مجله کنترل
ISSN 2008-8345
جلد ۸، شماره ۱، بهار ۱۳۹۳، صفحه ۴۵-۳۱

مروری بر امنیت سایبری سیستم‌های کنترل صنعتی

احمد افشار[۱]، عاطفه ترمه‌چی[۲]، عارفه گلشن[۳]، آزاده آقائیان[۴]، حمیدرضا شهریاری[۵]

[۱] دانشیار، پژوهشکده پدافند غیرعامل، دانشگاه صنعتی امیرکبیر، aafshar@aut.ac.ir

[۲،۳،۴] فارغ التحصیل کارشناسی ارشد کنترل، پژوهشکده پدافند غیرعامل، دانشگاه صنعتی امیرکبیر

atefetermehchy@aut.ac.ir, arefeh.golshan@aut.ac.ir, aghaeeyan@aut.ac.ir

[۵] استادیار، پژوهشکده پدافند غیرعامل، دانشگاه صنعتی امیرکبیر، shahriari@aut.ac.ir

(تاریخ دریافت مقاله ۱۳۹۳/۲/۴، تاریخ پذیرش مقاله ۱۳۹۳/۳/۱۹)

چکیده: امروزه کلیه زیرساخت‌های حیاتی، واحدهای صنعتی و تجهیزات مدرن شهری و کشوری از سیستم‌های کنترل و اتوماسیون مبتنی بر شبکه، برای پایش و کنترل فرآیندهای خود استفاده می‌نمایند. این سیستم‌ها امکان مدیریت، هماهنگی و بهره‌برداری ایمن، مؤثر و کارآمد از این واحدها را امکان پذیر می‌سازند. به بیان دیگر سیستم‌های کنترل و اتوماسیون نقش مغز و سیستم عصبی پیکره زیرساخت‌های حیاتی و سیستم‌های صنعتی را ایفا می‌کنند. استفاده از فناوری ارتباطات و رایانه که به منظور افزایش کیفیت، کارایی و ضریب اطمینان در سیستم‌های کنترل واتوماسیون به کار می‌روند، تهدیدات ناخواسته‌ای را متوجه این سیستم‌ها کرده‌اند، از جمله مهمترین این تهدیدات حمله‌های سایبری می‌باشد. بررسی تهدیدها و آسیب پذیری‌های سایبری سیستم‌های کنترل و مقابله با آن‌ها بعد از حمله استاکس نت[۱]، به عنوان یک چالش جدی وارد حوزه مطالعاتی و کاربردی گرایش کنترل در دانشگاه‌ها شده است. در واقع شدت تهدیدات سایبری برای سیستم‌های کنترل، بعد از این حمله به وضوح آشکار گردید. طی چند سال گذشته کارهای پژوهشی زیادی در زمینه امنیت سایبری سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی توسط متخصصین رشته کنترل و سایر رشته‌های مرتبط ارائه شده است. هدف از این مقاله مروری بر منابع علمی و دانشگاهی ارائه شده در این زمینه از دید مهندسی کنترل و آشنایی متخصصین این حوزه با ضرورت و فرصت‌های پژوهشی مربوطه می‌باشد.

کلمات کلیدی: حمله سایبری، امنیت سایبری، سیستم‌های کنترل صنعتی، زیرساخت‌های حیاتی.

Survey on Cyber Security of Industrial Control Systems

Ahmad Afshar, Atefe Termehchy, Arefeh Golshan, Azade Aghaeeyan, Hamidreza Shahriyari

Abstract: Today all critical infrastructure and industrial systems apply network-based automation and control systems to monitor and control their processes. Safe, effective and efficient management, coordination and operation of these units are possible through these control systems. In other words, automation and control systems are considered as the brain and nervous systems of critical infrastructure and industrial systems. Using computer and information technology to enhance the quality, performance and reliability of control systems, caused them facing unexpected threats; Cyber attacks are the most important ones. Following the Stuxnet attack, Industrial Cyber Security (ICS) has become a serious challenge for control engineering studies. Over the last few years, many researches have been conducted in the field of ICS. In this paper, we survey the literature of this area from the perspective of control engineering to present an overview of this issue and informing experts of this field with the related importance and research opportunities.

Keywords: Cyber attack, Cyber Security, Industrial Control System, Critical Infrastructure System.

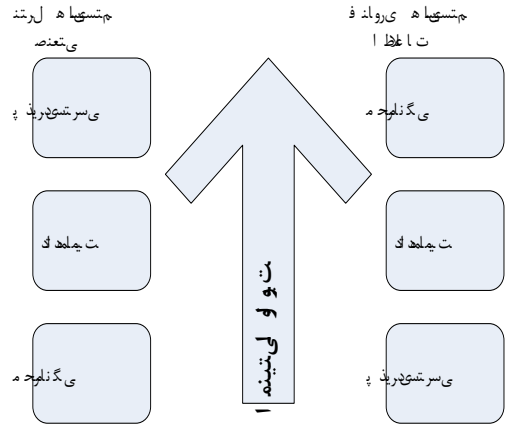
[1] Stuxnet

۱- مقدمه

امروزه کلیه زیرساخت‌های حیاتی، واحدهای صنعتی و تجهیزات مدرن شهری و کشوری از سیستم‌های کنترل و اتوماسیون مبتنی بر شبکه، برای پایش و کنترل فرآیندهای خود استفاده می‌نمایند. این سیستم‌ها امکان مدیریت، هماهنگی و بهره‌برداری ایمن، مؤثر و کارآمد از این واحدها را امکان پذیر می‌سازند. به بیان دیگر سیستم‌های کنترل و اتوماسیون نقش مغز و سیستم عصبی پیکره زیرساخت‌های حیاتی و سیستم‌های صنعتی را ایفا می‌کنند. قطع عملکرد عادی این سیستم‌های کنترل صنعتی[۱] می‌تواند اثر قابل ملاحظه‌ای بر سلامت عمومی و امنیت هر جامعه‌ای داشته باشد و منجر به تلفات اقتصادی زیادی شود.

بسیاری از اتفاقات ناشی از خرابی‌های غیرعمدی، ممکن است عملکرد عادی این سیستم‌ها را تحت تأثیر قرار دهد. با این حال، بزرگترین تهدید برای سیستم‌های کنترل صنعتی، خرابی‌های عمدی هدف‌دار است که در گذشته به صورت حمله فیزیکی به اجزای سیستم کنترل صورت می‌پذیرفت و هدف آن‌ها مختل کردن عملکرد سیستم بود. حملات سایبری، تکامل طبیعی برای این نوع حمله‌ها می‌باشند که برای مهاجمان ارزان‌تر و کم‌خطرتر بوده و تحت اثر فاصله نیستند، در عین حال تکرار و هماهنگی آن‌ها بسیار راحت‌تر است. در بین حمله‌های سایبری که تا به حال به سیستم‌های کنترل صنعتی انجام شده است، هیچ حمله‌ای به اندازه حمله استاکس نت نتوانسته‌است آشکارکننده اهمیت این نوع تهدیدات، برای سیستم‌های کنترل و به تبع آن سیستم‌های صنعتی و زیرساخت‌های حیاتی باشد.

وضعیت کنونی امنیت سایبری در سیستم‌های کنترل صنعتی ناامید کننده است و قابل قیاس با وضعیت امنیت سایبری IT در ۱۵ سال پیش می‌باشد[۱]. از سویی دیگر، به علت ماهیت متفاوت سیستم‌های کنترل صنعتی و IT، راه حل‌های امنیتی IT کفایت نیازهای مربوطه در سیستم‌های کنترل صنعتی را نمی‌دهد. به طور کلی هدف از امنیت در IT، حفاظت از داده‌ها است، در حالی‌که در سیستم کنترل صنعتی، حفظ عملکرد عادی سیستم و جلوگیری از خرابی[۲] در آن می‌باشد. به عبارت ساده‌تر هدف راهبردهای امنیتی سیستم‌های کنترل صنعتی، حفظ کارکرد اجزا می‌باشد به طوری‌که کل سیستم بتواند به خوبی و ایمن، کار خود را انجام دهند. تفاوت در هدف، منجر به تفاوت در اولویت‌های امنیتی این دو سیستم نیز می‌شوند، در شکل ۱ این تفاوت نمایش داده شده است:



شکل ۱: اولویت‌های امنیت در سیستم‌های IT و کنترل صنعتی[۲]

طی چند سال گذشته کارهای پژوهشی زیادی در زمینه امنیت سایبری سیستم‌های کنترل صنعتی توسط متخصصین رشته کنترل و سایر رشته‌های مرتبط ارائه شده است. با وجود گستردگی و تنوع موضوعی مقاله‌های منتشر شده، متأسفانه تعداد مقالات مروری[۳] در این زمینه اندک هستند. ازاینرو قلمروی بحث برای محققین تازه وارد، مبهم و ناشناخته می‌باشد. از جمله مقالات مروری در این زمینه می‌توان به مراجع [۳-۵] اشاره کرد. منبع [۳] به بررسی مقاله‌های ارائه شده در زمینه سیستم‌های تشخیص نفوذ در سیستم‌های سایبر فیزیکی[۴](سیستم‌های کنترل صنعتی یک سیستم فیزیکی سایبری محسوب می‌شوند) می‌پردازد. این منبع ابتدا مفهوم سیستم‌های سایبر فیزیکی را تبیین می‌کند، سپس ضمن بررسی منابع، تکنیک‌های سیستم تشخیص نفوذ در این سیستم‌ها را دسته‌بندی کرده و مزایا و معایب هر یک را عنوان می‌کند. در منبع [۴]، بررسی جامع و وسیعی از مقالات علمی مرتبط با مسائل امنیت سایبری شبکه‌های هوشمند[۵] انجام گرفته است. هدف این منبع ارائه درک عمیقی از آسیب‌پذیری‌های امنیتی و راه‌حل‌های آن‌ها در شبکه‌های هوشمند بوده و به بیان نیازمندی‌های امنیتی، آسیب‌پذیری‌های شبکه، پروتکل‌های ارتباطی امن و معماری شبکه‌های هوشمند می‌پردازد. منبع [۵] مقاله‌های ارزیابی ریسک در سیستم‌های SCADA و DCS را بررسی و مفاهیم اصلی مرتبط با ارزیابی ریسک حمله‌های سایبری در این سیستم‌ها را بیان می‌کند.

بنابراین، کمبود مقاله‌های مروری در زمینه "امنیت سایبری سیستم‌های کنترل صنعتی" از یک سو و ناشناخته بودن زمینه‌های تحقیقاتی آن در جامعه دانشگاهی مهندسی کنترل کشور از سویی دیگر، هدف این مقاله را مروری بر منابع علمی و دانشگاهی ارائه شده در این زمینه از دید مهندسی کنترل قرار داده است. نوآوری این مقاله ارائه یک تقسیم‌بندی جامع از مسائل پیشروی امنیت سیستم‌های

[۱] سیستم‌های کنترل زیر ساخت‌های حیاتی و واحدهای صنعتی در این مقاله به اختصار، با عنوان سیستم‌های کنترل صنعتی شناخته می‌شوند.

[2] Failure

[3] Survey Papers
[4] Cyber Physical System(CPS)
[5] Smart Grid

کنترل صنعتی در مقابل حملات سایبری و بررسی مقاله‌ها در چهارچوب این دسته‌بندی می‌باشد.

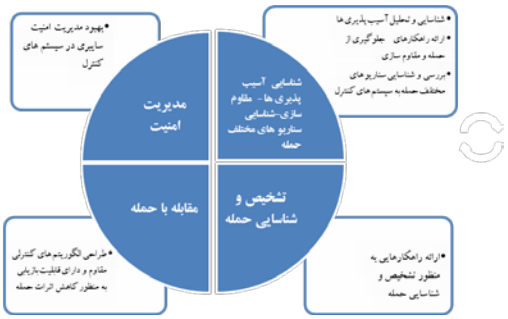
مسائل پیشروی امنیت سیستم‌های کنترل صنعتی در مقابل حملات سایبری مطابق شکل ۲ به چهار دسته زیر تقسیم‌بندی می‌شود:

اول) شناسایی آسیب‌پذیری‌ها و سناریوهای مختلف حمله به سیستم‌های کنترل صنعتی و تلاش برای جلوگیری از آن

دوم) ارائه راهکارهایی به منظور تشخیص و شناسایی حمله

سوم) بازترکیب و استفاده از ابزارهای کنترلی به منظور کاهش اثرات حمله و افزایش خاصیت خودترمیمی سیستم

چهارم) بهبود مدیریت امنیت سایبری در سیستم‌های کنترل صنعتی

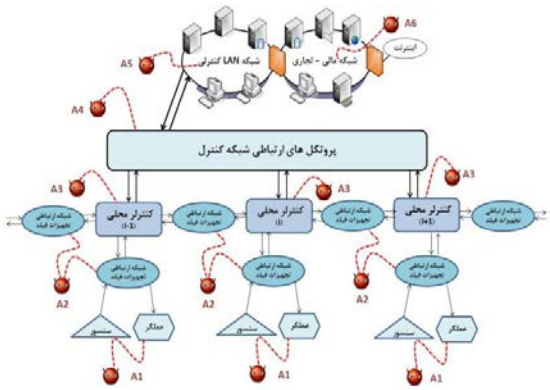


شکل ۲: تقسیم‌بندی زمینه‌های مطالعاتی امنیت سایبری سیستم‌های کنترل صنعتی

در این مقاله مروری، ابتدا یک مدل مفهومی از آسیب‌پذیری‌های سیستم کنترل صنعتی ارائه خواهد شد تا بدین وسیله یک چارچوب کلی از موضوع آسیب‌پذیر بودن سیستم کنترل صنعتی در مقابل حمله‌های سایبری ترسیم شود. بخش سوم این مقاله به بررسی مقالات ارائه شده در زمینه شناسایی آسیب‌پذیری‌های و سناریوهای مختلف حمله به سیستم‌های کنترل صنعتی و مقاوم‌سازی آن‌ها می‌پردازد. در بخش چهارم مقاله، به بررسی راهکارهای ارائه شده در زمینه تشخیص و شناسایی حملات سایبری در سیستم‌های کنترل صنعتی می‌پردازد. مقابله با حمله و استفاده از ابزارهای کنترلی به منظور کاهش اثرات حمله و خودترمیمی سیستم در بخش پنجم مورد بررسی قرار می‌گیرد. هدف کلی از مقالات بررسی‌شده در این بخش، از بین بردن و یا کاهش اثرات حمله بر روی عملکرد نامی سیستم و حفظ پایداری آن می‌باشد. با توجه به گستردگی تهدیداتی که سیستم‌های کنترل صنعتی در معرض آن‌ها هستند، علاوه بر راهبردهای امنیتی مختلف، مدیریت امنیت از نقطه اثر بسیار بالایی برای حفظ امنیت در برابر حملات سایبری برخوردار می‌باشد. از اینرو در بخش ششم به این مهم پرداخته می‌شود. در پایان، جمع‌بندی و نتیجه‌گیری ارائه می‌گردد.

۲- مدل مفهومی آسیب‌پذیری‌های سیستم کنترل صنعتی

سیستم‌های کنترل صنعتی وظیفه‌ی هدایت و کنترل فرآیندهای فیزیکی را برعهده دارند که معمولاً متشکل از مجموعه‌ای از اجزای متعدد شامل حسگرها، عملگرها، واحدهای پردازش داده مانند کنترل‌کننده‌های منطقی قابل برنامه ریزی (PLCs)، شبکه‌های ارتباطی و رایانه‌های مرکزی می‌باشند. چندین مدل کلی برای تبیین ساختار سیستم کنترل صنعتی وجود دارد که یکی از پرکاربردترین آن‌ها ساختار ارائه‌شده توسط استاندارد ISA-88/01 می‌باشد [۶, ۷]. در این مقاله با الهام از این ساختار و منبع [۸]، مدل مفهومی آسیب‌پذیری‌های سیستم کنترل صنعتی مطابق شکل ۳ بیان می‌شود:



شکل ۳: مدل مفهومی آسیب‌پذیری‌های سیستم کنترل صنعتی

در این شکل آسیب‌پذیری‌های سیستم کنترل صنعتی به شش دسته زیر تقسیم‌بندی می‌شوند:

۱. آسیب‌پذیری‌های تجهیزات فیلد
۲. آسیب‌پذیری‌های شبکه ارتباطی تجهیزات فیلد
۳. آسیب‌پذیری‌های کنترل‌کننده‌های محلی مانند RTU، PLC
۴. آسیب‌پذیری‌های پروتکل‌های ارتباطی شبکه کنترل
۵. آسیب‌پذیری‌های شبکه LAN کنترلی
۶. آسیب‌پذیری‌های شبکه‌های همکار و مالی – تجاری

ساختار لایه‌ای این مدل مفهومی بر این نکته تأکید می‌کند که نوع آسیب‌پذیری‌های هر لایه سیستم کنترل صنعتی متفاوت است و به تبع آن هر لایه نیازمند اقدامات امنیتی متفاوتی نیز می‌باشد[۱].

[۱] توضیح کامل این مدل مفهومی در مقاله‌ای جداگانه ارائه خواهد شد.

۳- شناسایی آسیب‌پذیری‌ها و سناریوهای مختلف حمله به سیستم‌های کنترل صنعتی و تلاش برای جلوگیری از حمله

با پیشرفت سیستم‌های کنترل صنعتی و استفاده آن‌ها از سکوهای نرم‌افزاری، سخت‌افزاری و شبکه‌ای یکسان و دارای استانداردهای واحد، دسترسی افراد غیرمجاز به لایه‌های درونی این سیستم‌ها امکان‌پذیر شده است. به طور کلی مهاجمی که قصد حمله سایبری و صدمه به یک سیستم کنترل صنعتی را دارد، با ۲ چالش عمده مواجه است:

۱) شناسایی سیستم، نفوذ و دسترسی به آن
۲) دردست‌گرفتن کنترل کامل و یا قسمتی از فرآیند و ایجاد صدمه به آن

بنابراین قدم اول در امن کردن سیستم‌های کنترل صنعتی، شناسایی آسیب‌پذیری‌ها و نقاط دسترسی به آن‌ها می‌باشد که می‌توان آن را در دو زمینه عمده تجهیزات (از لحاظ سخت‌افزاری، سفت‌افزاری[1]، نرم‌افزاری) و پروتکل‌های ارتباطی تقسیم‌بندی کرد. تجهیزاتی که در سیستم‌های کنترل صنعتی به‌کار گرفته می‌شوند نیز بر دو دسته هستند:

۱. تجهیزاتی که صرفاً در سیستم‌های کنترل مورد استفاده قرار می‌گیرند مانند سنسورها، عملگرها، PLC ها، RTU ها،و ...
۲. تجهیزات فناوری اطلاعات که در دیگر سیستم‌ها و شبکه‌ها نیز استفاده می‌شوند مانند روتورها، سوئیچ‌ها، رایانه‌ها و ...

در این بخش ابتدا تعدادی از مقالاتی که آسیب‌پذیری‌های پروتکل‌های ارتباطی سیستم کنترل صنعتی و راهکارهای مقابله با آن‌ها را مورد توجه قرار داده‌اند، مورد بررسی قرار می‌گیرند. سپس با توجه به گستردگی آسیب‌پذیری‌های تجهیزات و مقالات در این زمینه، در این مجال فقط به آسیب‌پذیری‌های تجهیزات دسته اول پرداخته می‌شود. در نهایت نیز چهار دسته از سناریوهای مطرح شده در زمینه‌ی حمله به سیستم‌های کنترل صنعتی بررسی می‌گردد.

۳-۱ آسیب‌پذیری‌های پروتکل‌های ارتباطی و تلاش برای جلوگیری از نفوذ مهاجم

امروزه پروتکل‌های بسیار زیادی در سیستم‌های کنترل صنعتی استفاده می‌شوند. بیشتر این پروتکل‌ها با هدف افزایش کارایی، قابلیت اطمینان در عملیات بلادرنگ و پشتیبانی از الزامات اقتصادی و عملکردی طراحی شده‌اند. متأسفانه اکثر این پروتکل‌ها به جهت بالا بردن کارایی، از هر ویژگی غیرضروری از جمله ویژگی‌های امنیتی نظیر احراز اصالت و رمزنگاری صرف‌نظر کرده‌اند. از سوی دیگر بسیاری از آن‌ها برای استفاده از پروتکل اترنت و اتصال به شبکه اینترنت توسعه داده شده‌اند. بنابراین پروتکل‌های ارتباطی سیستم‌های کنترل صنعتی بسیار آسیب‌پذیر بوده و در معرض حملات زیادی قرار گرفته‌اند[۹].

طبق گزارش انجمن گاز آمریکا[2] [۱۰] در حدود ۱۵۰ تا ۲۰۰ پروتکل اسکادا[3] وجود دارد. یکسان‌سازی این پروتکل‌ها در سال‌های اخیر، منجر به کسب اطلاعات بسیار دقیق مهاجمان از کارکرد و ساختار آن‌ها شده است. به این ترتیب مهاجمان با شناسایی آسیب‌پذیری‌های این پروتکل‌ها می‌توانند به بسته‌های داده دسترسی پیدا کرده و به دلخواه در آن‌ها تغییراتی ایجاد کنند [۱۱]. مانند حمله به سیستم کنترل آب و فاضلاب شهر کوئیزلند استرالیا در سال ۲۰۰۰ که مهاجم به واسطه داشتن اطلاعات کامل از پروتکل مورد حمله، توانست به شبکه ارتباطی لایه فیلد نفوذ کرده و هشتصد هزار لیتر فاضلاب را وارد چرخه آب سالم این شهر کند.

آسیب‌پذیری‌های این پروتکل‌ها در منابع متعددی [۹, ۱۱-۲۱] و مورد بررسی قرار گرفته است. در منبع [۹] انواع پروتکل‌های صنعتی، آسیب‌پذیری‌ها و راهکارهای امنیتی آن‌ها بررسی می‌شود. یکی از موارد بررسی‌شده در این منبع پروتکل مودباس[4] است که فاقد احراز اصالت، رمزگذاری و مجموع مقابله‌ای پیام‌ها[5] می‌باشد. یکی از سودمندترین و درعین‌حال خطرناک ترین ویژگی‌های مودباس، قابلیت استفاده از آن به منظور برنامه‌ریزی کنترل‌کننده‌ها می‌باشد که بسیاری از پروتکل‌های صنعتی در این ویژگی با مودباس اشتراک دارند. به‌واسطه این ویژگی خطرناک، مهاجم می‌تواند از این طریق برای تزریق برنامه‌های مخرب در PLCها و RTU ها استفاده کند. آسیب‌پذیری پروتکل مودباس به عنوان پرکاربردترین پروتکل صنعتی، در منابع دیگر [۱۳, ۱۴] نیز تشریح شده است. در منبع [۱۳] چهار کلاس از آسیب پذیری های پروتکل مودباس از جمله آسیب پذیری منع خدمت[6] و تزریق فرمان به این پروتکل و راه‌های نفوذ مهاجم به آن بررسی شده است. از جمله روش‌های تشخیص نفوذ در پروتکل‌های مودباس، استفاده از سیستم‌های تشخیص نفوذ مبتنی بر مدل[7] می‌باشد. منبع [۱۴] سه روش مبتنی بر مدل را برای پایش و تشخیص حمله به پروتکل Modbus TCP معرفی می‌کند. این روش‌ها با توجه به توپولوژی و ساختار ارتباطی شبکه اسکادا، مکانیسمی حفاظتی برای پروتکل Modbus/TCP IP ارائه می‌دهد. مدل‌های ارائه شده توسط این منبع به منظور توصیف درخواست‌ها و پاسخ‌های این نوع مودباس بر اساس اسناد توصیف کاربرد آن و راهنمای پیاده‌سازی Modbus، به کار گرفته شده‌اند [۲۲, ۲۳]. یکی دیگر از پروتکل‌های بررسی شده در منابع، پروتکل WirelessHART می‌باشد که به طور خاص برای سیستم‌های کنترل صنعتی طراحی و در سال ۲۰۰۷ توسط سازمان ارتباطات HART[8] تصویب شده است [۲۰].

[1] Firmware

[2] American Gas Association (AGA)
[3] SCADA
[4] Modbus
[5] Message Checksum
[6] Denial Of Service
[7] Model-based Detection
[8] HART Communication Foundation

منابع گوناگونی از جمله [۱۸-۲۰, ۲۴] مکانیزم‌های امنیتی این پروتکل را تشریح کرده‌اند. منبع [۲۰] به منظور تضمین محرمانه بودن و تمامیت داده، روش‌های مختلف رمزگذاری در این پروتکل را بررسی کرده است.

در راستای جلوگیری از ورود غیرمجاز به سیستم تحت حفاظت، دیوار آتش[1] به عنوان راهکار امنیتی در اکثر منابع پیشنهاد شده است [۱۱, ۲۵-۲۷]. یکی از وظایف آن ممانعت از ورود پیام‌هایی است که ساختار آن‌ها مطابق با پروتکل ارتباطی ناحیه تحت حفاظت نمی‌باشد. مرکز همکاری امنیت زیرساخت‌های ملی انگلستان[2] کتابچه راهنمایی مبنی بر راهکارهای استفاده، پیکربندی و مدیریت دیوارهای آتش در شبکه اسکادا[3] را منتشر کرده است. برای جلوگیری از نفوذ مهاجمان در سیستم، وجود سیستم‌های تشخیص متجاوز[4] به همراه دیوار آتش لازم و ضروری است. البته بهبود این سیستم‌ها وابسته به شناسایی آسیب‌پذیری شبکه و پروتکل‌های اسکادا می‌باشد [۲۸].

یکی دیگر از راهکارهای رایج در افزایش امنیت پروتکل‌های ارتباطی استفاده از رمزنگاری[5] است. روش‌های سنتی گوناگونی برای رمزنگاری وجود دارد، اما اکثر آن‌ها قابلیت استفاده در سیستم‌های کنترل صنعتی را ندارند. دلیل این امر، توانایی محاسباتی محدود و سرعت انتقال داده کم اجزای این سیستم‌ها می‌باشد که در عین حال باید پاسخگوی ضرورت عملکرد بلادرنگ[6] نیز باشند. این محدودیت‌ها، اجرای رمزنگاری‌های پیچیده را با مشکل مواجه می‌کنند [۱۱, ۲۹, ۳۰]. استاندارد AGA-12 [۱۰] مشکلات اجرای رمزنگارها و راهکارهای تکنیکی اجرایی آن را توضیح داده است. برای غلبه به این مشکلات، اتصال ماژول سخت‌افزاری رمزنگار به هر گره توسط [۳۱] پیشنهاد شده است.

۳-۲ آسیب‌پذیری‌های تجهیزات کنترلی

بسیاری از حملات سایبری در سیستم‌های کنترل صنعتی با سوءاستفاده ازآسیب‌پذیری‌های موجود در تجهیزات کنترلی انجام گرفته که یکی از مشهورترین آن‌ها، حمله استاکس نت است. ازاینرو شناسایی این آسیب‌پذیری‌ها یکی از موضوعات مورد توجه محققین در این حوزه می‌باشد [۲۱, ۳۲-۳۷]. در سال‌های اخیر علاوه بر آسیب‌پذیری‌های نرم‌افزاری، انواع سخت‌افزاری و سفت‌افزاری نیز به‌شدت مورد توجه کارشناسان امنیت قرار گرفته است. این موارد در پردازنده‌ها و قطعات الکترونیکی به‌طور گسترده وجود دارند و حتی در سطوح مخابراتی و یا نظامی نیز یافت می‌شوند. نمونه‌ی بارزی از این آسیب‌پذیری‌ها، وجود یک نقطه‌ی دسترسی مخفی در تراشه‌های ساخت یک شرکت چینی می‌باشدکه در تجهیزات نیروی هوایی آمریکا نیز به‌کار می‌روند[۳۸] و توسط تیم تحقیقاتی دانشگاه کمبریج شناسایی شده است. عموماً این نوع تهدیدات به عنوان آسیب‌پذیری‌های درپشتی[7] در تجهیزات در نظر گرفته می‌شوند. [۳۹, ۴۰]

سیستم‌های کنترل شامل تجهیزات الکترونیکی و پردازشی متنوعی است که از جمله مهمترین این تجهیزات، عملگرها، سنسورها، PLC ها و RTU ها می‌باشند. مهاجمان با دسترسی به کد نرم‌افزاری و یا سفت‌افزاری این تجهیزات، می‌توانند به راحتی به سامانه‌ی کنترل نفوذ کرده و کنترل فرآیند را در دست گیرند[8]. منابع بسیاری از جمله [۳۲, ۴۱, ۴۲] این نوع آسیب‌پذیری‌های PLC ها را مورد بررسی قرار داده‌اند که حاکی از ضعف شدید این ابزارها در حوزه امنیت سایبری می‌باشد. نمونه‌هایی از اشکالات امنیتی همه تجهیزات کنترلی نیز در مرجع [۴۳] موجود است. از جمله آسیب‌پذیری‌های عنوان شده در این مرجع برای RTUها، تایید ورودی نامناسب و غیر ایمن این تجهیز می‌باشد که منجر به نفوذ مهاجم به سیستم کنترل صنعتی می گردد.

۳-۳ بررسی و شناسایی سناریوهای مختلف حمله به سیستم‌های کنترل صنعتی

چهار دسته از سناریوهای مطرح شده در زمینه‌ی حمله به سیستم‌های کنترل صنعتی، به شرح زیر است:

۳-۳-۱ حمله فریب[9](حمله تزریق داده غلط استاتیک[10])

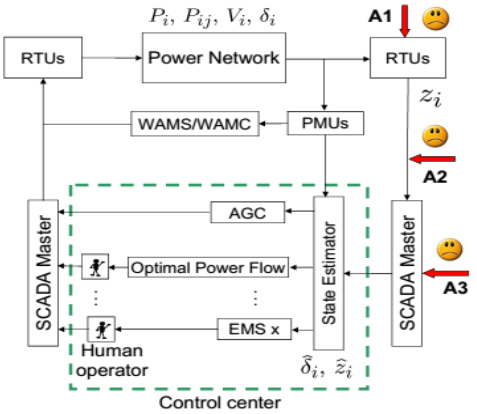
در حمله فریب، مهاجم خروجی حسگرها را به شکلی تغییر می‌دهد که سیستم کنترل فریب خورده و متوجه ارسال داده غلط به کنترل‌کننده نمی‌شود. این سناریو اولین بار توسط آقای Liu در سال ۲۰۰۹ برای حمله به سیستم قدرت و سیستم تشخیص داده غلط آن، با فرض آگاهی کامل مهاجم از سیستم مطرح شد [۴۴, ۴۵]. در منبع [۴۶, ۴۷] نویسنده اثبات کرده است که مهاجم حتی با داشتن آگاهی نسبی نیز می‌تواند حمله موفقیت‌آمیزی را صورت دهد. در راستای تلاش برای مقابله با این حمله، منبع [۴۸] دو مقیاس امنیتی برای تخمینگر حالت شبکه قدرت پیشنهاد می‌دهد که در واقع مقیاسی از حداقل تلاش‌های ضروری مهاجم برای اجرای موفق حمله می‌باشد. این مقیاس‌ها وابسته به توپولوژی فیزیکی شبکه قدرت و میزان دسترسی‌پذیری مقادیر خروجی حسگرها می‌باشند. منبع [۴۹] عنوان می‌کند که اجرای حفاظت کامل و رمزنگاری از خروجی تمام تجهیزات مقرون به صرفه و قابل اجرا نیست و با حفاظت از تعداد محدودی از اندازه‌گیرها و خروجی آن‌ها می توان از موفقیت حمله تزریق جلوگیری کرد. تعداد این اندازه‌گیرها برابر با تعداد متغیرهای

[1] Firewall
[2] National Infrastructure Security Coordination Center (NISCC)
[3] SCADA (Supervisory Control and Data acquisition)
[4] Intrusion Detection Systems (IDS)
[5] Cryptography
[6] Real Time
[7] Backdoor
[8] حمله به خطوط انتقال گاز سیبری(۱۹۸۲)، حمله استاکس نت(۲۰۱۰) و ...
[9] Stealth Attack
[10] False Data Injection Attack(Static)

حالت سیستم می‌باشد. منبع [۵۰] دو الگوریتم دیگر حفاظت از تعداد محدودی از تجهیزات را به نحوی پیشنهاد می‌دهد که حداکثر امنیت در مقابل حمله تزریق فراهم شود. منبع [۵۱] ابتدا راهبرد حمله بهینه‌ای را تشریح می‌کند که می‌تواند حداکثر صدمه را به سیستم وارد کند، سپس با فرموله کردن مسئله دفاع، توانسته است راهبرد دفاع بهینه‌ای را مطرح و میزان صدمه را حداقل کند. اثرات اقتصادی حمله تزریق داده بر روی عملکرد بازار شبکه برق در منبع [۵۲] فرموله شده است.

۳-۳-۱-۱ حمله به تخمینگر حالت شبکه قدرت و تزریق داده غلط

هدف تخمینگر حالت شبکه‌های قدرت، تخمین متغیرهای حالت آن سیستم بر اساس داده‌های اندازه گیری شده است. در منبع [۵۳]، نحوه ساخت ماتریس متغیرهای حالت سیستم قدرت توسط مرکز کنترل بیان شده است. تخمین‌های نامناسب می‌تواند به دلایل مختلف مانند خرابی اندازه‌گیرها و یا حملات خرابکارانه باشد. در سناریو مطرح شده توسط آقای Liu فرض می‌شود مهاجم ماتریس متغیرهای حالت سیستم قدرت مورد هدف را می‌داند و اندازه‌گیری‌های خرابکارانه را با علم به این ماتریس می‌سازد. سپس این اندازه‌گیری‌های غلط را به سیستم کنترل تزریق می‌کند تا فرآیند تخمین حالت را دچار اشتباه نماید.



شکل ۴: حمله تزریق داده وشبکه قدرت [۴۸]

۳-۳-۲ حمله تزریق داده غلط دینامیک

در این حمله سعی می‌شود تزریق داده غلط به صورت دینامیک بوده و یک مد ناپایدار و مشاهده‌ناپذیر در سیستم ایجاد کند. در منبع [۵۴] فرض شده است که هدف مهاجم، تزریق داده غلط، ناپایدار کردن سیستم و مخفی ماندن است. نویسنده برای پایش و کنترل سیستم خطی ناپیوسته نامتغیر با زمان و همچنین شناسایی حمله تزریق داده غلط دینامیک، از فیلتر کالمن و کنترل‌کننده LQG استفاده می‌کند. در نهایت این مقاله شرایط لازم و کافی را برای اجرای یک حمله موفقیت‌آمیز را نیز تشریح کرده و روشی را برای مقابله با حمله براساس استفاده از سنسورهای افزونه[1] پیشنهاد می‌دهد.

منبع [۵۵] اثر این حمله را بر روی شناساگری در نظر می‌گیرد که از ابزار رویتگر با ورودی نامشخص[2] استفاده می‌کند و پس از بررسی چگونگی فریب، راهکاری بهینه بر مبنای شناسایی حسگرهای بحرانی و حفاظت کامل از آن‌ها ارائه می‌دهد.

۳-۳-۳ حمله بازسازی اطلاعات[3]

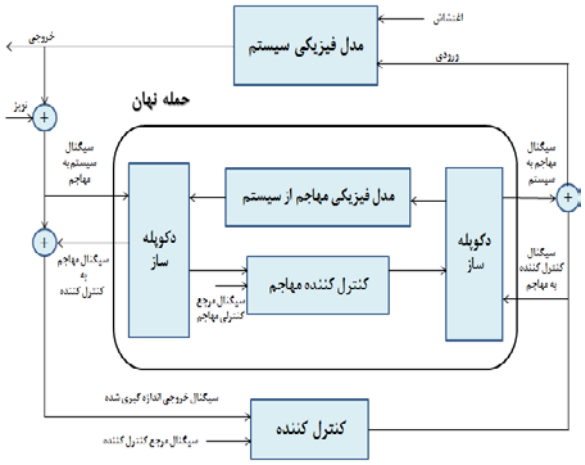
از جمله خطرناک ترین حملات، حمله بازسازی اطلاعات به شمار می‌آید. همان طور که در حمله‌های "تزریق داده" نیز ملاحظه شد، درصورتی‌که مهاجم بتواند به داده خروجی حسگر یا عملگر دسترسی پیدا کند، می‌تواند داده غلط را به صورت هوشمند و هدف‌دار و یا به طور تصادفی وارد سیستم کند و کنترل‌کننده را دچار خطا نماید[۵۶]. در حمله بازسازی اطلاعات، مهاجم اطلاعات حسگر و یا عملگر را در شرایط عادی سیستم ثبت کرده و آن را در زمان حمله و خرابکاری برای شبکه کنترل ارسال می‌کند[۵۷]. به این ترتیب سیستم کنترل به طور هوشمند فریب می‌خورد و علاوه بر از بین رفتن کنترل حلقه بسته، سیستم به حالت خطرناک می‌رود. یکی از روش‌های مقابله با این حمله، اضافه کردن ورودی تصادفی گوسین با میانگین صفر به ورودی سیستم است[۵۶]. ورودی تصادفی، یک سیگنال تأیید هویت محسوب می‌شود و تلاش بر این است که به صورت بهینه طراحی شود تا کمترین اثر را روی بازدهی سیستم بگذارد[۵۸] .

۳-۳-۴ حمله نهان[4]

این حمله در واقع یک حمله بازسازی اطلاعات حلقه بسته می‌باشد. به عبارت دیگر خروجی حمله به صورت حلقه بسته بازسازی می‌شود تا اثر آن بر خروجی حسگرها از بین برود و حمله مخفی بماند. در این حمله، مهاجم باید آشنایی کامل از مدل فیزیکی سیستم تحت کنترل داشته باشد تا بتواند مدلی مشابه با آن را شبیه‌سازی کند. مهاجم، مدل شبیه‌سازی شده و کنترل‌کننده‌ی مورد نظر خود را به صورت شکل ۵ بین سیستم و کنترل‌کننده اصلی قرار داده و با ارسال همزمان سیگنال‌های دلخواه به ورودی کنترل‌کننده اصلی و سیستم تحت کنترل، حمله را مخفی و نقطه کار دلخواه خود را جایگزین می‌کند[۵۹].

[1] Redundant Sensor

[2] Unknown Input Observer (UIO)
[3] Replay Attack
[4] Covert Attack



شکل ۵: حمله نهان

٤- ارائه راهکارهایی به منظور تشخیص و شناسایی حمله

هدف هر مهاجم از حمله به سیستم کنترل صنعتی، صدمه زدن و ایجاد اثر نامطلوب بر روی سیستم فیزیکی تحت کنترل آن است. از این رو مهندسین کنترل تلاش می‌کنند با نظارت بر رفتار سیستم تحت کنترل، راهکاری برای شناسایی حمله بیان کنند. پژوهش‌ها و مقاله‌های زیادی در این راستا انجام گرفته است که می‌توان به صورت زیر آن‌ها را دسته‌بندی کرد:

۱. مدل کردن حمله،

۲. تشخیص و شناسایی حمله و اثرات آن.

۴-۱ مدل کردن حمله

همان طور که اشاره شد در سیستم‌های صنعتی و زیرساخت‌های حیاتی هدف نهایی حمله، ایجاد خرابی یا اختلال در عملکرد تجهیزات و لایه فیزیکی سیستم می‌باشد. در حوزه علم کنترل مطالعه و تحقیق بر روی اختلال و یا خرابی غیرعمدی تجهیزات از دهه ۸۰ میلادی آغاز شده است اما خرابی‌های عمدی، موضوع نوظهوری است که در سال‌های اخیر به منظور توصیف خرابی‌ها و اختلال‌های ناشی از حمله‌های سایبری و همچنین مدل کردن این حمله‌ها به کار می‌رود. محققین متعددی برای مدل‌سازی حمله تلاش کرده‌اند[۸, ۵۵, ۶۰-۶۳]. در منابع [۸, ۶۴]، مدلی برای تعریف حمله به حسگرها به صورت زیر ارائه داده شده است:

$$\tilde{y}_i(t)=\begin{cases} y_i(t) & for\ t \notin t_a \\ a_i(t) & for\ t \in t_a \end{cases} \quad (۱)$$

$$\text{such that } t_a=\{t_s,\ldots,t_e\}$$

در این مدل t_s زمان شروع حمله و t_e زمان اتمام حمله می‌باشد. نویسنده این منبع تأکید می‌کند این مدل می‌تواند دو حمله به تمامیت اطلاعات[۱] و حمله منع خدمت[۲] را تشریح کند.

منبع [۶۰]، مدلی مشابه ارائه کرده است با این تفاوت که در مدل خود تغییراتی در نظر گرفته است تا بتواند اثرات حمله بر سیستم را نیز بر مبنای آن استخراج کند. همچنین منبع [۵۵] با توجه مدل مطرح شده در منبع [۸]، علاوه بر حمله به حسگرها، حمله به عملگرها را به صورت زیر در نظر گرفته است:

$$\dot{x}(t)=Ax(t)+Bu(t)+Ed(t)+Bf_a(t) \quad (۲)$$

$$y(t)=Cx(t)+f_s(t)$$
$$X(t)\in R^n, U(t)\in R^p, Y(t)\in R^m, d\in R^q \quad (۳)$$

که در این مدل $d(t)$ نمایانگر اغتشاش و نویز، $f_a(t)\in R^p$ نشان‌دهنده حمله به عملگر و $f_s(t)\in R^m$ نشان‌دهنده حمله به حسگر می‌باشد. همچنین مدلی متناسب با حمله به تمامیت اطلاعات و حمله منع خدمت به منظور استخراج اثرات مالی و هزینه‌های حمله، در منبع [۶۰] نیز مطرح شده است.

۴-۲ تشخیص و شناسایی حمله و اثرات آن

با توجه به این که در سیستم‌های کنترل صنعتی تبادل داده باید بدون وقفه صورت گیرد. منبع [۶۵] ایده‌ی تبدیل کد محدوده زمانی[۳] به کد میکرو زمان[۴]، و بررسی آن توسط تجهیزات یا سیستم عامل را برای تشخیص حمله پیشنهاد می‌دهد.

در راهبردهای امنیتی از دیدگاه مهندسی کنترل برای مقابله با حملات سایبری، تمرکز روی هدف نهایی حمله کننده است. از این رو مدل فیزیکی و دینامیک سیستم یا به طور کلی مدل کمی-کیفی مورد توجه قرار گرفته است.

منابع [۸, ۳۳, ۵۵, ۶۳, ۶۶, ۶۷] استفاده از الگوریتم‌های تشخیص خطا را برای تشخیص حمله پیشنهاد داده‌اند. البته این نکته باید مورد توجه قرار گیرد که حمله، یک خطای عمدی و تحت سناریو بوده و همچنین از لحاظ دامنه کمی ممکن است متفاوت با خطا باشد. در این دیدگاه برای

---

[۱] حمله به تمامیت اطلاعات (Integrity Attack) در سیستم‌های کنترل صنعتی : مهاجم سعی می‌کند خروجی حسگر ویا عملگر ویا کنترل‌کننده را تغییر دهد و خروجی غلط را به مقصد برساند.

[۲] حمله منع خدمت (Denial Of Service) در سیستم‌های کنترل صنعتی: مهاجم سعی می‌کند مانع دسترسی کنترل‌کننده ویا عملگر به داده مورد نیاز خود شود.

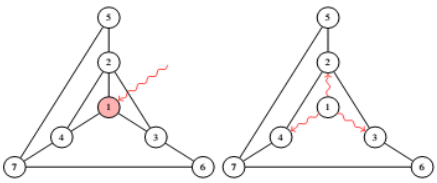
[3] timing bound
[4] micro-timings

تشخیص یک حمله یا خطای عمدی، باید تخمینی نسبتاً دقیق از خروجی سیستم وجود داشته باشد و نیز الگوریتمی برای تشخیص، انتخاب و یا طراحی شود. مثلاً با استفاده از تفاوت خروجی تخمین‌زده‌شده و خروجی به‌دست‌آمده از حسگرها و مقایسه‌ی آن‌ها با یک حد آستانه، می‌توان به وجود حمله پی برد [۸, ۳۳, ۵۵, ۶۳, ۶۸, ۶۹]. درمنبع [۸] از رویتگر با ورودی ناشناخته به عنوان ابزار تخمین‌گر مقاوم استفاده می‌شود، اما این تخمین‌گر دو ناکارآمدی عمده دارد:۱) ناتوانایی در استفاده از این تخمین‌گر در سیستم‌های نامینیمم فاز و ۲) ناتوانایی در زمان حمله‌های همزمان. راهکارهای حل این دو ناکارآمدی در منبع [۵۵] پیشنهاد داده شده است.

منبع [۶۸] از یک مدل خطی برای سیستم تحت کنترل استفاده می‌کند و حمله را به عنوان یک ورودی ناشناخته در نظر می‌گیرد. این منبع با بهره‌گیری از نظریه کنترل هندسی[1]، شرایطی را برای تشخیص[2] و شناسایی‌پذیری[3] حمله ارائه می‌دهد و به منظور تشخیص و شناسایی حمله‌هایی که این شرایط را ندارند، از نظریه گراف بهره می‌گیرد. این منبع با استفاده از فیلتر مبتنی بر شکل موج ساده شده[4] به منظور تشخیص حمله، نشان می‌دهد که مسئله تشخیص حمله از لحاظ محاسباتی بسیار پیچیده است و باید از یک پروسه تشخیصی توزیع شده بهینه[5] و زیربهینه[6] استفاده شود. منبع [۶۶] با کمک تکنیک‌های انتخاب حسگرها[7] و آموزش فعال[8]، روشی توزیع شده[9] برای تشخیص و شناسایی حمله‌های شناخته‌شده و ناشناخته پیشنهاد می‌دهد. این روش توانسته است حجم محاسبات را بدون تحت تأثیر قرار دادن میزان کارایی کاهش دهد. این روش شامل یک قانون ترکیب داده به منظورر ترکیب تصمیم های بدست آمده از کلاسی فایرهای محلی توزیع شده، می باشد.

منبع [۷۰] بر روی حملات بازسازی اطلاعات و محرومیت از خدمات[10] در سیستم‌های کنترل صنعتی تمر کز می‌کند. فرض شده است که این حملات قابل تشخیص هستند. نویسنده به منظور مقابله با این نوع حملات در هر نمونه زمانی، با استفاده از کنترل‌کننده مبتنی بر افق محدود، ورودی را محاسبه می‌نماید و به عملگر ارسال می‌کند. در منبع [۷۱] روشی بر مبنای برنامه‌ریزی نیمه‌معین[11] برای شناسایی و مقابله با حمله منع خدمت در این سیستم‌ها پیشنهاد شده است. هدف نویسنده طراحی کنترل کننده بهینه مبتنی بر فیدبک ای است که توابع هدف را (که در ارتباط با ایمنی و مصرف انرژی تعریف شده اند) کمینه می کند. در منبع [۷۲] یک ماژول پایشی ارائه شده است که روی تراشه پردازنده (مثلاً پردازنده کنترل‌کننده) قرار می‌گیرد. مکانیزم تشخیص به این صورت است که برنامه‌ی در حال اجرا با گراف جریان کنترلی[12] (که در حافظه بارگذاری شده است)، مورد مقایسه قرار می‌گیرد و در صورت تناقض بین این دو، هشدار حمله فعال می‌شود.

منبع [۷۳] ابتدا به بررسی اثرات حمله‌ی تمامیت داده به سیستم قدرت می‌پردازد سپس الگوریتمی را به منظور طراحی تشخیص‌گر حمله سایبری به سیستم قدرت پیشنهاد می‌دهد. عملکرد این تشخیص‌گر مبتنی بر مدل سیستم و دانشی است که از رفتار عادی سیستم به دست آمده است. منبع[۶۳] با دیدگاه کنترل تحت شبکه[13] دو کلاس حمله به گره و حمله به مسیرهای ارتباطی گره را در نظر گرفته و فرموله می‌کند (شکل ۶). همچنین این منبع روشی توزیع شده به منظور شناسایی و تشخیص حمله پیشنهاد می‌دهد. در این روش از دینامیک خطی برای توصیف سیستم کنترل تحت شبکه و تخمین‌گر با ورودی نامشخص[14] به منظور شناسایی و تشخیص حمله، استفاده می‌شود.



شکل ۶: حمله به مسیرهای ارتباطی یک گره- حمله به یک گره [۶۳]

در منابع [۷۴, ۷۵] شبکه به صورت یک سیستم چندعامله در نظر گرفته شده است که حمله به عنوان یک ورودی خارجی و غیرقابل اندازه گیری مدل شده است. با توجه به اینکه فرض شده است عامل خوش رفتار (عاملی که به آن حمله نشده است) ورودی صفر دارد به منظور تشخیص حمله سعی می شود با استفاده از تخمین متغیرهای حالت سیستم، غیر صفر بودن ورودی عامل ها تشخیص داده شود.

اغلب سیستم‌های کنترل صنعتی بزرگ، دارای ساختار ارتباطی پیچیده‌ای هستند و وابستگی گسترده‌ای بین فعالیت‌های زیرسیستم‌های مختلف آن‌ها وجود دارد. یکی از روش‌های بسیار رایج به منظور شناسایی و تحلیل اثرات حمله در شبکه‌های کامپیوتری، استفاده از روش درخت حمله است. یکی از محدودیت های اصلی استفاده از گراف حمله، ضرورت وجود دانش کافی نسبت به سیستم به منظور ورود به جزئیات می باشد. استفاده از پتری نت به منظور مدل کردن حمله به عنوان یک روند تکاملی طبیعی محسوب می شود [۷۶]. مدل کردن حمله با استفاده از پتری نت را پت نت[15] نامیده می شود که هدف آن افزایش قابلیت های درخت حمله می باشد [۷۷]. منابع [۷۸-۸۱] استفاده از نظریه پتری نت را به منظور مدل کردن حمله و شناسایی اثرات آن در سیستم‌های کنترل صنعتی پیشنهاد کرده‌اند.

[1] Geometric Control Theory
[2] Detectability
[3] Identifiability
[4] waveform relaxation technique
[5] Optimal Distributed Attack Detection
[6] Sub-Optimal
[7] Sensor Selection
[8] Active Training Technique
[9] Distrbuted
[10] Denial Of Service(DOS)
[11] Semi definite Programming
[12] Control Flow Graph (CFG)
[13] Networked Control Systems
[14] Unknown Input Observer
[15] PETNET

منبع [۸۲] به منظور مطالعه و بررسی تأثیر حملات سایبری (به خصوص حملات محرومیت از خدمات[۱])در سیستم‌های کنترل تحت شبکه، از ابزارهای امنیت موجود در بستر آزمایش DETERLAB [۲] استفاده می‌کند. این منبع برای طراحی کنترل‌کننده مقاوم از حلقه فیدبک ساده بهره می‌گیرد و در نهایت بعد از تهیه چیدمان مناسب و اجرای پیکربندی‌های لازم، دو نکته موقعیت واحد صنعتی حمله شده نسبت به کنترل‌کننده اصلی و نیز طول زمان حمله را مورد بررسی قرار می‌دهد.

۵- بازترکیب و استفاده از ابزارهای کنترلی به منظور کاهش اثرات حمله و خودترمیمی سیستم

به طور کلی هدف محققان مورد اشاره در بخش‌های ۴ و ۵، طراحی و توسعه‌ی الگوریتم‌های کنترل و ایجاد سامانه‌های امنیتی خاص می‌باشد، که در صورت عبور موفق مهاجمان از مکانیزم‌های امنیتی مبتنی بر فناوری اطلاعات، حمله شناسایی، پایداری سیستم حفظ و در نهایت اثرات آن بر روی عملکرد نامی سیستم کنترلی حداقل شود[۵۵]. در این راستا در منابع [۸، ۳۳] حمله به‌وسیله مشاهده‌گر با ورودی نامشخص، شناسایی می‌شود، سپس مدلی به منظور مقابله با حمله پیشنهاد می‌دهند که در آن، سیستم کنترل بعد از تشخیص حمله، از حالت بدون وقفه[۳] خارج شده و از داده‌های محاسبه شده توسط مدل خطی سیستم استفاده می‌کند. در منبع [۵۵] نویسنده با استفاده از نظریه‌های بازپیکربندی سیستم در زمان خطا، سیستمی تحمل پذیر در مقابل حمله معرفی می‌کند. نویسنده همچنین تلاش کرده است با استفاده از تعریف عملگر مجازی، ورودی جدید را به نحوی محاسبه کند که در صورت حمله به یک یا چند عملگر و ازدست‌رفتن آن‌ها، سیستم همچنان پایدار بماند و خروجی مطلوب را دنبال کند. منبع [۸۳] به تحلیل و طراحی سیستم‌های کنترل مقاوم در برابر حملات پنهان[۴] می‌پردازد. این منبع ابتدا شرایط لازم و کافی برای این که در یک سیستم کنترل صنعتی امکان حمله پنهانی وجود نداشته باشد را مطرح می‌کند. سپس دو روش برای امن کردن سیستم کنترل صنعتی پیشنهاد کرده است. روش اول بر مبنای بازترکیب سیستم بعد از حمله به منظور کاهش اثرات حمله و روش دوم بر مبنای گسترش سیستم و افزایش تعداد متغیرهای اندازگیری می باشد. در منبع [۸۴]، نویسنده ابتدا نشان داده است که اگر تعداد سنسور های تحت حمله بیشتر از نصف کل سنسورهای سیستم باشد، امکان بازسازی و تخمین درست متغیرهای حالت بعد از حمله وجود ندارد. سپس نشان داده است که چطور طراحی حلقه‌های کنترل محلی امن، می‌تواند به قابلیت ارتجاعی بودن[۵] کل سیستم کمک کند. این نویسنده همچنین روشی را به منظور طراحی کنترل‌کننده‌ها مبتنی بر فیدبک خروجی پیشنهاد داده است. این کنترل‌کننده‌ها تحت شرایطی خاص، به پایداری ماندن سیستم بعد از حمله به سنسورها کمک می‌کند. منبع [۸۵] به مطالعه طراحی کنترل مقاوم در سیستم‌های کنترل تحت شبکه می‌پردازد و " قانون کنترلی افق بازگشتی استاکبرگ[۶] " را به منظور پایدار کردن سیستم کنترل با وجود حمله و صدمه به شبکه ارتباطی پیشنهاد می‌دهد. در منبع [۸۶] به طراحی و پیاده‌سازی سیستم‌های کنترل پیش‌بین امن تحت شبکه[۷] در برابر حملات فریبکارانه پرداخته می‌شود. در این مقاله یک سیستم کنترل پیش‌بین امن تحت شبکه پیشنهاد می‌شود که از الگوریتم رمزنگاری DES[۸]، الگوریتم MD5[۹]، راهبرد برچسب زمانی[۱۰] (به منظور ایجاد سازوکار انتقال امن بین کنترل‌کننده و واحد صنعتی) و نیز روش کنترل پیش‌بین تحت شبکه بازگشتی (RNPC)[۱۱] به منظور اطمینان از کارایی مناسب در حضور حملات فریبکارانه و پایداری حلقه بسته سیستم استفاده می‌نماید.

با توجه به این که برخی از محققین، حملات سایبری و بدافزاری را، یک خطای تصادفی در نظر گرفته‌اند، برای مقابله با آن‌ها از ابزارهای علم فرآیندهای اتفاقی[۱۲] کمک می‌گیرند. منبع [۸۷] تلاش می‌کند پایداری تصادفی[۱۳] سیستم تحت کنترل را زمانی که یک خرابی عمدی به طور تصادفی رخ داده است، بررسی کند. این خرابی تصادفی باعث می‌شود که پروسه تخمین سیستم و کنترل آن ناقص انجام گیرد. همچنین در این منبع شرایط محدوده پایداری و ملزومات حفظ آن را بررسی کرده است. منبع [۸۸] روشی برای بهینه‌سازی تصادفی[۱۴] سیستم‌های سایبر فیزیکی، در زمان وقوع حمله پیشنهاد می‌کند. منبع [۸۹] فرض کرده است که خرابی عمدی تصادفی در مسیر سیگنال کنترلی ارسالی، از کنترل‌کننده به واحد صنعتی اتفاق افتاده است. این منبع روشی برای تخمین حالت سیستم در زمان حمله مبتنی بر فیلتر کالمن با ورودی نامشخص پیشنهاد می‌دهد و همچنین پایداری فیلتر پیشنهادی و سیستم را مطالعه کرده است. منبع [۹۰] به بررسی پایداری تصادفی تخمینگر حالت مبتنی بر فیلتر کالمن پرداخته است در حالتی که تخمینگر اطلاعات خود را از یک شبکه سنسوری توزیع شده و در معرض خرابی های تصادفی دریافت می‌کند. در شبکه سنسوری که در این مقاله در نظر گرفته شده، هر سنسور وظیفه ارسال داده‌های مربوط به نودها یا متغیرهای حالت حوزه همسایگی خود را دارد

[1] Denial Of Service(DOS)

[۲] بستر آزمایش DETER نسخه توسعه یافته Emulab است که برای آموزش و نیز بهبود امنیتی طراحی شده است. این بستر، یک زیرساخت آزمایشگاهی چند کاربری است و امکان تکرار چندباره آزمایشات نمونه سازی شده از جمله وارد کردن کدهای بدافزار را فراهم می‌آورد.

[3] Real Time

[۴] حمله پنهانی به حمله ای اطلاق می‌شود که در آن مهاجم ورودی و یا خروجی یک سیستم حلقه بسته را تغییر می‌دهد اما از طریق اندازه گیری خروجی این حمله قابل تشخیص نمی‌باشد.

[5] Resilience
[6] Receding-Horizon Stackelberg Control Law
[7] Networked Predictive Control
[8] Data Encryption Standard
[9] Message Digest
[10] Time Stamp
[11] Recursive Networked Predictive Control
[12] Stochastic Events
[13] Stochastic Stability
[14] Stochastic Optimization

و حوزه همسایگی دو سنسور ممکن است دارای اشتراک باشد. همچنین اتصال همه سنسورها به تخمین‌گر از طریق چند مسیر ارتباطی می‌باشد. نویسنده با در نظر گرفتن این فرضیات تلاش می‌کند که محدوده پایداری تخمین‌گر را بر اساس احتمال دریافت صحیح مقادیر سنسورها در مسیر ارتباطی مستقل، محاسبه کند.

منبع [۹۱] با در نظر گرفتن دو حالت دستی و خودکار برای شناسایی و پاسخ سیستم به حمله، ابتدا با استفاده از دنباله مارکوف حالت گذرای سیستم از خودکار به دستی را مدل می کند. سپس مدت زمان مجاز و بهینه جایگزینی را نیز به‌دست‌آورده و از روش کنترل تطبیقی، به منظور محاسبه این بازه زمانی (در هنگام خرابی‌های عمدی) استفاده کرده است.

منبع [۹۲] از روش کنترل پیش‌بین به منظور شناسایی و کاهش اثر حملات سایبری استفاده می‌کند. وقتی کنترل‌کننده پیش‌بین به نتیجه برسد که هیچ ورودی کنترلی مجازی وجود ندارد تا خروجی حاصل در محدوده نرمال خودش باشد، هشدار حمله فعال می‌شود. سپس به منظور مقابله با اثر حمله با استفاده از یک کنترل‌کننده بهینه، خروجی را به حالت قابل قبول برمی‌گرداند و به کنترل‌کننده پشتیبان تغییر می‌کند.

منبع [۶۲] حمله جمینگ و اثرات آن را به صورت دینامیکی مدل و به منظور کاهش دادن اثر حمله از کنترل فیدبک و دیدگاه پاسیویتی[1] استفاده می‌کند؛ به گونه‌ای که سیستم به نقطه کار مطلوب همگرا گردد. در این مقاله بیان می شود که انتخاب کنترل کننده هایی با مرتبه بالاتر منجر به افزایش پایدارپذیری و مقاومت سیستم می شود ولی در عین حال سرعت همگرایی سیستم نیز کاهش می یابد. منبع [۹۳] چارچوب جدیدی از نظریه بازی‌ها را ارائه می‌کند تا به کمک آن بتواند مسائل مرتبط با امنیت وارتجاعی بودن در لایه‌های مختلف سیستم‌های سایبری- فیزیکی را تحت پوشش قرار دهد. در واقع تصمیمات بهینه در سیاست‌های امنیت سایبری با نگاهی بر اثراتی که بر روی لایه فیزیکی می گذارند، اتخاذ می‌شود.

منبع [۹۴] بیان می‌کند که هدف همه تلاش‌ها در نهایت، به‌دست‌آوردن روش‌ها و تکنیک‌هایی است که باعث خودترمیمی سیستم‌های کنترل صنعتی در زمان وقوع حمله شوند. در سیستم خودترمیم اجزای سیستم‌های کنترلی به نحوی باهم همکاری می‌کنند که نه‌تنها خود کارایی مناسب داشته باشند، بلکه بتوانند کارایی مناسبی برای کل سیستم برآورده کنند. به عبارت دقیق‌تر از دیدگاه این منبع، سیستم خودترمیم، سیستمی است که با استفاده از اطلاعات سیستم، داده‌های اندازه‌گیری‌شده، کنترل و فناوری ارتباطات بتواند مشکلات ناشی از اتفاقات نامطلوب پیش‌بینی نشده را حل و اثرات آن را حداقل کند. همچنین این منبع لایه‌های کنترلی یک سیستم خودترمیم شبکه قدرت را تشریح کرده است. منبع [۹۵] طرحی حفاظتی برای شبکه‌های کنترل صنعتی به ویژه شبکه‌های برق ارائه می‌دهد. نویسنده تلاش کرده است که طرحی پیشنهاد دهد که قابلیت کنترل خودکار و شرایط خودترمیم را در زمان وقوع حمله فراهم می‌کند.

٦- بهبود مدیریت امنیت سایبری در سیستم‌های کنترل

برای رسیدن به یک امنیت مطلوب، علاوه‌بر استفاده از راهبردهای امنیتی مناسب باید مدیریت امنیتی خوبی نیز وجود داشته باشد. ابزارهای مدیریت امنیتی مناسب عبارتند از سیاست، راهبرد و برنامه امنیتی که بر مبنای تحلیل تهدید و ریسک دقیق برآورده می‌شوند. به عبارت دیگر با توجه به گستردگی تهدیدات سایبری که سیستم‌های کنترل صنعتی در معرض آن‌ها هستند، شناسایی این تهدیدات و تحلیل آن‌ها جهت ارائه راهبرد حفاظتی بهینه و مقرون به صرفه بسیار ضروری است.

به طور کلی زمینه مطالعاتی مقالات این بخش را به صورت زیر می‌توان دسته‌بندی کرد:

- ارائه روش‌هایی به منظور شناسایی تهدیدات سایبری و ارزیابی ریسک آن در سیستم‌های کنترل صنعتی
- استفاده از این تحلیل‌ها و ارزیابی‌ها به منظور استخراج و انتخاب راهبرد دفاع بهینه و مقرون‌به‌صرفه و تدوین برنامه امنیتی

تلاش‌های زیادی در زمینه ارائه روش‌های شناسایی تهدید و ریسک و همچنین تحلیل آن در سیستم‌های کنترل صنعتی انجام گرفته است. در منبع [۹۶] تلاش شده است با استفاده از روش نظریه بازی‌ها، تهدیدات امنیتی سیستم‌های سایبری- فیزیکی تخمین زده شوند. منبع [۵] یک مقاله "بررسی منابع"[2] در زمینه ارزیابی ریسک سیستم‌های SCADA و DCS می‌باشد، این منبع توانسته است بررسی کامل و لیستی جامع از مراکز و منابع تحقیقاتی در این زمینه را تا سال ۲۰۰۷ ارائه دهد. اکثر سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی دربرگیرنده زیرسیستم‌های متفاوت با شرایط اتصال مختلف هستند، در منبع [۹۷]، نویسنده به بررسی چگونگی ارزیابی و تفاوت اتخاذ راهبرد دفاع در سیستم‌های مستقل، موازی و سری پرداخته است. در سال‌های اخیر روابط و وابستگی بین زیرساخت‌های حیاتی چنان پیچیده شده است که نظریه های ریاضی و روش‌های کنترلی مرسوم، از عهده حل همه مسائل آن‌ها به تنهایی بر نمی‌آیند. ازاینرو زمینه مطالعاتی "سیستم‌سیستم‌ها"[3] مطرح و مورد توجه قرار گرفته است. در واقع محققین در این زمینه تلاش می‌کنند تا با مد نظر گرفتن پیچیدگی، وابستگی و ارتباط زیرسیستم‌هایی که خود جزء سیستم‌های بزرگ[4] محسوب می‌شوند، راهکارها، روش‌ها و نظریه‌های جدید ریاضی و کنترلی را به منظور حل مشکلات کنترل ، ارزیابی امنیتی و ... در آن‌ها توسعه دهند. با همین دیدگاه منبع [۹۸] تلاش می‌کند تا با مد نظر قرار دادن این پیچیدگی‌ها و وابستگی‌های موجود بین

[1] Passivity

[2] Survey Paper
[3] System Of Systems
[4] Large System

زیرسیستم‌های یک سیستم کنترل صنعتی، مدلی را به منظور توصیف این وابستگی ها بیان کند.

تحلیل کیفی ریسک با فرض شناخت و ریشه یابی ریسک‌های سیستم توسط روش‌هایی مانند مدل‌سازی هولوگرافی سلسه‌مراتبی[۱] (HHM) انجام می‌گیرد [۹۹]، ولی تحلیل کمی ریسک بر پایه بررسی احتمال وقوع ریسک[۲] می‌باشد. از جمله روش‌های مبتنی بر احتمال وقوع ریسک، می توان به تحلیل درختی خطا (یا حمله)[۳]، تحلیل درختی حادثه[۴]، تحلیل اثر و شرایط خرابی[۵]، تحلیل حساسیت و اثر شرایط خرابی[۶] و تحلیل دلایل و نتایج[۷] و همچنین روش‌های مبتنی بر استفاده از دیاگرام منطقی و گراف[۸] اشاره کرد. اکثر روش‌های دیگر ترکیب یا تعمیمی از روش‌های نام برده شده هستند. آزمایشگاه ملی سندیا[۹] در آمریکا در گزارش [۱۰۰] خود تلاش کرده است که روش‌های تحلیل ریسک را بر اساس سطح جزئیات و مفاهیم کاربردی آن‌ها، تقسیم‌بندی کند. محققان مؤسسه فناوری جورجیا[۱۰] در [۱۰۱] روشی کیفی و سیستماتیک را برای تحلیل ریسک سیستم‌های اطلاعاتی[۱۱] ارائه کرده‌اند. در منبع [۱۰۲]، بیان می شود که روش HHM می تواند همه منابع ریسک قابل متصور در سیستم اسکادا و زیرساخت‌های حیاتی تحت کنترل آن را شناسایی کند. این روش قادر به ساده‌سازی ارزیابی ریسک زیرسیستم‌ها و اثرات آن بر روی کل سیستم می‌باشد. این خصوصیت باعث می‌شود روش HHM به عنوان روشی ایده آل در بررسی سیستم‌های اسکادا و زیرساخت هایی که دارای زیرسیستم‌های به‌هم‌مرتبط هستند، شناخته شود [۱۰۳]. منبع [۷۸] با استفاده از نظریه پتری‌نت روشی به منظور تحلیل کمی ریسک حملات سایبری در سیستم‌های کنترل پیشنهاد داده است. در این منبع، نویسنده ریسک را به صورت تابعی از متغیرهای حالت پتری‌نت محاسبه می‌کند.

یکی از زیرساخت‌های حیاتی که دارای لایه‌های متفاوتی با شرایط اتصال مختلف است، سیستم قدرت می‌باشد. منابع [۷۷, ۱۰۴-۱۰۶] با ارائه راهکارهایی برای لایه بندی سیستم قدرت و شناسایی آسیب‌پذیری به ارزیابی تهدیدات و ریسک این سیستم پرداخته‌اند. در منبع [۱۰۴] با پیشنهاد یک تقسیم‌بندی لایه‌ای برای سیستم‌های قدرت، به بررسی امکان و اثرات یک حمله موفق، در این سیستم پرداخته است. منبع [۱۰۶] به ارزیابی کمی اثرات یک حمله سایبری به شبکه قدرت پرداخته است که به همین منظور این شبکه را به چهار لایه تقسیم کرده است: لایه فیزیکی، ارتباطات، کنترل و لایه امنیت سایبری و در نهایت به ارزیابی ارزش سرمایه‌گذاری هر لایه با توجه به خصوصیات آن‌ها پرداخته است.

به منظور اتخاذ راهبرد و برنامه امنیتی بهینه، بررسی صدمه مالی احتمالی هر حمله به هر زیرسیستم و به دنبال آن کل سیستم و همچنین سیستم‌های وابسته به آن ضروری است. در منبع [۱۰۷] نویسندگان تلاش کرده‌اند صدمات مالی و گسترش آن از طریق قسمت‌های مختلف در یک زیرساخت حیاتی بزرگ که با سیستم اسکادا کنترل و مدیریت می‌شود را بررسی کنند. همچنین همین نویسندگان در منبع [۱۰۸] به بررسی صدمات مالی حمله به یک سیستم قدرت و گسترش این صدمه مالی از طریق وابستگی بین زیرسیستم‌ها پرداخته‌اند. منبع [۱۰۹] با در نظر گرفتن تهدیدات و ریسک ناشی از حملات سایبری به یک سیستم کنترل شبکه قدرت، روشی را بر اساس برنامه‌ریزی دینامیک[۱۲] به منظور انتخاب راهبرد بهینه مقرون‌به‌صرفه ارائه می‌کند. در واقع هدف این مقاله پیشنهاد روشی است که بتوان با استفاده از آن، راهبرد و برنامه امنیتی سیستم طوری اتخاذ گردد که متناسب با تبعات مالی و ریسک ناشی از حمله به آن باشد.

۸- نتیجه‌گیری

مهاجمان سایبری به شکل روزافزون علاوه بر استفاده از آسیب‌پذیری‌های ناشناخته، روش‌های پیچیده‌تری را برای حمله به سیستم‌های کنترل صنعتی طراحی می‌نمایند. بدین‌ترتیب آن‌ها بعد از عبور از راهبردهای امنیتی مبتنی بر علم فناوری اطلاعات (ITB[۱۳])، عملا با یک سیستم کنترلی بدون حفاظت‌های امنیتی روبه‌رو می‌شوند. از سویی دیگر هدف نهایی مهاجمان، صدمه و ایجاد اختلال در عملکردمطلوب سیستم فیزیکی تحت کنترل می‌باشد که این موضوع در راهبردهای امنیتی ITB نادیده گرفته می‌شود. به طور خلاصه می‌توان بیان کرد که صرفاً راهبردهای امنیتی ITB، نمی‌توانند استراتژی دفاع در عمق (استراتژی دفاع در عمق این امکان را فراهم می‌کند که مهاجم با عبور از هر لایه، مجدداً به لایه‌ای امنیتی برخواهد خورد که در راستای از بین بردن حمله و یا کاهش اثر آن طراحی شده است) را برای سیستم‌های کنترل فراهم کند.

بنابراین محققین علم کنترل تلاش می‌کنند تا با لحاظ نمودن دینامیک و پایش عملکرد سیستم فیزیکی تحت کنترل، راهکارهایی برای شناسایی و تشخیص طیف گسترده‌ای از حملات ارائه دهند. همچنین الگوریتم‌های کنترل را طوری طراحی و یا توسعه دهند که در صورت عبور موفق مهاجمان از تمام مکانیزم‌های امنیتی ITB، سیستم نه‌تنها پایداری خود را حفظ نموده، بلکه آسیب‌های ناشی از حمله را شناسایی و حداقل کند. پیشینه علم کنترل در این راستا را می‌توان در مباحثی مانند کنترل مقاوم، کنترل تطبیقی، تشخیص خطا، سیستم‌های تحمل‌پذیر در مقابل خطا و ... یافت. البته باید توجه داشت مسئله امنیت سایبری با مسائل سنتی مطرح شده در این مباحث بعضاً دارای تفاوت‌های اساسی می‌باشد که این امر مستلزم ایجاد

[1] Hierarchical Holographic Modeling (HHM)
[2] Probabilistic Risk Assessment (PRA)
[3] Fault/Attack (FTA) Tree Analysis
[4] Event Tree Analysis (ETA)
[5] Failure Mode And Effect Analysis (FMEA)
[6] Failure Mode Effect And Criticality Analysis (FMECA)
[7] Cause/Consequence Analysis (CCA)
[8] Graphs And Logic Diagrams
[9] Sandia National Laboratories
[10] Georgia Institute of Technology
[11] Information Systems
[12] Dynamic Programming
[13] Information Technology Based

بعضی تغییرات بنیادی در ارائه راه‌حل‌ها می‌شود. مثلاً همان طور که در متن مقاله اشاره شد، مقالات زیادی را می‌توان یافت که حمله سایبری را به صورت خطای عمدی تعریف کرده‌اند. اما این نکته حائز اهمیت است که مواردی شامل دامنه، همزمانی و تکرار خطاهای عمدی با خطاهای غیرعمدی در یک سیستم متفاوت است. به عبارتی دیگر این موارد در خطاهای عمدی تحت سناریو بوده و به شکلی طراحی می‌شوند که مهاجم بتواند حتی الامکان حمله را مخفی کند و بیشترین صدمه را با کمترین تلاش به سیستم بزند.

همان طور که بیان شد تحقیقات بسیاری در راستای حل این مسائل انجام گرفته و یا در حال انجام است. از نظر نویسندگان این مقاله، ازجمله موارد مهمی که تا به حال در تحقیقات کمتر مورد توجه قرار گرفته است، به شرح زیر می‌باشد:

۱. تخمین بر خط[1] تأخیری که تجهیزات امنیتی (مانند دیوار آتش، سیستم تشخیص نفوذ و ...) در سیستم کنترل ایجاد می‌کنند.

در راستای مقاوم‌سازی سیستم کنترل، محققان استفاده از تجهیزات امنیتی زیادی را پیشنهاد داده‌اند. ولی باید توجه شود که ممکن است عملکرد این تجهیزات حتی با وجود سرعت پردازشی نسبتاً بالا، در زمان بعضی حملات خود موجب اختلال در سیستم کنترل شود. از اینرو لازم است با پایش تأخیر ایجاد شده توسط آن‌ها، در صورت لزوم از سیکل کاری سیستم حذف شوند.

۲. تخمین کمی از میزان امنیت سیستم‌های کنترل صنعتی

در راستای بهبود امنیتی سیستم کنترل ضروری است که تخمین دقیقی از میزان امنیت آن وجود داشته باشد. تحلیل‌هایی که به منظور تخمین میزان امنیت یک سیستم کنترل انجام می‌گیرد، بیشتر کیفی بوده و دقت آن‌ها وابسته به دقت کارشناسان بررسی‌کننده می‌باشد. بنابراین وجود یک مقدار کمی از میزان امنیت سیستم مشابه آنچه در مورد میزان ایمنی سیستم[2] استفاده می‌شود ضروری به نظر می‌آید.

۳. بررسی امکان کاهش ارادی اتصال به شبکه‌های ارتباطی بدون از دست دادن مرزهای پایداری مطمئن و عملکرد مطلوب سیستم تحت کنترل.

با توجه به تهدیدات ناخواسته‌ای که استفاده از فناوری ارتباطات و رایانه متوجه سیستم‌های کنترل صنعتی می کند، ضروری است که امکان کاهش ارادی وابستگی این سیستم ها به شبکه‌های ارتباطی با شرط از دست ندادن پایداری و عملکرد مطلوب مورد بررسی قرار گیرد.

۴. طراحی سیستم‌های کنترل صنعتی امن در مقابل تهاجمات سایبری با الهام از پدیده‌های زیستی

همان طور که بیان شد یکی از اهداف علم کنترل در مبحث امنیت سایبری یافتن جواب‌های مناسبی برای جبران‌سازی بهینه عملکرد سیستم بعد از حمله می‌باشد، به گونه‌ای که موجب پایداری سیستم و کاهش اثرات حمله شود. با توجه به این‌که این رفتار هدف اغلب پدیده‌های زیستی در زمان حمله‌های خارجی یا اختلال داخلی است، الهام گرفتن از عملکرد این پدیده‌ها احتمالاً می‌تواند منجر به طراحی سیستم‌های کنترل امن‌تر گردد.

تشکر و قدردانی

این مقاله در ضمن اجرای فاز مطالعاتی پروژه " طراحی و پیاده‌سازی سامانه جامع مقابله با بدافزارها در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی" تهیه شده است. این پروژه در راستای طرح کلان ملی "معماری و راه‌اندازی مرکز ملی دفاع سایبری و سامانه‌های زیرساختی فضای سایبری"، در پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر در حال اجرا می‌باشد.

مراجع

[۱] Weiss, Joseph M., “Control Systems Cyber Security—the Current Status of Cyber Security of Critical Infrastructures”, 2009; Available from: http://www.controlglobal.com/articles/2009/CyberSecurity0903.html.

[۲] http://embedded.communities.intel.com.

[۳] Mitchell, Robert, and Ing-Ray Chen, “A Survey of Intrusion Detection Techniques for Cyber Physical Systems”, ACM Computing Surveys (CSUR), 2014, Vol. 46, No. 4.

[۴] Wang, Wenye, and Zhuo Lu, “Cyber Security in the Smart Grid: Survey and Challenges”, Computer Networks, 2013, Vol. 57, No. 5, pp. 1344-1371.

[۵] Ralston, P. A. S., J. H. Graham, and J. L. Hieb, “Cyber Security Risk Assessment for SCADA and DCS Networks”, ISA transactions, 2007, Vol. 46, No. 4, pp. 583-594.

[۶] ISA SP-99, “Technical Security Requirements for an Industrial Automation and Control Systems”, 2008, pp. 23-26.

[۷] http:\\www.isa.org.

[۸] Amin, Saurabhs, “On Cyber Security for Networked Control Systems”,phd thesis, University of California, 2011.

[۹] Teumim, David J., “Industrial Network Security. Isa”, 2010.

[۱۰] American Gas Association, “Cryptographic Protection of SCADA Communications”, March 2006.

[۱۱] Igure, Vinay M., Sean A. Laughter, and Ronald D. Williams, “Security Issues in Scada Networks”, Computers & Security, 2006, Vol.25, No. 7, pp. 498-506.

[۱۲] Nai Fovino, Igor, Andrea Carcano, Marcelo Masera, and Alberto Trombetta, “An Experimental Investigation of Malware Attacks on SCADA Systems”, International Journal of Critical Infrastructure Protection, 2009 , Vol. 2, No. 4, pp. 139-145.

[1] Online
[2] Safety Integrity Level (SIL)

[۱۳] Morris, Thomas, Rayford Vaughn, and Yoginder Dandass. "A Retrofit Network Intrusion Detection System for Modbus Rtu and Ascii Industrial Control Systems", 45th Hawaii International Conference on System Science (HICSS), 2012, pp. 2338-2345.

[۱۴] Cheung, Steven, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. "Using Model-Based Intrusion Detection for SCADA Networks", In Proceedings of the SCADA Security Scientific Symposium, 2007, Vol. 46, pp. 1-12.

[۱۵] Byres, Eric J., Dan Hoffman, and Nate Kube, "On Shaky Ground–a Study of Security Vulnerabilities in Control Protocols", Proc. 5th American Nuclear Society Int. Mtg. on Nuclear Plant Instrumentation, Controls, and HMI Technology, 2006.

[۱۶] Byres, Eric J., Matthew Franz, and Darrin Miller, "The Use of Attack Trees in Assessing Vulnerabilities in Scada Systems", Proceedings of the International Infrastructure Survivability Workshop, 2004.

[۱۷] Bhatia, Sajal, Nishchal Kush, Chris Djamaludin, Ayodeji Akande, and Ernest Foo, "Practical Modbus Flooding Attack and Detection", Proceedings of Australasian Information Security Conference (ACSW-AISC 2014), 2014, Vol. 149.

[۱۸] Raza, Shahid, Adriaan Slabbert, Thiemo Voigt, and Krister Landernas, "Security Considerations for the WirelessHART Protocol", IEEE Conference on Emerging Technologies & Factory Automation(ETFA), 2009, pp. 1-8.

[۱۹] Raza, Shahid, Thiemo Voigt, Adriaan Slabbert, and Krister Landernas, "Design and Implementation of a Security Manager for WirelessHART Networks", IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009, pp. 995-1004.

[۲۰] Song, Jianping, Song Han, Aloysius K. Mok, Deji Chen, Mike Lucas, and Mark Nixon, "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", Real-Time and Embedded Technology and Applications Symposium, 2008, RTAS'08. IEEE, pp. 377-386 .

[۲۱] Abbasi, A., "Critical Infrastructure Vulnerability Assessment and Protection from Protocol Layer to Hardware Layer", 2013.

[۲۲] Modbus, I. D. A., "Modbus Application Protocol Specification v1. 1a.", North Grafton, Massachusetts (www. modbus. org/specs. php), 2004.

[۲۳] Modbus, I. D. A., "Modbus Messaging on TCP/IP Implementation Guide v1. 0a", North Grafton, Massachusetts (www. modbus. org/specs. php), 2004.

[۲۴] Zenner, Erik, "Nonce Generators and the Nonce Reset Problem", Information Security, Springer Berlin Heidelberg, 2009, pp. 411-426.

[۲۵] Krutz, Ronald L., "Securing SCADA Systems", John Wiley & Sons, 2005.

[۲۶] Creery, A., and E. J. Byres., "Industrial Cybersecurity for Power System and SCADA Networks", Petroleum and Chemical Industry Conference, Industry Applications Society 52nd Annual, 2005, pp. 303-309.

[۲۷] Cai, Ning, Jidong Wang, and Xinghuo Yu., "SCADA System Security: Complexity, History and New Developments", 6th IEEE International Conference on Industrial Informatics, 2008, pp. 569-574.

[۲۸] Byres, Eric, John Karsch, and Joel Carter, "NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks", National Infrastructure Security Co-Ordination Centre, 2005.

[۲۹] Patel, Sandip C., Ganesh D. Bhatt, and James H. Graham, "Improving the Cyber Security of SCADA Communication Networks", Communications of the ACM, 2009, Vol. 52, No.7, pp. 139-142.

[۳۰] Piètre-Cambacédès, Ludovic, and Pascal Sitbon, "Cryptographic Key Management for Scada Systems-Issues and Perspectives", IEEE International Conference on Information Security and Assurance, 2008, pp. 156-161.

[۳۱] Wright, Jason, "Control Systems Communications Encryption Primer", Department of Homeland Security, December 2009.

[۳۲] Valentine, Sidney E., "PLC Code Vulnerabilities through SCADA Systems", PhD diss, University of South Carolina, 2013 ,

[۳۳] Cardenas, Alvaro A., Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry, "Attacks against Process Control Systems: Risk Assessment, Detection, and Response", In Proceedings of the 6th ACM symposium on information, computer and communications security, 2011, pp. 355-366.

[۳۴] Barnes, Ken, Briam Johnson, and Reva Nickelson. "Introduction to SCADA Protection and Vulnerabilities", Idaho National Engineering and Environmental Laboratory, January 2004.

[۳۵] Stidham, Jonathans, "Can Hackers Turn Your Lights Off: The Vulnerability of the US Power Grid to Electronic Attack", SANS Institute, 2001.

[۳۶] Robles, R., Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park, and S. Yeo, "Vulnerabilities in SCADA and Critical Infrastructure Systems", International J. of Future Generation and Networking, 2008, Vol. 1, No. 1, pp. 102-103.

[۳۷] Robles, Rosslin John, and Min-kyu Choi, "Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems", 2009, Assessment 2, No. 2.

[۳۸] Skorobogatov, Sergei, and Christopher Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip", Springer Berlin Heidelberg, 2012.

[۳۹] King, Samuel T., Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou., "Designing and Implementing Malicious Processors", Wild and Crazy Ideas Session VI (ASPLOS XIII), 2008.

[۴۰] قادری، ف.، "نگاهی به تهدیدات سخت افزاری"، فصلنامه مرکز تحقیقات صنایع انفورماتیک، ۱۳۹۱.

[۴۱] http://ics-cert.us-cert.gov/alerts

[۴۲] http//:ics-cert.us-cert.gov/advisories.

[۴۳] http://nvd.nist.gov

[۴۴] Liu, Yao, Peng Ning, and Michael K Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids", ACM Transactions on Information and System Security (TISSEC), 2011. Vol. 14, No. 1, pp. 13 .

[۴۵] Yao Liu, Peng Nin, Michael K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids", National Science Foundation (NSF), 2009

[۴۶] Teixeira, André, Saurabh Amin, Henrik Sandberg, Karl Henrik Johansson, and Shankar S. Sastry, "Cyber Security Analysis of State Estimators in Electric Power Systems",

[۴۷] Liu, Xuan and Zuyi Li, "Local Load Redistribution Attacks in Power Systems with Incomplete Network Information", IEEE Transactions On Smart Grid, July 2014, Vol. 5, pp. 1665-1676.

[۴۸] Sandberg, Henrik, André Teixeira, and Karl H. Johansson, "On Security Indices for State Estimators in Power Networks", in Preprints of the First Workshop on Secure Control Systems, CPSWEEK, Stockholm, Sweden, 2010.

[۴۹] Bobba, Rakesh B., Katherine M. Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J. Overbye, "Detecting False Data Injection Attacks on dc State Estimation", Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[۵۰] Dán, György and Henrik Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems", First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 214-219.

[۵۱] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao, "On False Data Injection Attacks against Power System State Estimation: Modeling and Countermeasures", IEEE Transactions on Parrallel and Distributed Systems, 2014, Vol. 25, No. 3, pp. 717-729.

[۵۲] Xie, Le, Yilin Mo, and Bruno Sinopoli, "Integrity Data Attacks in Power Market Operations", IEEE Transactions on Smart Grid, 2011, Vol. 2, No. 4, pp. 659-666.

[۵۳] Monticelli, Alcir, "State Estimation in Electric Power Systems, a Generalized Approach", Springer, 1999, vol. 507.

[۵۴] Mo, Yilin and Bruno Sinopoli. "False Data Injection Attacks in Control Systems", In Preprints of the 1st Workshop on Secure Control Systems, 2010, pp. 1-6.

[۵۵] ترمه‌چی، عاطفه.، "کنترل آسیب‌های ناشی از حملات سایبری به زیرساخت‌های حیاتی"، پایان نامه کارشناسی ارشد، دانشگاه صنعتی امیر کبیر، ۲۰۱۳.

[۵۶] Bruno Sinopoli, Yilin Mo, "Secure Control against Replay Attacks", Trust Autumn 2009 Conference, 2009.

[۵۷] Mo, Yilin and Bruno Sinopoli. "Secure Control against Replay Attacks", 47th Annual Allerton Conference on Communication, Control, and Computing, 2009, pp. 911-918.

[۵۸] Chabukswar, Rohan, Yilin Mo, and Bruno Sinopoli, "Detecting Integrity Attacks on SCADA Systems", Proceedings of the 18th IFAC World Congress, Milano, Italy, 2011, pp. 11239-11244.

[۵۹] Smith, Roy S., "A Decoupled Feedback Structure for Covertly Appropriating Networked Control Systems", Network, 2011, Vol. 6.

[۶۰] Huang, Yu-Lun, Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Hsin-Yi Tsai, and Shankar Sastry, "Understanding the Physical and Economic Consequences of Attacks on Control Systems", International Journal of Critical Infrastructure Protection, 2009, Vol. 2, No. 3, pp. 73-83.

[۶۱] Burmester, Mike, Emmanouil Magkos, and Vassilis Chrissikopoulos, "Modeling Security in Cyber–Physical Systems", International Journal of Critical Infrastructure Protection, 2012, Vol 5, No.3, pp.118-126.

[۶۲] Lee, Phillip, Andrew Clark, Linda Bushnell, and Radha Poovendran" ,Modeling and Designing Network Defense against Control Channel Jamming Attacks: A Passivity Based Approach", Control of Cyber-Physical Systems, Springer International Publishing, 2013, pp. 161-175.

[۶۳] Teixeira, André, Henrik Sandberg, and Karl H. Johansson. "Networked Control Systems under Cyber Attacks with Applications to Power Networks", American Control Conference (ACC), 2010, pp. 3690-3696.

[۶۴] Amin, Saurabh, Xavier Litrico, S. Shankar Sastry, and Alexandre M. Bayen, "Stealthy Deception Attacks on Water SCADA Systems", in Proceedings of the 13th ACM international conference on Hybrid systems: computation and control. 2010, pp. 161-170.

[۶۵] Zimmer, Christopher, Balasubramanya Bhat, Frank Mueller, and Sibin Mohan, "Time-Based Intrusion Detection in Cyber-Physical Systems", In Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, 2010, pp. 109-118.

[۶۶] Nguyen, Hoa Dinh, Sandeep Gutta, and Qi Cheng, "An Active Distributed Approach for Cyber Attack Detection", Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers, 2010, pp. 1540-1544.

[۶۷] Hashimoto, Hideaki and Tomohisa Hayakawa, "Distributed Cyber Attack Detection for Power Network Systems", 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), 2011, pp. 5820-5824.

[۶۸] Pasqualetti, Fabio, Florian Doörfler, and Francesco Bullo, "Attack Detection and Identification in Cyber-Physical Systems--Part I: Models and Fundamental Limitations", arXiv preprint arXiv:1202.6144, 2012.

[۶۹] Pasqualetti, Fabio, Florian Dörfler, and Francesco Bullo, "Attack Detection and Identification in Cyber-Physical Systems--Part Ii: Centralized and Distributed Monitor Design", arXiv preprint arXiv:1202.6049, 2012.

[۷۰] Zhu, Minghui, and Sonia Martinez, "On the Performance Analysis of Resilent Networked Control Systems under Replay Attacks", 2013.

[۷۱] Amin, Saurabh, Alvaro A. Cárdenas, and S. Shankar Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks", Hybrid Systems: Computation and Control, Springer, 2009, pp. 31-45.

[۷۲] Abdi Taghi Abad, Fardin, Joel Van Der Woude, Yi Lu, Stanley Bak, Marco Caccamo, Lui Sha, Renato Mancuso, and Sibin Mohan, "On-Chip Control Flow Integrity Chech for Real Time Embeded Systems", IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), 2013, pp. 26-31.

[۷۳] Sridhar, Siddharth and Manimaran Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control", IEEE Transaction On Smart Grid, 2014, Vol. 5, pp. 580-591.

[۷۴] Pasqualetti, Fabio, Ruggero Carli, Antonio Bicchi, and Francesco Bullo, "Identifying Cyber Attacks Via Local Model Information", 49th IEEE Conference on Decision and Control (CDC), 2010, pp. 5961-5966.

[۷۵] Pasqualetti, Fabio, "A control-theoretic approach to cyber-physical security", University Of California, Santa Barbara, 2012.

[۷۶] E. Ciancamerla, A. Di Pietro, M. Minichino, S. Palmieri , et al., "Cybersecurity on Scada: Risk Prediction,Analysis and Reaction Tools for Critical Infrastructures", 2012: ENEA.

[۷۷] Ten, Chee-Wooi, Manimaran Govindarasu, and Chen-Ching Liu. "Cybersecurity for Electric Power Control and Automation Systems", IEEE International Conference on Systems, Man and Cybernetics, 2007, pp. 29-34.

[۷۸] Henry, Matthew H., Ryan M. Layer, Kevin Z. Snow, and David R. Zaret. , "Evaluating the Risk of Cyber Attacks on SCADA Systems Via Petri Net Analysis with Application to

[۹۵] Yuksel, Murat, K. Bekris, Cansin Y. Evrenosoglu, Mehmet Hadi Gunes, S. Fadali, Mehdi Etezadi-Amoli, and F. Harris, “Open Cyber-Architecture for Electrical Energy Markets”, IEEE 35th Conference on Local Computer Networks (LCN), 2010, pp. 1024-1031.

[۹۶] Amin, Saurabh, Galina A. Schwartz, and Alefiya Hussain, “In Quest of Benchmarking Security Risks to Cyber-Physical Systems”, IEEE network, Feb 2013, Vol. 27, No. 1, pp. 19-24.

[۹۷] Hausken, Kjell, “Strategic Defense and Attack for Series and Parallel Reliability Systems”, European Journal of Operational Research, 2008, Vol. 186, No. 2, pp. 856-881.

[۹۸] Eusgeld, Irene, Cen Nan, and Sven Dietz, “ "System-of-Systems" Approach for Interdependent Critical Infrastructures ”, Reliability Engineering & System Safety, 2011, Vol. 96, No. 6, pp. 679-686.

[۹۹] Doremami, Nadia, Ahmad Afshar, and A. D. Mohammadi, “Hierarchical Risk Assessment in Gas Pipelines Based on Fuzzy Aggregation”, IEEE 2nd International Conference on Reliability, Safety and Hazard (ICRESH), 2010, pp. 631-636.

[۱۰۰] Campbell, Philip L. and Jason E. Stamp, “A Classification Scheme for Risk Assessment Methods.”, SANDIA Report, 2004.

[۱۰۱] Farahmand, Fariborz, Shamkant B. Navathe, Philip H. Enslow, and Gunter P. Sharp, “Managing Vulnerabilities of Information Systems to Security Incidents”, in Proceedings of the 5th international conference on Electronic commerce, 2003, pp. 348-354.

[۱۰۲] Chittester, Clyde G. and Yacov Y. Haimes, “Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures”, Journal of Homeland Security and Emergency Management, 2004, Vol. 1, No. 4 .

[۱۰۳] BC, Ezells, Thesis/Dissertation, University of Virginia, 1998.

[۱۰۴] Sridhar, Siddharth, Adam Hahn, and Manimaran Govindarasu, “Cyber–Physical System Security for the Electric Power Grid”, Proceedings of the IEEE, 2012, Vol. 100, No. 1, pp. 210-224.

[۱۰۵] Nai Fovino, Igor, Luca Guidi, Marcelo Masera, and Alberto Stefanini, “Cyber Security Assessment of a Power Plant”, Electric Power Systems Research, 2011, Vol. 81, No. 2, pp. 518-526.

[۱۰۶] Negrete-Pincetic, Matias, Felipe Yoshida, and George Gross. “Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment”, PowerTech, IEEE Bucharest, 2009, pp. 1-8.

[۱۰۷] Haimes, Yacov Y. and Clyde G. Chittester, “A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent Scada Systems”, Journal of Homeland Security and Emergency Management, 2005. Vol. 2, No. 2, pp. 1-23.

[۱۰۸] Crowther, Kenneth G. and Yacov Y. Haimes, “Application of the Inoperability Input—Output Model (IIM) for Systemic Risk Assessment and Management of Interdependent Infrastructures”, Systems Engineering, 2005, Vol. 8, No. 4, pp. 323-341.

[۱۰۹] Zahid Anwar, Mirko Montanari, Alejandro Gutierrez, Roy H. Campbell, “Budget Constrained Optimal Security Hardening of Control Networks for Critical Cyber-Infrastructures ”, International Journal of Critical Infrastructure Protection, May 2009, Vol. 2, No. 1, pp. 13–25.

Hazardous Liquid Loading Operations”, IEEE Conference on Technologies for Homeland Security, 2009, pp. 607-614.

[۷۹] Chen, Thomas M. , Juan Carlos Sanchez-Aarnoutse, and John Buford., “Petri Net Modeling of Cyber-Physical Attacks on Smart Grid”, IEEE Transactions on Smart Grid, 2011, pp. 741-749.

[۸۰] Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran, “Vulnerability Assessment of Cybersecurity for SCADA Systems”, IEEE Transactions on Power Systems, 2008, Vol. 23, No. 4, pp. 1836-1846.

[۸۱] Calderaro, Vito, Vincenzo Galdi, Antonio Piccolo, and Pierluigi Siano, “A Petri Net Based Protection Monitoring System for Distribution Networks with Distributed Generation”, Electric Power Systems Research, 2009, Vol. 79, No. 9, pp. 1300-1307.

[۸۲] Alefiya, Hussain and Saurabh Amin, “NCS Security Experimentation Using DETER”, In Proceedings of the 1st international conference on High Confidence Networked Systems, 2012, pp. 73-80.

[۸۳] Bopardikar, Shaunak D., and Alberto Speranzon, “On Analysis and Design of Stealth Resilient Control Systems”, 6th international symposium on resilient control systems (ISRCS), Aug 2013, pp. 48-53. 2013, pp. 48-53.

[۸۴] Fawzi, Hamza, Paulo Tabuada, and Suhas Diggavi, “Secure Estimation and Control for Cyber-Physical Systems under Adversarial Attacks”, IEEE Transactions on Automatic Control, 2014, Vol. 59, No. 6, pp. 1454-1467.

[۸۵] Zhu, Minghui, and S. Martinez, “Stackelberg-Game Analysis of Correlated Attacks in Cyber-Physical Systems”, American Control Conference (ACC), 2011, pp. 4063-4068. 4068.

[۸۶] Pang, Zhong-Hua, and Guo-Ping Liu, “Design and Implementation of Secure Networked Predictive Control Systems under Deception Attacks”, IEEE Transactions on Control, Systems Technology, Sep 2012, Vol. 20, No. 5, pp. 1334-1342.

[۸۷] Siddharth, Deshmukh, “Estimation & Control in Spatially Distributed Cyber Physical Systems”, 2013.

[۸۸] Yang, Leis, “Stochastic Optimization and Real-Time Scheduling in Cyber-Physical Systems”, PhD diss , Arizona State University, 2012

[۸۹] Keller, Jean-Yves, Dominique Sauter, and Karim Chabir, “State Filtering for Discrete-Time Stochastic Linear Systems Subject to Random Cyber Attacks and Losses of Measurements”, 20th Mediterranean Conference on Control & Automation, 2012, pp. 935-940.

[۹۰] Deshmukh, Siddharth, Balasubramaniam Natarajan, and Anil Pahwa, “State Estimation over a Lossy Network in Spatially Distributed Cyber-Physical Systems”, IEEE Transactions on Signal Processing 2014, Vol. 62, pp. 3911-3923.

[۹۱] Dohi, Tadashi and Toshikazu Uemura, “An Adaptive Mode Control Algorithm of a Scalable Intrusion Tolerant Architecture”, Journal of Computer and System Sciences, 2012, Vol. 78, No. 6, pp. 1751-1774.

[۹۲] Rosich, Albert, Holger Voos, Yumei Li, and Mohamed Darouach, “A Model Pedictive Approach for Cyber Attack Detection and Mitigation in Control Systems”, 52nd IEEE Annual Conference on Decision and Control (CDC), Florence, Italy, 2013, pp. 6621-6626.

[۹۳] Zhu, Quanyan, “Game-Theoretic Methods for Security and Resilience in Cyber-Physical Systems”, PhD diss., University of Illinois at Urbana-Champaign, 2013.

[۹۴] Amin, Massoud, “Toward Self-Healing Energy Infrastructure Systems”, Computer Applications in Power, 2001, Vol. 14, No. 1, pp. 20-28.