مجله کنترل
ISSN (print) 2008-8345
ISSN (online) 2538-3752
جلد ۱۲، شماره ۳، پاییز ۱۳۹۷، صفحه ۷۵-۶۳

تشخیص حملات سایبری نفوذ به زیرساخت‌های حیاتی با بکارگیری روش شبکه‌پتری ترکیبی مرتبه اول فازی عصبی

زینب قاضی[۱]، علی دوست محمدی[۲]

[۱] دانشجوی دکترای مهندسی برق، گروه کنترل، دانشگاه صنعتی امیرکبیر، z.ghazi@aut.ac.ir

[۲] استادیار، دانشکدهٔ مهندسی برق، گروه کنترل ، دانشگاه صنعتی امیرکبیر ، dad@aut.ac.ir

دریافت: ۱۳۹۵/۷/۲۲ ویرایش: ۱۳۹۶/۶/۶ پذیرش: ۱۳۹۶/۱۱/۲۳

چکیده: تقاضای روزافزون برای دست یافتن به سیستم‌هایی با امنیت و قابلیت اطمینان بالاتر، توسعهٔ مدل‌ها، آنالیز و طراحی روش‌های مناسب را ضروری ساخته است. طراحی کنترلر جهت تشخیص حملات سایبری نفوذ، از اهداف این مقاله است. جهت طراحی کنترلری که قادر باشد حملات نفوذ را به دقت و در کوتاهترین زمان ممکن تشخیص دهد، در این مقاله نظریه شبکه‌پتری ترکیبی مرتبه اول فازی عصبی بکار گرفته شده است. پایداری سیستم تشخیص نفوذ پیشنهادی، به ازای هر گونه شرایط موجود در شبکه ارتباطی و پارامترهای ورودی اثبات شده است. جهت ارزیابی عملکرد کنترلر، مجموعه داده استاندارد DARPA مورد استفاده قرارگرفته است. نتایج شبیه‌سازی‌ها، نرخ گزارشات مثبت نادرست اندک، نرخ تشخیص مناسب و همچنین سرعت همگرایی بسیار بالای کنترلر پیشنهادی را تایید می‌نماید.

کلمات کلیدی: زیرساخت‌های حیاتی، حملات سایبری، سیتم‌های تشخیص نفوذ، شبکه‌پتری ترکیبی مرتبه اول فازی عصبی.

Cyber intrusion detection on critical infrastructures using fuzzy neural first order hybrid Petri net

Z. Ghazi and A. Doustmohammadi

Abstract: Due to the growing demand to achieve more secure and reliable systems, development of models, analysis and design of appropriate procedures seems to be necessary. The aim of this paper is designing a controller in order to detect cyber intrusion. In this paper fuzzy neural first order hybrid Petri net is used to design a controller that is capable of detecting cyber intrusions accurately as soon as possible. The stability of the proposed intrusion detection system has been proven for any network conditions and input parameters. To evaluate controller performance, DARPA standard data set is used. The simulation results confirm proper detection rate, low of false positive rate, and also surprisingly high convergence speed.

Keywords: critical infrastructures, cyber attacks, intrusion detection systems, fuzzy neural first order hybrid Petri net.

۱- مقدمه

سیستم‌های کنترل، سیستم‌هایی هستند که فرآیندهای فیزیکی را کنترل و هدایت می‌کنند. تبادل اطلاعات در اکثر این سیستم‌ها، بر پایه علم کامپیوتر و فناوری اطلاعات می‌باشد. سیستم‌های کنترلی در زیر ساخت‌های حیاتی[۱] سیستم‌های حساسی هستند که هر گونه اختلال در آن‌ها می‌تواند پیامدهای جبران ناپذیری برای سیستم فیزیکی تحت کنترل و افراد مرتبط با آن داشته باشد. کشورهای مختلف با توجه به ضرورت‌ها و اولویت‌های خود، تعاریف متنوعی از زیرساخت و زیرساخت حیاتی ارائه می‌نمایند. تعاریف مختلف می‌تواند باعث ایجاد مصادیق متفاوت گردد. انرژی، آب آشامیدنی و سیستمهای مربوط به تصفیه، مخابرات، رآکتورها، مواد و پسماندهای هسته‌ای، سدها و ... را می‌توان از زیرساخت‌های حیاتی برشمرد.

با افزودن قابلیت‌های جدید، هوشمندسازی شبکه و بکارگیری امکانات مخابراتی روز دنیا در زیرساخت‌های حیاتی، ساختارهای شبکه‌های هوشمند می‌توانند بسیار کاراتر و بهبود پذیرتر جهت اداره و عملکرد گردند. این مسائل هر چند فواید بسیاری از جهت کارایی در شبکه‌ها دارند، اما ریسک‌های بزرگ و چالش‌های دشواری در مقولهٔ حفاظت در برابر حملات امنیتی سایبری به وجود خواهند آورد. با توجه به مقیاس وسیع شبکه‌های زیرساخت‌های حیاتی، منطقی به نظر می‌رسد که آسیب پذیری سیستم‌های ارتباطی این شبکه‌ها نیز به همین میزان گسترده باشد. بنابراین تمامی کارشناسان اذعان دارندکه شاخهٔ امنیت سایبری در زیرساخت‌های حیاتی بسیار با اهمیت بوده و نیازمند توجه و تحقیقات بسیار است.

حملات سایبری می‌تواند با انگیزه‌های متفاوتی انجام گیرد از جمله: چالش‌های ذهنی و فکری، نشان دادن خود و یافتن رقیب، تست کردن امنیت سیستم، بدست آوردن پول، انتقام، تروریسم. حملات سایبری انواع مختلفی دارند که می‌توان به برخی موارد از قبیل : حملهٔ دسترسی به منابع، حملهٔ صحت اطلاعات، حملات پروتکل، حملات مسیر یابی[۲]، نفوذ[۳]، بدافزار، تزریق داده‌های نادرست[۴] اشاره نمود [۱]. رویدادهای اخیر از جمله استاکس‌نت، الزاماتی در خصوص پرداختن به حملات سایبری پیچیده و اثرات بسیار مخرب آنها بر زیرساخت‌های حیاتی را ضروری ساخته است. برای دستیابی به این هدف با توجه به مزایای قابل توجه نظریه شبکه‌پتری، به نظر می‌رسد بکارگیری این ابزار مفید واقع خواهد شد. تمرکز این مقاله بر تشخیص حملات نفوذ می‌باشد. به طور کلی تشخیص نفوذ به دو نوع مختلف دسته بندی می‌گردد: تشخیص سوء استفاده[۵]، تشخیص غیرمتعارف[۶].

در نوع اول تشخیص بر مبنای خصوصیات شناخته شدهٔ حملات است. دادهٔ جدید با پایگاه دانش حملات مورد مقایسه قرار می‌گیرد و در صورت تطابق به عنوان حمله تشخیص داده می‌شود. از مزایای این روش نرخ گزارشات مثبت نادرست (FPR) کم می‌باشد. با این حال این روش قابلیت شناسایی حملات ناشناخته را ندارد. در نوع دوم یا همان تشخیص غیرمتعارف، رفتار متعارف و نرمال سیستم تعریف می‌شود و در صورت عدم تطابق داده‌های ثبت شده با رفتار نرمال سیستم، به عنوان حملهٔ سایبری گزارش خواهد شد. هر چند این روش قابلیت شناسایی حملات ناشناخته را دارد، اما FPR در این روش بالا بوده که این امر خصوصا در کنترل زیرساخت‌های حیاتی یک مشکل بزرگ محسوب می‌شود [۲]. در این مقاله روشی جهت تشخیص نفوذ بر مبنای تشخیص غیرمتعارف مبتنی بر نظریه شبکه‌پتری ترکیبی مرتبه اول فازی عصبی[۷] پیشنهاد شده است که نه تنها نرخ تشخیص مناسبی ایجاد خواهد نمود، بلکه بر اساس نتایج شبیه‌سازی زمان همگرایی و FPR بسیار کمی خواهد داشت.

تشخیص نفوذ اولین بار توسط [۳] مطرح گردید. پس از آن مطالعات بسیاری بر روی این حو زه متمرکز گردید[۵،۴]. در حوزهٔ تشخیص نفوذ بر اساس روش تشخیص سوء استفاده تحقیقات بسیاری متمرکز شده است. از جمله روش‌های مورد استفاده در این حوزه می‌توان به تطبیق الگو اشاره نمود[۷،۶]. روش‌های تطبیق الگو، از جمله روش‌های رایج جهت ارتقا امنیت تبادل داده هستند. روش‌های ارائه شده در این حوزه، معرفی و مقایسه آنها در [۸] گردآوری شده است. استخراج داده فرآیندی جهت شناسایی داده‌های معتبر و استخراج الگوی قابل فهم از آن‌هاست، که بر این اساس قادر خواهیم بود رفتارهای مشکوک را شناسایی نماییم [۱۱-۹]. الگوریتم ژنتیک با بهره‌گیری از بهینه‌سازی جستجوی سناریوی حمله، در زمان پردازش منطقی زیرمجموعه‌ای از حملات بالقوه را فراهم می‌نماید [۱۳،۱۲]. در [۱۴] با بهره‌گیری از الگوریتم ژنتیک و الگوریتم فازی، روشی جهت تشخیص برخط نفوذ ارائه شده است. از شبکه‌پتری رنگی می‌توان به عنوان ابزاری برای تعریف ویژگی‌های رفتارهای مخرب و همچنین تشخیص آن‌ها نام برد [۱۷-۱۵].

برخی روش‌های موجود در حوزهٔ تشخیص غیرمتعارف بر مبنای روش طبقه بندی[۸] است [۲۰-۱۸]. طبقه بندی یکی از محبوب‌ترین روش‌های تشخیص نفوذ است. در این روش الگوریتمی برای یافتن شباهت بین نمونه‌ها جهت ساخت خوشه ارائه می‌شود، به گونه‌ای که نمونه‌های متعلق به یک خوشه دارای ویژگی‌های مشابهی باشند. اگرچه در این روش نمونه‌های جدید به خوبی تشخیص داده می‌شوند، اما پیش بینی با دقت کمی صورت می‌پذیرد. [۲۱] با افزودن کمیت‌های فازی الگوریتمی بر پایهٔ طبقه بندی جهت تشخیص حملات نفوذ پیشنهاد داده است که قادر است

[۱] Critical infrastructure System
[۲] Routing attack
[۳] Intrusion
[۴] False Data Injection
[۵] Misuse detection
[۶] Anomaly detection
[۷] fuzzy neural first order hybrid Petri net
[۸] Clustering

کارایی را به نسبت روش‌های طبقه بندی موجود بهبود ببخشد. شبکه عصبی در حوزهٔ تشخیص غیرمتعارف به صورت گسترده بکار گرفته شده است و از مزایای آن می‌توان از نرخ تشخیص مناسب نام برد [۲۴-۲۲]. الگوریتم فازی با وزن‌های تصادفی جهت تشخیص نفوذ در [۲۵] بکار گرفته شده است،که توان محاسباتی و یادگیری بالایی ایجاد نموده است. الگوریتم ژنتیک [۲۷،۲۶] و ویولت [۲۸] از دیگر راهکارهای مورد استفاده در تشخیص غیرمتعارف می‌باشند. در [۲۹] روش PSO[1] برای ایجاد وزن‌ها بکارگرفته شده است تا مجموعه‌ای از طبقه بندی‌ها را با دقت بیشتری ایجاد نماید. الگوریتم مبتنی بر اطلاعات متقابل، ویژگی مطلوب برای طبقه بندی را به صورت تحلیلی انتخاب می‌نماید. الگوریتم انتخابی مبتنی بر اطلاعات متقابل می‌تواند ویژگی‌های خطی و غیر وابسته به داده‌ها را نیز بررسی نماید [۳۰]. امروزه تحقیقات محدودی بر تشخیص حملات سایبری با استفاده از ایدهٔ شبکه‌پتری، متمرکز شده است. در [۳۱] از شبکه‌پتری رنگی جهت طراحی درخت خطا و ارائه و پیاده سازی سیستم‌های تشخیص نفوذ مبتنی بر عامل‌ها، استفاده شده است. همچنین ایدهٔ شبکه‌پتری تصادفی تعمیم‌یافته برای مدلسازی حملات و تهدیدات در سیستم اسکادا بکار گرفته شده است [۳۲]. توماس چن و همکاران، توانایی شبکه‌پتری در مدلسازی حملات سایبری-فیزیکی به شبکه‌های هوشمند را نشان داده‌اند [۳۳].

از آنجایی که زیرساخت‌های حیاتی سیستم‌هایی ترکیبی از دینامیک‌های پیوسته و رخداد گسسته هستند [۳۴]، بکارگیری هر روش پیوسته و یا رخداد گسسته جهت مدلسازی و تشخیص خطا (خطای فیزیکی و یا سایبری) بخشی از دینامیک سیستم را در نظر نگرفته و قادر نخواهد بود همزمان دینامیک‌های پیوسته و رخداد گسسته و ارتباطات مابین آن‌ها را مدل نماید. از این رو امروزه مدلسازی و تشخیص خطا بر اساس روش‌های ترکیبی در زیرساخت‌های حیاتی مورد توجه قرار گرفته است [۳۵،۳۴]. در این مقاله، روش شبکه‌پتری ترکیبی فازی عصبی جهت تشخیص نفوذ در زیرساخت‌های حیاتی پیشنهاد شده است، که علاوه بر در نظرگرفتن همزمان دینامیک‌های پیوسته و رخداد گسسته وارتباطات مابین آن‌ها، قادر است حملات نفوذ را در کوتاهترین زمان و با دقت بالا تشخیص دهد. عملکرد روش پیشنهادی با اعمال به مجموعه داده استاندارد DARPA (تنها پایگاه داده معتبر جهت تشخیص حملات نفوذ) مورد ارزیابی قرار گرفته است. پایداری سیستم تشخیص نفوذ پیشنهادی، به ازای هر گونه شرایط موجود در شبکه ارتباطی و پارامترهای ورودی اثبات شده است.

در ادامهٔ این مقاله ابتدا در بخش ۲ مروری کوتاه بر نظریه شبکه‌پتری ترکیبی مرتبه اول (FOHPN) ارائه خواهد شد. بخش ۳ روش پیشنهادی شبکه‌پتری ترکیبی مرتبه اول فازی عصبی در تشخیص نفوذ شرح داده خواهد شد. جهت ارزیابی عملکرد، روش پیشنهادی به داده‌های استاندارد DARPA اعمال شده است. پردازش اولیه و استخراج مولفه‌های اصلی داده‌ها در بخش ۴ شرح داده شده است. بخش ۵ نتایج شبیه سازی ارائه و تحلیل خواهد شد. اثبات پایداری مدل پیشنهادی به ازای هر شرط اولیه ای در بخش ۶ ارائه گردیده است. در نهایت بخش۷ مقاله، حاوی مطالب جمع بندی است.

۲- شبکه‌پتری ترکیبی مرتبه اول

ایدهٔ شبکه‌پتری در سال ۱۹۶۲ توسط کارل آدام پتری ارائه گردید [۳۶]. در کنار شبکه‌پتری گسسته، ایده شبکه‌پتری پیوسته جهت مدلسازی سیستم‌ها و سیگنال‌های پیوسته در سال ۱۹۸۷ مطرح شد [۳۷]. در مدل شبکه‌پتری هیبرید که در سال ۱۹۹۱ ارائه شده است، به صورت همزمان از شبکه‌پتری پیوسته برای مدل‌کردن جریان‌های پیوسته و از شبکه‌پتری عادی برای مدل کردن وقایع گسسته استفاده شده است [۳۸]. شبکه‌پتری ترکیبی قادر است سیستم‌های دارای دو دینامیک همزمان پیوسته و رویداد گسسته را به خوبی مدل نماید [۳۹]. این ابزار در عین حال که صورت نمایش گرافیکی جذاب و قابل درکی دارد، قادر است تحلیل‌های آنالیتیکی دقیقی نیز از سیستم ارائه دهد [۴۱،۴۰]. در این مقاله شبکه‌پتری هیبرید مرتبهٔ اول مورد استفاده قرار گرفته است [۴۲]. در این روش دینامیک پیوسته سیستم توسط مدل‌های سیال[2] مرتبه اول توصیف می‌گردد. در این مدل فلوهای پیوسته نرخ قطعه‌ای ثابت داشته و محتوای سیال هر جایگاه پیوسته به صورت خطی با زمان تغییر می‌کند. استفاده از این روش در عین داشتن دقت مطلوب، سرعت عملکرد بالا،که از جمله نیازهای حیاتی سیستم‌های تشخیص نفوذ است را مسیر می‌سازد. برخی مزایای بکارگیری FOHPN در تشخیص نفوذ در ادامه ذکر شده است:

- شبکه‌پتری ابزاری قدرتمند، گرافیکی و جذاب است که بکارگیری آن در مدلسازی سبب می‌شود که اپراتور ارتباط گرافیکی و مؤثری با محیط برنامه نویسی برقرار نماید و درک مناسبی از مدل، ساختار و اجزای سیستم داشته باشد.
- ریاضیات و محاسبات نظریه شبکه‌پتری در مقایسه با سایر ابزارها تا حدود زیادی ساده و قابل فهم بوده و این امر اجرای برنامه را نسبت به سایر ابزارها به مراتب سریعتر می‌نماید. تشخیص نفوذ در کوتاهترین زمان یک الویت مهم در زیرساخت‌های حیاتی است.
- کنترل نمودن سیستمی که توسط شبکه‌پتری مدل شده است، ساده‌تر بوده و قانون کنترل صراحتاً قابل محاسبه و اعمال خواهد بود.
- مانیتور سیستم و تشخیص خطا با بکارگیری نظریه شبکه‌پتری قابل پیاده سازی، مؤثر و کارا می‌باشد. خطا در ابزار شبکه‌پتری به عنوان یک حالت ممنوع قابل تعریف بوده و از این رو تشخیص خطا به نحو مطلوبی امکان پذیر است.

[1] Particle Swarm Optimization

[2] Fluid

- نمایش عملکرد موازی[۱]، همزمان[۲] و متقارن[۳] در مدل شبکه‌پتری بسیار آسان و قابل درک است.
- پارامترهای تشخیص نفوذ هر دو ماهیت پیوسته و گسسته را دارا هستند. FOHPN یک ابزار مناسب برای مدل کردن این دینامیک‌ها و ارتباطات بین آنهاست.

شبکه‌پتری ترکیبی مرتبهٔ اول به صورت $\langle N, m(\tau_0)\rangle$ تعریف می‌شود که N یک سیستم FOHPN با شرایط اولیهٔ $m(\tau_0)$ است. یک سیستم FOHPN بصورت $N=(P,T,Pre,Post,m_0)$ بوده که در آن P مجموعه محدودی از $|P|$ جایگاه[۴] بصورت $P=P_d\cup P_c$ می‌باشد. P_d بیانگر مجموعه جایگاه‌های گسسته و P_c بیانگر مجموعه جایگاه‌های پیوسته است. $T=T_c\cup T_d$ مجموعه محدودی از $|T|$ گذر[۵] است، که در آن T_c مجموعه گذرهای پیوسته و T_d مجموع گذرهای گسسته متشکل از گذرهای آنی T_i، گذرهایی با زمان حقیقی T_t و گذرهایی با زمان تصادفی T_s است. همانند شبکه‌پتری عادی در شبکه‌پتری ترکیبی نیز رابطه $T\cap P=\phi$ برقرار می‌باشد. فرمول‌بندی یک سیستم FOHPN مشابه [۴۲] در نظر گرفته شده است. در این بخش به اختصار نظریه شبکه‌پتری ترکیبی مرتبهٔ اول بیان گردیده، جزییات فرمول بندی در [۴۲] شرح داده شده است.

توابع تلاقی Pre و $Post$ بصورت زیر تعریف می‌شوند. تابع $Post$ بیانگر وزن کمان[۶] ورودی به (خروجی از) هر گذر است. که داریم: $R_0^+=R^+\cup\{0\}$.

$$Pre:\begin{cases}P_d\times T\to\mathbb{N}\\ P_c\times T\to\mathbb{R}_0^+\end{cases}\qquad Post:\begin{cases}P_d\times T\to\mathbb{N}\\ P_c\times T\to\mathbb{R}_0^+\end{cases}\qquad (۱)$$

$Pre(P_i,t_j)$ بیانگر وزن کمانی است که جایگاه i-ام را به گذر j-ام متصل می‌نماید و $Post(P_i,t_j)$ بیانگر وزن کمانی است که گذر j-ام را به جایگاه i-ام متصل می‌کند. نماد $t^\bullet$ مجموعه جایگاه‌هایی است که کمان ورودی به گذر t دارند. $t^{(d)}=t^\bullet\cap P_d$ مجموعه جایگاه‌های گسسته متعلق به $t^\bullet$ و $t^{(c)}=t^\bullet\cap P_c$ مجموعه جایگاه‌های پیوسته متعلق به $t^\bullet$ است. $t^\bullet$ بیانگر مجموعه جایگاه‌هایی از شبکه است که از گذر t به آنها وارد می‌شود. $t^{(d)}=t^\bullet\cap P_d$ جایگاه‌های گسسته و $t^{(c)}=t^\bullet\cap P_c$ مجموعه جایگاه‌های پیوسته متعلق به $t^\bullet$ است. همین تعاریف را می‌توان برای گذرهای ورودی و خروجی یک جایگاه نیز نوشت. بیان گرافیکی شبکه‌پتری ترکیبی در شکل ۱ نشان داده شده است.

شکل ۱: جایگاه‌ها و گذرهای تشکیل دهنده شبکه‌پتری هیبرید

تابع $D:T_d/T_I\to R^+$ زمان مرتبط با گذرهای گسستهٔ زمانی را نشان می‌دهد. در این نظریه به هر $t_i\in T_D$ یک تاخیر آتش کردن ثابت $\delta_i=D(t_i)$ متناظر می‌گردد. به هر گذر زمانی با توزیع نمایی $t_i\in T_E$ یک نرخ آتش کردن متوسط $\lambda_i=D(t_i)$ نسبت داده می‌شود. $1/\lambda_i$ تاخیر آتش کردن متوسط است، که λ_i پارامتر مربوط به توزیع نمایی متناظر می‌باشد.

تابع سرعت‌های آتش کردن گذرهای پیوسته به صورت $C:T_c\to R_0^+\times R_\infty^+$ تعریف می‌شود که داریم: $R_\infty^+=R^+\cup\{\infty\}$. برای هر گذر پیوسته $t_i\in T_c$ داریم $C(t_i)=(V_i',V_i)$ ، $V_i'\le V_i$. V_i' می‌نیمم سرعت آتش کردن (mfs) و V_i ماکزیمم سرعت آتش کردن (MFS) می‌باشد. عبارت C_{xy}، که $x,y\in\{c,d\}$ مرتبط با P_x و T_y است. حالت فعال بودن یک گذر پیوسته، سرعت فایر کردن آنی[۷] (IFS) قابل قبول آن گذر v_i را تعریف می‌نماید. ماتریس تلاقی در یک شبکه به فرم $A(p,t)=Post(p,t)-Pre(p,t)$ تعریف می‌شود. برای ماتریس تلاقی داریم:

$$A=\begin{bmatrix}A_{cc} & A_{cd}\\ A_{dc} & A_{dd}\end{bmatrix}\qquad (۲)$$

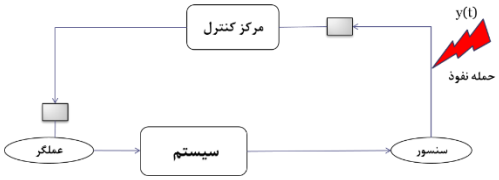
$$A_{xy}=Post(P_i,t_j)-Pre(P_i,t_j),$$
$$P_i\in P_x,t_j\in T_y,x,y\in\{c,d\}$$

نشانه‌گذاری[۸] تابعی است که به هر جایگاه گسسته مقداری غیرمنفی از نشانه[۹] (که با نقاط مشکی رنگ نمایش داده می‌شود) و به هر جایگاه پیوسته مقداری سیال نسبت می‌دهد m_p نشانه‌گذاری جایگاه p می‌باشد. مقدار نشانه‌گذاری در زمان τ با $m(\tau)$ نمایش داده می‌شود. نمادهای m^d و m^c متناظر با مقدار نشانه‌گذاری P_d و P_c هستند.

۳- روش پیشنهادی شبکه‌پتری ترکیبی مرتبه اول فازی عصبی در تشخیص نفوذ

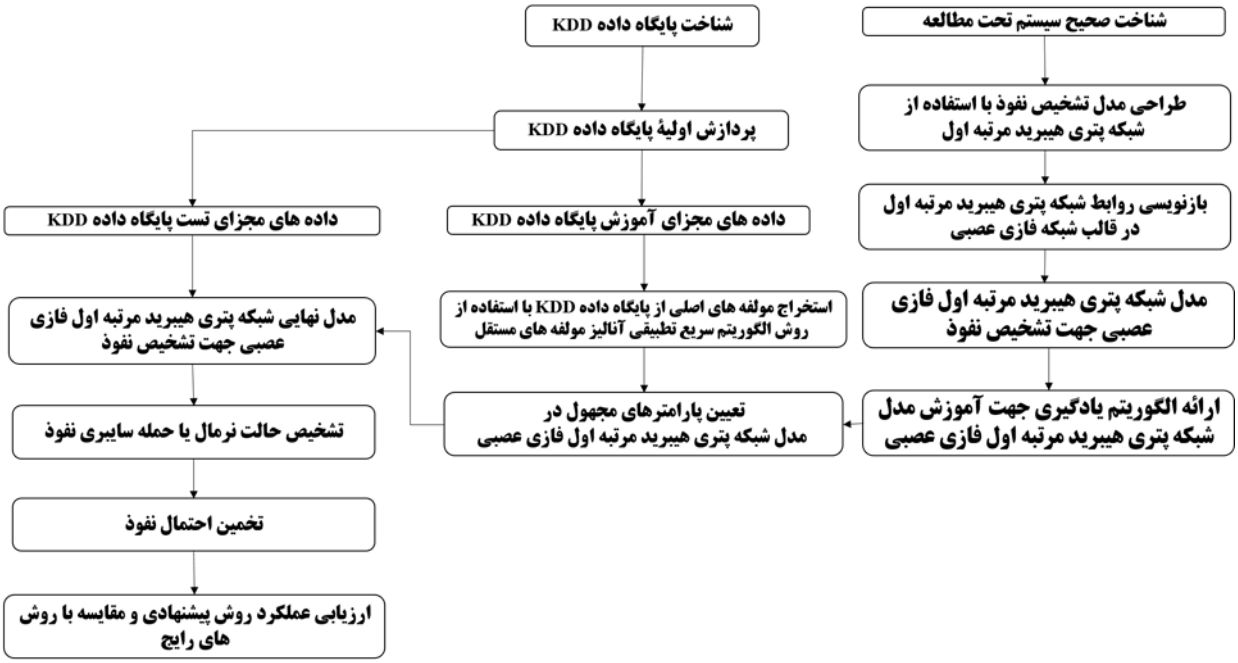
[۱] Parallel
[۲] Synchronic
[۳] Concurrent
[۴] Place
[۵] Transition
[۶] Arc
[۷] Instantaneous firing speed
[۸] Marking
[۹] Token

همانگونه که شکل ۲ نشان می‌دهد، حملات سایبری می‌تواند با هدف ایجاد اختلال در عملکرد سنسور طراحی شوند و یا مستقیماً کنترل کننده را مورد تهاجم قرار دهند. در هر حالت با نفوذ به اطلاعات و تزریق داده‌های نادرست، اطلاعاتی که کنترلر بر اساس آن تصمیم‌گیری و عمل می‌نماید، مخدوش گردیده و بدیهی است که کنترل کننده با تحلیل این اطلاعات نادرست، عملکرد صحیحی نخواهد داشت و ممکن است این تصمیمات کنترلر، اثرات مخرب جبران ناپذیری به سیستم تحمیل نماید.



شکل ۲: نمایش حملات نفوذ به کنترلر از طریق سنسور

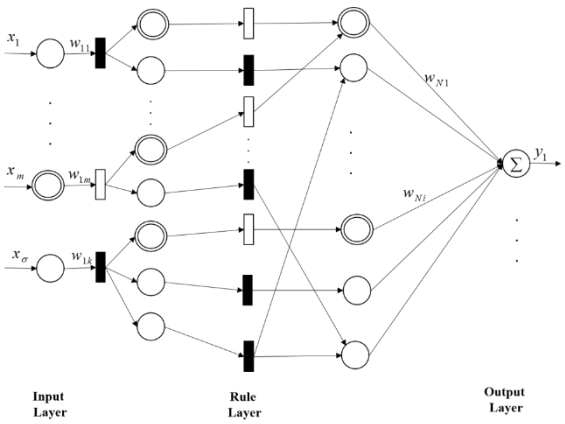
از این رو تشخیص حملات سایبری نفوذ در سیستم‌های کنترل به صورت زمان حقیقی و در زمان کوتاه اهمیت بسیاری دارد و از جمله اهداف این مقاله است. الگوریتم شکل ۳ گام‌های عملکردی در مقاله را نمایش می‌دهد. گام‌های عملکردی به سه فاز کلی تقسیم می‌گردند: طراحی مدل شبکه پتری ترکیبی فازی عصبی، پردازش پایگاه داده و استخراج مولفه‌های اصلی و ارزیابی عملکرد روش پیشنهادی با اعمال به پایگاه داده تست.



شکل ۳: الگوریتم نمایش گام‌های عملکردی

در ادامه این بخش مراحل طراحی مدل تشخیص نفوذ با استفاده از مدل شبکه پتری ترکیبی مرتبه اول فازی عصبی تشریح می‌گردد. پردازش پایگاه داده و استخراج مولفه‌های اصلی در بخش ۴ و ارزیابی عملکرد روش پیشنهادی با اعمال پایگاه داده تست در بخش ۵ ارائه شده است.

شبکهٔ FOHPN با سه لایه که در شکل ۴ نمایش داده شده است را در نظر بگیرید. مدل پیشنهادی دارای سه لایه است: لایه ورودی، لایه قانون، لایه خروجی.



شکل ۴: ساختار پیشنهادی شبکه‌پتری ترکیبی مرتبه اول فازی عصبی

t_j مجموعه گذرهای لایهٔ jام از مدل شبکه‌پتری ترکیبی مرتبه اول فازی عصبی است که می‌تواند پیوسته یا گسسته باشد $j=1,2,...,n$. وزن کمان‌های لایهٔ jام به صورت $w_1^j, w_2^j, ..., w_\vartheta^j$ در نظر گرفته شده است. جهت تعریف رفتار نرمال و حملات در مدل پیشنهادی، می‌توان به ازای هر حالت وزن به خصوصی تعریف نمود. در این حالت یک مدل شبکه‌پتری هیبرید مرتبه اول با ابعاد بسیار بالاخواهیم داشت، که عملکرد مطلوبی ندارد. ایدهٔ مطرح شده در این مقاله استفاده از روش شبکه‌پتری ترکیبی مرتبه اول فازی عصبی جهت تشخیص حملات نفوذ است. در ادامه مفاهیم شبکه‌پتری ترکیبی مرتبه اول به گونه‌ای بازنویسی می‌گردد که بتواند بر فرمول بندی فازی عصبی انطباق یابد.

دینامیک مدل FOHPN با وقوع رخداد ماکرو[۱] تغییر می‌یابد. ابتدا فرمول بندی برای گذرهای گسسته شرح داده خواهد شد. رخداد ماکرو با آتش کردن گذر گسسته رخ می‌دهد. این امر باعث تغییر نشانه‌گذاری گسسته یا فعال/غیرفعال شدن گذر پیوسته می‌گردد. مدل پشنهادی این مقاله جهت تشخیص نفوذ به گونه‌ای است که هر گاه گذر گسسته فعال گردد، تنها نشانه‌گذاری گذرهای گسسته تغییر پیدا می‌کند.

فرض کنید $\sigma(k)$ بردار شمارش آتش کردن[۲] در زمان k باشد. رفتار میکرو در مدل FOHPN در طول دورهٔ ماکروی kام بدین صورت تعریف خواهد شد.

$$m^d(k+1) = m^d(k) + C_{dd}.\sigma(k+1) \qquad (۳)$$
$$m^c(k+1) = m^c(k)$$

با انجام فرآیند فازی سازی، وروردی قطعی[۳] x_i به ورودی‌هایی فازی با تابع عضویت انطباق یافتهٔ گوسین با تعریف زیر تبدیل می‌گردد.

$$\mu_{ij} = \exp(-\frac{1}{2}\frac{(x_i - c_{ij})^2}{s_{ij}^{\ 2}}) \qquad (۴)$$

S_{ij}, C_{ij} به ترتیب مرکز و عرض تابع عضویت می‌باشند. در این صورت برای آتش کردن گذر گسسته داریم:

$$t_{ij} = \begin{cases} 1 & if \quad \mu_{ij} > d_{th} \\ 0 & if \quad \mu_{ij} < d_{th} \end{cases} \qquad (۵)$$

d_{th} یک مقدار آستانه است که بر اساس [۴۳] داریم:

$$d_{th} = \frac{\alpha_{th}\exp(-\beta_{th}E_{th})}{1+\exp(-\beta_{th}E_{th})} \qquad (۶)$$

β_{th}, α_{th} ضرایب مثبت هستند که به صورت تصادفی انتخاب می‌شوند. ملاحظات تنظیم پارامترها در [۴۳] به تفصیل بیان شده است. خروجی لایهٔ jام مدل FOHPN بدین صورت تعریف می‌گردد:

$$X^{\ j} = W^{\ T}M = \sum_{i=1}^{\vartheta} m(p_i^{\ j}) \prod_i^{\sigma} \mu_{ij} w_i^{\ j} \qquad (۷)$$
$$Y(X^{\ j}) = F(X^{\ j}) = F(W^{\ T}M)$$

m نشانه‌گذاری شبکه است که از (۳) قابل محاسبه است. σ تعداد ورودی‌های شبکهٔ پیشنهادی است. X، Y، W، M به ترتیب بردارهای ورودی، خروجی، وزن کمان و نشانه‌گذاری می‌باشند. برای گذرهای پیوسته در مدل پیشنهادی شبکه‌پتری ترکیبی مرتبه اول فازی عصبی، فرمول بندی مشابهی می‌توان نوشت. سرعت آتش کردن آنی گذر $t_i \in T_c$ در زمان τ با $v_i(\tau)$ نمایش داده می‌شود. نشانه‌گذاری جایگاه پیوسته با این فرض که هیچ گذر گسسته ای آتش نکند و تمامی سرعت‌ها پیوسته باشند، به فرم زیر تغییر می‌نماید.

$$m(\tau + d\tau) = m(\tau) + w.v(\tau)d(\tau) \qquad (۸)$$
$$\frac{m(\tau+d\tau)-m(\tau)}{d(\tau)} = w.v(\tau)$$

از این رو داریم:

$$\frac{dm(\tau)}{d\tau} = \sum_{t_i \in T_c} C(p,t_i).v_i(\tau) \qquad (۹)$$

رخداد ماکرو همچنین زمانی روی می‌دهد که جایگاه پیوسته تهی گردد. در نظر بگیرید τ_k, τ_{k+1} زمان‌های وقوع رخداد ماکرو باشند. این بازهٔ زمانی ماکرو پریود (Δ_k) نامیده می‌شود. در این مقاله فرض شده است که در طول یک ماکرو پریود گذرهای پیوسته، IFS ثابتی دارند.

فرض کنید τ_0 زمان اولیه و $\tau_k (k>0)$ زمانی است که رخداد ماکرو اتفاق می‌افتد. $v(\tau_k)$ بردار IFS در طول ماکرو پریود Δ_k است. $\sigma(\tau_k)$ بردار شمارش آتش کردن در زمان τ_k است. رفتار میکرو مدل FOHPN در طول ماکرو پریود k ام به صورت زیر نتیجه می‌شود [۴۲]:

$$m^c(\tau) = m^c(\tau_k) + C_{cc}.v(\tau_k).(\tau - \tau_k) \qquad (۱۰)$$
$$m^d(\tau) = m^d(\tau_k)$$

خروجی لایهٔ j ام مدل FOHPN در این حالت نیز به فرم $Y(X^j) = F(X^j) = F(W^T M)$ می‌تواند نوشته شود.

[۱] Macro event
[۲] Firing count vector
[۳] Crisp input

m نشانه‌گذاری پیوسته و $F = v(t)$ می‌باشد. روش انتشار معکوس[۱]، در این مقاله جهت محاسبهٔ وزن کمان‌های مدل شبکه‌پتری پیشنهادی مورد استفاده قرار گرفته است.

شبکهٔ پتری ترکیبی مرتبه اول فازی عصبی با k لایهٔ پنهان را در نظر بگیرید. با احتساب لایهٔ ورودی و خروجی $k+2$ لایه داریم که به صورت ۰، ... ،$k+1$ شماره گذاری شده است. تعداد جایگاه‌های ورودی r و تعداد جایگاه‌های خروجی L در نظر گرفته شده است. در سایر لایه‌ها N جایگاه داریم.

$$Y(n) = [y_1^{k+1}(n), ..., y_L^{k+1}(n)]^T \qquad (۱۱)$$
$$X^{\circ}(n) = [x_1^{\circ}(n), ..., x_r^{\circ}(n)]^T$$

n نشاندهندهٔ زمان آموزش است. برای خروجی لایهٔ jام می‌توان نوشت:

$$\bar{y}_i^{j+1}(n) = F\Big(\sum_{\beta=1,...,N^j} w_{i\beta}^j \prod_i^{\beta} \mu_{ij} x_\beta(n)\Big) \qquad (۱۲)$$
$$\bar{Y}(n) = [\bar{y}_1^{k+1}(n), ..., \bar{y}_L^{k+1}(n)]^T$$

$w_{i\beta}$ وزن کمان بین جایگاه‌های i و β در لایه‌های مختلف است. جهت محاسبهٔ وزن کمان‌ها در مدل پیشنهادی، با استفاده از q جفت دادهٔ آموزش ورودی و خروجی، می‌بایست یک بهینه سازی انجام شود. وزن کمان‌ها بایستی به گونه ای تعیین گردد که خطا حداقل گردد. تابع هزینهٔ خطای مربعی جمعی به صورت زیر تعریف می‌شود:

$$E = \sum_{n=1,...,q} \left\| Y(n) - \bar{Y}(n) \right\|^2 = \sum_{n=1,...,q} E(n) \qquad (۱۳)$$

با استفاده از مفهوم گرادیان داریم:

$$\frac{\partial E}{\partial w_{i\beta}^j} = \sum_{t=1,...,q} \frac{\partial E(n)}{\partial w_{i\beta}^j} \qquad (۱۴)$$

با داشتن مقدیر مناسب نرخ آموزش γ داریم:

$$w_{i\beta}^j(\kappa+1) = w_{i\beta}^j(\kappa) - \gamma \frac{\partial E(n)}{\partial w_{i\beta}^j}. \qquad (۱۵)$$

وزن‌های جدید با انجام محاسبات برای همهٔ نمونه‌های آموزش قابل محاسبه خواهند بود. یکبار طی این مراحل برای همهٔ نمونه‌ها یک دوره[۲] نامیده می شود. قبل از شروع اولین اپیک تعداد قوانین فازی، وزن‌های اولیه، مرکز و عرض اولیهٔ تابع‌های عضویت و سایر پارامترهای تعریف شده در روش پیشنهادی، بایستی مقدار دهی شوند. این مقادیر می‌توانند به صورت تصادفی انتخاب شوند. البته انتخاب هوشمندانه این مقادیر در کاهش زمان همگرایی موثر خواهد بود. برای محاسبهٔ $\frac{\partial E(n)}{\partial w_{i\beta}^j}$ داریم:

$$\frac{\partial E(n)}{\partial w_{i\beta}^j} = \frac{\partial E(n)}{\partial Y(n)} * \frac{\partial Y(n)}{\partial w_{i\beta}^j} = \qquad (۱۶)$$
$$\sum_{n=1,...,q} \left\| Y(n) - \bar{Y}(n) \right\| * \frac{\partial F(X^j)}{\partial X^j} * \frac{\partial X^j}{\partial w_{i\beta}^j}$$

پیش از این نیز اشاره شد که در شبکهٔ FOHPN برای گذر گسسته $t_i \in T_D$ یک گذر زمانی با توزیع نمایی $t_i \in T_E$ با نرخ آتش متوسط $\lambda_i = D(t_i)$ متناظر می‌گردد. $1/\lambda_i$ تاخیر آتش متوسط است. λ_i ، ζ و b پارامترهای توزیع نمایی متناظر می‌باشند. بنابراین می‌توان نوشت:

$$\frac{\partial F(X^j)}{\partial X^j} = \frac{\zeta^j}{1+\exp(-b(X^j - \lambda^j))} + \qquad (۱۷)$$
$$\frac{\zeta^j X^j b * \exp(-b(X^j - \lambda^j))}{[1+\exp(-b(X^j - \lambda^j))]^2}$$
$$\frac{\partial X^j}{\partial w_{i\beta}^j} = m(p_i^j) \prod_i^{\sigma} \mu_{ij}$$

الگوریتم ۱ برای حداقل کردن خطای روش انتشار معکوس ارائه خواهد شد.

الگوریتم ۱:

گام ۰ : قرار دهید $\kappa = 0,\ \rho = \mathrm{P}$ و $error = \varepsilon$ (ρ مقدار ماکزیمم اپیک‌ها است).

گام ۱ : تمامی وزن‌ها و پارامترهای از پیش تعیین شده می‌بایست مقدار دهی اولیه شوند.

گام ۲ : محاسبهٔ خروجی هر لایه از شبکه توسط فرمول (۱۲).

گام ۳ : محاسبهٔ خطای انتشار لایهٔ خروجی $\Delta_i^j(n)$ به صورت رو به عقب $j = k+1, k, ..., 1$.

$$\Delta_i^{k+1}(n) = [y_i(n) - \bar{y}_i(n)] \frac{\partial F}{\partial X}\Big|_{X = z_i^{k+1}} \qquad (۱۸)$$

گام ۴ : محاسبهٔ ترم خطای انتشار مربوط به لایه‌های میانی با استفاده از رابطهٔ زیر:

$$\Delta_i^j(n) = \sum_{\varphi=1}^{N^{j+1}} \Delta_\varphi^{j+1} w_{\varphi i}^j \frac{\partial F}{\partial X}\Big|_{X = z_i^m} \qquad (۱۹)$$
$$z_i^j(n) = \sum_{\alpha=1}^{N^{j-1}} x_\alpha^{j-1}(n) w_{i\alpha}^{j-1} \prod_i^{\alpha} \mu_{ij}$$

گام ۵ : به روز نمودن وزن‌ها، C_{ij} و S_{ij} با بکارگیری روابط زیر .

[۱] Back Propagation

[۲] Epoch

$$w_{i\beta}^{j-1}(\kappa+1)=w_{i\beta}^{j-1}(\kappa)+\gamma\sum_{n=1}^{q}\Delta_i^j(n)x_\beta^{j-1}(n)\prod_i^\alpha\mu_{ij}. \quad (۲۰)$$

$$c_{ij}(\kappa+1)=c_{ij}(\kappa)-\gamma_c\frac{\partial E}{\partial c_{ij}}.$$

$$s_{ij}(\kappa+1)=s_{ij}(\kappa)-\gamma_s\frac{\partial E}{\partial s_{ij}}.$$

$$\frac{\partial E}{\partial c_{ij}}=(Y(n)-\bar{Y}(n))m(p_i^{\,j})\prod_i^\sigma\mu_{ij}\frac{(x_i-c_{ij})}{s_{ij}^{\,2}}$$

$$\frac{\partial E}{\partial s_{ij}}=(Y(n)-\bar{Y}(n))m(p_i^{\,j})\prod_i^\sigma\mu_{ij}\frac{(x_i-c_{ij})^2}{s_{ij}^{\,3}}$$

گام ۶: پس از هر اپیک ترم خطا (۱۳) می‌بایست محاسبه گردد. در صورتی که $error>\varepsilon$ یا $\kappa<\mathrm{P}$ باشد $\kappa=\kappa+1$ برو به گام ۱. در غیر اینصورت برو به گام ۷.

گام ۷: پایان .

٤- پردازش مجموعه داده استاندارد DARPA

مجموعه داده‌های ارزیابی DARPA توسط آزمایشگاه‌های MIT Lincoln تهیه شده است. هر ارتباط ثبت شده به صورت نرمال یا حمله با ذکر نوع دقیق حمله مشخص شده است. هر ارتباط ثبت شده از ۱۰۰ بایت تشکیل شده است. داده‌های تست ثبت شده در بازهٔ دو هفته جمع آوری شده اند و حدود دو میلیون داده است. داده‌های KDD 99 که جهت آموزش بکار می‌رود، به صورت تقریبی از ۴,۹۰۰,۰۰۰ بردار داده تشکیل شده است. هر یک از بردارها از ۴۱ پارامتر شامل فاصله، نوع پروتکل، سرویس، پرچم[۱]، بایت‌های ورودی و... تشکیل شده است که بر حسب نرمال یا حمله برچسب زده شده اند. از آنجا که این پارامترها برخی پیوسته و برخی ماهیت گسسته دارند، شبکه‌پتری ترکیبی قادر است خصوصیات شبکه را مدل نماید. اطلاعات جامع در خصوص این مجموعه داده در [۴۴] موجود است. حملات به ۴ دسته تقسیم بندی می‌شوند:

- Denial of service (DOS): وقتی مهاجم تلاش می کند کاربر معتبر را از استفاده از سرویس منع کند.
- Remote to Local (R2l): مهاجم نام کاربری بر روی سیستم قربانی ندارد، ولی تلاش می کند به آن دسترسی پیدا کند.
- User to Root (U2R): مهاجم دسترسی محلی به سیستم قربانی دارد و سعی می‌نماید امتیازات فوق العاده ای برای خود ایجاد نماید.
- Probe: مهاجم تلاش می کند از میزبان هدف اطلاعات حیاتی بدست آورد.

در همهٔ مقالات این حوزه در بخش آموزش "10% KDD" مورد استفاده قرار گرفته است. تعداد نمونه‌های هر حمله در جدول ۱ نمایش داده شده است.

جدول ۱ : مجموعه داده تشخیص نفوذ 10% KDD 99 [۴۴]

دسته بندی	تعداد نمونه‌ها	حمله	تعداد نمونه‌ها
DOS	391458	smurf	280790
		neptune	107201
		back	2203
		teardrop	979
		pod	264
		land	21
R2l	1126	warezclient	1020
		guess_passwd	53
		warezmaster	20
		imap	12
		ftp_write	8
		multihop	7
		Phf	4
		Spy	2
U2R	52	buffer_overflow	30
		rootkit	10
		loadmodule	9
		perl	3
Probe	4107	satan	1589
		ipsweep	1247
		portsweep	1040
		nmap	231
Normal	97277		

بر اساس [۴۵] در مجموعه دادهٔ KDD 99 داده‌های تکراری بسیاری ثبت شده است که بکارگیری این داده‌ها در بحث آموزش تنها باعث اتلاف زمان می گردد. از آنجا که بحث زمان در تشخیص حملات سایبری حیاتی است، داده‌های مجزا و متفاوت از این پایگاه داده استخراج شده است. تعداد داده‌های مجزا در هر طبقه بندی در جدول ۲ نمایش داده شده است.

[۱] Flag

جدول ۲: نمایش تعداد داده‌های مجزا در مجموعه KDD 99

دسته بندی	Normal	Probe	U2R	R2l	DOS
داده‌های مجزای آموزش	2996	11656	52	995	45927
داده‌های مجزای تست	9711	1106	37	2199	5741

جهت استخراج داده‌های مستقل در بحث آموزش، الگوریتم سریع تطبیقی آنالیز مولفه‌های مستقل[۱] (FastAdaptiveOgICA) در این مقاله بکار گرفته شده است. این الگوریتم سیگنال چند متغیره را به سیگنال‌های مستقل غیرگوسینی[۲] تبدیل می‌نماید[۳۲]. پایگاه دادهٔ تشخیص نفوذ KDD 99 توزیع غیرگوسینی دارد. از این رو الگوریتم‌های ICA می‌توانند در استخراج مولفه‌های اصلی مؤثر واقع شوند. کاهش ابعاد داده قادر است پیچیدگی این مسئله را کاهش دهد و نقش مهمی در افزایش کارایی به خصوص در تشخیص نفوذ زمان حقیقی ایفا می‌نماید.

الگوریتم FastAdaptiveOgICA نه تنها سریع، تطبقی و تکرار شونده با الگوریتم شبکه عصبی است، بلکه با سرعت همگرایی و کارایی بالا سیگنال‌های گوسین را تفکیک می‌نماید. جزئیات فرمول بندی این الگوریتم به تفصیل در [۴۶] شرح داده شده است. جدول۳ تعداد داده‌های آموزش پس از استخراج مولفه‌های اصلی را نمایش می‌دهد.

جدول ۳: نمایش تعداد داده‌های مجموعه KDD 99 پس از استخراج مولفه‌های اصلی

	Normal	Probe	U2R	R2l	DOS
ابعاد قبل از اعمال ICA	2996	11656	52	995	45927
ابعاد کاهش یافته	138	132	30	86	138

۵- ارزیابی روش پیشنهادی و نتایج شبیه سازی

جهت ارزیابی عملکرد، روش شبکه‌پتری ترکیبی مرتبه اول فازی عصبی که در بخش۳ به تفصیل ارائه گردید، به پایگاه داده (پس از استخراج مولفه‌های اصلی که در بخش ۴ شرح داده شد) اعمال گردیده و نتایج شبیه سازی توانایی روش پیشنهادی در تشخیص انواع حملات نفوذ را تایید می‌نماید. ۴۱ پارامتر تعریف شده در پایگاه داده که پیش از این به آن اشاره گردید، معیار تشخیص حالت نرمال یا حمله قرار خواهند گرفت. جزییات و تعریف دقیق این پارامترها در [۴۴] شرح داده شده است. این پارامترها به عنوان شرایط اولیه به شبکه پیشنهادی اعمال گردیده و نشانه‌گذاری نهایی شبکه بیانگرعملکرد در حالت نرمال یا تشخیص هر یک از حملات نفوذ است.

معیارهای نرخ تشخیص (DR[۳]) و نرخ مثبت نادرست (FPR[۴]) ملاک ارزیابی عملکرد سیستم‌های تشخیص نفوذ است [۴۸،۴۷]. جهت محاسبه معیار نرخ تشخیص در ساختار شبکه پیشنهادی داریم:

$$P_{i,j}^{DR} = \frac{M_{i,j}^{ID}}{N_j} \qquad (۲۱)$$

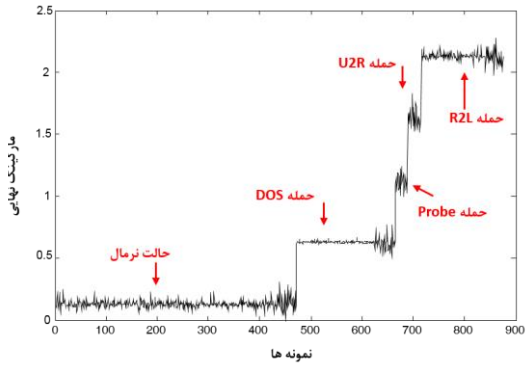
$$P_{i,j}^{FPR} = \frac{F_{i,j}^{alarm} - M_{i,j}^{ID}}{F_{i,j}^{alarm}}$$

$$P_{i,j}^{ND} = 1 - P_{i,j}^{DR}$$

$P_{i,j}^{DR}$ احتمال تشخیص صحیح حمله از نوع j توسط سیستم تشخیص نفوذ i ام است. $M_{i,j}^{ID}$ تعداد حملات صحیح تشخیص داده شده از نوع j توسط سیستم تشخیص نفوذ i ام می‌باشد. N_j تعداد کل حملات از نوع j وارد شده به سیستم تحت مطالعه است.

احتمال تشخیص $P_{i,j}^{FPR}$ ثبت نادرست حمله از نوع j توسط سیستم تشخیص نفوذ i ام است. $F_{i,j}^{alarm}$ تعداد کل هشدارهای حمله از نوع j توسط سیستم تشخیص نفوذ i ام می‌باشد. این مقدار در مدل شبکه‌پتری، متناظر است با نشانه‌گذاری جایگاه خروجی مرتبط با حمله j ام (p_j^{DR}) یا نرخ آتش نمودن گذرهای p_j^{DR} •.

شکل ۵ تشخیص حملات با بکارگیری روش شبکه‌پتری ترکیبی مرتبه اول عصبی را نمایش می‌دهد. استفاده از این سیستم تشخیص نفوذ شبکه‌پتری ترکیبی مرتبه اول عصبی [۴۹] بدون در نظر گرفتن الگوریتم فازی، اگرچه نرخ تشخیص مطلوبی خواهد داشت، اما نرخ مثبت نادرست در این روش تا حدودی نامطلوب است. میزان نرم خطا با بکارگیری این روش ۰٫۴۷ می‌باشد. بالا بودن نرخ مثبت نادرست اثرات مخربی بر سیستم خواهد داشت، زیرا با گزارش حملهٔ نادرست توسط سیستم تشخیص نفوذ، عملکرد سیستم تحت کنترل مختل می گردد.

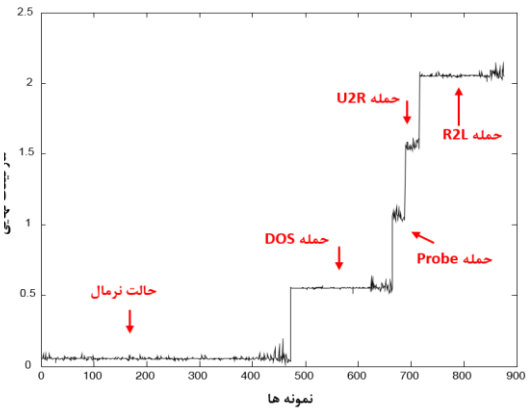


شکل ۵ : نمایش تشخیص حملات با بکارگیری روش شبکه‌پتری ترکیبی مرتبه اول عصبی

شکل ۶ تشخیص حملات با بکارگیری روش شبکه‌پتری ترکیبی مرتبه اول فازی عصبی را نمایش می‌دهد. میزان نرم خطا با استفاده از این روش ۰٫۱۸۳ می‌باشد. با بکارگیری الگوریتم فازی نه تنها نرخ تشخیص حملات

[۱] Fast Adaptive Independent Component Analysis
[۲] non-Gaussian
[۳] Detection Rate
[۴] False Positive Rate

مناسب است، بلکه نرخ مثبت نادرست به میزان قابل قبولی کاهش یافته است. این امر با توجه به خصوصیات نظریه فازی قابل پیش بینی به نظر می رسید.



شکل ۶ : نمایش تشخیص حملات با بکارگیری سیستم تشخیص نفوذ

در جدول ۴ نتایج عملکرد روش پیشنهادی بر اساس دو معیار ذکر شده و همچنین سرعت تشخیص، با برخی روش‌های تشخیص نفوذ مورد مقایسه قرار گرفته است.

مقایسه روش پیشنهادی (جدول۴)، نرخ تشخیص حملات مناسب سیستم تشخیص نفوذ را در مقایسه با روش‌های مشابه نشان می‌دهد. نرخ مثبت نادرست در این روش به میزان قابل قبولی کاهش یافته است. سرعت تشخیص حملات سایبری یکی از مهمترین معیارها در عملکرد سیستم‌های تشخیص نفوذ است. تشخیص حملات در کوتاهترین زمان ممکن، امنیت سیستم را تضمین خواهد نمود. همانگونه که نشان داده شده است، روش تشخیص نفوذ مبتنی بر شبکه‌پتری پیشنهادی، از سریعترین روش مورد مقایسه، ۱۳ برابر در تشخیص حملات سریعتر عمل کرده است. این امر با توجه به سادگی ریاضیات نظریه شبکه‌پتری و توانایی عملکرد موازی و همزمان امری مورد انتظار به نظر می‌رسید. روش شبکه‌پتری ترکیبی فازی عصبی که در این مقاله جهت تشخیص حملات سایبری نفوذ در زیرساخت‌های حیاتی پیشنهاد گردید، قادر است همزمان دینامیک‌های پیوسته و رخداد گسسته و ارتباطات آن‌ها را مدل نماید. این خصوصیت در کنار سرعت عملکرد مناسب، برتری روش پیشنهادی در قیاس با روش‌های مرسوم است. در صورت مدلسازی ترکیبی زیرساخت‌های حیاتی در کنار الگوریتم‌های تشخیص خطای ترکیبی است که مدلی جامع خواهیم داشت که در برگیرندهٔ تمامی خصوصیات این ابرسیستم‌ها خواهد بود.

٦-اثبات پایداری مدل پیشنهادی

اثبات پایداری و کراندار بودن شبکه‌پتری ترکیبی همچنان به عنوان یک چالش پیش روی محققان است. در این مقاله با استفاده از هم ارزی شبکه‌پتری ترکیبی تک نرخی (single-rate) با ترکیبی اتوماتا (skewed clocks hybrid automata)، مدل پیشنهادی ترکیبی شبکه‌پتری مرتبهٔ اول با یک مدل شبکه‌پتری گسسته هم ارز گردیده است. سپس با بکارگیری قضایای اثبات کراندار شبکه‌پتری گسسته، کراندار مدل پیشنهادی نشان شده است [۵۴].

جدول ۴ : مقایسه نتایج عملکرد روش پیشنهادی

	Normal		DOS		Probe		U2R		R2L		زمان اجرا (s)
	DR	FPR	DR	FPR	DR	FPR	DR	FPR	DR	FPR	
Fuzzy neural FOHPN	98.1	0.4	100	0.3	99.6	0.35	99.0	0.2	96.2	0.15	0.1237
back propagation neural FOHPN Feedforward [49]	98.2	2.9	100	1.6	99.5	1.2	99.0	0.6	96.2	0.4	0.1228
BPNN [50]	79.8	-	97.5	-	99.1	-	34.5	-	98.9	-	2.50
RBF [51]	-	-	98.8	1.6	98.0	1.6	-	-	97.2	1.6	1.60
HPCANN [52]	-	-	100	0.7	100	0.5	-	-	97.2	0.6	-
MLP [53]	-	-	99.9	-	99.8	-	99.9	-	40	-	3.0

تعریف۱ [۵۴] : شبکه‌پتری ترکیبی تک نرخی، شبکه‌پتری ترکیبی مرتبه اول است به گونه ای که داشته باشیم:

(۲۲)

$$T_c = \{t_c\},$$
$$^\bullet t_c = \phi,$$
$$C(t_c) = (v, v'),\ v \in \mathbb{N}^+,$$
$$\forall i \mid p_i \in P_c : Post(p_i, t_c) = w_i \in \mathbb{N}^+$$

بدون از دست دادن کلیت فرض شده است $\{w_i\}$ها یک مجموعه اول هستند و w_i ها هیچ فاکتور مشترکی ندارند.

ساختار یک شبکه‌پتری ترکیبی مرتبه اول به گونه ای است که در هر گام مجموعه IFSهای مجاز $S(N,m)=\{v\}$ یک مجموعه یکتا است. این مجموعه صرف نظر از نشانه‌گذاری همواره یکسان می‌باشد.

با در نظر گرفتن $C(t_c)=(v',v)$ نتایج ذکر شده در حوزه خصوصیات HPN همواره برقرار است. در این حالت $S(N,m)$ یک

سگمنت است و نشانه‌گذاری همهٔ جایگاه‌های پیوسته ممکن است با نرخ‌های متفاوت افزایش یابد، اما نرخ‌های مرتبط با جایگاه‌های متفاوت، همواره یکسانند. از آنجایی که شبکه‌پتری ترکیبی تک نرخی با ترکیبی اتوماتا (skewed clocks hybrid automata) هم ارز است، خصوصیات شبکه‌پتری ترکیبی مرتبه اول قابل تصمیم‌گیری خواهد بود. با در نظر گرفتن این هم ارزی و دنبال نمودن نظریه‌ها و قضایای مربوطه، مدل شبکه‌پتری گسسته معادل با مدل ترکیبی شبکه‌پتری مرتبهٔ اول پیشنهادی بدست آمده، از این رو پایداری و کراندار بودن مدل پیشنهادی در این مقاله قابل ارزیابی خواهد بود.

قضیه ۱ [۵۴] : یک شبکه‌پتری ترکیبی مرتبه اول به صورت $N=(P,T,Pre,Post,C)$ را در نظر بگیرید، شبکه‌پتری گسسته هم ارز با N را می‌توان بدین صورت می‌توان تعریف نمود. شبکه $\lfloor N \rfloor = (P',T',Pre',Post')$ P/T به گونه ای است که:

$P'=P$ همهٔ جایگاه‌های N را شامل می‌شود، با این تفاوت که همه گسسته هستند.

$T'=T$ همهٔ گذرهای N را شامل می‌شود، با این تفاوت که همه گسسته هستند.

$$Pre'(p,t)=\lfloor Pre(p,t) \rfloor,$$
$$Post'(p,t)=\lfloor Post(p,t) \rfloor$$

[•] نماد بخش صحیح است. جزییات و اثبات این قضیه در [۵۰] شرح داده شده است.

بر اساس قضیه ۱، شبکه‌پتری گسستهٔ هم ارز با مدل شبکه‌پتری مرتبه اول پیشنهادی دارای ماتریس تلاقی زیر می‌باشد.

$$A_{51\times 41}=\begin{bmatrix} -1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & 0 & \ddots & 0 & \vdots & \vdots & \vdots \\ 0 & \ddots & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & -1 & 0 & 0 \\ 1 & 1 & \cdots & 1 & 1 & 1 & -1 \\ 1 & 1 & \cdots & 1 & 1 & 1 & -1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & 1 & 1 & 1 & -1 \\ 1 & 1 & \cdots & 1 & 1 & 1 & -1 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ 39 \\ \\ \\ \\ 11 \\ \\ \end{matrix}$$

استنباط ۱: مدل شبکه‌پتری مرتبه اول پیشنهادی جهت تشخیص نفوذ، کراندار ساختاری[۱] است.

قضیه ۲ [۵۵]: فرض کنید $A(n\times m)$ ماتریس تلاقی یک شبکه‌پتری گسسته باشد. این شبکه‌پتری کراندار ساختاری است اگر وتنها اگر بردار $x(n\times 1)$ از مقادیر مثبت صحیح وجود داشته باشد به گونه ای که داشته باشیم $x^T A \le 0$.

با در نظر گرفتن ماتریس تلاقی مدل شبکه‌پتری مرتبه اول پیشنهادی، بردار $x(n\times 1)$ برابر است با

$$x=\left[\underbrace{1 \ \cdots \ 1}_{39} \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0\right]$$
$$x^T A=\left[\underbrace{-1 \ \cdots \ -1}_{39} \ 0 \ 0\right]$$

با استناد به قضیه ۲ مدل شبکه‌پتری مرتبه اول پیشنهادی جهت تشخیص نفوذ، کراندار ساختاری است. در صورتی که یک شبکه‌پتری کراندار ساختاری باشد، بدین معنی است که به ازای هر نشانه‌گذاری اولیه، کراندار خواهد بود. از این رو می‌توان نتیجه گرفت که مدل پیشنهادی به ازای هر شرایطی موجود در شبکه ارتباطی و هر مقداری در پارامترهای ورودی تعریف شده، کراندار و پایدار خواهد بود.

۸- نتیجه‌گیری

زیرساخت‌های حیاتی در هر کشور از جمله آسیب‌پذیرترین سیستم‌ها در برابر حملات سایبری بوده و بیشترین حملات به شبکه‌های ارتباطی در زیرساخت‌های حیاتی، با هدف مختل نمودن عملکرد این سیستم‌ها طراحی می‌گردند. تشخیص حملات سایبری با دقت بالا و در کوتاهترین زمان، از مهمترین اهداف طراحی سیستم‌های کنترل می‌باشد. در این مقاله کنترلر شبکه‌پتری ترکیبی مرتبه اول فازی عصبی جهت تشخیص حملات نفوذ پیشنهاد گردید. ارزیابی عملکرد، نه تنها نرخ تشخیص مناسب این روش را تایید می‌نماید، بلکه نشان می‌دهد که نرخ مثبت نادرست و زمان تشخیص حملات نفوذ در این روش به میزان چشمگیری کاهش یافته است. همچنین، اثبات پایداری مدل پیشنهادی بدون در نظرگرفتن شرایط موجود در شبکه ارتباطی و پارامترهای ورودی ارائه گردید.

مراجع

[1] M. Govindarasu, A. Hahn, P. Sauer, Cyber-Physical Systems Security for Smart Grid, Future Grid Initiative White Paper, PSERC Publication, May 2012.

[2] Depren, Ozgur, et al. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." Expert systems with Applications 29.4, pp. 713-722, 2005.

[3] J.P. Anderson, Computer security threat monitoring and surveillance, Technical Report, James P. Anderson Co., Fort Washington, PA, 1980.

[4] Liao, Hung-Jen, et al, Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications, 36.1, pp. 16-24, 2013.

[۱] Structurally bounded

[5] Modi, Chirag, et al, A survey of intrusion detection techniques in cloud, Journal of Network and Computer Applications, 36.1, pp. 42-57, 2013.

[6] Dagar, Vishwajeet, Vatsal Prakash, and Tarunpreet Bhatia. "Analysis of pattern matching algorithms in network intrusion detection systems." Advances in Computing, Communication, & Automation (ICACCA)(Fall), International Conference on. IEEE, 2016.

[7] S. Antonatos, K.G. Anagnostakis, and E.P. Markatos, Generating realistic workloads for network intrusion detection systems, ACM SIGSOFT Software Engineering Notes 29, no. 1, 207215, 2004.

[8] Gharaee, Hossein, Shokoufeh Seifi, and Nima Monsefan. "A survey of pattern matching algorithm in intrusion detection system." Telecommunications (IST), 2014 7th International Symposium on. IEEE, 2014.

[9] Sahasrabuddhe, Atmaja, et al. "Survey on Intrusion Detection System using Data Mining Techniques.", 2017.

[10] Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications Surveys & Tutorials 18.2, pp. 1153-1176, 2016.

[11] Denatious, D. K., John, A., Survey on data mining techniques to enhance intrusion detection, In Computer Communication and Informatics (ICCCI), International Conference IEEE, pp.1-5, 2012.

[12] Kshirsagar, Vivek K., Sonali M. Tidke, and Swati Vishnu, Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview, International Journal of Computer Science and Informatics ISSN (PRINT), pp. 2231-5292, 2012.

[13] Goyal, Mayank Kumar, and Alok Aggarwal, composing signatures for misuse intrusion detection system using genetic algorithm in an offline environment, Advances in Computing and Information Technology, Springer Berlin Heidelberg, pp. 151-157, 2012.

[14] Desai, Anuja S., and D. P. Gaikwad. "Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA." Advances in Electronics, Communication and Computer Technology (ICAECCT), IEEE International Conference on, 2016.

[15] S. Kumar, Classification and detection of computer intrusions, Ph.D. thesis, Purdue University, 1995.

[16] Dolgikh, A., Nykodym, T., Skormin, V., Antonakos, J., Baimukhamedov, M., Colored Petri nets as the enabling technology in intrusion detection systems, In MILITARY COMMUNICATIONS CONFERENCE IEEE, pp. 1297-1301, 2011.

[17] Helmer, Guy, et al, Software fault tree and coloured Petri netbased specification, design and implementation of agent-based intrusion detection systems, International Journal of Information and Computer Security, 1.1, pp. 109-142, 2007.

[18] Horng, Shi-Jinn, et al, A novel intrusion detection system based on hierarchical clustering and support vector machines, Expert systems with Applications, 38.1, pp. 306-313, 2011.

[19] Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. "A survey of network anomaly detection techniques." Journal of Network and Computer Applications 60, pp. 19-31, 2016.

[20] XU, Yan-qun, Bin ZHANG, and Xiao-tie QIN, Clustering intrusion detection model based on grey fuzzy K-mean clustering, Journal of Chongqing Normal University (Natural Science), 1, 019, 2013.

[21] Pandeeswari, N., and Ganesh Kumar. "Anomaly detection system in cloud environment using fuzzy clustering based ANN." Mobile Networks and Applications 21.3, pp. 494-505, 2016.

[22] Goh, Jonathan, et al. "Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks." High Assurance Systems Engineering (HASE), IEEE 18th International Symposium on., 2017.

[23] C. Bitter, J. North, D. A. Elizondo, T. Watson, An Introduction to the Use of Neural Networks for Network Intrusion Detection, Computational Intelligence for Privacy and Security, Springer-Verlag Berlin Heidelberg, SCI 394, 524, 2012.

[24] Roy, Sanjiban Sekhar, et al. "A Deep Learning Based Artificial Neural Network Approach for Intrusion Detection." International Conference on Mathematics and Computing. Springer, Singapore, 2017.

[25] Ashfaq, Rana Aamir Raza, et al. "Fuzziness based semi-supervised learning approach for feed-forward neural network. In Computer intrusion detection system." Information Sciences 378, pp. 484-497, 2017.

[26] Li, Wei, Using genetic algorithm for network intrusion detection, Proceedings of the United States Department of Energy Cyber Security Group, pp. 1-8, 2004.

[27] Srinivasu, P., and P. S. Avadhani, Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in Intrusion Detection, Procedia Engineering, 38, pp. 144-153, 2012.

[28] Lu, Wei, and Ali A. Ghorbani, Network anomaly detection based on wavelet analysis, EURASIP Journal on Advances in Signal Processing, 4, 2009.

[29] Aburomman, Abdulla Amin, and Mamun Bin Ibne Reaz. "A novel SVM-kNN-PSO ensemble method for intrusion detection system." Applied Soft Computing 38, pp. 360-372, 2016.

[30] Ambusaidi, Mohammed A., et al. "Building an intrusion detection system using a filter-based feature selection algorithm." IEEE transactions on computers 65.10, pp. 2986-2998, 2016.

[31] G. Helmer, J. Wong, M. Slagell,V. Honavar, L. Miller, Y. Wang,X. Wang and N. Stakhanova, Software fault tree and coloured Petri net–based specification, design and implementation of agent-based intrusion detection systems, Int. J. Information and Computer Security, Vol. 1, No. 1/2, 2007.

[32] C. Wooi Ten, C. Ching Liu, and M. Govindarasu, Vulnerability Assessment of Cybersecurity for SCADA Systems, IEEE TRANSACTIONS ON POWER SYSTEMS, 2008.

[33] T. M. Chen, J. Carlos Sanchez-Aarnoutse, and J. Buford, Petri Net Modeling of Cyber-Physical Attacks on Smart Grid, IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, 2011.

[34] Heracleous, Constantinos, et al. "Hybrid systems modeling for critical infrastructures interdependency analysis." Reliability Engineering & System Safety 165, pp. 89-101, 2017.

[35] Ghazi, Z., and A. Doustmohammadi. "Fault detection and power distribution optimization of smart grids based on hybrid Petri net." Energy Systems 8.3, pp. 465-493, 2017.

[36] Petri, C.A., Kommunikation mit Automaten. Bonn: Institut für Instrumentelle Mathematik, Schriften des IIMNr. 2, 1962.

[37] David, R. and Alla, H.,, Continuous Petri nets. 8th European Workshop on Application and Theory of Petri Nets Zaragoza, 1987.

[38] Le Bail, J., Alla, H., and David, R. Hybrid Petri nets. European Control Conference Grenoble, pp. 1472–1477, 1991.

[39] G.W. Brams, Réseaux de Petri, Vol I et II, Masson, Paris, 1983.

[40] P. J. Hawrylak, M. Haney, M. Papa, and J. Hale, Using Hybrid Attack Graphs to Model Cyber-Physical Attacks in the Smart Grid, IEEE 2012.

[41] T. Murata, Petri nets: properties, analysis and applications, Proceedings IEEE, vol.77, no. 4, pp 541-580, 1989.

[42] F. Balduzzi, A. Giua, and G. Menga, First-Order Hybrid Petri Nets: A Model for Optimization and Control, IEEE TRANSACTIONS ON ROBOTICS AND AUTOMATION, 16.4, pp. 382-399, 2000.

[43] Wai, Rong-Jong, and Chia-Ming Liu., Design of dynamic petri recurrent fuzzy neural network and its application to path-tracking control of nonholonomic mobile robot, IEEE transactions on Industrial Electronics 56, no.7, pp. 2667-2683, 2009.

[44] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[45] Tavallaee, Mahbod, et al, A detailed analysis of the KDD CUP 99 data set, Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications, 2009.

[46] Ye, Yalan, et al, A fast and adaptive ICA algorithm with its application to fetal electrocardiogram extraction, Applied Mathematics and Computation, 205.2, pp. 799-806, 2008.

[47] Mitchell, Robert, and Ing-Ray Chen. "A survey of intrusion detection techniques for cyber-physical systems." ACM Computing Surveys (CSUR) 46.4: 55, 2014.

[48] Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications Surveys & Tutorials 18.2, pp. 1153-1176, 2016.

[49] Z. Ghazi, A. Doustmohammadi, Intrusion detection in cyber-physical systems based on Petri net, accepted in journal of information technology and control.

[50] Haddadi, F., Khanchi, S., Shetabi, M., & Derhami, V. (2010, April). Intrusion detection and attack classification using and Network Technology (ICCNT), pp. 262-266, IEEE 2010.

[51] Z. Chunlin, J. Ju, K. Mohamed, Intrusion detection using hierarchical neural networks, Pattern Recognition Lett. 26 (6), pp. 779–791, 2005.

[52] Liu, Guisong, Zhang Yi, and Shangming Yang. "A hierarchical intrusion detection model based on the PCA neural networks." Neurocomputing 70.7, pp. 1561-1568, 2007.

[53] Jawhar, Muna Mhammad T., and Monica Mehrotra. "Design network intrusion detection system using hybrid fuzzy-neural network." International Journal of Computer Science and Security 4.3, pp. 285-294, 2010.

[54] Balduzzi, Fabio, et al. "Decidability results in First–Order Hybrid Petri Nets." Discrete Event Dynamic Systems 11.1-2, pp. 41-57, 2001.

[55] Alan A. Desrochers and Robert Y. AI-Jaar, Applications of Petri Nets in Manufacturing Systems; Modeling, Control, and Performance Analysis IEEE Press, ISBN 0-87942-295-5, 1995.