مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال ششم، شماره ۱، بهار ۱۳۹۷، ص ۱۰۸-۹۵

ارزش‌گذاری بودجه دفاع و حمله در امنیت سایبری پست‌های فشارقوی مبتنی بر طبقه‌بندی کاربردی به روش AHP فازی

نورالله فرداد[۱]، سودابه سلیمانی[۲*]، فرامرز فقیهی

۱- دانشجوی دکتری، ۲- دانشیار، ۳- استادیار، دانشگاه آزاد اسلامی، واحد علوم وتحقیقات تهران، گروه برق قدرت، تهران، ایران

چکیده

حفاظت و دفاع از پست‌های فشارقوی در شبکه هوشمند بستگی به ملاحظات شرکت‌های برق نسبت به سطح تهدیدات و ارزش دارایی‌های آن‌ها دارد. تعداد اقدامات متقابل یا دفاعی برای سطح خطر قابل قبول بستگی به تعداد تجهیزات دفاعی نظیر امکانات و روش‌های نرم‌افزاری، سخت‌افزاری، شیلدینگ و انتخاب مسیر بهینه برای تجهیزات ارسال اطلاعات در سطح پست دارد. تعداد این اقدامات با توجه به وضعیت هر پست و میزان سرمایه‌گذاری و اهمیت آن بایستی تخمین زده شود. روش‌های دفاعی مناسب با توجه به تعداد، نوع، وضعیت طراحی و موقعیت پست‌ها، می‌تواند نقاط ضعف امنیتی سیستم را پوشش دهد. در این مقاله براساس داده‌ها و تجربیات قبلی مبتنی بر دانش افراد خبره و داده‌های آموزشی، میزان اهمیت پست‌های فشارقوی مورد مطالعه در مقابل حملات سایبری تعیین می‌گردد. پست‌ها از نقطه‌نظر کاربرد به انواع ژئواستراتژیک، راهبردی صنعتی، سیستم‌های اتوماسیون و کنترلی و مخاطره‌آمیزبودن تقسیم می‌شوند. با استفاده از اطلاعات به‌دست‌آمده از نظرسنجی و تحلیل با روش سلسله مراتبی فازی (FAHP) سهم بودجه مورد نیاز برای انواع دفاع سایبری در پست‌های فشارقوی محاسبه می‌گردد. تحلیل حساسیت، صحت نتایج روش ارائه‌شده را تایید می‌نماید.

کلمات کلیدی: امنیت سایبری، سلسله مراتبی فازی، شبکه هوشمند، حملات سایبری، دفاع سایبری

۱- مقدمه

تعامل بین حمله و دفاع یک فرایند بسیار پیچیده بوده و درنظرگرفتن دقیق تمام عوامل تقریباً غیرممکن است. برای سادگی، سطح حمله توسط تعداد اندازه‌گیری‌هایی که مهاجم قادر به تغییر موفقیت‌آمیز آن‌ها می‌باشد شرح داده می‌شود [۱]. از آن‌جا که هدف مهاجم به حداکثررساندن از دست‌دادن دارایی و هدف مدافع سیستم قدرت به‌حداقل‌رساندن ازدست‌دادن است، راهبردهای تخصیص منابع مختلف می‌تواند توسط مهاجمان و مدافعان ایجاد شود. در [۲]، مدل راهبردی تخصیص منابع دفاعی پیشنهاد شده است که هنگام تعادل، ترجیح مدافع تخصیص منابع به‌صورت متمرکز می‌باشد. عموماً پست‌های فشار قوی دارای کمترین حفاظت می‌باشند، البته این به معنای این نیست که شرکت‌ها بالاترین ریسک را برای پست‌ها قبول کرده‌اند بلکه ممکن است آن‌ها تا زمانی‌که حملاتی متوجه آن نشود، سرمایه‌گذاری لازم را انجام نداده باشند. خطرات ممکن می‌تواند توسط روش‌های هوشمند و تخصصی و همچنین، بهره‌برداری‌های هوشمند امنیتی اندازه‌گیری شود. ضوابط امنیتی ممکن است سطح حفاظت و اقدامات دفاعی در پست‌ها را تعیین نماید اما برخی موارد، مقررات و قوانین دولتی یا استاندارد مالی موجود نیز ممکن است این سطح را دچار تغییر نماید. عمر مفید سیستم نیز بر عملکرد اقدامات دفاعی تأثیرگذار است که آن نیز می‌تواند بر تصمیم‌گیری سطح دفاع تأثیرگذار باشد و مشخص نماید که میزان در سرویس‌بودن سیستم و زمان تعمیر آن به چه صورتی خواهد بود. اثربخشی روش‌های تدافعی و ترکیب با روش‌های حفاظت از پست‌های فشارقوی جهت ارزیابی روش‌های مؤثر برای

* رایانامه نویسنده پاسخگو: s.soleymani@srbiau.ac.ir

ایمنی بالای سیستم اتوماسیون پست‌های فشارقوی و تصمیم‌گیری در این خصوص ضروری می‌باشد [۳].

با منابع کافی حمله، مهاجمین ممکن است قادر به نفوذ به شبکه‌های مختلف پست با چند سطح کنترل و ارسال فرمان‌های ساختگی به تجهیزات محلی فیلد[1] شوند [۴]. برای هرگونه حفاظت از زیرساخت‌های حیاتی، هزینه‌های حفاظت بایستی مبتنی بر اهمیت امکانات و تجهیزات به‌کاررفته در آن‌ها باشد [۵]. تأمین‌کنندگان طیف وسیعی از تجهیزات دفاع سایبری مانند دیواره آتش[2]، دروازه عبور[3]، تجهیزات ناحیه غیرنظامی (DMZ)[4] و تجهیزات دیگر را ارائه می‌کنند که مشتمل بر اعمال مقرراتی درخصوص استفاده از این تجهیزات می‌باشد [۶]. لازم به ذکر است که راه‌حل‌های دفاع سایبری بر نرخ اطلاعات تبادل‌شده و تأخیر زمانی تأثیر می‌گذارد و اغلب نیاز به ایجاد تغییرات در سیستم می‌باشد. بدون تخصیص منابع کافی برای اطمینان از ایمنی، دفاع سایبری جدید جهت تجهیزات امکان‌پذیر نمی‌باشد. دفاع مؤثر برای سیستم اتوماسیون پست‌ها در شبکه هوشمند با تحلیل میزان ترافیک اطلاعات صورت می‌گیرد. برای شناسایی و توقف حملات و جلوگیری از توسعه آن‌ها سیستم تشخیص نابهنجاری[5]، سیستم تشخیص نفوذ (IDS)[6] و سیستم ممانعت از نفوذ (IPS)[7] استفاده می‌شود.

به‌نظر می‌رسد مهاجم، حملات را در واکنش به افزایش مکانیسم‌های دفاعی یا تغییر در دفاع تغییر خواهد داد، لذا ضروری است مدافعان، واکنش‌های از پیش اندیشیده‌ای را در مقابل اثرات حمله تدارک ببینند. از آن‌جا که بخش مهندسی اجتماعی حمله، ایمیل‌ها و تجهیزات سایبری متصل به اینترنت را شامل می‌شود، این تجهیزات و شبکه‌هایی که مبتنی بر این تجهیزات کار می‌کنند جزو محدوده غیرقابل اطمینان به‌حساب می‌آیند. ارتباط با این مناطق غیرقابل اطمینان می‌بایست منطقه‌بندی، مانیتور و کنترل شود. مهاجمان ممکن است روش‌های خود را به‌گونه‌ای اصلاح کنند تا از ابزارهای دسترسی از راه دور استفاده کنند یا از محافظ‌های هوشمند از راه دور بهره گیرند یا این‌که از میان ارتباطات دیوارآتش تعریف‌شده تونل بزنند. در واکنش به چنین روش‌های اصلاحی در حمله، روش‌های پیشگیری می‌بایست جهت ممانعت از اجرای برنامه‌های غیرقانونی به‌کار گرفته شود [۷]. به‌منظور فراهم‌نمودن شبکه هوشمند با حداکثر مقاومت در برابر حملات سایبری، مدافع بایستی منابع محدود دفاعی خود را براساس بهبود بهره‌برداری و برطرف‌نمودن نقاط دارای ضعف در سیستم تخصیص دهد [۸]. اگر اندازه‌گیری‌هایی که در مرکز اسکادا و براساس اطلاعات دریافتی از پست‌ها صورت می‌گیرد از امنیت لازم برخوردار نباشد، حملات سایبری که منجر به قطع خطوط و بریکرهای پست‌ها می‌گردند به‌راحتی شناسایی نمی‌شوند. در ضمن، در عمل اغلب بودجه‌ای که برای دفاع و جلوگیری از حملات سایبری درنظر گرفته می‌شود محدود بوده که ممکن است دستیابی به راه‌بردهای حفاظت کامل مقدور نباشد [۹]، لذا تعیین مناسب‌ترین و بهینه‌ترین تجهیزات دفاع سایبری می‌تواند در حداقل‌سازی تأثیر حملات سایبری کمک شایانی نماید. به‌دلیل پیچیدگی موضوع و وجود گزینه‌های مختلف و معیارهای کمی و کیفی متعدد در تعیین آسیب‌پذیری و امنیت شبکه، روش سلسله مراتبی می‌تواند مورد استفاده قرار گیرد [۱۰].

در ادامه در فصل دوم، تحلیل پدافند غیرعامل در پست‌های فشارقوی ارائه می‌شود. فصل سوم شبکه هوشمند و اهمیت نگاه سایبری به رخداد حملات در پست‌های فشارقوی را مورد تجزیه و تحلیل قرار می‌دهد. در فصل چهارم، انواع روش‌های دفاعی در پست‌های فشارقوی مبتنی‌بر واقعیت‌های موجود در آن‌ها مورد ارزیابی قرار می‌گیرد. فصل پنجم به طبقه‌بندی پست‌های فشارقوی از نقطه‌نظر کاربرد و میزان تأثیر امنیت سایبری در آن‌ها می‌پردازد. در فصل ششم، روش تحلیل سلسله مراتبی فازی برای حداقل‌سازی هزینه دفاعی بیان می‌گردد. نتیجه‌گیری در فصل هفتم انجام می‌گیرد.

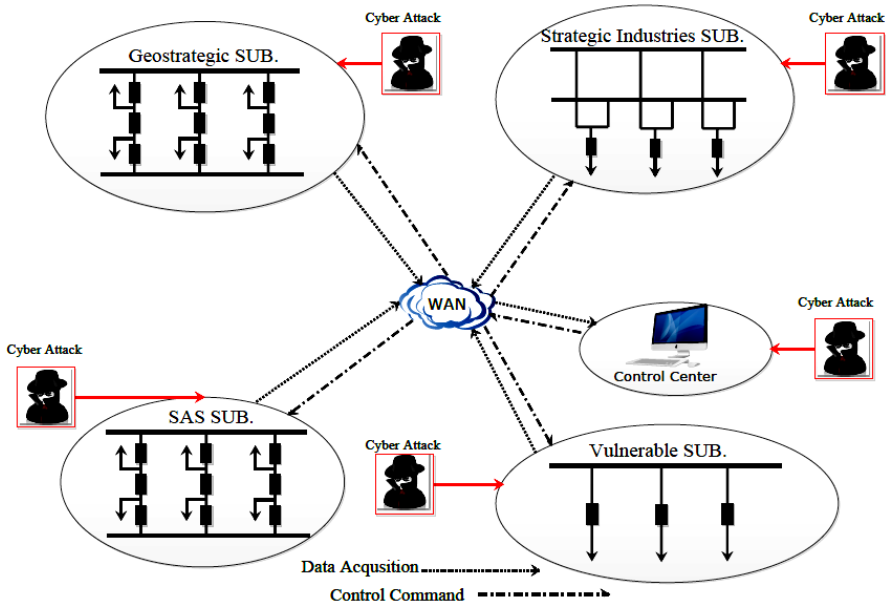
۲- طبقه‌بندی پست‌های فشارقوی براساس کاربرد و تأثیر امنیت سایبری آن‌ها

مطابق شکل (۱)، هر پست دارای یک اهمیت در شبکه هوشمند قدرت می‌باشد. یک پست برای دفاع و امنیت سایبری خود از دیواره آتش و سیستم تشخیص نفوذ[8] و ویژگی‌های رمزنگاری می‌تواند بهره ببرد و پست دیگر تنها از دیواره آتش استفاده نماید. ملاحظه می‌شود که افزایش سطح امنیت، افزایش هزینه امنیت را به‌دنبال خواهد داشت. با تجزیه و تحلیل سطح امنیتی پست و اهمیت آن در شبکه هوشمند برق، مهاجم ممکن است از یک راه‌برد برای هدف قراردادن پست‌ها بهره ببرد تا بتواند مجموعه‌ای

1- Field
2- Firewall
3- Gateway
4- Demilitarized Zone
5- Anomaly
6- Intrusion Detection System
7- Intrusion Prevention System

8- Ids: Intrusion Detection System

از حوادث در شبکه برق را به‌وجود آورد [۱۱]. در ذیل طبقه‌بندی پست‌ها با توجه به کاربرد آن‌ها به تفکیک معرفی شده‌اند:



شکل (۱): تهدیدات سایبری بالقوه به پست‌های فشارقوی با توجه به کاربرد آن‌ها

۲-۱- پست‌های فشار قوی ژئواستراتژیک

این پست‌ها در شرایط خاص جغرافیایی و راهبردیی ازقبیل مناطق مرزی، جزایر، قرارگرفتن در شرایط ویژه اقلیمی و ... قرار دارند. با توجه به موقعیت‌های ویژه و دوردستی از مرکز کشور، این پست‌ها مستعد حملات سایبری از سوی مهاجمین از کشورهای خارجی و مجاور آن‌ها قرار دارند. مهم‌ترین موارد برای جلوگیری از حملات سایبری و استحکام دفاع سایبری می‌تواند محافظت تجهیزات مخابراتی و ارتباطی و مسیریابی بهینه کابل‌ها در سطح پست به‌منظور جلوگیری از تأثیر امواج الکترومغناطیسی بر روی تجهیزات حساس کنترلی و الکترونیکی باشد.

۲-۲- پست‌های فشارقوی راهبردی صنعتی

این گروه از پست‌ها، پست‌های به‌کاررفته در صنایع مختلف از جمله نفت و گاز و پتروشیمی و همچنین، پست‌های نیروگاهی و انتقال می‌باشد. برای بیش‌تر پست‌ها در این گروه و از جمله پست‌های حساس نیروگاهی و خصوصاً پست نیروگاه که فرکانس شبکه را کنترل می‌نماید و همچنین، پست‌های صنعتی که تأمین‌کننده انرژی در یک مجموعه صنعتی می‌باشند، به‌منظور استحکام‌بخشیدن به دفاع سایبری، بودجه دفاعی در بخش‌های سخت‌افزاری و نرم‌افزاری علاوه بر سایر موارد در اولویت قرار دارد.

۲-۳- پست‌های فشارقوی از دیدگاه سیستم‌های اتوماسیون و کنترلی

تقسیم‌بندی پست‌ها در این حالت براساس سیستم کنترلی پست می‌باشد که می‌تواند از نوع کنترل سنتی باشد که کنترل و نظارت تجهیزات به‌صورت متمرکز از اتاق کنترل مرکزی صورت گرفته و این ارتباطات عموماً به‌صورت کابل‌های مسی باشد و از تجهیزات هوشمند و فن‌آوری جدید کمتر استفاده شده است. همچنین، سیستم کنترل پست می‌تواند از نوعSAS[1] یا سیستم کنترل توزیع‌شده در سطح پست باشد که ارتباطات عموماً توسط تجهیزات مخابراتی هوشمند و کابل‌های فیبر نوری صورت می‌گیرد و با توجه به به‌کارگیری IT در اتوماسیون پست، به‌منظور جلوگیری از حملات سایبری ضروری است که تجهیزات دفاعی نرم‌افزاری و سخت‌افزاری در آن‌ها مورد استفاده قرار گیرد.

۲-۴- پست‌های فشارقوی از دیدگاه مخاطره‌آمیزبودن

این پست‌ها با توجه به قرار گرفتن آنها در محل‌هایی که دارای امواج الکترومغناطیسی و سیگنالینگ قوی هستند مخاطره‌آمیز می‌باشند. این پست‌ها بر اساس میزان آسیب‌پذیری ناشی از به‌کارگیری تجهیزات مخابراتی در آنها و تداخل امواج الکترومغناطیسی طبقه‌بندی شده‌اند. بیشترین هزینه دفاعی بایستی در بخش مسیریابی بهینه تجهیزات و کابل‌های ارتباطی و همچنین محافظ و امکانات نرم‌افزاری از جمله کدینگ، رمزنگاری و تشخیص هویت صورت گیرد.

۳- تحلیل پدافند غیرعامل در پست‌های فشارقوی

1- Substation Automation System

یک تابع احتمال موفق [۱۱-۱۰] برای نشان دادن روابط مهاجم و مدافع در نظر گرفته می‌شود. فرض بر این است که N هدف با اندیس i وجود دارد. مهاجم دارای بودجه یا اعتبار کل (BA)[1] به‌عنوان منبع حمله و مدافع دارای بودجه یا اعتبار کل (BD)[2] برای دفاع در برابر حملات می‌باشد. وقتی مهاجمین و مدافعین، مقادیر BA و BD را به N هدف تخصیص داده‌اند، احتمال حمله موفق در هر هدف (i) می‌تواند محاسبه شود. فرض بر این است که آسیب‌پذیری، احتمال صدمه به دارایی مورد هدف باشد و آسیب‌پذیری توسط مهاجم به‌صورت رابطه زیر، افزایش می‌یابد.

$$P_i(A_i) = 1 - e^{-\lambda_i A_i} \qquad 0 < P_i(A_i) \le 1 \qquad (۱)$$

که A_i، منبع حمله[3] اختصاص داده شده به هدف (i) توسط مهاجمین می‌باشد که بودجه یا میزان سرمایه‌گذاری[4] حمله است که نشان‌دهنده سطح قدرت مهاجم می‌باشد و λ_i عامل یا ضریب آسیب‌پذیری است که سطح دشواری حمله را نشان می‌دهد و توسط اقدامات متقابل و دفاعی مربوط به هر مرحله از حمله تعیین می‌شود. در رابطه (۱)، احتمال موفقیت حمله با ضریب آسیب‌پذیری شبکه و منابع حمله افزایش می‌یابد که منطبق بر اصول امنیت سایبری می‌باشد. همچنین احتمال حمله موفق، توسط آسیب‌پذیری به مدافع نشان داده می‌شود. آسیب‌پذیری توسط سرمایه‌گذاری مدافع یعنی احتمال حمله موفق با افزایش سطح D_i کاهش می‌یابد و به‌صورت زیر مدل‌سازی می‌شود.

$$P_i(D_i) = e^{-\alpha_i D_i} \qquad 0 < P_i(D_i) \le 1 \qquad (۲)$$

که D_i حداقل منبع دفاع[5] اختصاص‌یافته به دارایی (i) می‌باشد که اعتبار یا بودجه فراهم شده برای مدافع بوده و α_i ضریب آسیب‌پذیری را نشان می‌دهد. با آسیب‌پذیری‌های مهاجم و مدافع برای دارایی (i)، احتمال توام حمله موفق برای هدف برابر است با:

$$P_i(A_i, D_i) = P_i(A_i)P_i(D_i) = (1 - e^{-\lambda_i A_i})(e^{-\alpha_i D_i}) \qquad (۳)$$

بر این اساس رابطه کلی خطر در هر هدف به‌صورت زیر تعریف می‌گردد:

Risk = Combined Probability of Attack * Consequence of Attack

و خطر کلی سیستم به‌صورت رابطه زیر خواهد بود:

$$R(A_i, D_i) = \sum_{i=1}^{N} P_i(A_i, D_i).\, d_i \qquad (۴)$$

که در آن، d_i نتیجه و تأثیر حاصل بر هدف (i) است وقتی که با موفقیت حمله صورت می‌گیرد که به معنی خسارت مورد انتظار یا تلفات اقتصادی هدف می‌باشد. N، تعداد کل اهداف برای مهاجمین می‌باشد. خطر شبکه هدف $R(A_i,D_i)$ تحت تأثیر آسیب‌پذیری اصلی مدافع و مهاجم و خسارت هر هدف می‌باشد. خطر را می‌توان با افزایش منبع مدافع D_i کاهش و با افزایش منبع مهاجم A_i افزایش داد. فرمول ارائه‌شده در رابطه (۴) مطابق نظریه بازی‌ها یک بازی با دو بازیکن با دریافتی صفر است، بنابراین، هدف، تخصیص بهینه منابع توسط مدافعان و مهاجمین می‌باشد. تابع هدف به‌صورت زیر بیان می‌شود:

$$Min[Max\{R\}] = Min[Max(\sum_{i=1}^{N} P_i(A_i, D_i).\, d_i)] \qquad (۵)$$

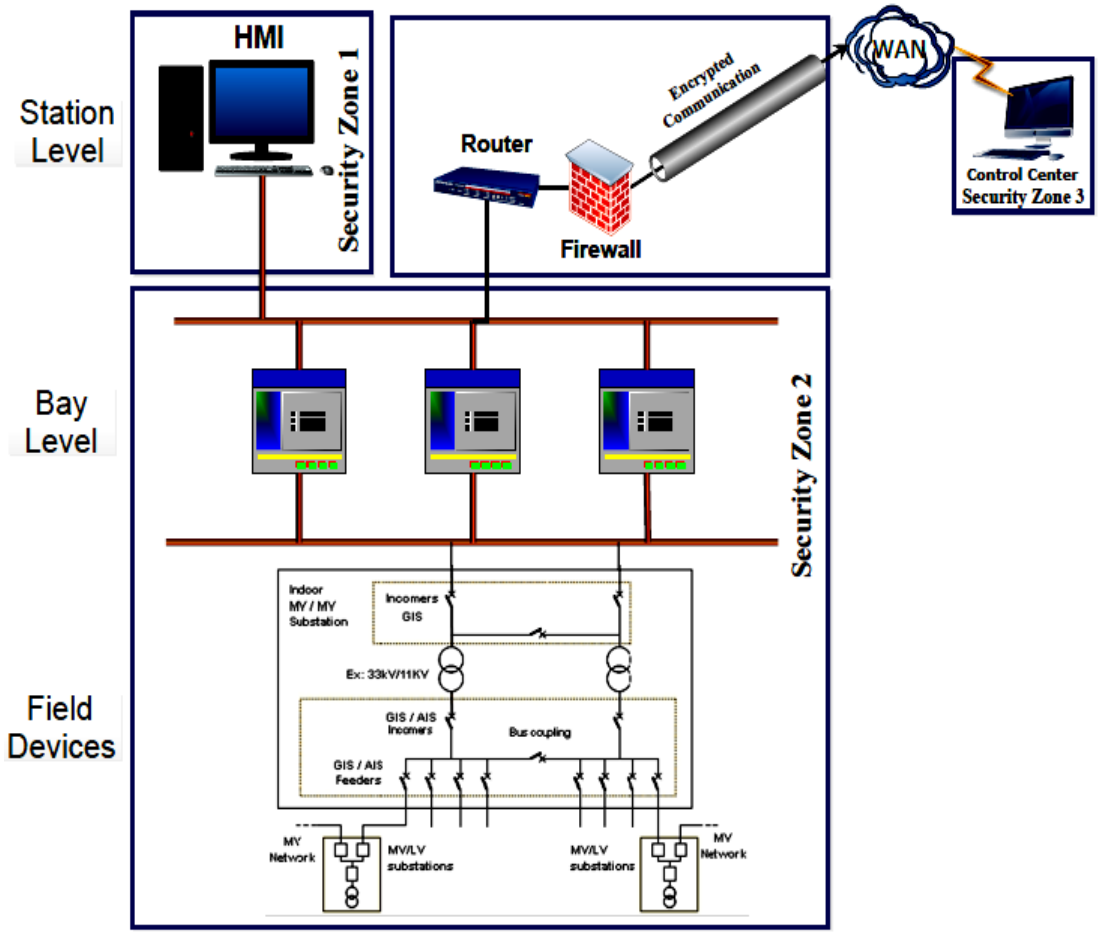
$$\sum_{i=1}^{N} A_i = BA \qquad , A_i \ge 0 \qquad (۶)$$

$$\sum_{i=1}^{N} D_i = BD \qquad , D_i \ge 0 \qquad (۷)$$

تجارب مهاجم باعث می‌شود که با سرمایه‌گذاری کمتری اهداف با الویت بالا را مورد حمله قرار دهد. ولی در عین حال برای کاهش آسیب‌پذیری و خطر کلی سیستم مدافع بایستی مراکز با اهمیت بالا را با تخصیص منابع کافی محافظت نماید. با توجه به کاربرد هر پست، میزان تأمین دفاع سایبری مورد نیاز و در واقع میزان بودجه دفاعی متفاوت خواهد بود. مهاجمان با حمله به زیرساخت‌های IT پست، شروع به سرقت اطلاعات لازم و شناسایی تجهیزات و ارسال فرمان برای قطع کلیدها منجر به خاموشی می‌شوند. این امر با حملات تخریبی روی Workstationها، سرورها و تجهیزاتی که مرتبط با پست‌ها می‌باشند صورت می‌گیرد. از تجهیزات سخت‌افزاری و نرم‌افزاری از قبیل دیواره آتش، سیستم‌های تشخیص و ممانعت از نفوذ، روترهای VPN، تجهیزات دروازه عبور و نرم‌افزارهای مربوطه و همچنین کدینگ، رمزنگاری و تشخیص هویت در سطح اتوماسیون و تجهیزات مخابراتی با توجه به اهمیت هر پست استفاده می‌شود. مسیر بهینه کابل‌های ارتباطی و محافظ کابل آن‌ها جهت ممانعت از تأثیر حملات از نوع میدانی نیز به‌کار می‌رود. علاوه بر آن، سیستم می‌تواند به چند ناحیه امنیتی مورد نیاز مطابق شکل (۲) جهت بهبود بیشتر امنیت تقسیم گردد [۱۴].

با دسترسی و دید کافی روی سیستم‌های کنترل صنعتی، مدافعان قادر به تشخیص فعل و انفعالات غیرمعمول حول‌وحوش تجهیزات فیلد را خواهند داشت [۷].

1- Total Budget for attack
2- Total budget for defending
3- Attack Resource
4- Investment
5- least Defense Resource



شکل (۲): نواحی مختلف امنیتی یک پست فشارقوی

۴- شبکه هوشمند و اهمیت نگاه سایبری به رخداد حملات در پست‌های فشار قوی

اهمیت شبکه هوشمند تا حدود زیادی متمرکز به تهدیدات سایبری شده است که می‌تواند دلایل مختلفی داشته باشد. نخست، تکامل امروزه شبکه‌های برق با سیستم اندازه‌گیری پیشرفته[1] (AMI) است که بعد جدید و ناشناخته‌ای از تهدیدات سایبری به‌اضافه آسیب‌پذیری‌های موجود در شبکه هوشمند برق را معرفی کرده است. دوم، احتمالاً این تصور وجود دارد که حملات سایبری آسان‌تر از حملات فیزیکی می‌توانند صورت گیرند. حملات فیزیکی نیاز به ابزار و حضور فیزیکی دارند درحالی‌که حملات سایبری ممکن است از طریق رایانه صورت گیرد. سوم، دستگاه اندازه‌گیری هوشمند با سایر تجهیزات اندازه‌گیری در شبکه‌های محلی و لوازم خانگی هوشمند و سیستم‌های مدیریت انرژی در شبکه‌های خانگی ارتباط و اینترفیس دارند. این ارتباطات، شبکه هوشمند را در معرض تهدیدات از راه دور قرار می‌دهد. چهارم، تجربیات گذشته درخصوص ناامنی اینترنتی نشان داده است که حملات الکترونیکی یا سایبری اگر طرح پیشگیری و دفاع کافی از نقطه شروع برای سیستم صورت نگیرد، می‌تواند برای مقابله، بسیار جدی و دشوار باشد [۱۶-۱۵]. تهدیدات امنیتی به سیستم اتوماسیون پست به دو بخش فیزیکی و سایبری تقسیم می‌شود. بخش فیزیکی، تجهیزات سخت‌افزاری را شامل می‌شود، درحالی‌که بخش سایبری شامل منابع فیزیکی و نرم‌افزاری می‌شود. تهدیدات حملات سایبری نسبت به گذشته بیشتر شده است چراکه ارتباطات و دسترسی از راه دور برای نگهداری پست‌ها بیشتر شده است.

۵- روش‌های دفاعی در پست‌های فشارقوی

شبکه هوشمند دارای چند لایه شبکه بوده و هر لایه شبکه و فناوری مورد استفاده، بیانگر یک مسیر مستعد برای حمله می‌باشد. در پست‌ها با افزایش سطح اتوماسیون، افزایش

1- Advanced Metering Infrastructure

آسیب‌پذیری‌های بالقوه در عناصرکنترلی- الکترونیکی را به‌دنبال خواهد داشت. جهت تأمین دفاع مناسب در پست‌های فشارقوی ضروری است که آن‌ها با حداقل هزینه تأمین شده و تا حد ممکن کمتر به عوامل انسانی نیازمند باشند. امروزه سیستم کنترلی شبکه قدرت معیارهای اندازه‌گیری کافی برای تضمین اقدامات حفاظتی در برابر حملات سایبری یا فیزیکی مخرب را دارا نیست که این امر آن‌را بسیار آسیب‌پذیر می‌کند. الگوریتم‌های دفاعی می‌بایست یک ترکیب جامع از دفاع سایبری و دفاع شبکه الکتریکی را ایجاد کند. کاربر نهایی، شرکت توانیر (مدیریت شبکه برق) است که در بخش مرکز کنترل ملی بایستی به این موضوع توجه شود. لازم به ذکر است که از نقطه‌نظر توانیر، این موضوع فقط به هزینه‌های اقتصادی ناشی از قطع برق و خسارات مستقیم آن باز می‌گردد، حال آن‌که، شرکت توانیر در به‌کارگیری این مدل جهت متغیرهای ورودی از جمله (d_i) باید ملاحظات سازمان‌های دفاعی کشور یا پلیس امنیت سایبری را نیز جویا شود و درصورت درخواست آن‌ها جهت هزینه‌های مازاد در استفاده از مدل مذکور، هماهنگی‌های بودجه‌ای فی‌مابین را به انجام رساند. از جمله روش‌هایی که برای افزایش سطح امنیت پست‌های فشارقوی می‌توان استفاده کرد به شرح زیر خواهد بود:

۵-۱- محافظ کابل

پالس‌های الکترومغناطیسی، میدان‌هایی از انرژی هستند که می‌توانند در یک‌بار با القاء ولتاژ و ایجاد خطر[1] یا نویز یا تبدیل و تغییر در اطلاعات دیجیتال باعث صدمه به مدارات الکتریکی و الکترونیکی شوند. فن‌آوری مدارات میکروالکترونیک نسبت به تداخل قدرت حساس می‌باشند. خطر عمدی یا غیرعمدی و ایجاد خسارات جبران‌ناپذیر و پیش‌بینی‌نشده، برای تداخل الکترومغناطیسی از نقطه‌نظر 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 القاء در هادی‌های حامل ولتاژهای پایین می‌نمایند. در هر محفظه فلزی مشتمل بر مجموعه‌ای از تجهیزات الکتریکی و الکترونیکی و سیم‌های انتقال، موضوع سازگاری الکترومغناطیسی (EMC)[2] اساس طراحی محسوب می‌شود. تولید عمدی و خرابکارانه انرژی الکترومغناطیسی به‌صورت اعمال نویز یا سیگنال به سیستم‌های الکتریکی و الکترونیکی منجر به اختلال، اغتشاش یا آسیب به این سیستم‌ها برای اهداف تبهکارانه یا تروریستی می‌شود. از آن‌جا که یکی از روش‌های اختلال از طریق محیط انتقال است، روش‌های ایجاد ایمن‌سازی انتقال در مقابل میدان‌های تداخلی مورد توجه قرار می‌گیرد. تجهیزات به دو گروه EMC جریان بالا (قدرت) و جریان پایین (الکترونیکی- دیجیتال) دسته‌بندی می‌شود. بدیهی است که تجهیزات قدرت، به‌دلیل حمل جریان بزرگ، تولیدکننده میدان مغناطیسی تشعشعی برای ادوات الکترونیکی و کنترلی هستند. کابل‌هایی که برای حمل اطلاعات در سیستم استفاده می‌شوند و کابل‌هایی که حاوی سیگنال‌های نمایشگر و اندازه‌گیری و ارسال فرامین هستند به‌عنوان کابل‌های حساس در نظر گرفته می‌شوند، این‌ها تحت تأثیر میدان‌های تداخلی موجود قرار می‌گیرند. رابطه زیر ارتباط سازگاری الکترومغناطیسی را با میدان‌های پراکندگی تزاحمی نشان می‌دهد.

$$EMC \propto \frac{\sum_{k=1}^{p} I\left(B_{pu,Max}^{k}-\Delta B_{pu,Max}^{k}\right)*a_{1k}+\left(B_{pu,avg}^{k}-\Delta B_{pu,avg}^{k}\right)*a_{2k}]}{[(a_{1Max})_{Selected}+(a_{2Max})_{Selected}]} \quad (۸)$$

که در آن، B_{avg} و B_{Max} مقادیر میدان‌های پراکندگی تزاحمی حاصل از شبیه‌سازی میدان و یا اندازه‌گیری است. i تعداد کابل‌های مورد اشاره و ضرایب α_1 و α_2 ضرایب تصحیح با توجه به کاربرد هستند که $\alpha_2 \leq \alpha_1$ و $1 \leq \alpha_1 \leq 10$ و $1 \leq \alpha_2 \leq 5$ می‌باشند. کاهش میدان تزاحمی می‌تواند با روش‌های مختلفی از جمله کابل مجازی مد مشترک، لوله فلزی صورت گرفته و با ΔB^i مدل‌سازی می‌گردد که با روابط زیر قابل محاسبه می‌باشد:

$$SE = 20log\frac{B_{out}^{k}}{B_{in}^{k}} \quad (۹)$$

$$SE = 3.4t\sqrt{\mu_r\sigma_r f} + 168 - 10\,log_{10}(\frac{\mu_r f}{\sigma_r}) \quad (۱۰)$$

که در آن، t ضخامت شیلد و r فاصله منبع از شیلد بر حسب اینچ می‌باشد. μ_r ضریب گذردهی مغناطیسی ماده شیلد و σ_r ضریب هدایت الکتریکی ماده شیلد می‌باشد. SE[3] میزان مؤثربودن یک شیلد، کمیتی است که مؤثربودن شیلد را در کاهش امواج الکترومغناطیسی تابیده‌شده، نشان می‌دهد [۱۹-۱۷]. تهدید تداخل الکترومغناطیسی در زمانی‌که سلاح الکترومغناطیسی درون یک ساک یا چمدان قرار گرفته، می‌تواند درون یک ساختمان با نزدیک‌شدن زیاد به مدارهای الکترونیکی حساس اعمال شود. از آن‌جا که تهدید ماهیت الکترومغناطیسی

1- Hazard
2- Electromagnetic Compatibility
3- Shielding Effectiveness

دارد، آشفتگی و آسیب به تجهیز بدون هیچ نشانه‌ای می‌تواند رخ دهد. یک دشمن با سلاح الکترومغناطیسی قوی می‌تواند به‌صورت بالقوه بهره‌برداری از چندین تجهیز را تنها با حرکت از یک محل به محل دیگر مختل کند. لذا به‌عنوان بهترین و کم‌هزینه‌ترین روش‌های تکنولوژی‌های شیلدینگ فرکانس بالا (بالاتر از یک مگاهرتز)، زمین‌کردن، اتصال و محافظ کابل در کابل‌های کنترلی و ارتباطی در پست‌های فشارقوی اعمال می‌گردد [۲۰].

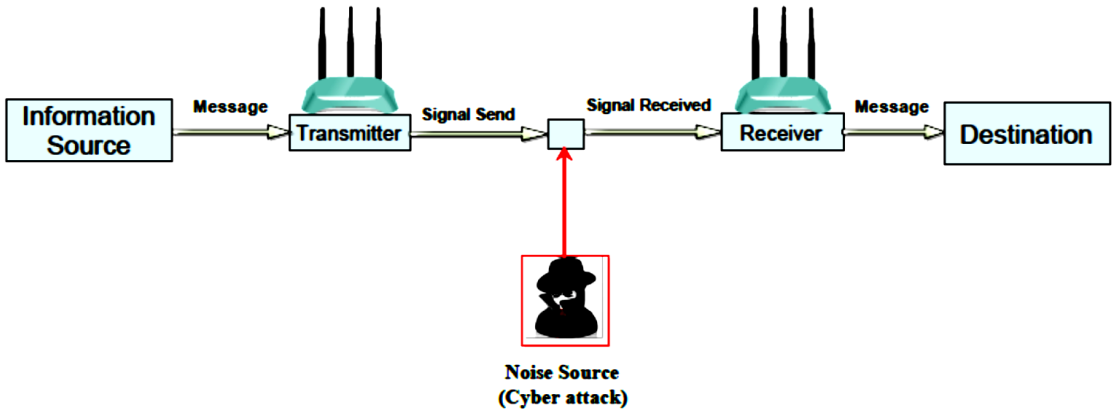
۵-۲- نرم افزار

نرم‌افزارهای به‌کاررفته در سیستم اتوماسیون پست‌های فشارقوی به‌منظور افزایش میزان دفاع سایبری مشتمل بر آنتی‌ویروس، سیستم تشخیص و ممانعت از نفوذ، فایل‌های سیستم، نرم‌افزار دائمی، نرم‌افزارهای مربوط به دیواره آتش و روتر، کدینگ، رمزنگاری و احراز هویت و غیره می‌باشد. یک تابع چکیده‌ساز نوعی تبدیل است که رشته‌ای طولانی را به‌عنوان ورودی دریافت می‌کند و رشته‌ای با طول ثابت را در خروجی می‌دهد. پس از احراز اصالت برای مبادله پیام از متن رمزشده استفاده می‌گردد [۲۱]. از توابع درهم‌سازی برای بررسی صحت پیام‌ها و امضای دیجیتال متون در طیف گسترده‌ای از کاربردها، همچون تصدیق اصالت و تصدیق صحت پیام استفاده می‌شود. توابع درهم یا درهم‌ساز به‌عنوان توابع مهم در مباحث امنیتی به‌کار می‌روند. پس از انتقال مقادیر زیاد اطلاعات، بررسی این‌که آیا توسط دشمن جعل شده است، مهم می‌باشد. در کانال‌های ناامن مثل اینترنت، نیاز به روشی است که قادر به بررسی‌نمودن صحت و تمامیت یک پیام و همچنین تصدیق فرستنده اصلی آن باشد. این امر می‌تواند با استفاده از توابع رمزنگاری به‌دست آید [۲۲].

با توجه به وقوع حملات سایبری که می‌تواند منجر به نویز و ایجاد خطا در مسیر ارسال اطلاعات شود، ضروری است که جهت کاهش نرخ خطا و تأیید انتقال اطلاعات از کدینگ کانال در انتقال سیگنال استفاده شود. در یک کانال مخابراتی با قدرت سیگنال S (برحسب وات) و قدرت نویز N (بر حسب وات) و درصورتی‌که کانال دارای عرض باند W (برحسب هرتز) باشد، طبق رابطه شانون ظرفیت کانال از رابطه زیر محاسبه می‌گردد [۲۳].

$$C = W log_2\left(1+\frac{S}{N}\right) \qquad \frac{bits}{second} \qquad (۱۱)$$

برای رسیدن به ظرفیت‌های قابل توجه در رابطه فوق، عموماً راهی جز استفاده از کدینگ کانال وجود ندارد. همیشه در سامانه‌های انتقال دیجیتال از کدینگ کانال برای افزایش بهره طیفی و کاهش احتمال خطای سامانه استفاده می‌شود. بلوک دیاگرام شکل (۳) وضعیت کدینگ و دکدینگ را نشان می‌دهد. کانال‌های شیلدشده در مقابل نویز نسبت به کانال‌های شیلدنشده بسیار ایمن‌تر می‌باشد و ظرفیت کانال شیلدشده مقدار اطلاعات بیشتری را نسبت به حالت شیلدنشده تحویل می‌دهد.



شکل (۳): تأثیر حملات سایبری بر سیستم ارتباطی و تأثیر به‌کارگیری کدینگ

۵-۳- سخت افزار

تجهیزات دفاع سایبری که به‌صورت سخت‌افزاری در پست به‌کار گرفته می‌شوند عبارتند از:

دیواره آتش: عموماً دیواره‌های آتش شبکه‌های دیجیتالی را محدود و ترافیک آن‌ها را کنترل می‌کنند. دیواره آتش‌ها نه تنها از ارتباطات غیرمجاز جلوگیری به‌عمل می‌آورند، در عین حال براساس قواعد تعریف‌شده توسط کاربر و پیکربندی صورت‌گرفته یک ترافیک مجاز و قانونی را ایجاد می‌نمایند.

1- Firmware
2- Hash Function

شبکه خصوصی مجازی (VPN)[1]: VPNها اتصالات رمزگذاری شده مطمئن را به‌وجود می‌آورند و به‌عنوان تونلی بین تجهیزات ایستگاه مشتری[2] و سرور در یک شبکه ناامن مثل اینترنت استفاده می‌شود. به‌عنوان مثال، یک VPN برای ایستگاه پردازشگر می‌تواند یک لب‌تاپ تعمیر و نگهداری[3] باشد و VPN مربوط به سرور می‌تواند یک وسیله امنیتی نصب‌شده در شبکه کنترل باشد. معمولاً Client ارتباط را ایجاد می‌کند و سرور درخواست ارتباط ورودی را با احراز هویت از یک یا چند Client مورد تأیید قرار می‌دهد. به‌عبارت دیگر، یک ارتباط خصوصی و امن بین مبدأ و مقصد با ایجاد تونل در شبکه WAN انجام می‌گردد. برای اطمینان از امنیت شبکه ضروری است که VPN به‌صورت یکپارچه با یک دیواره آتش ترکیب شود [۲۴].

همچنین تجهیزاتی نظیر روتر[4] و سویچ‌های اترنت[5] و دروازه عبور[6] که در جلوگیری از نفوذ غیرمجاز از طریق پروتکل‌های ارتباطی ممانعت به‌عمل می‌آورند، می‌تواند مورد استفاده قرار گیرد.

۵-۴- مسیریابی

مسیریابی بهینه در پست‌های فشارقوی با توجه به فرضیات زیر صورت می‌گیرد:

۱) مسیر مربوطه دور از منابع تولید میدان تداخلی از جمله ترانسفورماتورهای قدرت باشد.

۲) کمترین مسیر با درنظرگرفتن قیمت و افت ولتاژ صورت گیرد.

۳) مسیرهای انتخابی با حداقل اختلال الکترومغناطیسی ضمن کلیدزنی یا سوئیچینگ در پست باشد تا از احتمال وقوع اضافه/ کاهش ولتاژ و اضافه جریان جلوگیری به‌عمل آید.

با توجه به فرضیات فوق و با توجه به مشخصات فنی پست‌های فشارقوی معیارهای زیر می‌تواند برای انتخاب مسیر بهینه و مناسب در سطح پست لحاظ شود:

- هزینه: به‌واسطه کابل‌ها و کانال‌های کابل متعدد در پست معیار قیمت مهم می‌باشد.
- افت ولتاژ: با توجه به فواصل نسبتاً دور کابل‌ها در داخل پست‌های فشارقوی این معیار نیز بسیار مهم می‌باشد.
- سازگاری الکترومغناطیسی (EMC): عدم توجه به سازگاری الکترومغناطیسی و وجود تداخل الکترومغناطیسی می‌تواند منجر به عملکرد غلط در انتقال داده‌ها در پست شود.

با روش‌هایی نظیر شبیه‌سازی شدت میدان تداخلی و شناسایی نقاط ضعیف، مسیر بهینه و مناسب کابل‌های ارتباطی مشخص می‌گردد. همچنین، استفاده از لوله فلزی در محل‌های دارای میدان زیاد هادی‌ها را در مقابل میدان تداخلی موضعی حفاظت می‌نماید [۱۹-۱۷].

براساس موارد فوق، حداقل و حداکثر هزینه‌های دفاعی مستخرج از مراجع[7] به شرح جدول (۱) قابل ارائه می‌باشد:

جدول (۱): هزینه‌های دفاع سایبری پست‌های فشارقوی

آیتم دفاعی	حداقل و حداکثر هزینه براساس اطلاعات استخراج شده از مراجع داخلی و خارجی (دلار)
تجهیزات سخت‌افزاری مشتمل بر دیواره آتش، روتر VPN، Gateway، سیستم تشخیص نفوذ و ...	۳۰۰۰=۸۰۰۰
نرم‌افزار شامل نرم‌افزارهای مربوط به دیواره آتش، کدینگ، رمزنگاری و تشخیص هویت و ...	۹۰۰=۲۰۰۰
مسیر بهینه کابل‌های اطلاعات به‌منظور حداقل‌سازی اثر میدان و سازگاری الکترومغناطیسی	۵۰۰۰=۷۰۰۰
شیلددار نمودن کابل‌های ارتباطی به منظور جلوگیری از تأثیر میدان‌های اطراف و جلوگیری از تداخل اطلاعات	۱۰۰۰=۴۰۰۰

۶- روش تحلیل سلسله مراتبی فازی برای حداقل‌سازی هزینه دفاعی

تصمیم‌گیری چندمعیاره برپایه چندین شاخص، گزینه یا انتخاب رتبه‌بندی می‌گردد. روش‌های مختلفی برای تصمیم‌گیری

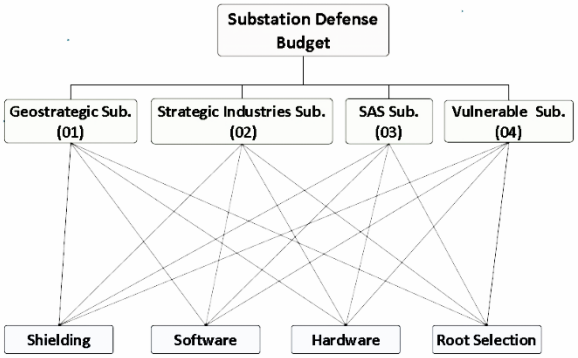
1- Virtual Private Network
2- Client
3- Maintenance
4- Router
5- Ethernet Switch
6- Gateway

۷- اطلاعات تجهیزات سخت‌افزاری و نرم‌افزاری با توجه به قیمت اخذشده از سازندگان MOXA و WESTERMI تکمیل شده است.

چندمعیاره وجود دارد که یکی از مهم‌ترین آن‌ها روش تحلیل سلسله مراتبی فازی (FAHP)[1] می‌باشد. در این روش، یک وضعیت پیچیده، به بخش‌های کوچک‌تر آن تجزیه شده، سپس این اجزا در یک ساختار سلسله مراتبی قرار گرفته و قضاوت‌های ذهنی با توجه به اهمیت هر متغیر اختصاص داده می‌شود و متغیرهایی که بیشترین اهمیت را دارند، مشخص می‌گردند. در ابتدا لازم است معیارهای گزینش به‌درستی تعیین و ارزش هریک مشخص شود. چانگ در سال ۱۹۹۲ روشی بسیار ساده را برای بسط فرآیند تحلیل سلسله مراتبی به فضای فازی ارائه داد. این روش که مبتنی‌بر میانگین حسابی نظرات خبرگان و روش طبیعی ساعتی و با استفاده از اعداد مثلثی فازی توسعه داده شده بود، مورد استقبال محققین قرار گرفت.

۶-۱- درخت سلسله مراتبی و تعیین معیارها و گزینه‌ها

روند تعیین بودجه دفاعی در پست‌های فشارقوی به عوامل مختلفی بستگی دارد. روش تحلیل سلسله مراتبی برای تعیین وزن هر عامل در شکل (۴) نشان داده می‌شود. اولین لایه، لایه هدف است که برای تعیین مقدار بودجه دفاعی مورد استفاده قرار می‌گیرد. لایه دوم، لایه معیارها، شامل قرارگرفتن پست‌ها در مناطق جغرافیایی با راه‌برد خاص (شامل نقاط مرزی، نواحی خاص اقلیمی و جزایر کشور و ...)، پست‌های مورد استفاده در صنایع مهم و راه‌بردی (شامل صنایع نفتی و پتروشیمی، فولاد و نیروگاه‌ها و ...)، پست‌های با توجه به ملاحظات فنی و سیستم کنترلی آن‌ها (شامل سیستم کنترل سنتی، کنترل SAS و...) و پست‌های آسیب‌پذیر دارای مخاطرات مخابراتی و سیگنالیسم می‌باشد. لایه سوم، لایه گزینه‌ها شامل عوامل اساسی در امنیت سایبری از جمله حفاظت، نرم‌افزار، سخت‌افزار و انتخاب مسیر بهینه کابل‌های ارتباطی می‌باشد.



شکل (۴): درخت سلسله مراتبی تعیین بودجه دفاعی پست

1- Fuzzy Analytical Hierarchy Process

۶-۲- نتایج تحلیل سلسله مراتبی فازی در تحلیل حمله و دفاع سایبری پست

با توجه به این‌که ارائه قضاوت به‌صورت کلامی برای تصمیم‌گیری آسان‌تر از ارائه پاسخ به‌صورت قطعی است، لذا به‌کارگیری مفاهیم فازی در تصمیم‌گیری اهمیت بیشتری دارد. روش «چانگ» [۲۵] با استفاده از اعداد مثلثی فازی در روش تحلیل سلسله مراتبی فازی بیشتر مورد استفاده قرار می‌گیرد. به‌منظور ایجاد اعداد فازی و به‌علت تطابق بیشتر با مشخصات پرسش‌نامه و دقت بیشتر نتایج، از اعداد موجود در جدول (۲) استفاده شده است.

جدول (۲): اعداد فازی تعریف شده در روش تحلیل سلسله مراتبی فازی

عدد فازی مثلثی	عبارت زبانی
(۸،۹،۱۰)	Perfect
(۷،۸،۹)	Absolute
(۶،۷،۸)	Very good
(۵،۶،۷)	Fairly good
(۴،۵،۶)	Good
(۳،۴،۵)	Preferable
(۲،۳،۴)	Not bad
(۱،۲،۳)	Weak advantage
(۱،۱،۱)	Equal

ماتریس مقایسه زوجی با بهره‌گیری از اعداد فازی مثلثی به‌صورت M=(l,m,u) به‌کار می‌رود.

$$M_1 + M_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2) \qquad (۱۲)$$

$$M_1 \times M_2 = (l_1 \times l_2, m_1 \times m_2, u_1 \times u_2) \qquad (۱۳)$$

$$M_1^{-1} = (\frac{1}{u_1}, \frac{1}{m_1}, \frac{1}{l_1}) \qquad (۱۴)$$

$$M_2^{-1} = (\frac{1}{u_2}, \frac{1}{m_2}, \frac{1}{l_2}) \qquad (۱۵)$$

با استفاده از نظر تصمیم‌گیرنده، ماتریس مقایسه زوجی $\tilde{A}$ با بهره‌گیری از اعداد فازی مثلثی براساس نظرات چندین تصمیم‌گیرنده تشکیل می‌شود [۲۶].

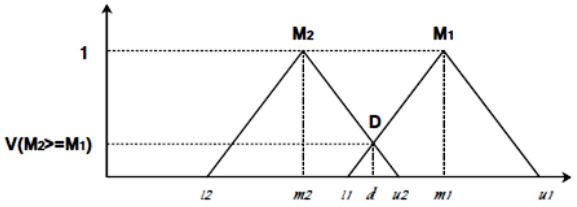
$$\tilde{A} = \begin{bmatrix} (1,1,1) & (a_{12}^l, a_{12}^m, a_{12}^u) & \cdots & (a_{1n}^l, a_{1n}^m, a_{1n}^u) \\ \left(\frac{1}{a_{21}^u}, \frac{1}{a_{21}^m}, \frac{1}{a_{21}^l}\right) & (1,1,1) & \cdots & (a_{2n}^l, a_{2n}^m, a_{2n}^u) \\ \vdots & \vdots & \vdots & \vdots \\ \left(\frac{1}{a_{m1}^u}, \frac{1}{a_{m1}^m}, \frac{1}{a_{m1}^l}\right) & \left(\frac{1}{a_{m2}^u}, \frac{1}{a_{m2}^m}, \frac{1}{a_{m2}^l}\right) & \cdots & (1,1,1) \end{bmatrix} \qquad (۱۶)$$

برای هریک از سطرهای ماتریس مقایسه زوجی، S_k که خود یک عدد فازی مثلثی است به‌صورت زیر انجام می‌شود:

$$S_k = \sum_{j=1}^{n} M_{kj} \times [\sum_{i=1}^{m}\sum_{j=1}^{n} M_{ij}]^{-1} \quad (۱۷)$$

که در آن، k بیانگر شماره سطر، i و j به‌ترتیب نشان‌دهنده گزینه‌ها و معیارها می‌باشند. پس از تعیین S_k ها، درجه بزرگی آن‌ها نسبت به هم بایستی مشخص شود. به‌طورکلی، اگر M1 و M2 دو عدد فازی مثلثی مطابق شکل (۵) باشند، درجه بزرگی M_2 نسبت به M_1 به‌صورت زیر خواهد بود:

$$V(M_2 \geq M_1) = \begin{cases} 1 & if\ m_2 \geq m_1 \\ 0 & if\ l_2 \geq u_1 \\ hgt(M_1 \cap M_2) = \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)} & otherwise \end{cases} \quad (۱۸)$$



شکل (۵): اولویت دو عدد فازی مثلثی

برای مقایسه M_1 و M_2 محاسبه هر دو مقدار $V(M_2 \geq M_1)$, $V (M_1 \geq M_2)$ ضروری است. درجه احتمال بزرگ‌تربودن یک عدد فازی محدب (M) از K عدد فازی محدب دیگر $(M_i; i = 1,2,\ldots,k)$ به‌صورت زیر تفکیک می‌شود:

$$d(M) = V(M \geq M_1, M_2, \ldots, M_k) = V[(M \geq M_1), (M \geq M_2), \ldots, (M \geq M_k)] = \min V(M \geq M_i) \quad i = 1,2,\ldots,k \quad (۱۹)$$

با نرمالیزه‌کردن بردار وزن‌ها، وزن‌های نرمالیزه‌شده به‌دست می‌آیند:

$$W = [\frac{d(A_1)}{\sum_{i=1}^{n} d(A_i)}, \frac{d(A_2)}{\sum_{i=1}^{n} d(A_i)}, \ldots, \frac{d(A_n)}{\sum_{i=1}^{n} d(A_i)}]^T \quad (۲۰)$$

وزن‌های فوق، وزن قطعی (غیرفازی) هستند. با تکرار این فرایند، اوزان تمامی ماتریس‌ها به‌دست می‌آید. با انجام این محاسبات، نتایج به‌ترتیب زیر به‌دست می‌آید. ماتریس مقایسه زوجی معیارها نسبت به هم به‌صورت جدول (۳) خواهد بود.

جدول (۳). وزن معیارها نسبت به هم

	Geostrategic	Strategic Industries	SAS	Vulnerable
Geostrategic	(۱،۱،۱)	(۱،۱،۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۰/۲۵ ، ۰/۳۳۳ ، ۰/۵)
Strategic Industries	(۱،۱،۱)	(۱،۱،۱)	(۰/۲ ، ۰/۲۵ ، ۰/۳۳۳)	(۰/۱۶۶ ، ۰/۲ ، ۰/۲۵)
SAS	(۱،۲،۳)	(۳،۴،۵)	(۱،۱،۱)	(۰/۲۵ ، ۰/۳۳۳ ، ۰/۵)
Vulnerable	(۲،۳،۴)	(۴،۵،۶)	(۲،۳،۴)	(۱،۱،۱)

مقادیر مقایسه زوجی گزینه‌ها نسبت به هر معیار در جداول (۴-۷) ارائه شده است.

جدول (۴): وزن گزینه‌ها نسبت به معیار پست‌های Geostrategic

	Shielding	Software	Hardware	Route Selection
Shielding	(۱،۱،۱)	(۳،۴،۵)	(۱،۱،۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Software	(۰/۲ ، ۰/۲۵ ، ۰/۳۳۳)	(۱،۱،۱)	(۰/۲ ، ۰/۲۵ ، ۰/۳۳۳)	(۰/۱۴۲ ، ۰/۱۶۶ ، ۰/۲)
Hardware	(۱،۱،۱)	(۳،۴،۵)	(۱،۱،۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Route Selection	(۱،۲،۳)	(۵،۶،۷)	(۱،۲،۳)	(۱،۱،۱)

جدول (۵): وزن گزینه‌ها نسبت به معیار پست‌های Strategic Industries

	Shielding	Software	Hardware	Route Selection
Shielding	(۱،۱،۱)	(۱،۱،۱)	(۱،۱،۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Software	(۱،۱،۱)	(۱،۱،۱)	(۰/۲ ، ۰/۲۵ ، ۰/۳۳۳)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Hardware	(۲،۳،۴)	(۳،۴،۵)	(۱،۱،۱)	(۱،۲،۳)
Route Selection	(۱،۲،۳)	(۱،۲،۳)	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۱،۱،۱)

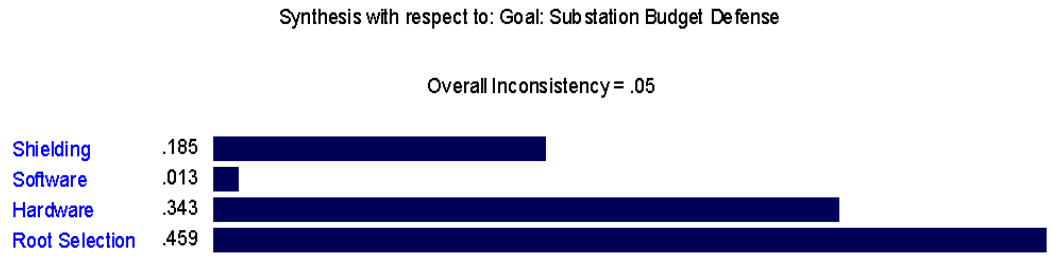
جدول (۶): وزن گزینه‌ها نسبت به معیار پست‌های با سیستم کنترل SAS

	Shielding	Software	Hardware	Route Selection
Shielding	(۱،۱،۱)	(۱،۲،۳)	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Software	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۱،۱،۱)	(۰/۲ ، ۰/۲۵ ، ۰/۳۳۳)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Hardware	(۲،۳،۴)	(۳،۴،۵)	(۱،۱،۱)	(۱،۲،۳)
Route Selection	(۱،۲،۳)	(۱،۲،۳)	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۱،۱،۱)

جدول (۷): وزن گزینه‌ها نسبت به معیار پست‌های مخاطره‌آمیز

	Shielding	Software	Hardware	Route Selection
Shielding	(۱،۱،۱)	(۱،۲،۳)	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Software	(۰/۳۳۳ ، ۰/۵ ، ۱)	(۱،۱،۱)	(۰/۲۵ ، ۰/۳۳۳ ، ۰/۵)	(۰/۱۶۶ ، ۰/۲ ، ۰/۲۵)
Hardware	(۱،۱،۱)	(۲،۳،۴)	(۱،۱،۱)	(۰/۳۳۳ ، ۰/۵ ، ۱)
Route Selection	(۱،۲،۳)	(۴،۵،۶)	(۱،۲،۳)	(۱،۱،۱)

وزن نهایی و انتخاب گزینه برتر در بودجه دفاعی پست‌های فشار قوی در شکل (۶) نشان داده شده است.



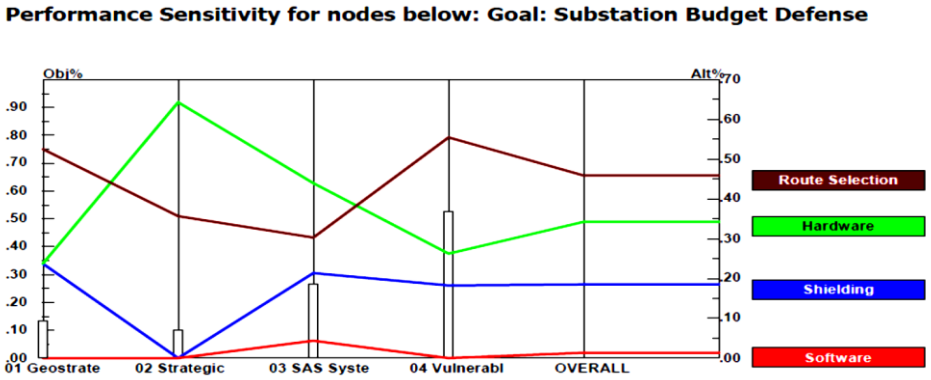
شکل (۶): وزن نهایی گزینه‌ها نسبت به معیارها

با توجه به مقادیر نهایی ملاحظه می‌شود که مسیریابی کابل‌های ارتباطی بیشترین تأثیر را در ارزیابی بودجه دفاع سایبری پست‌های مورد مطالعه دارد که با توجه به هزینه کابل‌ها و همچنین، به‌کارگیری آن‌ها خصوصاً در کاندوئیت پیوسته جهت جلوگیری از اثرات میدان، بیشترین بودجه را خواهد داشت. پس از مسیریابی بهینه کابل‌ها، اولویت بعدی هزینه دفاعی سخت‌افزاری در سطح اتوماسیون پست ازقبیل دیواره آتش، سوئیچ‌های روتر VPN و سیستم‌های تشخیص نفوذ می‌باشد. بعد از این دو مورد، شیلددارکردن کابل‌های ارتباطی قرار دارد که با تجربیات قبلی حدوداً ۱۵ ٪ افزایش هزینه را در پست‌ها در پی دارد. همان‌طور که پیش‌بینی می‌شد نرم‌افزار به‌تنهایی هزینه چندانی ندارد و بدون تجهیزات سخت‌افزاری کاربرد قابل‌توجهی ندارد.

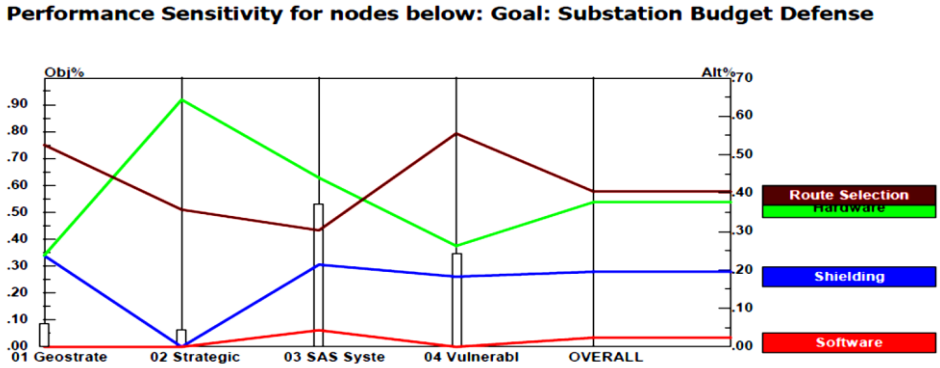
۶-۳- تحلیل حساسیت

یکی از مهم‌ترین شاخص‌های قضاوت درخصوص صحت نتایج مدل ارائه‌شده، استفاده از تحلیل حساسیت است. در تحلیل حساسیت تأثیر جابه‌جایی وزن معیارها بر تغییر رتبه‌بندی گزینه‌ها مورد ارزیابی قرار می‌گیرد. لذا وزن هر معیار با وزن سایر معیارها به‌صورت دو به دو جابه‌جا شده و با محاسبه وزن نهایی گزینه‌ها، تغییرات صورت‌گرفته در رتبه‌بندی نهایی آن‌ها مورد تجزیه و تحلیل قرار می‌گیرد. نتایج حاصل از تحلیل حساسیت مدل ارائه‌شده برای انتخاب مناسب‌ترین هزینه دفاعی پست‌های فشارقوی در شکل (۷) آمده است. در این نمودار، مورد مسیریابی بهینه کابل‌های ارتباطی به‌عنوان اولویت نخست در بودجه دفاعی در مقابل حملات سایبری می‌باشد. با جابه‌جایی صورت‌گرفته در وزن معیارها تغییری در رتبه‌بندی گزینه‌ها حاصل نمی‌شود و همان‌طورکه در اشکال (۹-۸) ملاحظه می‌شود با جابه‌جایی وزن معیارهای پست‌های فشارقوی از دیدگاه سیستم‌های اتوماسیون و کنترلی و پست‌های فشارقوی از دیدگاه مخاطره‌آمیزبودن با اختلاف ناچیز، رتبه‌بندی کماکان برقرار است و همچنین، با تغییر وزن معیارهای پست‌های فشارقوی راه‌بردی صنعتی و پست‌های

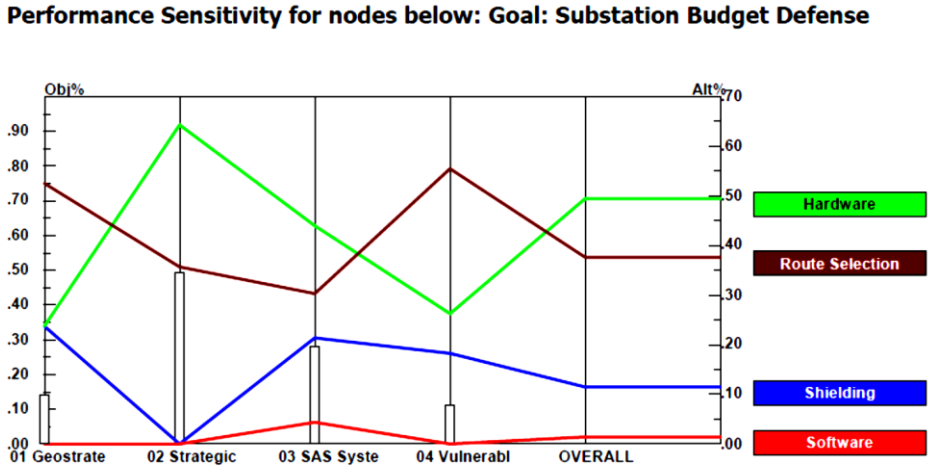
فشارقوی از دیدگاه مخاطره‌آمیزبودن، گزینه تجهیزات سخت‌افزاری با اختلاف ناچیزی در رتبه نخست نسبت به مسیریابی بهینه کابل‌های ارتباطی قرار می‌گیرد.



شکل (۷): تحلیل حساسیت با توجه به وزن‌های نهایی محاسبه‌شده



شکل (۸): تحلیل حساسیت با جابه‌جایی وزن معیارهای پست‌های فشارقوی از دیدگاه سیستم‌های اتوماسیون و کنترلی و پست‌های فشارقوی از دیدگاه مخاطره‌آمیزبودن



شکل (۹): تحلیل حساسیت با جابجایی وزن معیارهای پست‌های فشار قوی راهبردی صنعتی و پست‌های فشار قوی از دیدگاه مخاطره‌آمیز بودن

۷- نتیجه‌گیری

برای کاهش آسیب‌پذیری و جلوگیری از حملات سایبری در پست‌های فشارقوی، امنیت آن‌ها دارای اهمیت فراوان می‌باشد. توسعه پست‌های فشارقوی با دفاع سایبری بهینه مورد انتظار سیستم، این اطمینان را می‌دهد که آن‌ها در حضور حملات سایبری عملکرد قابل اطمینانی خواهند داشت. در این مقاله، براساس محل و نوع استفاده از پست‌های فشارقوی، آن‌ها به چهار دسته ژئواستراتژیک، راه‌بردی صنعتی، سیستم‌های اتوماسیون و کنترلی و مخاطره‌آمیزبودن طبقه‌بندی شده‌اند. با روش تصمیم‌گیری تحلیل سلسله مراتبی فازی، تابع هزینه دفاعی در هر پست که مشتمل بر تجهیزات سخت‌افزاری و نرم‌افزاری و مسیریابی بهینه کابل‌های انتقال اطلاعات و محافظ کابل می‌باشد، ارائه شده است. درصدهای بودجه‌ای برای هر کدام از این آیتم‌های دفاعی با این روش به‌دست می‌آید که چگونگی پیاده‌سازی آن در این مقاله به تفصیل ارائه شده است. تصمیم‌گیری بین مدافع و مهاجم به‌صورت همزمان انجام می‌گیرد و به‌عنوان کار آینده، تصمیم‌گیری به‌صورت ترتیبی می‌تواند مورد تحلیل قرار گیرد. از روش‌های دفاعی معرفی‌شده، مسیر بهینه برای کابل‌های ارتباطی و تجهیزات سخت‌افزاری به‌کار رفته در پست‌ها از اهمیت بیشتری نسبت به سایر موارد برخوردار بوده و وزن بیشتری را به خود اختصاص می‌دهند.

۸- مراجع

[1] Y. Xiang, Z. Ding, and L. Wang, "Power system adequacy assessment with load redistribution attacks," in Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society, Washington, DC, USA, pp. 1-5, 18-20 Feb. 2015.

[2] V. Bier, S. Oliveros, and L. Samuelson, "Choosing what to protect: Strategic defensive allocation against an unknown attacker," Journal of Public Economic Theory, vol. 9, pp. 563-587, July 2007.

[3] G. Dondossola, F. Garrone, and J. Szanto, "Cyber risk assessment of power control systems, A metrics weighed by attack experiments," in Power and Energy Society General Meeting, 2011 IEEE, Detroit, MI, USA, pp. 1-9, 24-29 July 2011.

[4] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," IEEE Transactions on Power Systems, vol. 31, pp. 4379-4394, Jan. 2016.

[5] T. S. Popik, "Testimony of the Foundation for Resilient Societies," in Reliability Technical Conference, Federal Energy Regulatory Commission, Docket No. AD16-15-000, pp. 1-15, June 2016.

[6] K. Stouffer, J. Falco, and K. Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Recommendations of the National Institute of Standards and Technology," NIST Standard Special Publication 800-82, Sep. 2006.

[7] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), 2016.

[8] L. 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. 9, pp. 684 – 694, May 2016.

[9] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," IEEE Transactions on Smart Grid, vol. 7, pp. 2260-2272, Aug. 2015.

[10] J. Yue and K. Zhang, "Vulnerability Threat Assessment Based on AHP and Fuzzy Comprehensive Evaluation," in Computational Intelligence and Design (ISCID), 2014 Seventh International Symposium on, Hangzhou, China, pp. 513-516, 13-14 Dec. 2014.

[11] S. K. Khaitan, J. D. McCalley, and C. C. Liu, "Cyber physical systems approach to smart electric power grid," Springer, 2015.

[12] W. Al Mannai and T. Lewis, "A general defender-attacker risk model for networks," The Journal of Risk Finance, vol. 9, pp. 244-261, 2008.

[13] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," IEEE Transactions on Smart Grid, vol. 7, pp. 669-683, June 2015.

[14] "Cyber Security for Substation Automation Systems by ABB," Dec. 2010.

[15] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Transactions on Power Systems, vol. 23, pp. 1836-1846, Oct. 2008.

[16] A. Creery and E. Byres, "Industrial cybersecurity for power system and SCADA networks, " in Petroleum and Chemical Industry Conference, Industry Applications Society 52nd Annual, Denver, CO, USA, pp. 303-309, 12-14 Sept. 2005.

[17] H. Heydari, F. Faghihi, and V. Abbasi, "Optimization of Conductor routs within Metal Enclosure of the Electrical Equipments based on EMC Approach Using Multi criteria Decision Making Case Study: Metal Enclosure of Current Injection System," Modares Technical And Engineering, no. 38, pp. 1–16, 2010. (In Persian)

[18] F. Faghihi, H. Heydari and V. Abbasi, "Optimization of Conductor routs within Metal Enclosure of the Electrical Equipments based on EMC Approach Using Multi criteria Decision Making Case Study: Metal Enclosure of Current Injection System," Journal of Algorithms and Computation, vol. 43, pp. 681–692, 2009. (In Persian)

[19] V. Abbasi, H. Heydari, and F. Faghihi, "Heuristic mathematical formulations and comprehensive algorithm for optimal decision making for power system cabling," Scientia Iranica, vol. 19, pp. 707-720, June 2012.

[20] "High-Impact, Low-Frequency Event Risk (HILF) to the North American Bulk Power System," Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy, Nov. 2009.

[21] A. B. Mirghadri, R. Shirbanian, and A. Mirghadri, "A New Lightweight Authentication Scheme for Wireless Sensor Networks," Journal of Electronical & Cyber Defence, vol. 4, no. 3, pp.1–10, 2016. (In Persian)

[22] B. Yang, R. Karri, and D. A. McGrew, "A high-speed hardware architecture for universal message authentication code," IEEE journal on selected areas in communications, vol. 24, pp. 1831-1839, Oct. 2006.

[23] S. Benedetto, E. Biglieri, and V. Castellani, "Digital Transmission Theory," Englewood Cliffs, NJ: Prentice Hall, 1988.

[24] "Get Smart about Electrical Grid Cyber Security," Hirschmann, A Belden Brand, 2011.

[25] D.-Y. Chang, "Applications of the extent analysis method on fuzzy AHP," European journal of operational research, vol. 95, pp. 649-655, Dec. 1996.

[26] Y.-M. Wang and K.-S. Chin, "Fuzzy analytic hierarchy process: A logarithmic fuzzy preference programming methodology," International Journal of Approximate Reasoning, vol. 52, pp. 541-553, June 2011.

Journal of Electronical & Cyber Defence
Vol. 6, No. 1, 2017, Serial No. 21

Evaluation of Attack and Defense Budget for Cyber Security of High Voltage Substations Based on Application Classification Via Fuzzy AHP Method

N. Fardad, S. Soleymani*, F. Faghihi

*Department of Electrical Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran

(Received: 23/12/2016, Accepted: 09/08/2017)

ABSTRACT

Protection (i.e. defense) of high voltage substation in smart grid depends on electricity utilities' considerations for threat levels and their asset value. The aim of countermeasures is to decrease threat to an acceptable level. Such countermeasures depend on protective equipment/methods e.g. software, hardware, shielding and optimal route selection of data transferring media. These measures as a whole are function of quantity, type, scheme and location of substations in the network. The focus is to estimate volume of such countermeasures based on status, investment and criticality of each substation, as proper protective measures shall cover weaknesses in the system security. This paper presents an analysis of substations criticality based on the previous experience of experts and their knowledge to provide cyber security. The substations are classified as geostrategic, strategic industries, SAS and vulnerable by the use of the data derived from polling and through fuzzy analytic hierarchy process (FAHP) method. The share of each mentioned defense method in the budget is calculated for typical substations. Validity of the proposed method is examined by the sensitivity analysis.

Keywords: Cyber Security, Fuzzy Analytic Hierarchy Process, Smart Grid, Cyber Attack, Cyber Defense

* Corresponding Author Email: s.soleymani@srbiau.ac.ir