل می شود. این الگوریتم در شکل ۷ نشان داده شده است.

مجموعه گره‌های تصمیم‌گیر و ترمینال به ترتیب در هر نقطه از این فرآیند X و Z هســتند. فرض شــود برای هر گره تصــمیم گیر $x \in X$، گره‌های بعدی $N(x) \subset V$ باشــند. وقتی عملکرد $a \in A(x)$ در گره x با شد آنگاه مستقیماً به گره $\bar{v}(a|x) \in N(x)$ خواهد رسید. همچنین فرض شــود که $\overline{X} \subset X$ و $\overline{Z} \subset V$ به ترتیب مجموعه گره های تصــمیم‌گیر و گره های ترمینال باشــند، آنگاه $P(\overline{X},\overline{Z})$ گره های تصمیم‌گیری یکی مانده به آخر آن گره‌های تصمیم گیر می‌باشد که:

$$P(\overline{X},\overline{Z}) = \{x \in \overline{X} : N(x) \subset \overline{Z}\}$$

بردار $\mu : Z \to \mathbb{R}^n$ اختصــاص به دریافتی گره‌های ترمینال در بازی اصلی دارد.

فرض شــود که $\overline{P}$ مجموعه گره‌های تصــمیم‌گیر یکی مانده به آخر در هر مرحله از فرآیند استنتاج معکوس با شد. گره تصمیم‌گیری یکی مانده به آخر $x \in \overline{P}$ متعلق به بازیگر $i = l(x)$ می‌باشــد. بازیگر i عملکرد $a \in A(x)$ را در این گره انتخاب می‌کند به‌نحوی‌که

$$a \in \arg\max_{a' \in A(x)} \mu_i(\bar{v}(a'|x))$$

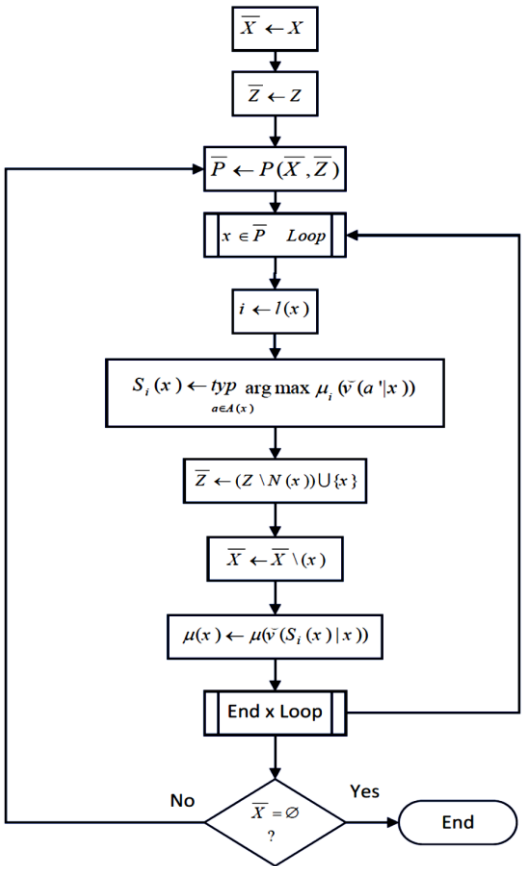
این تصمیم در گره x با تنظیم $S_i(x) = a$ صورت می‌گیرد.

حال همه گره‌های بعدی x از مجموعه گره‌های ترمینال بازی $N(x)$ حذف می‌شــود و آن‌ها با مجموعه‌ای از گره‌های ترمینال با x جایگزین می‌شــوند یعنی $\overline{Z} \leftarrow (Z \setminus N(x)) \cup \{x\}$. اکنون کــه x دیگر گره تصــمیم‌گیر نیســت، x از مجموعه گره‌های تصــمیم‌گیر حذف می‌شــود یعنی $\overline{X} \leftarrow \overline{X} \setminus \{x\}$. بردار دریافتی اختصــاص‌یافته به گره ترمینال جدید x، بردار دریافتی در ارتباط با گره ترمینال $\bar{v}(S_i(x)|x)$ می

باشد وقتی‌که بازیگر i عملکرد $S_i(x)$ را در گره x انجام می‌دهد یعنی $\mu(x)=\mu(\bar{v}(S_i(x)|x))$.

$a'\in A(x)$

نهایتاً هر گره تصمیم‌گیر تبدیل به گره تصمیم‌گیر یکی مانده به آخر می‌شود و یک عملکرد برای آن ثبت می‌شود و آن تبدیل به یک گره ترمینال می‌شود. آخرین گره تصمیم گیر تبدیل به گره یکی مانده به آخر گره اولیه O است. وقتی یک عملکرد برای گره اولیه تعیین می‌شود آن از مجموعه گره‌های موجود X حذف شده و مجموعه خالی می شود که نقطه توقف الگوریتم است[۴۲] .



شکل ۷: الگوریتم استنتاج از عقب

مراجع

[1] M. Panteli and D. S. Kirschen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," Power Systems Conference and Exposition (PSCE) , pp. 1-7, 2011.

[2] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," IEEE Power and Energy magazine, vol. 7, no. 1, 2009.

[3] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," Communication, Control, and Computing (Allerton), , pp. 212-219, 2012.

[4] W. Saad, Z. Han, H. V. Poor, and T. Basar, "Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications," IEEE Signal Processing Magazine, vol. 29, no. 5, pp. 86-105, 2012.

[۵] معصومه جوادی، سیدمازیار میرحسینی مقدم، موسی مرزبند، «مدیریت بهینه انرژی ریزشبکه‌ها در بازار خرده‌فروشی بر پایه روش تئوری بازی غیر همکارانه با در نظر گرفتن عدم قطعیت»، مجله مهندسی برق دانشگاه تبریز، دوره ۴۶، شماره ۱، صفحه ۷۴-۶۳ بهار ۱۳۹۵.

[6] X. Liang and Y. Xiao, "Game theory for network security, " IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 472-486, 2013.

[7] A. K. Farraj, E. M. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic control approach to mitigate cyber switching attacks in smart grid systems, " IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 958-963, 2014.

[8] R. Hewett, S. Rudrapattana, and P. Kijsanayothin, "Smart Grid security: Deriving informed decisions from cyber attack game analysis," IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 946-951, 2014.

[9] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, "A game-theoretical model for security risk management of interdependent ict and electrical infrastructures, " IEEE 16th International Symposium on High Assurance Systems Engineering (HASE), pp. 101-109, 2015.

[10] M. Sheng-Wei and Z. Jian-Quan, "Mathematical and control scientific issues of smart grid and its prospects," Acta Automatica Sinica, vol. 39, no. 2, pp. 119-131, 2013.

[11] A. A. Cardenas, T. Roosta, and S. Sastry, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems," Ad Hoc Networks, vol. 7, no. 8, pp. 1434-1447, 2009.

[12] C. Wang, C-W. Ten, Y. Hou, and A. Ginter, "Cyber Inference System for Substation Anomalies Against Alter-and-Hide Attacks," IEEE Transactions on Power Systems, vol. 32, pp. 896-909, 2016.

[13] M. Marzband, F. Azarinejadian, M. Savaghebi, and J. M. Guerrero, "An optimal energy management system for islanded microgrids based on multiperiod artificial bee colony combined with Markov chain," IEEE Systems Journal, vol. 11, pp. 1712-1722, 2015.

[14] M. Marzband, S. S. Ghazimirsaeid, H. Uppal, and T. Fernando, "A real-time evaluation of energy management systems for smart hybrid home Microgrids," Electric Power Systems Research, vol. 143, pp. 624-633, 2017.

[15] S. Mousavian, J. Valenzuela, and J. Wang, "A probabilistic risk mitigation model for cyber-attacks to PMU networks," IEEE Transactions on Power Systems, vol. 30, no. 1, pp. 156-165, 2015.

[16] M. T. A. Rashid, S. Yussof, and Y. Yusoff, "Trust System Architecture for Securing GOOSE Communication in IEC 61850 Substation Network," *I*nternational Journal of Security and Its Applications, vol. 10, no. 4, pp. 289-302, 2016.

[17] T. A. Youssef, M. El Hariri, N. Bugay, and O. Mohammed, "IEC 61850: Technology Standards and Cyber-Security Threats," in Proceedings of the 16th IEEE International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, vol. 710, pp. 1-6, 2016.

[18] R. Macwan et al., "Collaborative defense against data injection attack in IEC61850 based smart substations,"

IEEE Power and Energy Society General Meeting (PESGM), pp. 1-5, 2016.

[19] J. Yue and K. Zhang, "Vulnerability Threat Assessment Based on AHP and Fuzzy Comprehensive Evaluation," IEEE Seventh International Symposium on Computational Intelligence and Design (ISCID), vol. 2, pp. 513-516, 2014.

[20] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Vulnerability assessment for communication network of substation automation systems to cyber attack," PSCE'09. IEEE/PES Power Systems Conference and Exposition, pp. 1-7, 2009.

[21] C. Taylor, P. W. Oman, and A. W. Krings, "Assessing Power Substation Network Security and Survivability: A Work in Progress Report," Security and Management, pp. 281-287, 2003.

[22] Y. Xiang, L. Wang, and Y. Zhang, "Power system adequacy assessment with probabilistic cyber attacks against breakers," IEEE Conference & Exposition in PES General Meeting, pp. 1-5, 2014.

[23] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," IEEE Transactions on Smart Grid, vol. 7, no. 2, pp. 669-683, 2016.

[24] M. Wei and Z. Chen, "Reliability analysis of cyber security in an electrical power system associated WAN," IEEE Meeting in Power and Energy Society General, pp. 1-6, 2012.

[25] A. Patrascu and E. Simion, "Applied cybersecurity using game theory elements," 10th International Conference on Communications (COMM), pp. 1-4, 2014.

[26] Q. Zhu, *Game-theoretic methods for security and resilience in cyber-physical systems*, Ph.D. Thesis, University of Illinois, Urbana, Illinois, 2013.

[27] M. Adamiak, D. Baigent, and R. Mackiewicz, "IEC 61850 Communication Networks and Systems In Substations," The Protection & Control Jurnal-Smart Grid, pp. 61-68, 2010.

[28] M. Humphreys and J. J. Heon, *Research Topics in Game Theory*, Political ScienceW4210 , 2004.

[29] L. Wei, A. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," IEEE Transactions on Smart Grid, vol. PP, pp. 1-11, 2016.

[30] M. Marzband, M. Javadi, J .L. Domínguez-García, and M. M. Moghaddam, "Non-cooperative game theory based energy management systems for energy district in the retail market considering DER uncertainties," IET Generation, Transmission & Distribution, vol. 10, no. 12, pp. 2999-3009, 2016.

[31] T. Alpcan and T. Başar, *Network security: A decision and game-theoretic approach*, Cambridge University Press, 2010.

[32] Y. Yang et al., "Cybersecurity test-bed for IEC 61850 based smart substations," IEEE in Power & Energy Society General Meeting, pp. 1-5,2015.

[33] P. Wood , *Symantec internet security threat report 2016*, Symantec Corp., Mountain View, CA, USA, Tech. Rep, 2016.

[34] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," IEEE PES in Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5, 2014.

[35] P. Maynard, K. McLaughlin, and B. Haberler, "Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks," in Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research, pp. 30-42, 2014.

[۳۶] رضا رافع، فرشته خدادادی، "ارائه یک الگوریتم شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم به کمک انتشارات محلی و کانال‌های کرم‌چاله قانونی،" مجله مهندسی برق دانشگاه تبریز، دوره ۴۴، شماره ۴، صفحه ۳۳-۲۲ زمستان ۱۳۹۳.

[37] S. Jeba and B. Paramasivan, "False data injection attack and its countermeasures in wireless sensor networks," European Journal of Scientific Research, vol. 82 ,no. 2, pp. 248-257, 2012.

[38] E. Fabrizio et al., "Monitoring of a micro-smart grid: Power consumption data of some machineries of an agro-industrial test site," Data Brief, vol. 10, pp. 564-568, 2017.

[39] I. Syamsuddin and J. Hwang, "The application of AHP to evaluate information security policy decision making," International Journal of Simulation, Systems, Science and Technology, vol. 10, no. 4, pp. 46-50, 2009.

[40] F. P. DRAFT, "Recommended security controls for federal information systems and organizations," NIST Special Publication, vol. 800, p. 53, 2009.

[41] L. Evans, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199, 2004

[42] J. Ratliff. *Extensive-Form Solution Concepts*, 1994, http://virtualperfection.com/gametheory.

زیرنویس‌ها

[1] Supervisory Control and Data Acquisition
[2] Remote Terminal Unit
[3] Nash Equilibrium
[4] Phasor Measurement Unit
[5] Manufacturing Message Specification
[6] Generic Object Oriented Substation Event
[7] Sampled Message Value
[8] Payoff
[9] Merging Unit
[10] Intelligent Control Unit
[11] Simple Network Time Protocol
[12] Gateway
[13] Gas Insulation Substation
[14] Air Insulation Substation
[15] Firewall
[16] Backward induction
[17] Subgame Perfect Nash Equilibrium
[18] Subgame
[19] Firmware
[20] Hash Function