فصلنامهٔ پدافند غیرعامل و امنیت (علمی‌ترویجی)
/ سال ششم/ شمارهٔ بیست‌ودوم / بهار ۱۳۹۷
Quarterly of Passive Defense & Security
Vol.6, No.22, Spring 2018
تاریخ دریافت: ۱۳۹۷/۰۴/۳۰ تاریخ پذیرش:۱۳۹۷/۰۵/۲۷

ارایه الگوریتم جامع پدافند غیرعامل در حملات سایبری- میدانی به سیستم کنترل گسترده پست‌های فشار قوی مبتنی بر بودجه دفاع وحمله

امیرحسین پورسلطان محمدی[۱]
مهدی چهل امیرانی[۲]
فرامرز فقیهی[۳]

چکیده

حملات عامدانه و غیرعامدانه دشمن در راستای تخریب و آسیب‌رساندن به زیر ساختهای ارتباطی کشور به عنوان حقیقتی غیرقابل انکار اهمیت رویکرد ساختارگرایانه دفاعی را بیش از پیش نمایان می‌سازد. در این راستا متعادل‌سازی بودجه دفاع و حمله در جهت جلوگیری از افزایش شاخص انتظار افت خدمات مورد مطالعه قرار گرفته است. افزایش امنیت زیرساختهای پراهمیت کشور از نقطه نظر رویکرد پدافندغیرعامل بررسی و ضمن ارائه الگوریتم ساختاریافته جامع دفاعی در جهت افزایش قدرت‌دفاعی و کاهش آسیب‌پذیری در برابر حملات عامدانه مهاجمین اقدام گردیده است. سیستم کنترل گسترده پستهای فشار قوی به عنوان مطالعه موردی انتخاب و با در نظر گرفتن ریسک حملات نیل به الگوریتم جامع دفاعی مطالعات اساسی انجام گرفته است. در جهت افزایش امنیت سیستم کنترل گسترده پست‌های فشار قوی دو روش سخت افزاری و نرم‌افزاری پیشنهاد شده که توامان می‌تواند ریسک آسیب‌پذیری را به مقدار زیادی کاهش داده و نهایتاً امنیت سامانه را تامین نماید. استفاده از شیلدینگ با بهره‌گیری از مواد مختلف به عنوان روش سخت‌افزاری در جهت مقابله با حملات میدانی بررسی و نتایج مطلوب آن به کمک‌نرم‌افزار FEKO ارائه شده، استفاده از کدینگ اطلاعات به عنوان روش نرم‌افزاری پیشنهادی، افزایش امنیت انتقال اطلاعات را تضمین می‌کند. ما در این مقاله ضمن ارائه الگوریتمی ساخت‌یافته در جهت نیل به ملزومات پدافند غیرعامل در زیرساخت‌های حیاتی کشور، راهکارهای عملی افزایش امنیت انتقال اطلاعات را بررسی و ارائه کردیم که می‌تواند در جهت مقابله با حملات سایبری- میدانی مورد استفاده قرار گیرد.

واژگان کلیدی: *پدافند غیر عامل، سپر محافظ، کدینگ، بودجه دفاع، بودجه حمله*

---

۱. دانشجوی دکتری برق مخابرات دانشگاه ارومیه (نویسنده مسئول) ah.poursoltan@gmail.com
۲. عضو هیات علمیٔ گروه برق و کامپیوتر دانشگاه ارومیه m.amirani@urmia.ac.ir
۳. عضو هیات علمیٔ گروه برق و کامپیوتر دانشگاه علوم و تحقیقات faramarz_faghihi@hotmail.com

مقدمه

نزدیـــک کردن منابع حمله و دفاع با در نظر گرفتن تمامی نکات کلیدی بســـیار مشـــکل اســـت. برنامه ریزی برای تخصیص بودجه دفاع و حمله مستقیما به ارزش هدف مهاجم و مدافع بستگی دارد (فقیهی و همکاران،۱۳۹۷: ۱۰۸-۹۵). هدف مهاجم به حداکثر رساندن خســـارت و نابودی دارایی ها و هدف مدافع شـــبکه، به حداقل رساندن خسارات است. در این راســـتا و در جهت افزایش امنیت زیر ســـاخت های مهم کشور بررسی بودجه دفاع و حمله برای تحلیل و بررســـی موفقیت آمیز بودن حملات ضروری اســـت. عموماً حفاظت پستهای فشارقوی و سیســـتمهای ارتباطی بسیار ضعیف است و این مشکل به دلیل عدم آینده‌نگری درســـت می‌تواند نقطه ضعف بزرگی برای سیســـتم باشـــد (فرداد و همکاران، ۱۳۹۷:۵۵). میزان خطرات می‌تواند توسط روشهای هوشمند و همچنین بهره‌برداری‌های هوشـــمند امنیتی بررسی و اندازه‌گیری شـــود. ضوابط امنیتی ممکن است سطح حفاظت و اقدامـــات دفاعی در پســـتها را تعیین نماید اما در برخی مـــوارد، محدودیت های دولتی یا اســـتاندارد مالی موجود نیز ممکن اســـت این ســـطح را دچار تغییر نماید (سلیمانی و همکاران، ۱۳۹۶:۲۶-۱۸). عمر مفید سیستم نیز بر عملکرد اقدامات دفاعی تأثیرگذار است و می‌تواند بر انتخاب ســـاختار دفاعی تأثیرگذار باشد. اثربخشی روشهای تدافعی و ترکیب با روشـــهای حفاظت از پستهای فشـــارقوی جهت ارزیابی روشهای مؤثر برای ایمنی بالای سیستم اتوماسیون پستهای فشـــارقوی و تصمیم گیری در این خصوص ضروری می‌باشد (فرداد و همکاران، ۱۳۹۵:۴۵).

با منابع کافی حمله، مهاجمین ممکن اســـت قادر به نفوذ به شـــبکه‌های مختلف پســـت با چند ســـطح کنترل و ارســـال فرمانهای ســـاختگی بـــه تجهیزات محلی فیلد[1] شـــوند (Zhang,2016:669-683). بـــرای هرگونه حفاظت از زیرســـاختهای حیاتی، هزینه های حفاظت بایســـتی مبتنی بر اهمیـــت امکانات و تجهیزات بکار رفته در آنها باشـــد. تأمین کنندگان طیف وســـیعی از تجهیزات دفاع سایبری مانند فایروال[2]، دروازه عبور[3]، تجهیزات ناحیـــه غیرنظامی [4]و تجهیزات دیگر را ارائه میکنند که مشـــتمل بـــر اعمال مقرراتی در خصوص اســـتفاده از این تجهیزات می‌باشـــد (Stouffer, 2006). لازم به ذکر است که راه حلهای دفاع ســـایبری بر نرخ اطلاعات تبادل شـــده و تأخیر زمانی تأثیر میگذارد و اغلب نیاز به ایجاد تغییرات در سیســـتم می‌باشـــد. بدون تخصیص منابع کافی برای اطمینان از

1. *Field*
2. *Firewall*
3. *Gateway*
4. *Demilitarized zone*

ایمنی، دفاع سایبری جدید جهت تجهیزات امکان‌پذیر نمی‌باشد. دفاع مؤثر برای سیستم اتوماسیون پســـتها در شبکه هوشـــمند با تحلیل میزان ترافیک اطلاعات صورت میگیرد (Donald, 2016). برای شناســـایی و توقف حملات و جلوگیری از توســـعه آنها سیســـتم تشخیص نابهنجاری[1]، سیستم تشخیص نفوذ[2] و سیستم ممانعت از نفوذ[3] استفاده می‌شود (Wei, 2018:684-694).

بـــا افزایش راهکارهای دفاعی، حملات مهاجم تغییـــر خواهدیافت، لذا پیش بینی واکنش مدافع در مقابل تغییرات روشـــها و منابع حمله ضروری است. ارتباط با ایمیلها و تجهیزات سایبری متصل به اینترنت و شبکه هایی غیرقابل اطمینان می‌بایست منطقه بندی، مانیتور و کنترل شـــود. مهاجمان با دسترســـی از راه دور یا تونل زدن از میان ارتباطات فایروال شـــرایط حمله را مهیا میکنند (Stouffer,2006:70-82). در این راستا و در واکنش به این تغییـــر رویکرد حمله، پیش بینی لازم در جهت ممانعـــت از اجرای برنامه های غیرقانونی بکار گرفته شـــود. اســـتفاده حداکثری از منابع محدود دفاعی جهـــت افزایش مقاومت در برابر حملات ســـایبری در شبکه می‌تواند سبب بهبود در بهره برداری و افزایش اعتماد به سیســـتمهای ارتباطی گردد. عدم وجود امنیت در اطلاعات دریافتی از پستها که به کمک اندازه‌گیری‌های مرکز اسکادا انجام گرفته است، می‌تواند منجر به قطع خطوط و بریکرهای پســـتها گردیده و مشـــکلات امنیت اجتماعی را به همراه داشـــته باشد. با توجه به کمبود بودجهای دفاعی، شـــاید جلوگیری از تمامی حملات سایبری و دستیابی به استراتژی‌های حفاظت کامل مقدور نباشـــد، لذا بررســـی دقیق و بهینه ســـازی تجهیزات دفاع سایبری می‌تواند در حداقل سازی تأثیر حملات سایبری کارآمد باشد (Yue, 2014).

امروزه با به کارگیری گســـترده کامپیوتر و فناوریهای ارتباطی حملات ســـایبری به شبکه هوشمند برق و سیستمهای ارتباطی پست های فشارقوی رو به افزایش است. جمع آوری، نظارت و کنترل همه جانبه داده ها ''اسکادا'' برای کنترل متمرکز یک تجهیز خاص جهت تأیید عملکرد آن در راســـتای صحیح و برنامه ریزی شـــده مورد استفاده قرار گرفته شده است. اسکادا زمانی به کار میرود که عمل '' کنترل از راه دور '' برای سیستم اعمال می‌شود. طبیعی است که کنترل یک تجهیز یا سیستم، بدون داشتن اطلاعات دقیق از وضعیت آن ناممکن اســـت، بنابراین کنترل متمرکز همیشه با یک سیستم جمع آوری اطلاعات توأم اســـت. در حقیقیت هر جا تعدادی پایانه راه دور برای جمع آوری اطلاعات وجود داشـــته

1. *Anomaly*
2. *Intrusion Detection System*
3. *Intrusion Prevention system*

باشـــد. یک سیستم اسکادا نیز وجود خواهد داشت تا اطلاعات جمع آوری شده را به مرکز انتقال داده و پس از پردازش فرامین جدید را ارســـال نماید. هر پست مجهز به یک پایانه راه دور جهت جمع آوری و ارســـال داده ها به مرکز است. وضعیت و فرامین کلیه کلیدها، مقادیر اندازه‌گیری ولتاژ و جریان خطوط و ترانســـها، 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 بســـتر فیبر نوری به مرکز اسکادا انتقال مییابد. پست های مبتنی بر پروتکل *IEC61850* و دســـتگاه های الکترونیکی هوشمند و به طور کلی تمامی تجهیزات مبتنی بر اینترنت در دســـترس آسیب پذیری های ســـایبری هستند. مهاجمین سایبری ممکن اســـت از طریق نفوذ اینترنتی به سیســـتم های مانیتورینگ یا تجهیزات حفاظت و کنترل ویا سیســـتم اسکادا دسترســـی پیدا کنند. مهاجمین می توانند با ارسال مستقیم فرامین بهره برداری ســـاختگی به دســـتگاه های الکتریکی و یا ارســـال اندازه‌گیری‌های ساختگی بهره برداری صحیح از سیستم را مختل کنند و امنیت شبکه را مورد هدف قرار دهند. در شـــبکه های مخابراتی، مهاجم با هدف نفوذ به سیستم برای دریافت اطلاعات به منظور ضربه زدن به شـــبکه و مدافع با هدف محافظت از اطلاعات شبکه به منظور حداقل نمودن خســـارات احتمالی، مقابل یکدیگر قرار گرفته اند. با توجه به انگیزه‌های تشـــویقی استفاده از حسگرها توسط شرکت ها در شبکه های ارتباطی صنعتی به طور قابل توجهی افزایش یافته و توانایی سیســـتم را بهبود بخشیده است. امنیت این شبکه‌های ارتباطی به دلیل به کارگیری حســـگرها و احتمال نفوذ توسط مهاجمین از اهمیت بیشتری برخوردار می‌باشـــد. یکی از اهدافی که ممکن است توسط مدافعین شبکه هوشمند کاملاً شناسایی نشود، سیستم اتوماسیون پست ها است که بر مدیریت انرژی شبکه هوشمند تأثیر خواهد داشـــت. مهاجمین با یادگیری مداوم نقاط ضعف شبکه و متغیرهای کنترلی آنها اقدامات مخرب خود را برای نفوذ به سیستم اتوماسیون پستها و تجهیزات به منظورقطعی گسترده شـــبکه برق انجام می‌دهند. استاندارد *IEC61850* به عنوان یک استاندارد مبتنی بر اترنت در سیستم های اتوماسیون پست‌ها استفاده می‌شود. ازجمله پروتکلهایی که بر اساس این استاندارد تعریف می‌شـــود می‌توان به *MMS*[1]، *GOOSE*[2] و *SMV*[3] اشاره نمود. به منظور شناســـایی و کاهش تأثیر حملات سایبری مانند تزریق اطلاعات غلط به سیستم حفاظتی پســـتها، بایستی نیازمندی‌های امنیت ســـایبری و اقدامات پیشگیرانه مشخص شود. حال

1. *Manufacturing Message Specification*
2. *Generic Object Oriented Substation Event*
3. *Sampled Message Value*

با توجه به جمیع جوانب و مشـــخص شـــدن ضرورت مبحث پدافنـــد غیرعامل با دیدگاه بهتری در جهت کاهش ریسک ها و آسیب‌پذیری‌ها قدم بر خواهیم داشت. زیرساخت‌های با موقعیت ژئواســـتراتژیک و استراتژیک صنعتی و سیســـتم‌های ارتباطی و مخابراتی این زیر ســـاخت‌ها مستعد حملات سایبری از ســـوی مهاجمین از کشورهای خارجی و مجاور آنها قرار دارند. راهکارهای دفاعی مهمترین موارد برای جلوگیری از حملات ســـایبری به تجهیزات مخابراتی و ارتباطی و تجهیزات حساس کنترلی و الکترونیکی باشد. مساله مهم و اساســـی این اســـت که تحلیل بودجه دفاع و حمله و تخصیص منابع به روشهای دفاعی چگونه می‌تواند امنیت زیر ساخت های حیاتی را تضمین کند.

آیا چاره ای برای مقابله با افزایش منابع مهاجم در حمله به اهداف مهم وجود دارد؟

آیا می‌توان روش دقیق و کارآمدی برای کاهش سیستماتیک آسیب پذیری زیرساخت‌های ارتباطی کشور ارائه کرد؟

آیا می‌توان راهکارهای توانمندی را جهت ایســـتادگی در برابر حملات مهاجمین سایبری و میدانی معرفی و اجرایی کرد؟

مفروض اینســـت که: با متعادل ســـازی بودجه دفاع و حمله در حالی که شاخص ''انتظار افت خدمات'' ثابت بماند می‌توان قدرت دفاعی را در برابر حملات حفظ و امنیت سیستم ارتباطی را تامین نمود.

ارائه الگوریتم جامع پدافند غیر عامل می تواند آسیب پذیری و ریسک موفقیت آمیز بودن حمله را تا مقدار مطلوبی کاهش دهد.

راهکارهای نرم افزاری کدینگ اطلاعات و شـــیلدینگ ســـخت افزاری تجهیزات به عنوان روشهای قدرتمند، می‌تواند مقاومت دفاعی را در برابر حملات مهاجمین سایبری و میدانی افزایش و امنیت اطلاعات را تضمین کند.

روش تحقیق و مبانی نظری:

روش تحقیق در این مقاله روش حل عددی فرم دیفرانســـیلی معادلات ماکسول است که جهت بررســـی عکس العمل میدان های الکترومغناطیسی بر روی محفظه و فصل مشترک آنها مورد اســـتفاده قرار میگیرد. استفاده از روشهای حل عددی به عنوان پایه نرم افزاری تحلیل ضریب موثرسازی شیلدینگ، با مش بندی فضای محفظه، تحلیلی دقیق از جذب، عبور و انعکاس میدانهای الکترومغناطیسی انجام میدهد و در جهت افزایش امنیت سیستم و کاهش آسیب پذیری زیر ساخت های حیاتی بسیار کارگشا خواهد بود.

در دنیای متاثر از تکنولوژی امروزی جنگهای پر خطر و پر هزینه فیزیکی جای خود را به جنگهای سایبری و میدانی داده است. به طوری که اثر مخرب این حملات گاهاً بیشتر و این حملات بدون شناسایی مهاجم خواهد بود. پدیده دفاع غیر عامل به عنوان راهکاری جهت کاهش آسیب پذیری منابع حیاتی کشور و جان انسانها بسیار پر اهمیت می باشد. جهت حل مشکل حملات سایبری الگوریتم جامع دفاعی شامل راهکارهای توام نرم‌افزاری و سخت افزاری ارائه شده و اثر کارکرد آن بر کاهش نرخ خطای بیت در انتقال اطلاعات مورد مطالعه قرار گرفته است و میزان ریسک احتمالی آسیب پذیری شبکه ارتباطی مشخص گردیده است. در راستای رسیدن به راهکار مطلوب یک الگوریتم دفاعی با رویکرد پدافند غیرعامل ارائه شده است. با در نظر گرفتن این نکته که دستکاری‌های عمدی اطلاعات در زمان خوانش و انتقال اطلاعات و عدم نمایش وضعیت بحرانی، می‌تواند در زمان بهره برداری بسیار خطرناک و جبران ناپذیر باشد. الگوریتم دفاعی فوق برای سیستم کنترل گسترده پست های فشار قوی پیاده سازی می‌شود.

پیچیدگی و حساسیت سیستم ها و شبکه های الکترونیکی و مخابراتی و کاربرد روز افزون آنها در محیط های اداری، صنعتی، پزشکی و نظامی سبب شده است تا ایمنی و کارکرد آنها مورد توجه ویژه قرار گیرد، در این زمینه تلاش برای استفاده از مسیرهای امن انتقال اطلاعات در مقابله با تداخلات خواسته یا نا خواسته الکترومغناطیسی به امری مهم تبدیل شده است. نفوذ به دستگاه‌ها، تجهیزات شبکه و سرقت و دستکاری اطلاعات در حال مخابره می‌تواند در عین سادگی و کم هزینه بودن صدمات جبران ناپذیری را به ماهیت ساختاری یک کشور وارد نماید. در حالی که تهدیداتی مثل بمب یا حملات به هواپیماها می‌تواند عواقب مادی و غیرمادی زیادی را به کشور مهاجم تحمیل کند (*Donald, 2016*).

حملات سایبری:

حملات می‌تواند سیستم های خاص و زیر سیستمهای مربوطه را به طور همزمان و از راه دور مورد هدف قرار دهد. انواع مختلف حمله، مکانیزم‌های مربوطه و دیگر مشکلات ایجاد شده بایستی در طراحی امن شبکه های ارتباطی در نظرگرفته شود (*Kundur,2011:2-13*). از سوی دیگر، مهاجم‌های خارجی به آسانی می توانند حملات را راه اندازی کرده و معمولاً حمله نیز شناسایی نمی شود، بنابراین سیستمهای هوشمند مراکز انتقال اطلاعات بیشتر در معرض خطر قرار دارند. لازم بذکر است که امکان ایجاد و استقرار دفاع قوی و موانع در مقابل حملات سایبری به شبکه های مرکز کنترل به دلیل طیف گسترده‌ای از مکانیزم

های حمله، ماهیت متمرکز کنترل و عدم هماهنگی بالقوه سازمان های مختلف بسیار مشکل است. برای رسیدن به ساختار شبکه امن، استراتژی‌های جامع فراگیر، جنبه های فنی، تحلیل هزینه- فایده در نیازمندی های امنیتی بایستی توسعه داده شود. با وجود تلاش های صورت گرفته برای امنیت سایبری، تزریق داده های جعلی، سرقت اطلاعات و دستکاری مخرب داده ها توسط مهاجمان خبره مشکلات زیاد و گاهاً پر هزینه ای را به بار می‌آورد (Sondoval, 2010). مسیر انتقال امن پیام ها، نقش اساسی برای عملکرد حفاظتی نرمال در مراکز صنعتی و نظامی را به عهده دارد. ابتدا لازم است که دریافت کننده بررسی نماید که پیامهای دریافتی از فرستنده، به صورت مطمئن دریافت شده است. ثانیاً، دریافت کننده بایستی محتوا و اصالت پیام را تأیید نماید و این که به هر دلیلی پیام ضمن ارسال تغییر نکرده باشد، بررسی گردد. یک مهاجم، به صورت بالقوه می‌تواند برخی از تجهیزات ارتباطی نظیر مالتی پلکسرها را پیکربندی مجدد کرده و به خطر بیاندازد. بنابراین ارتباط ناامن در شبکه ممکن است آن را در معرض خطر حمله و تهدید قرار دهد (Mousavian, 2014: 2174-2179).

حملات میدانی:

حساسیت بالای تجهیزات الکترونیکی و مخابراتی در مقابل امواج الکترومغناطیسی باعث شده است که استفاده از تکنولوژی مغناطیسی و امواج الکترومغناطیسی در جنگ‌افزارهای نسل الکترونیک این قرن، جایگاه ویژه‌ای پیدا کند و مورد توجه سران کشورها و سازندگان این قبیل سلاح‌ها قرار گیرد. در این‌راستا می‌توان از بمب‌های الکترومغناطیسی[1] نام برد (توکلی مقدم و همکاران، ۱۳۸۸). بمب‌های الکترومغناطیسی را شاید بتوان سلاح‌های کشتار الکتریکی نامید که طیف وسیعی از اهداف الکتریکی و الکترونیکی را در بر می‌گیرند. قابلیت تخریبی آنها نتایج جبران ناپذیری روی سامانه‌های اطلاعاتی و تأسیسات ارتباطی حریف بر جای می‌گذارد، لذا این نوع مهمات نقش مهمی در فرآیند جنگ اطلاعات ایفا می‌کنند. این بمب‌ها، سلاح‌هایی هستند که برای تخریب هدف، ازیک پالس شدید الکترومغناطیسی (EMP[2]) بهره می‌برند و اثرات مخرب این پالس الکترومغناطیسی، تمام سامانه‌های الکتریکی و الکترونیکی را در شعاع تخریب، از کار می‌اندازد. بنابراین پدآفند غیرعامل در برابر تهاجم الکترومغناطیسی مانند هر نوع آفندی نیاز به طراحی و ایجاد پدآفند خاص و مناسب خود را دارد اگر چه اثرات و میزان تخریب این سلاح، بر روی تجهیزات گوناگون کاملاً مشخص نشده است؛ اما راه‌های مقابله با آن تا حدودی قابل

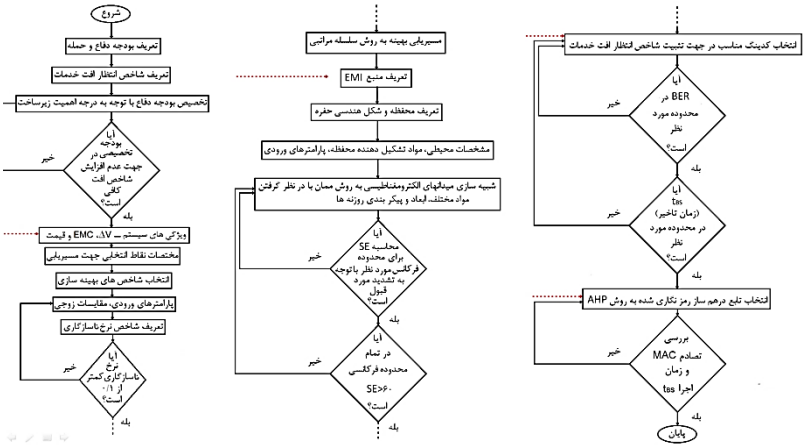
1. Electromagnetic – Bomb
2. Electromagnetic – pulse

بررســـی اســـت. یکی از راههای مؤثر و متداول که برای سایر سلاح‌های آفندی نیز کاربرد دارد، جلوگیری از پرتاب مولد EMP است. اما این کار همیشه امکان‌پذیر نیست، بنابراین روی آوردن به پدآفند غیرعامل کاملاً منطقی اســـت (چهارسوقی و همکاران، ۱۳۹۲:۳۳-۳۲). که در واقع دفاع همه جانبه را حتی با داشـــتن دفاع عامل قدرتمند، پوشش می‌دهد. بنابراین بسیاری از این مشکلات را می‌توان با اطمینان حاصل نمودن از جدایی کافی منابع و قربانی‌های تداخـــل، حل و فصل نمود. اصلی‌ترین روش برای مقابله با چنین تهدیداتی، از بین بردن مناطق نفوذ امواج الکترومغناطیســـی همراه با ایجاد پوشش (شیلد[1]) مناسب در بخش‌های مختلف یک سیســـتم است. پوشش الکترومغناطیسی قادر است با انعکاس و جذب امواج الکترومغناطیسی، میزان عبور آن‌ها را کاهش دهد. بنابراین شیلدها باید برای کاهش تداخل الکترومغناطیسی طوری طراحی شوند که بتوانند کارکرد سایر اجزاء داخل سیســـتم را تضمین کنند. به منظور دستیابی به این هدف، مطالعه مواد و تعداد لایه های شیلدینگ و پیکربندی‌های متفاوت محفظه شیلدینگ، به عنوان روش‌های کلاسیک انجام می‌شود و عملکرد دقیق سیســـتم در حضور میدان‌های تداخلی توسط ساخت شیلدهای مناســـب برای محفظه آن سیستم، مورد بررسی قرار می‌گیرد (جلالی فراهانی و همکاران، ۱۳۹۲:۴۵).

ارایه الگوریتم پدافند غیر عامل:

جهت حل مشـــکل حملات سایبری- میدانی الگوریتم جامع دفاعی شامل راهکارهای توام نرم‌افزاری و ســـخت افزاری ارائه شـــده و اثر کارکرد آن بر کاهـــش نرخ خطای بیت مورد مطالعه قرار گرفته اســـت ویک الگوریتم دفاعی با رویکرد پدافند غیر عامل ارائه شده است که در شـــکل ۱ قابل مشـــاهده اســـت. با در نظر گرفتن این نکته که دستکاریهای عمدی اطلاعـــات در زمان خوانش و انتقال اطلاعات و عـــدم نمایش وضعیت بحرانی، می‌تواند در زمان بهره برداری بسیار خطرناک و جبران ناپذیر باشد. الگوریتم دفاعی فوق برای سیستم کنترل گســـترده پست فشار قوی پیاده سازی می‌شود. اســـتفاده دقیق و پیروی منظم از الگورتم ارائه شـــده می‌تواند امنیت سیســـتم را با کاهش آســـیب پذیری در برابر حملات سایبری-میدانی تضمین کند.

1. shield



شکل ۱- ارائه الگوریتم جامع دفاعی جهت کاهش آسیب پذیری سیستم و با رویکرد پدافند غیر عامل

برای نشـــان دادن روابط مهاجم و مدافع یک تابع احتمال در نظر گرفته می شود. مهاجم دارای بودجه یا اعتبار کل (BA)[1] به عنوان منبع حمله و مدافع دارای بودجه یا اعتبار کل (BD)[2] برای دفاع در برابر حملات می باشد (*Al mannai, 2008*). احتمال حمله موفق در هر هدف (i) در صورتی که مهاجمین و مدافعین، مقادیر بودجه حمله و دفاع را به N هدف اختصاص دهند، از رابطه زیر محاسبه خواهد شد.

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

که A_i بودجه حمله اختصاص داده شـــده به هدف i توسط مهاجم است. λ_i عامل یا ضریب آســـیب پذیری است که ســـطح دشواری حمله را نشـــان می‌بدهد که با توجه به اقدامات دفاعی تعیین می شـــود. آنچه در رابطه مشخص است این است که احتمال موفقیت حمله با افزایش بودجه حمله در صورتی که اقدامات دفاعی افزایش نیابد، بیشـــتر خواهد شـــد. از طرفی احتمال حمله موفق با افزایش ســـطح D_i کاهـــش پیدا می‌کند و به صورت زیر مدلسازی می‌شود.

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

1. *Budget for attack*
2. *Budget for defending*

که D_i اعتبار یا بودجه فراهم شـــده برای مدافع بوده و α_i ضریب آســـیب پذیری را نشان می‌دهد. احتمال توام حمله موفق برابر است با:

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

خطر شـــبکه هدف $R(A_i, D_i)$ تحت‌تأثیرآســـیب‌پذیری اصلی مدافع ومهاجم وخســـارت هرهدف می‌باشدو به صورت زیر بدست می‌آید (Zhang, 2015:1-16) .

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

که d_i نتیجه و تأثیر حاصل بر هدف iاست. تجارب مهاجم باعث می‌شود که با سرمایه‌گذاری کمتری اهداف با اولویت بالا را مورد حمله قرار دهد. ولی در عین حال برای کاهش آسیب پذیری و خطر کلی سیســـتم مدافع بایستی مراکز با اهمیت بالا را با تخصیص منابع کافی محافظت نماید (ABB, 2015). در این راســـتا مدافع با در نظر گرفتن شاخص انتظار افت خدمات به عنوان هدف تلاش می‌کند شـــاخص با رشد بودجه حمله افزایش نیابد. این امر سبب می‌شود ضمن تامین امنیت سیستم، تخصیص بودجه به صورت هدفمند انجام گیرد. رابطه شاخص انتظار افت خدمات برای سیستمهای قدرت و مخابرات به صورت زیر است.

$$\text{شاخص انتظار افت خدمات} = P_S \frac{\sum_{i=1}^{n} H_{i_{total}}}{N_S} + C_S \frac{\sum_{j=1}^{m} B_{j_{total}}}{N_S} \qquad (۵)$$

که$H_{i_{total}}$ برابر کل ساعتهایی است که کمبود بار وجود دارد، $B_{j_{total}}$ برابر کل بیت‌هایی است که با خطا ارسال میشود، n تعداد حالتهای قطعی، m تعداد حالتهای تکرار N_S، مدت زمان شبیه سازی، P_S ضریب ماهیت هدف حمله که برای سیستم قدرت ۱ و بقیه حالات صفر است، C_S ضریب هدف انتخابی از سوی مهاجم است که برای سیستم مخابرات ۱ و بقیه حالات صفر است. در این زمینه و با تثبیت این شاخص در زمان افزایش بودجه حمله می‌تـــوان امنیت را به حالت قبل از افزایش بودجه برگرداند. یهنی به زمانی که فرض ما بر تامین امنیت سیستم است.

پیاده سازی الگوریتم برای سیستم کنترل گسترده پست های فشار قوی:

کاربرد سیســـتم های کنترل گسترده[1] سبب بهبود مقدار و کیفیت تولید، ایمنی و قابلیت

1. Distributed Control System (DCS)

اطمینان و انعطاف پذیری بیشـــتر قســـمتهای صنعتی و افزایش حـــوزه نظارت بر مراحل اجرای یک پروســـه می گردد. سیســـتم های کنترل گسترده هم اکنون بیشتر در خطوط پردازش بســـته بکار گرفته می شود تا در نهایت شاهد افزایش بازده خط باشیم در سطح قدرت نیز این سیســـتم به دلیل قابلیت اطمینان بالا امـــروزه در جهت مدیریت و کنترل سیســـتم اتوماسیون نیروگاه ها و پست های هوشـــمند مورد استفاده قرار می گیرد. کلیه مراحل کنترل، مانیتورینگ، و فرمان توســـط یک یا دو سرور اصلی که به صورت مستقل عمل می‌نمایند انجام می شـــود. اتوماســـیون به معنای کنترل و هدایت یک دســـتگاه به صورت خودکار اســـت و مشـــخصه سیستم هایی اســـت که تصمیم برای انجام فعالیت یا فعالیت هایی به جای انســـان توسط دســـتگاه های خودکار صورت می پذیرد. بدین معنی کـــه ابزارهای کنترلی مثل کامپیوتر و ابزار مکانیکی مثل رباط یا ماشـــین های الکتریکی جایگزین قدرت تفکر و نیروی انســـانی می شوند. مساله اتوماسیون زمانی مطرح می شود کـــه به انجام کاری به صورت مکرر، نظارتی مســـتمر و دقیق، فعالیتـــی خطر آفرین و یا کارهایی با دقت یا ســـرعت فوق العاده زیاد نیاز داریم. به عبارت دیگر هنگامی که انســـان در فعالیتی احســـاس ضعف و ناتوانی می کند، با اســـتفاده از ابزار کنترلی و مکانیکی و با یاری جستن از اتوماسیون، بر مشکل خویش فایق می آید. این امر زیر ساخت لازم را برای حملات سایبری- میدانی دشمن مهیا می کند.

محاسبه ضریب اثرگذاری شیلدینگ به عنوان روش سخت افزاری:

امروزه استفاده ازمحفظه‌های فلزی بااشکال متفاوت بعنوان راهکاری مطلوب جهت کاهش تداخلات‌الکترومغناطیسی موردقبول واقع شده‌است. (Robinson,1998:240–248).

ضریب کارایی شـــیلدینگ[1] محفظه های فلزی بدون روزنه پارامتر مهم و اثرگذار در طراحی و انتخاب محفظه می باشد. این ضریب با استفاده از رابطه ۱ و ۲ قابل محاسبه است (Liu, 2009).

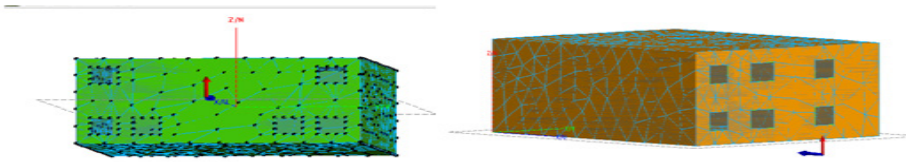
$$SE_E = 20\, log_{10} \left|\frac{E_i}{E_t}\right|\ dB \qquad (۶)$$

$$SE_B = 20\ log_{10} \left|\frac{H_i}{H_t}\right|\ dB \qquad (۷)$$

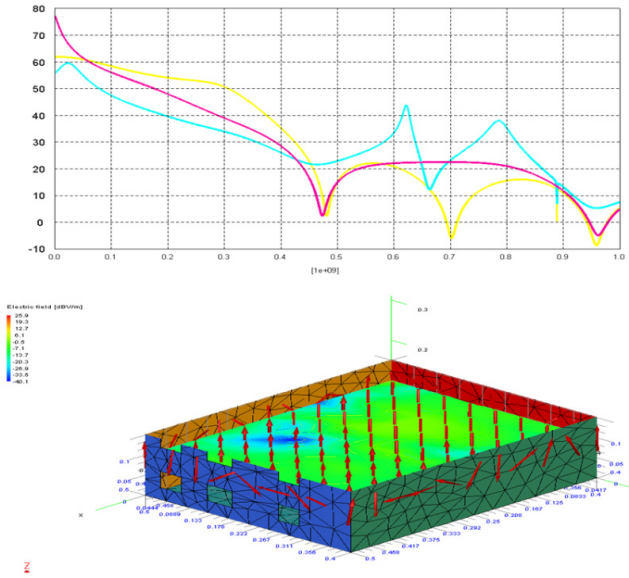
در راستای کاهش آسیب پذیری سیستم های مخابراتی و کنترلی در برابر حملات میدانی انتخاب و اســـتفاده از شیلدهای روزنه دار با مواد ساختاری مختلف بسیار کاربردی و اثرگذار است (Faghihi, 2009). در این راستا شبیه سازی محفظه روزنه دار با آرایش متفاوت روزنه

1. shielding effectiveness

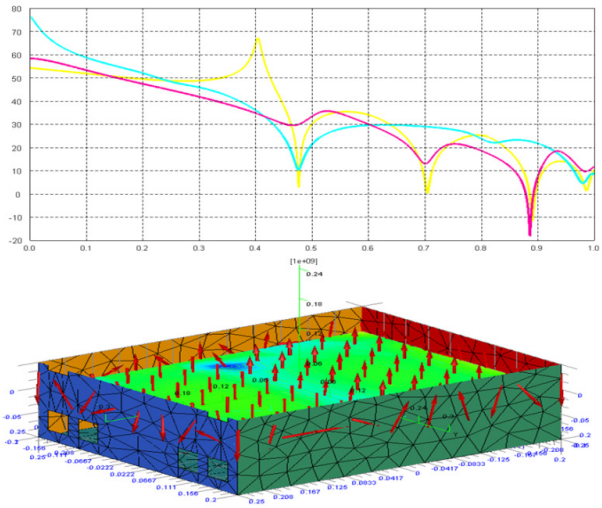
در دو نمونه در شـــکل ۲ نمایش داده شده اســـت. نتیجه نمودار ضریب کاربی شیلدینگ و نمایش سه بعدی شدت میدان الکتریکی در شکلهای ۳ و ۴ نشان داده شده می شود.



شکل ۲- دو محفظه با چیدمان متفاوت روزنه ها

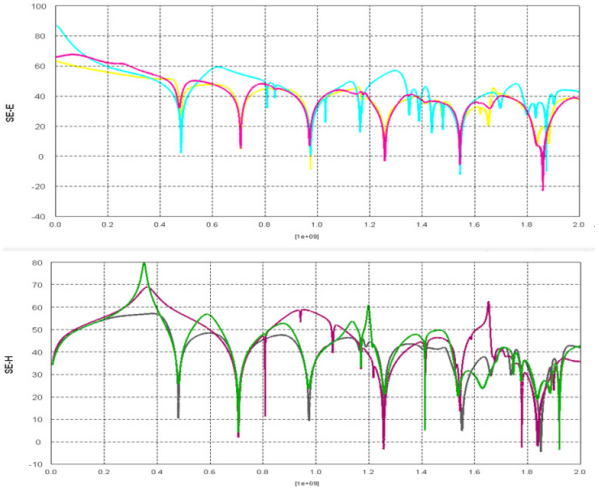


شکل ۳- نمایش سه بعدی ونمودار SE شدت میدان الکتریکی درمحفظه اول

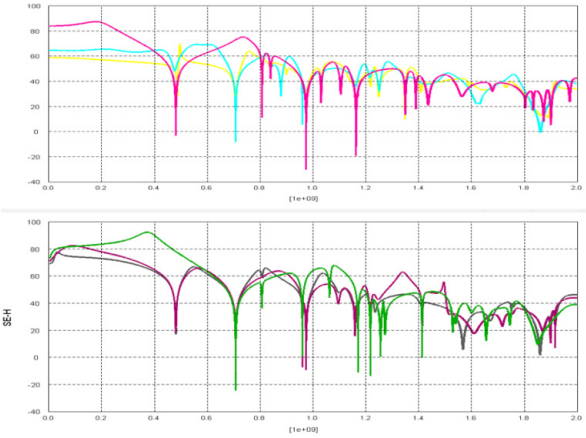


شکل ۴- نمایش سه بعدی ونمودار SE شدت میدان الکتریکی درمحفظه دوم

اســـتفاده از مواد مختلف در ســـاخت محفظه و تاثیر آن بر ضریب اثرگذاری شیلدینگ در راســـتای افزایش قدرت دفاعی شبکه برای دو ماده آهن و مس مورد مطالعه قرار گرفت و نتایج شـــبیه سازی ها در شکلهای ۵ و ۶ قابل مشاهده است. همانطور که در شبیه سازی ها مشـــخص است استفاده از شیلدینگ ســـخت افزاری نتایج مطلوبی در مقاومت سیستم در مواجهه با حملات میدانی دارد. شـــیلدینگ مســـی با بیشـــترین اثرگذاری در ضریب موثرسازی بهترین گزینه است. ولی با توجه به قیمت تمام شده بسیار بالای محفظه های مســـی، اســـتفاده از محفظه های آهنی با اینکه حدود ۲۰ درصد افت در ضریب SE ایجاد میکند، انتخاب نهایی است.



شکل ۵- مقادیر SE برای فلزآهن



شکل ۶- مقادیر SE برای فلز مس

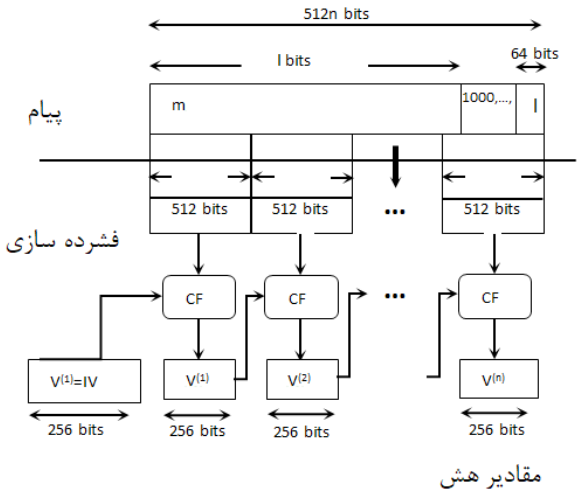
کدینگ و تصدیق اصالت پیام به عنوان حفاظ نرم افزاری ثانویه:

پـــس از افزایش مقاومت دفاعـــی در برابر حملات میدانی نوبت بـــه افزایش قابلیت های تدافعی نرم افزاری در مواجهه با حملات سایبری است. این امر به کمک کدینگ اطلاعات و اســـتفاده از یک الگوریتم احراز هویت از خانواده تابع درهم ساز امکان پذیر خواهد بود. حفاظ پیشـــنهادی ثانویه نرم افزاری می تواند جهـــت ثابت ماندن قدرت دفاعی در مقابل افزایش بودجه مهاجم در سیستم کنترل گسترده پست های فشار قوی و کلیه زیر ساخت های پراهمیت کشور مورد استفاده قرار گیرد.

با توجه به کاربرد و وضعیت کانال، یک کدینگ مناســـب بین کدینگ سنتی یا کانولوشن کد و توربوکد انتخاب میشـــود. برای بررسی دقت و صحت اطلاعات نیاز به یک روش امن می‌باشـــد که برای این منظور، اســـتفاده از کدهای تصدیق اصالت پیام[1]، توابع درهم ساز[2] پیشنهاد شده است (Brejs, 2015). در موضوع امنیت اطلاعات به خصیصه ای که بر حفظ دقـــت و تمامیت اطلاعات تأکید دارد، صحت اطلاعات گفته میشـــود. این خصیصه بدین معنی است که باید مطمئن شد که اطلاعات تنها توسط افراد یا موجودیت‌ها و فرآیندهای پردازش اطلاعات که مجاز به انجام این کار هســـتند، انجـــام میگیرد و همچنین مطمئن شد که این اقدام در زمان مجاز انجام شده است. در بسیاری از کاربردها، الگوریتم کلیدی نامتقارن[3] برای تأیید و تصدیق پیام اســـتفاده می شود. در این صورت، اگر یک پیام توسط کلید خصوصی فرســـتنده رمزگذاری شده باشد، آنگاه گیرنده میتواند بررسی نماید که آیا این پیام واقعاً توســـط فرستنده ارسال شده اســـت. اما رمزگذاری کل پیام نیازمند مقدار زیادی محاســـبات می‌باشد. برای کاهش هزینه محاسبات، یک فرستنده میتواند اطلاعات تصدیق با طول کم را بکار بگیرد که از پیام اصلی دریافت شـــده است (Brejs, 2015). این اطلاعات تصدیق، که کد تصدیق پیام نامیده می شـــود، با بکارگیری یک تابع در هم پیام اصلی و کدگذاری این پیام کوتاه حاصل می‌شود. وقتی که محاسبه MAC پیام ارسال می گردد در این حالت، فرستنده و گیرنده، اطلاعات محرمانه را به اشتراک می گذارند که به پیام اصلی افزوده می شـــود. وقتی پیام دارای MAC درســـت می باشد، گیرنده میداند که آن پیام بایســـتی توسط فرستنده موثق ارسال شده باشـــد، اما در عین حال باید مطمئن بود که پیام در ضمن عبور تغییر داده نمیشـــود. اســـتفاده از توربو کد و کد اصالت سنجی

1. *Hashed Message Authentication Code*
2. *Hash Function*
3. *Asymmetric Key*

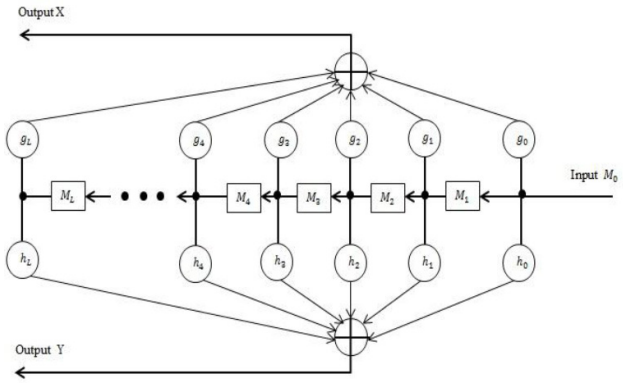
SM3 به عنوان حفاظ نرم‌افزاری در راســـتای عدم افزایش شـــاخص انتظار افت خدمات و در جهت افزایش مقاومت در برابر حملات ســـایبری می‌تواند راهکاری مطلوب و اثربخش باشد. این کد با بیت ورودی پیام m الگوریتم درهم ساز SM3 به کمک لایه گذاری پیام و تکرار فشـــرده ســـازی ۲۵۶ بیت هش خروجی تولید میکند. که الگوریتم آن در شکل ۷ قابل مشاهده است (Kaige, 2015:13).



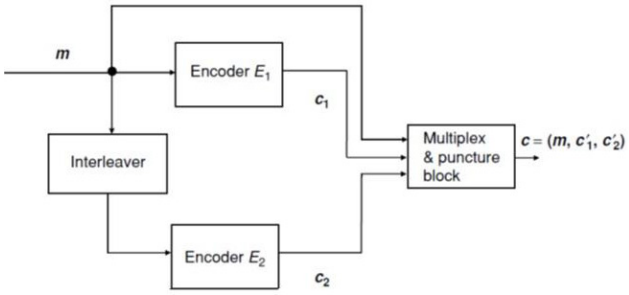
شکل ۷- الگوریتم SM3

در این مقاله برای ســـاختن یک شـــیلد نرم افزاری از کدهای کانولوشن و توربو با دیکدر های به ترتیب ویتربی و BCJR اســـتفاده شده است. تحلیل نرخ خطای بیت در دو روش پیشنهادی محاسبه و نمایش داده شده است. معروف ترین الگوریتم در دیکدینگ کدهای کانولوشن، الگوریتم ویتربی است. این روش یک الگوریتم ML جهت تخمین رشد بیت کد شـــده می باشـــد و برای دیکدینگ کدهای بلوکی نیز به کار می رود. این روش از دیاگرام ترلیس که بسط یافته زمانی دیاگرام حالت می باشد جهت تشخیص مسیر بهینه استفاده می کند. الگوریتم ویتربی روشـــی کارآمد برای یافتن مسیر بهینه بدون نیاز به جستجوی کامل اســـت. اســـاس الگوریتم ویتربی بر این اســـت که در هر مرحله زمانی مسیرهایی را که نمی توانند مربوط به مســـیر بهینه باشـــند را حذف کرده و لذا از ادامه جستجو در این

مسیرها جلوگیری می کند. در مقایسه با الگوریتم مشهور ویتربی برای دیکدینگ کدهای کانولوشـــن، الگوریتم BCJR دارای دو تفاوت اساسی است. الگوریتم BCJR یک الگوریتم دیکدینگ ورودی- نرم، خروجی- نرم با دو مرحله بازگشـــت پیشرو- پسرو است که هر دو بر مبنای تصمیم های نرم هســـتند. مدار انکدر کانولوشن و توربو به ترتیب در شکلهای ۸ و ۹ مشاهده میشوند.



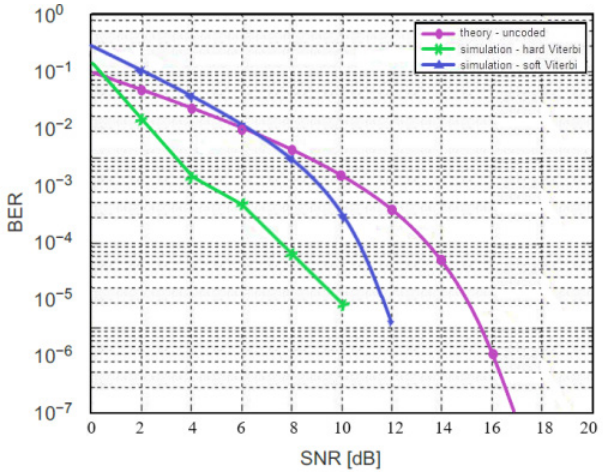
شکل ۸- مدار انکدر کانولوشن



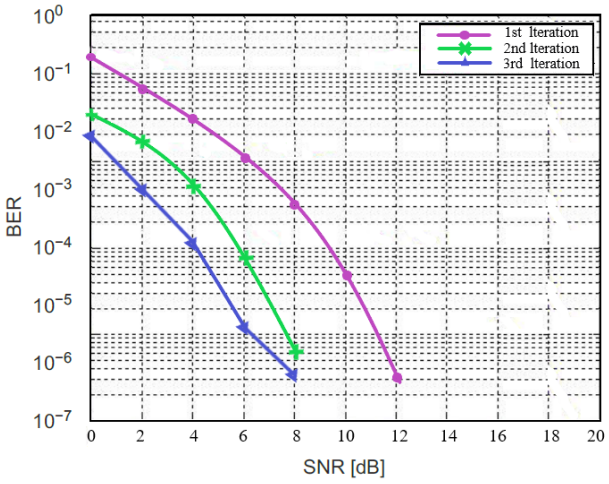
شکل ۹- مدار انکدر توربو

الگوریتم BCJR یک دیکدر MAP است که خطای بیت را توسط تخمین احتمالات پسین هر بیت در یک کلمه حداقل می سازد. نتایج بررسی نرخ خطای بیت در دیکدر با الگوریتم ویتربی و BCJR با نسبت سبگنال به نویز ۰ تا ۲۰ و با سه تکرار در شکلهای ۱۰ و ۱۱ قابل مشـــاهده می باشد. اســـتفاده از کدینگ نرم افزاری با دکدر های مختلف ویتربی و BCJR انجام گرفته و کاهش حدود ۵۰ درصدی به واسطه استفاده از دیکدر BCJR مشهود است.

با توجه به پیچیدگی کم این دیکدر استفاده از آن در الگوریتم پیشنهاد می‌گردد.



شکل ۹- عملکرد دیکدر ویتربی با نرخ



شکل ۱۰- عملکرد دیکدر BCJR با نرخ

نتیجه‌گیری

افزایش قدرت دفاعی در مراکز مهم و اســـتراتژیک نیازمند طرح و برنامه ریزی دقیق است. افزایش بودجه حمله توسط دشمن در دنیای به شدت آشفته امروزی برای حمله مهاجمان ســـایبری و میدانی به اهداف زیرســـاختی کشـــور فقط با افزایش تخصیص بودجه و طرح و برنامه جامع دفاعی قابل مقابله است. ارائه الگوریتم جامع دفاعی با رویکرد پدافند غیرعامل اولین گام در طرح ریزی این مهم می باشـــد. متعادلسازی بودجه دفاع و حمله با این هدف که شـــاخص انتظار افت خدمـــات افزایش نیابد، منابع مالی را جهت ایجاد ســـاختار دفاعی کامل بر پایه الگوریتم جامع دفاعی فراهم می‌آورد. شـــیلدینگ سخت‌افزاری به عنوان اولین راهکار عملی برای مقابله با حملات میدانی پیشنهاد و عملکرد سپر محافظ آهنی و مسی با هرینه‌های ســـاخت متفاوت بررسی گردید. آنچه مشخص شد عملکرد مطلوب سپر محافظ بود که به کمک تحلیل پارامتر ضریب کارایی ســـپر آسیب پذیری سیستم کنترل گسترده پست‌های فشار قوی را تا مقدار زیادی کاهش داده است. این شبیه سازی در رنج ۰ تا ۲ گیگا هرتز انجام و برای دو محفظه با جایگاه‌های نامتقارن روزنه مطالعه گردید. نتایج درخشان این شبیه سازی ها خصوصاً در رنج ۰ تا ۰/۵ گیگا هرتز کاملاً مشخص است. کدینگ و تصدیق اصالت پیام به عنوان حفاظ نرم افزاری ثانویه جهت مقابله با حملات سایبری پیشنهاد و شبیه سازی گردید. استفاده از کدهای سنتی کانولوشن با دکدر ویتربی و کد توربو با دکدر BJCR در کانال ارتباطی، عملکرد دقیق و کارآمد آن را نشان می دهد. به طوری که نرخ خطای بیت در بازه ۰ تا ۲۰ دسی بل نسبت سیگنال به نویز کاهش قابل ملاحظه ای داشته است که با توجه به بودجه حمله دشمن و متعادل‌سازی بودجه دفاعی قابل پیاده سازی در زیر ساخت های ارتباطی پســـت‌ها و دیگر مراکز انتقال اطلاعات می‌باشد. ما در این مقاله ضمن بررسی ریسک احتمالات حمله دشمن در جهت متعادل کردن بودجه دفاع و حمله با محوریت عدم افزایش شاخص انتظار افت خدمات اقدام نموده ایم. الگوریتم دفاعی جامع پیشنهادی بر پایه دو روش سخت افزاری و نرم افزاری دفاعی طرح ریزی و عملکرد مورد قبول دفاعی را در برابر حملات سایبری- میدانی دشمن تضمین میکند.

بررســـی و تحلیل محفظه‌های با ســـاختار پیچیده غیر متقارن و با تعداد روزنه مختلف در جهت افزایش اثر ســـپر محافظ در زیر ساخت های حیاتی کشور به عنوان راهکار فیزیکی کارآمد، جهت تحقیق های آتی پیشـــنهاد میگردد. تحقیقات پر دامنه در زمینه رمزنگاری دیتای انتقالی می تواند در جهت افزایش امنیت سیستم کارگشا باشد.

منابع

۱. توکلی مقدم، بابـــک و همکاران (۱۳۸۸)؛ «پدافند در مقابـــل بمبهای گرافیتی، مجله علمی- ترویجی پدافند غیرعامل ایران، سال اول، شماره ۱.

۲. جلالی فراهانی، غلامرضا و همکاران (۱۳۹۲)؛ ارزیابی ریسک مراکزداده بر اساس روش *FEMA* و ارائـــه الگـــوی پهنه‌بندی امنیتی، مجله علمی- پژوهشـــی پدافند الکترونیکی و سایبری، سال اول، شماره ۲.

۳. چهارســـوقی، صدیقه و همکاران (۱۳۹۲)؛ بکارگیری شـــبکه‌های عصبی مصنوعی در ارزیابی ریســـک امنیت اطلاعات، مجله‌علمی-پژوهشی پدافند الکترونیکی و سایبری، سال اول، شماره ۴.

۴. ســـلیمانی، سودابه و همکاران (۱۳۹۶)؛ امنیت ســـایبری سیستم اندازه گیری گسترده شبکه برق در صورت وقوع حملات سایبری به تجهیزات هوشمند خطوط انتقال اطلاعات آسیب پذیر، دومین کنفرانس ملی پدافند غیرعامل.

۵. فرداد، نور الله و همکاران (۱۳۹۷)؛ «تحلیل حمله و دفاع ســـایبری در ســـطح پردازش پستهای دیجیتال با روش تئوری بازی»، مجله مهندسی برق دانشگاه تبریز، شماره ۴۹.

۶. فقیهـــی، فرامـــرز و همـــکاران (۱۳۹۷)؛ ارزش گذاری بودجه دفـــاع و حمله در امنیت ســـایبری پستهای فشـــارقوی مبتنی بر طبقه بندی کاربردی به روش *AHP* فازی، مجله پدافند الکترونیکی و سایبری، جلد ۶، شماره ۱.

۷. فرداد، نور الله و همکاران (۱۳۹۶)؛ تحلیل امنیت سایبری در شبکه هوشمند برق مبتنی بر ارزیابی قابلیت اطمینان، اولین کنفرانس ملی پدافند غیرعامل.

8. *Al Mannai, W (2008), "A general defender-attacker risk model for networks", J Risk Finance, Vol. 9, No. 3, PP. 244–261.*

9. *Brejz, M (2015), "20 Years of Turbo Coding and Energy Aware Design Guidelines for Energy-Constrained Wireless Applications", IEEE Communications Surveys & Tutorials, Vol. 9, No. 3.*

10. *Cyber Security for Substation Automation Systems by ABB, (2010).*

11. *Donald, j (2016), "Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and analysis center", WWW.eisac.com.*

11. *Faghihi, F (2009), "Reduction of Leakage Magnetic Field in Electromagnetic Systems Based on Active Shielding Concept Verified by Eigenvalue Analysis", Progress In Electromagnetics Research, Vol. 96, PP.217-236.*

12. Kaige, Q (2015), "A Novel Masking Scheme for SM3 BasedMAC," SIDE CHANNEL ATTACKS AND COUNTERMEASURES.
13. Kundur, D (2011), "Towards modelling the impact of cyber-attacks on a smart grid", International Journal of Security Network, Vol. 6, No. 1, pp. 2–13.
14.Li, Z(2016),"Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems", IEEE Transactions on Smart Grid, Vol. 7.
15. Liu, Q (2009), "Accurate characterization of shielding effectiveness of metallic enclosures with thin wires and thin slots", IEEE Trans. Electromagnetic Compatabiliti, vol. 51, no. 2, pp. 293–300.
16. Mousavian, S (2014), "A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks," IEEE Transactions on Power Systems, pp. 2174 - 2179.
17. Robinson, M. (1998), "Analytical formulation for the shielding effectiveness of enclosures with apertures," IEEE Trans. Electromagnetic Compatibility, vol. 40, no. 3, pp. 240–248.
18. Sandoval, J (2010), "Measurement, Identification and Calculation of Cyber Defense Metrics",Military Communications Conference Unclassified Program- Cyber Security and Network Management, pp. 2174 - 2179.
19. Stouffer, K (2006), "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 pp 70-82.
20. Wei, L, (2018), "Stochastic Games for Power Grid Protection against Coordinated Cyber-Physical Attacks", IEEE Transactions on Smart Grid, Vol 9. PP 684-694.
21. Yue, J (2014), "Vulnerability Threat Assessment Based on AHP and Fuzzy Comprehensive Evaluation", 2014 Seventh International Symposium on Computational Intelligence and Design (ISCID).
22. Zhang, Y (2015), "Power System Reliability Analysis with Intrusion Tolerance in SCADA Systems," IEEE Transactions on Smart Grid, Vol. 7, PP.
23. Zhang, Y (2016), "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocatio, IEEE Transactions on Power Systems, Vol. 20, pp. 1 - 16.