تحلیل ایرادهای ارزیابی با کمک CPN برای سیستم‌های خرید آنلاین

رقیه حاجیان آرانی[۱]، محمدعلی سعادت‌جو[۲*]
۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر – گرایش نرم‌افزار، دانشگاه علم و هنر یزد، ایران
۲- استادیار گروه کامپیوتر، دانشگاه علم و هنر یزد، ایران
*نویسنده مسئول: **r.hajian.a@gmail.com**

خلاصه

امروزه سیستم‌های خرید آنلاین، کاربرد زیادی در سراسر جهان داشته و سبب رونق چشمگیر کسب‌وکارهای مختلف شده‌اند. بااین‌حال، طراحی این سیستم‌ها به دلیل پیچیدگی زیاد آن‌ها، با دشواری‌های زیادی همراه است. پیچیدگی در پیوند داده‌ها و رفتار این نوع سیستم‌ها، سبب ایرادهایی در ارزیابی شده و مشکلاتی را ایجاد کرده است. در این مقاله برای حل این مشکل و به‌منظور تحلیل ایرادهای ارزیابی، از روش‌های رسمی مبتنی بر CPN (شبکه‌های پتری رنگی) استفاده می‌شود. راهکار پیشنهادی، مبتنی بر زبان مدل‌سازی CPN است که از مشخصه‌های تراکنش سیستم‌های خرید آنلاین استفاده می‌کند. همچنین برای درک بهتر، یک نمونه کاربردی تشریح می‌شود.

کلمات کلیدی: خرید آنلاین، شبکه پتری، ارزیابی، مدل رسمی.

۱. مقدمه

سیستم‌های خرید آنلاین حاوی برنامه‌های توزیع‌شده‌ای هستند که پیچیدگی و نقاط ضعف زیادی را دربرمی گیرند. در مرحله ادغام بخش‌های مختلف این برنامه‌ها، چالش‌های امنیتی زیادی ایجاد می‌شود [Wen, ۲۰۱۷; Chen, ۲۰۱۵; Wang, ۲۰۱۸]. به‌عنوان‌مثال، ممکن است یک کاربر مجاز، با استفاده از برخی رفتارهای خاص، نقص‌های ارزیابی را کشف کرده و از آن برای کسب منافع غیرقانونی استفاده کند [Wang, ۲۰۱۱; Sun, ۲۰۱٤; Jiang, ۲۰۱۸]. این مشکل در سطح برنامه قرار دارد و در این مقاله برای حل آن، از روش‌های رسمی مبتنی بر CPN استفاده می‌شود.

روش‌های رسمی شامل مجموعه‌ای از فعالیت‌ها هستند که تلاش می‌کنند پروژه نرم‌افزاری را در قالب روابط رسمی و ریاضی، تعریف، توسعه، پیاده‌سازی و ارزیابی کنند. در این نوع مدل‌ها با استفاده از تحلیل ریاضی، بسیاری از ابهامات، نواقص و عدم سازگاری نرم‌افزار مشخص‌شده و تصحیح می‌گردد.

شبکه‌های پتری در سال ۱۹۶۲ توسط دکتر کارل آدام پتری معرفی شدند. این شبکه‌ها، ابزار قدرتمندی برای مدل‌سازی هم‌روندی هستند و قدرت توصیف بالایی دارند. امروزه امکانات زیادی به مدل اولیه شبکه پتری اضافه شده است تا قدرت مدل‌سازی آن افزایش‌یافته و در زمینه‌های مختلفی کاربرد داشته باشد. این شبکه‌ها ارائه‌دهنده چارچوبی برای تحلیل، اعتبارسنجی و ارزیابی کارایی هستند و ابزاری مناسب برای مدل‌سازی ریاضی و گرافیکی به شمار می‌روند. از این ابزار برای مدل‌سازی، توصیف و تحلیل سیستم‌هایی که دارای ماهیتی هم‌زمان، آسنکرون، توزیع‌شده، موازی، نامعین و یا اتفاقی هستند، استفاده می‌شود. در واقع شبکه‌های پتری جزو مدل‌هایی هستند که می‌توانند به‌صورت هم‌زمان، حالت و

عملکرد یک سیستم را نشان دهند. یکی دیگر از ویژگی‌های مهم شبکه‌های پتری، قابل‌اجرا بودن آن‌ها است که از این ویژگی می‌توان برای ارزیابی رفتار و کارایی یک سیستم استفاده کرد.

شبکه‌های پتری به‌صورت گرافیکی نمایش داده می‌شوند و معنای تعریف‌شده و ساختار خوش‌تعریفی دارند؛ بنابراین می‌توانند به‌طور غیرمبهم، رفتار یک سیستم با رویدادهای گسسته را نمایش دهند. این شبکه‌ها دارای عناصر کم ولی کارآمد هستند و در برابر تغییرات کوچک سیستم مقاومند. شبکه‌های پتری قدمت زیادی دارند و الگوریتم‌های زیادی برای تحلیل این شبکه‌ها وجود دارد. نرم‌افزارهای متعددی برای شبیه‌سازی شبکه‌های پتری وجود دارد که امکان رسم شبکه، شبیه‌سازی عملکرد شبکه و تحلیل آن را به‌سادگی فراهم می‌کنند [Jensen, ۱۹۹۷].

کاربرد عملی شبکه‌های پتری، طراحی و تحلیل سیستم‌هایی است که به روش‌های مختلف، قابلیت طراحی و ساخت دارند. بعد از مدل کردن سیستم با شبکه پتری، لازم است که مدل پتری تحلیل شود. هر شبکه پتری از چهارعنصر پایه تشکیل شده است: مکان، گذار، کمان و نشانه. مکان‌ها، بیانگر وضعیت‌های ممکن سیستم هستند. هر مکان می‌تواند شامل تعدادی نشانه باشد. نشانه‌ها بیان می‌کنند که سیستم یا بخشی از آن، در زمان جاری در چه وضعیتی ممکن است قرار داشته باشند. گذارها، فعالیت‌های سیستم را نشان می‌دهند. یک گذار، زمانی توانا می‌شود که تمام مکان‌های ورودی آن نشانه داشته باشند. کمان‌های جهت‌دار، مکان‌ها را به گذارها و برعکس وصل می‌کنند. بین دو مکان یا دو گذار نمی‌توان کمان داشت.

تفاوت اصلی شبکه‌های پتری رنگی و شبکه‌های پتری در نوع نشانه‌های آن‌ها است. شبکه‌های پتری رنگی از نشانه‌های رنگی پشتیبانی می‌کنند. رنگ‌ها معادل انواع داده در زبان‌های برنامه‌نویسی هستند و نشانه‌های رنگی نمایانگر مقادیر مجاز از هر نوع داده یا به عبارتی، نمونه‌ای از یک نوع داده می‌باشند. برای آشنایی بهتر با شبکه‌های پتری رنگی، بهتر است اصلاحات زیر را بیان کنیم:

- برچسب نوع: هر مکان دارای یک برچسب نوع است که نوع داده‌های ممکن در آن مکان را مشخص می‌کند.
- نشانه‌گذاری: حالت یک شبکه پتری رنگی، که شامل تعداد و مکان نشانه‌ها در یک مقطع زمانی معین است، نشانه‌گذاری نامیده می‌شود.
- مجموعه چندتایی: یک مجموعه از نشانه‌ها است که برخلاف مجموعه‌های معمولی، چنانچه یک عضو تکراری وارد آن شود، تعداد عضوهای آن افزایش می‌یابد.
- عبارت‌های کمان: تعداد دقیق نشانه‌ها و مقادیر داده‌ای آن‌ها توسط عبارت‌های کمان مشخص می‌شود.
- چسباندن: در هنگام وقوع یک گذار، مقادیر مجاز نشانه‌ها باید با توجه به نوع و تعداد مشخص‌شده روی کمان‌ها انتخاب شوند. این عمل چسباندن نام دارد.
- محافظ: یک عبارت بولی است که به یک گذار منسوب می‌شود و امکان شلیک کردن آن را محدود به‌شرط می‌کند.

برای ایجاد، شبیه‌سازی و تحلیل شبکه‌های پتری رنگی، ابزارهای گوناگونی موجود است. مهم‌ترین و پرکاربردترین این ابزارها، ابزارهای CPN و طرح CPN هستند.

ادامه مقاله به این صورت سازمان‌دهی می‌شود: در بخش دوم، مقالات مرتبط ارائه می‌شود. بخش سوم حاوی یک مثال نمونه است. بخش چهارم، روش‌های مدل‌سازی و تحلیل را بیان می‌کند. در نهایت بخش پنجم، نتیجه‌گیری مقاله را نشان می‌دهد.

۲. مقالات مرتبط

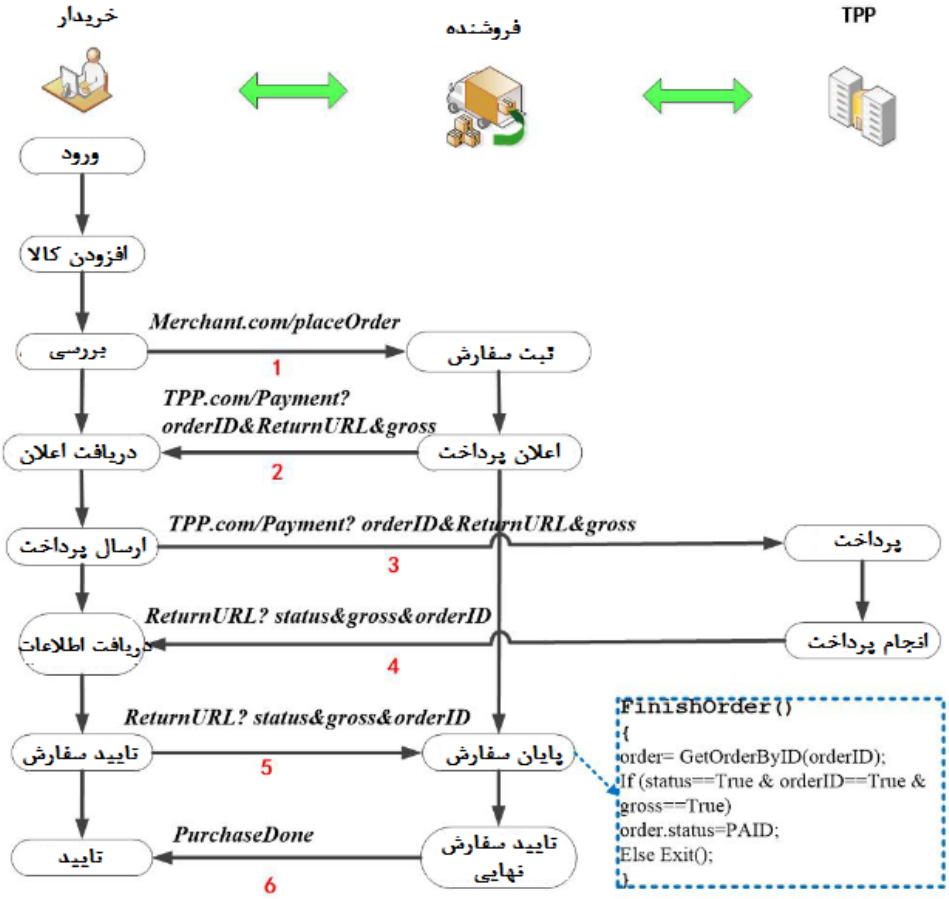
تاکنون برخی از پژوهشگران، تکنیک‌هایی را برای آزمایش برنامه‌های کاربردی وب در سطح برنامه پیشنهاد کرده‌اند [Pellegrino, ۲۰۱٤; Sudhodanan, ۲۰۱٦; Hirschberger, ۲۰۱٦; Matoug, ۲۰۱٤]. فانکی سان و همکارانش یک روش تشخیص ایستا را برای کشف آسیب‌پذیری‌های برنامه‌های تجارت الکترونیک وب پیشنهاد کردند [Sun, ۲۰۱٤]. اریک چن و همکارانش، CST (گواهی‌نامه تراکنش نمادین) را معرفی کردند [Chen, ۲۰۱٤]. از این رویکرد برای ساخت سرویس‌های آنلاین چندجانبه ایمن استفاده می‌شود. لویی ژینک و همکارانش، سیستمی ارائه دادند که حفاظت امنیتی را برای ادغام API وب فراهم می‌کند [Xing, ۲۰۱۳]. در مقالات [Fung, ۲۰۱۲; Fung, ۲۰۱٤] نیز یک روش اسکن برای حل مشکل دست‌کاری پارامترها ارائه شده است. بااین‌حال، راهکارهای ارائه شده معمولاً بر آزمایش یا تشخیص سیستم‌های پیاده‌سازی در سطح کد متمرکز هستند. در واقع نقص‌های طراحی، سبب رخداد مشکلات امنیتی مهمی می‌شوند [McGraw, ۲۰۰۲]. طراحان به‌سختی می‌توانند بررسی‌های کافی را برای ارزیابی سمت سرور برای پارامترهای درخواستی انجام دهند. موفقیت حمله عمدتاً به خطا یا عدم ارزیابی در سمت سرور بستگی دارد.

در اغلب موارد، مدل‌های رسمی در قیاس با روش‌های توسعه نرم‌افزار سنتی (همچون فناوری تست و روش‌های تحلیل UML) قوی‌تر هستند. مدل‌سازی و تحلیل مدل سیستم بر اساس روش‌های رسمی، می‌تواند مبنای کاملی برای فرآیند پیاده‌سازی فراهم کند. همچنین سبب کاهش هزینه پیاده‌سازی و تست‌شده و حجم ایرادات در سیستم نهایی را کم می‌کند.

بنابراین این مقاله بر روش تحلیل برای ارزیابی خطاهای سیستم خرید آنلاین تمرکز دارد و بدین منظور از شبکه‌های پتری رنگی استفاده می‌شود. شبکه‌های پتری رنگی (CPN) یک ابزار رسمی پرقدرت برای مدل‌سازی سیستم‌های همگام و آنالیز ویژگی‌های آن‌ها به شمار می‌روند. این شبکه‌ها از ترکیب شبکه‌های پتری و زبان‌های برنامه‌نویسی تشکیل شده‌اند. شبکه‌های پتری مبنای علائم گرافیکی و اصول اولیه مدل‌سازی هم‌زمانی، توزیع، ارتباط و همگام‌سازی را فراهم می‌کنند. زبان برنامه‌نویسی CPN ML، تعریف اولیه انواع داده را برای تشریح دست‌کاری داده‌ها و طراحی مدل‌های فشرده و قابل پارامترسازی ارائه می‌دهد [Jensen, ۲۰۰۹]. به‌علاوه از ابزار نسبتاً پیشرفته CPN برای ساخت و آنالیز مدل‌های CPN استفاده می‌شود.

۳. مثال نمونه

در این مقاله، یک سیستم خرید آنلاین را که از سناریوهای واقعی استخراج‌شده، ارائه می‌دهیم. این سیستم، انتزاعی است و ما فقط بر مهم‌ترین فرآیند تعامل تجاری تمرکز می‌کنیم که در شکل ۱ نشان داده شده است. در فرآیند بررسی، ابتدا کاربر (خریدار) کالا را انتخاب می‌کند و به فروشنده سفارش می‌دهد. سپس فروشنده پیامی را با آرگومان‌های orderID، gross و returnURL به کاربر ارسال می‌کند و مرورگر خریدار به API پلت فرم پرداخت واسطه (TPP) هدایت می‌شود. بعد از پرداخت توسط کاربر، اطلاعات پرداخت در پایگاه داده TPP ثبت می‌شود. در ادامه، TPP مرورگر کاربر را با استفاده از returnURL به سمت فروشنده هدایت می‌کند. در واقع returnURL برای فراخوانی API «پایان سفارش» مورد استفاده قرار می‌گیرد. تابع «پایان سفارش»، یکپارچگی orderID، gross و returnURL را ارزیابی می‌کند. به‌منظور کارایی و قابلیت استفاده‌ی فرآیند تجاری خرید آنلاین، پیام‌ها در این فرآیند پرداخت امضا نمی‌شوند. این یک ضعف امنیتی نیست، زیرا در اغلب موارد واقعی از مکانیزم تعاملی برای تضمین امنیت استفاده می‌شود [Wang, ۲۰۱۱; Sun, ۲۰۱٤; Pellegrino, ۲۰۱٤].



شکل ۱: یک نمونه از فرآیند خرید آنلاین

فرآیند تسویه‌حساب، ایمن به نظر می‌رسد. بااین‌حال ممکن است یک کاربر مخرب به‌عنوان فروشنده دیگر ثبت‌نام کند و به خودش پول پرداخت کند. سپس سفارشات فروشندگان دیگر را بررسی کند، مثلاً با دست‌کاری پارامترهای مبادله شده بین مشتری و سرور و شناسه‌های مختلف کاربران مخرب، سفارشات را جایگزین کند. بخش «پایان سفارش» بررسی نمی‌کند که پرداخت برای چه کسی صورت گرفته است و بنابراین متقاعد می‌شود که هزینه سفارش پرداخت شده است. در واقع این مشکل ناشی از سردرگمی بین فروشنده و TPP در مورد فعالیت‌های طرف مقابل است. این یک ایراد ارزیابی معمولی در سیستم‌های خرید آنلاین توزیع‌شده است. در واقع طراحی یک مکانیزم اعتبارسنجی امنیتی کامل در فرآیند تعامل، دشوار است. در این مقاله فرض می‌شود که فرآیند کسب‌وکار شکل ۱، مشخصه‌های طراحی را بیان می‌کند و ما از آن به‌عنوان یک مطالعه موردی برای نمایش راهکار پیشنهادی خود در این مقاله استفاده می‌کنیم.

۴. روش‌های مدل‌سازی و تحلیل

۴-۱. مدل‌سازی سیستم خرید آنلاین

از CPNها برای مدل‌سازی و تحلیل رفتارهای انتزاعیِ سیستم‌های توزیع‌شده استفاده می‌شود. هر مدل CPN می‌تواند رویدادها و حالت‌های یک سیستم واقعی را نمایش دهد. CPNها به مفاهیم زیادی اشاره دارند، همچون مجموعه چندتایی، مجموعه رنگ‌ها، چسباندن، علامت‌گذاری و نوشته‌های خطی. در ادامه، ابتدا تعاریف اساسی CPN را بیان می‌کنیم.

تعریف ۱: هر شبکه پتری رنگی، یک CPN نه‌تایی به‌صورت زیر است: $CPN = (P.T.A.\sum.V.C.G.E.I)$ که در آن:

(۱) P یک مجموعه کراندار از مکان‌ها است.

(۲) T یک مجموعه کراندار از گذارهای T است، به‌گونه‌ای که $P \cap T = \emptyset$.

(۳) $A \subseteq P \times T \cup T \times P$ یک مجموعه از کمان‌های جهت‌دار است.

(۴) $\sum$ یک مجموعه کراندار از مجموعه رنگ‌های غیرتهی است.

(۵) V یک مجموعه کراندار از متغیرهای نمونه است، به صورتی که برای تمامی متغیرهای $v \in V$ داریم: $Type[v] \in \sum$.

(۶) $C: P \to \sum$ یک تابع مجموعه رنگ است که یک مجموعه رنگ را به هر مکان تخصیص می‌دهد.

(۷) $G: T \to EXPR_V$ یک تابع محافظ است که به هر گذار t یک محافظ تخصیص می‌دهد، به‌گونه‌ای که $Type[G(t)] = Bool$ است.

(۸) $E: A \to EXPR_V$ یک تابع عبارت کمان است که توصیف هر کمان را به کمان a تخصیص می‌دهد، به‌گونه‌ای که $Type[E(a)] = C(p)_{MS}$ است. در اینجا p مکان متصل به کمان a است.

(۹) $I: P \to EXPR_\emptyset$ یک تابع مقداردهی اولیه است که یک عبارت مقداردهی اولیه را به مکان p تخصیص می‌دهد، به‌گونه‌ای که داریم: $Type[I(p)] = C(p)_{MS}$.

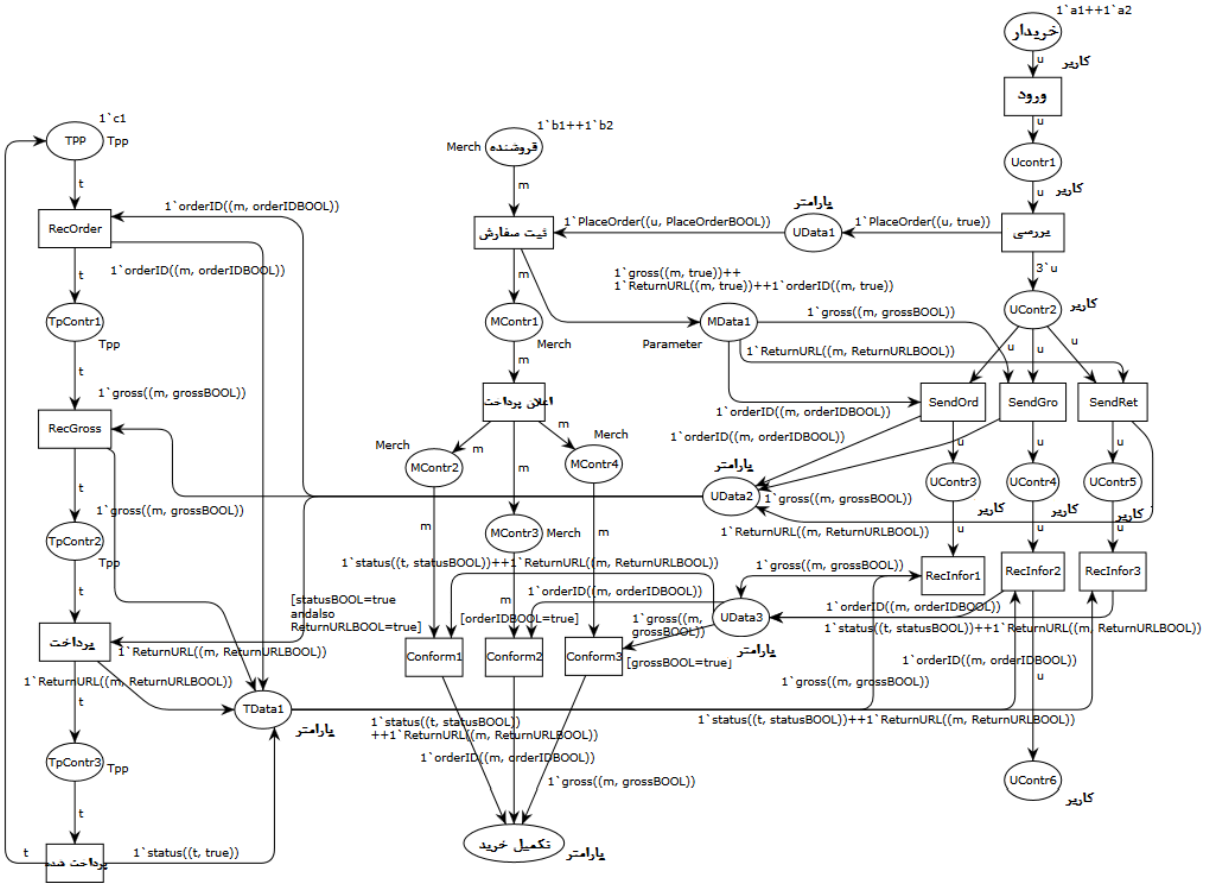
علامت M در CPN، هر مکان $p \in P$ را به چند مجموعه از نشانه‌ها نگاشت می‌کند. علامت اولیه $M.$ به‌صورت $M.(p) = I(p) <>. p \in P$ تعریف شده است. یک چسباندن از گذار t، هر متغیر $v \in Var(t)$ را به یک متغیر $b(v) \in Type[v]$ نگاشت می‌کند.

در این بخش، تعاریف داده را برای فرآیندهای تعامل تجاری در سیستم‌های خرید آنلاین ارائه می‌دهیم، از جمله طرح‌های نام‌گذاری که برای ساخت مدل سیستم خرید آنلاین مورد استفاده قرار می‌گیرند. زبان CPN ML مبتنی بر زبان برنامه‌نویسی تابعی استاندارد ML است (SML). در واقع CPN ML یک مجموعه از پیش تعریف شده از انواع پایه را ارائه می‌دهد که از ML استاندارد به ارث رسیده‌اند و می‌توان از آن‌ها به‌عنوان مجموعه رنگ‌های ساده استفاده کرد. از مجموعه رنگ‌های ساده با استفاده از مجموعه سازنده‌های مجموعه رنگ‌ها، می‌توان برای تعریف مجموعه رنگ‌های ساختاریافته استفاده کرد [Jensen, ۲۰۱۲; Jensen, ۲۰۱۳]. مجموعه رنگ‌ها را می‌توان به‌صورت انواع داده طراحی نمود که متناظر با سیستم‌های خرید آنلاین واقعی هستند و در فرآیند مدل‌سازی از متغیرها و ثابت‌ها استفاده می‌کنند. در ادامه برخی مؤلفه‌های داده را در زبان CPN ML تعریف می‌کنیم.

- *colset UNIT = unit;*
- *colset INT = int;*
- *colset BOOL = bool;*
- *colset STRING = string;*
- *colset User = with a1 | a2;*
- *var u. u1. u2: User;*
- *colset Merch = with b1 | b2;*
- *var m. m1. m2: Merch;*
- *colset Tpp = with c1 | c2;*
- *var t. t1: Tpp;*
- *colset UserPara = product User*BOOL;*
- *colset TPPara = product Tpp*BOOL;*
- *colset MerPara = product Merch*BOOL;*
- *var orderIDBOOL. grossBOOL. PlaceOrderBOOL. ReturnURLBOOL. statusBOOL: BOOL;*
- *colset Parameter = union orderID: MerPara + gross: MerPara + PlaceOrder: UserPara + ReturnURL: Mer- Para+status: TPPara;*

در اینجا User، Merch و Tpp مجموعه‌هایی هستند که طرفین معامله را نمایش می‌دهند و به ترتیب بیانگر کاربر (خریدار)، فروشنده و TPP هستند. مجموعه‌های UserPara، TPPara و MerPara برای نمایش پارامترهای معاملاتی در فرآیند خرید آنلاین مورد استفاده قرار می‌گیرند. این پارامترها بین طرفین معامله، ارسال و مبادله شده و بر اساس نوع محصول و اتحادیه ساخته می‌شوند. پیشوندهای User، Mer و TP به ترتیب بیانگر داده‌های تولیدشده توسط کاربر، فروشنده و TPP هستند. همچنین UserMer بیانگر انواع داده‌ای است که ارتباط نزدیکی با کاربر (خریدار) و فروشنده دارند.

هر سیستم خرید آنلاین در مقابل دست‌کاری پارامترهای وب آسیب‌پذیر است. این نقطه‌ضعف به دلیل دست‌کاری پارامترهای مبادله شده بین سرویس‌گیرنده و سرویس‌دهنده رخ می‌دهد، مثلاً قیمت و تعداد محصولات تغییر می‌کند. به‌ویژه ممکن است کنترل فرم HTML دست‌کاری شود و ارزیابی در سمت سرویس‌گیرنده را دور بزند و ارسال فرم‌ها را ره‌گیری کند (۱۳ و ۲۰). بنابراین ممکن است در حین فرآیند خرید، مقادیر Order ID، gross و ReturnURL دچار اشتباه شوند. بنابراین برای نمایش این وضعیت از نوع BOOL استفاده می‌شود و به هر پارامتر معاملاتی، یک مقدار BOOL تخصیص داده می‌شود. ما برای نام‌گذاری آن‌ها از «نام پارامتر» + BOOL استفاده می‌کنیم. از قرارداد «پیشوند» + "Datak" نیز برای نام‌گذاری مکان کانال استفاده می‌کنیم ($k \in N+$). به‌عنوان‌مثال در شکل ۲، UData۱ به معنای مکان کانالی است که توسط کاربر راه‌اندازی شده است.



شکل ۲: فرآیند تجاری مثال بخش ۳

در سیستم‌های خرید آنلاین، جنبه امنیت از طریق مکانیزم تعاملِ طراحی‌شده، تضمین می‌شود و توابع ارزیابی، گام‌های مهمی به شمار می‌روند. از این توابع برای ارزیابی پارامترهای معاملاتی بین طرفین استفاده می‌شود و قانونی بودن آن‌ها را تضمین می‌کند. ما در این مقاله از محافظ‌ها برای پیاده‌سازی این توابع استفاده می‌کنیم. به‌عنوان‌مثال در شکل ۱ یک تابع ارزیابی مهم تحت عنوان «پایان سفارش» وجود دارد که با استفاده از گذارهای اصلی در شکل ۲ بیان شده است، همچون Confirm۱، Confirm۲ و Confirm۳. در نهایت می‌توانیم تابع ارزیابی اصلی CPN را تحت عنوان «پایان سفارش» به دست آوریم که با استفاده از مدلِ متناظر با سیستم خرید آنلاین شکل ۱ نمایش داده می‌شود (شکل ۲).

۲-۴. تحلیل ایرادهای ارزیابی

در شکل ۲، علامت‌گذاری اولیه به‌صورت زیر است:

$$M_{\cdot}(Tpp) = ۱'c۱.$$
$$M_{\cdot}\left(\text{فروشنده}\right) = ۱'b۱ + +۱'b۲.$$
$$M_{\cdot}(\text{خریدار}) = ۱'a۱ + +۱'a۲$$

یعنی دو کاربر و دو فروشنده آماده در صحنه فعلی حضور دارند و TPP در حال آماده شدن برای دریافت درخواست‌های پرداخت است. براساس مدل CPN که یک سیستم خرید آنلاین را نشان می‌دهد، مسئله مهم در کشف

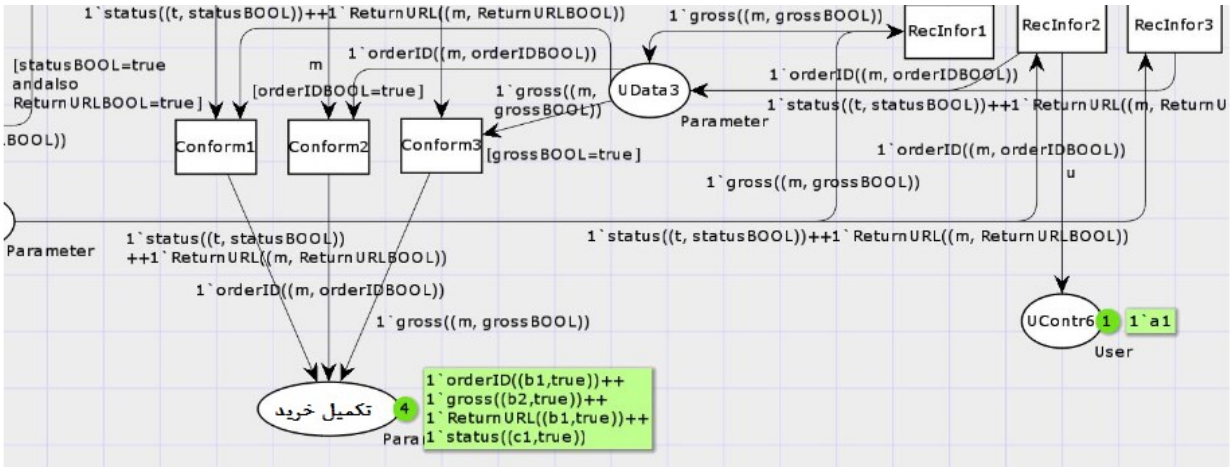
ایرادهای ارزیابی، بررسی تضمین امنیت ویژگی‌های تراکنش است. تجزیه‌ناپذیری، یکی از ویژگی‌های مهم سیستم‌های مدرن تجارت الکترونیک است (۲۱) که معمولاً در سطح شبکه مورد استفاده قرار می‌گیرد. ما در این مقاله، گزاره‌هایی را برای بیان ویژگی‌های امنیتی CPN ارائه می‌دهیم.

گزاره ۱: فرض کنید که $\mathrm{CPN} = (\mathrm{P.T.A.\Sigma.V.C.G.E.I})$ یک مدل CPN است که یک سیستم خرید آنلاین را به نمایش می‌گذارد. در اینجا $P' \in P$ مجموعه مکان‌هایی است که علامت‌گذاری کامل M_0 را نشان می‌دهد. اگر عدد توکن و نوع M(p) تراکنش برابر باشند، M یک علامت دسترس‌پذیر از ورودی اولیه تا مجموع تمام کمان‌های ورودی p است. سپس M را وضعیت تکمیل معامله در نظر می‌گیریم.

وضعیت تکمیل معامله بدین معناست که وضعیت پایان معامله در سیستم خرید آنلاین رخ داده است. سپس می‌توان تمامی وضعیت‌های تکمیل معامله را مورد تحلیل قرار داد تا ایرادهای ارزیابی مشخص شوند. گزاره ۲ را بر اساس گزاره ۱ به‌صورت زیر می‌نویسیم.

گزاره ۲: فرض کنید $\mathrm{CPN} = (\mathrm{P.T.A.\Sigma.V.C.G.E.I})$ یک مدل CPN است که یک سیستم خرید آنلاین را با علامت اولیه M_0 نشان می‌دهد و M_1 نیز وضعیت تکمیل معامله است. اگر برای هر پارامتر ψ در M، $\psi\mathrm{BOOL} = \mathrm{true}$ باشد، و برای هر متغیر μ در M که بیانگر یکی از طرفین معامله است، فقط یک مقدار وجود داشته باشد، در این صورت M را معتبر در نظر می‌گیریم.

گزاره ۲ نشان می‌دهد که هیچ پارامتر نادرست و داده نامعتبری در فرآیند معامله وجود ندارد و تمامی پارامترهای معامله به یک فرآیند تعلق دارند. گزاره ۲ منافع طرفین معامله را در یک وضعیت عادلانه تضمین می‌کند. با آنالیز فناوری‌های CPN، می‌توان ویژگی‌های فوق را با استفاده از ابزارهای CPN تائید نمود. برای فضای حالت محدود، می‌توان تمامی وضعیت‌های معامله کامل را جستجو نموده و مشخص نمود که آیا ایراد ارزیابی وجود دارد یا خیر.



شکل ۳: یک وضعیت تکمیل معامله

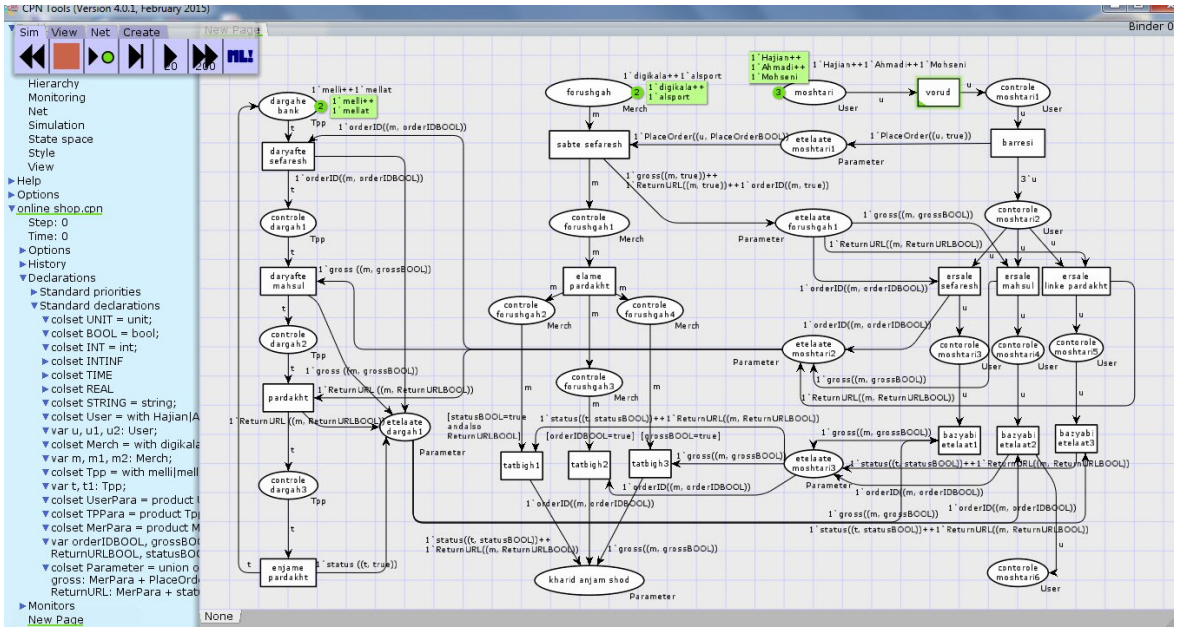
به‌عنوان‌مثال، شکل ۳ یک وضعیت معامله کامل است که توسط CPN برای شکل ۲ تولید شده است و حاوی شرایط گزاره ۲ نیست. بدین معنا که کاربر a_1 سفارشی را برای فروشنده b_1 ارسال کرده است، اما a_1 پرداخت را برای فروشنده b_2 انجام داده و b_2 می‌تواند CPN را در شکل ۲ ثبت کند، درحالی‌که شرایط گزاره ۲ برقرار نیست. این کار توسط a_1 قانونی است. هرچند که هیچ‌یک از پارامترها در این فرآیند معامله اشتباه نیستند، اما برای پارامتر ψ در وضعیت تکمیل

معامله، $\psi BOOL = true$، یک ایراد ارزیابی در فرآیند معامله وجود دارد. مکانیزم ارزیابی شکل ۱ فقط دست‌کاری پارامتر وب را بررسی می‌کند و تائید نمی‌کند که آیا پرداخت‌کننده و گیرنده پرداخت، با هم تطابق دارند یا خیر.

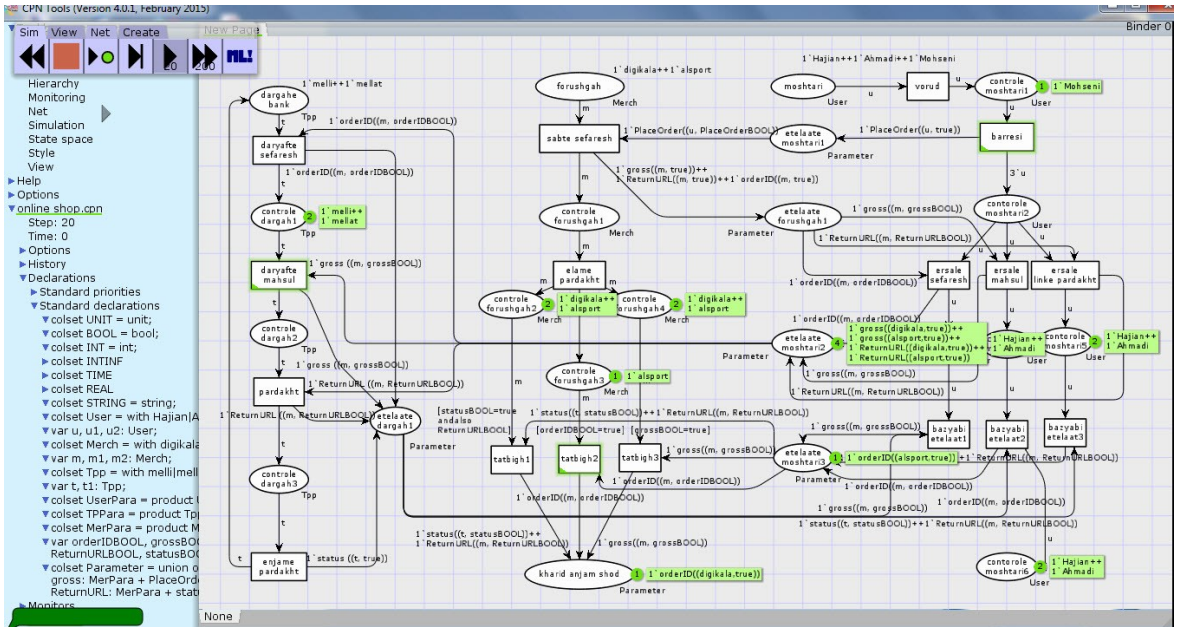
۵. مورد مطالعاتی

در این بخش، مدل ارائه شده در بخش ۴ روی دو نمونه فروشگاه آنلاین داخلی تست می‌شود. همان‌گونه که در مدل شکل ۲ مشاهده نمودید، ساختار مدل دارای سه موجودیت مشتری، بازرگان و درگاه پرداخت بانکی است. موجودیت بازرگان با دو فروشگاه digikala و alsport مقداردهی شده است. درگاه پرداخت بانکی شامل درگاه پرداخت melli و درگاه پرداخت mellat است. سه مشتری به نام‌های Hajian، Ahmadi و Mohseni در مکان ورود مشتری در نظر گرفته شده‌اند. مشتری پس از ورود به سیستم و گذر از فاز بررسی هویت، اقدام به ثبت سفارش در فروشگاه مورد نظر خود می‌کند. فروشگاه در پاسخ به مشتری، پیامی حاوی شماره سفارش، محصول و نیز لینک درگاه بانک ارسال می‌کند. مشتری مورد نظر پس از اقدام به پرداخت هزینه، در صورت انجام تراکنش مالی موفق، به صفحه‌ی صدور پایان ثبت سفارش هدایت می‌شود. تنها در صورت صدور پایان ثبت سفارش، سفارش مشتری معتبر خواهد بود. در این حالت، مکان مربوط به اتمام خرید، مجموعه‌ای از مهره‌ها شامل شماره سفارش، محصول و وضعیت پرداخت بانکی را خواهد داشت. همچنین در مکان پایانی مشتری، اسامی مشتریانی که اقدام به ثبت سفارش موفق نموده باشند، درج می‌شود.

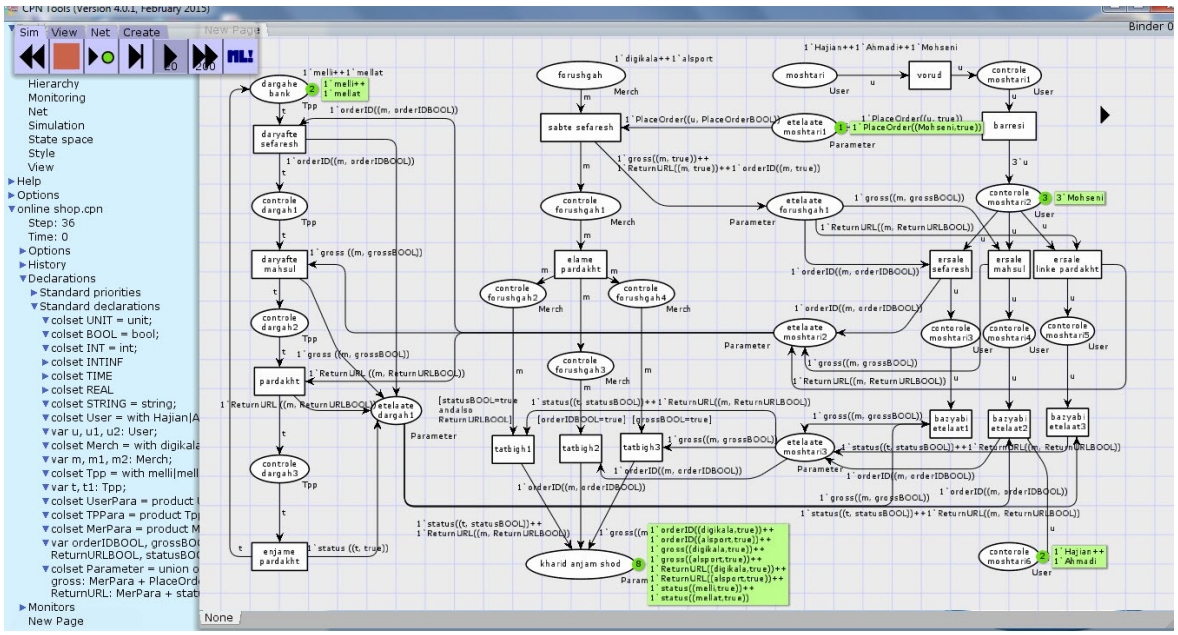
در طی اجرای مدل، در چندین مرحله، اطلاعات مشتری، فروشگاه و درگاه بانکی بررسی مجدد می‌شود. دلیل این امر این است که در هر مرحله از خرید آنلاین، ممکن است اطلاعات سفارش و نیز اطلاعات مالی مشتری به‌صورت غیرمجاز مورد دسترسی سایت‌های مداخله‌گر قرار گیرد. با بررسی‌های چندین‌باره، چنانچه در هر مرحله از ثبت سفارش، مداخله‌ی مشکوکی از سوی هر یک از موجودیت‌ها مشاهده شود، وضعیت بخش مورد نظر false شده و جهت تضمین امنیت فرایند ثبت سفارش، عملیات متوقف‌شده و می‌تواند مجدداً از نقطه شروع، از سر گرفته شود. مدل اجرایی شکل ۲ را روی مثال‌های فوق‌الذکر، پیش از شبیه‌سازی، در نشان‌گذاری میانی، و پس از شبیه‌سازی به ترتیب در شکل‌های ۴، ۵ و ۶ مشاهده می‌کنید.



شکل ۴. مدل پیش از شبیه‌سازی



شکل ۵. مدل در نشان‌گذاری میانی



شکل ۶. مدل پس از شبیه‌سازی

۶. نتیجه‌گیری

در این مقاله، یک روش رسمی برای مدل‌سازی سیستم‌های خرید آنلاین و تحلیل ایرادهای ارزیابی در موارد واقعی، ارائه شد. راهکار پیشنهادی از روش‌های رسمی مدل مبنای CPN استفاده می‌کند. ابزارهای CPN می‌توانند در آنالیز مشخصه‌های مرتبط با مدل‌های CPN به ما کمک کنند. بااین‌حال، راهکار پیشنهادی فقط برای مواردی مناسب است که فضای حالت، محدود باشد. برای فضای حالت نامحدود، می‌توان محدودیت زمان اجرا را در ابزارهای CPN تنظیم نمود تا ایرادهای ارزیابی بیشتری شناسایی شوند. بااین‌حال بازهم ممکن است تمام ایرادها مشخص نشوند. بنابراین در مقالات آینده، لازم است که تحلیل کارآمد فناوری‌ها برای فضای حالت نامحدود مورد بررسی قرار گیرد.

۶. مراجع

۱. Jensen, K. (۱۹۹۷). Colored petri nets- basic concepts, analysis methods and practical use. *EATCS, Monographs on Theoretical Computer Science*, vol:۱.
۲. Wen, S., Xue, Y., Xu, J., Yuan, L., Song, W., Yang, H., Si, G. (۲۰۱۷). Lom: Discovering logic flaws within mongodb-based web applications. *International Journal of Automation and Computing*, ۱٤(۱), ۱۰٦-۱۱۸.
۳. Chen, E., Chen, S., Oadeer, S., Wang, R. (۲۰۱٥). Securing multiparty online services via certification of symbolic transactions. *2015 IEEE Symposium on IEEE*, ۸۳۳- ۸٤۹.
٤. Wang, M., Ding, Z., Zhao, P., Yu, W., Jiang, C. (۲۰۱۸). A dynamic data slice approach to the vulnerability analysis of e-commerce systems. *IEEE Transactions on Systems, Man, and Cybernetics Systems*, ۱-۱٥.
٥. Wang, R., Chen, S., Wang, X., Oadeer, S. (۲۰۱۱). How to shop for free online- security analysis of cashier-as-a-service based web stores. *2011 IEEE Symposium on IEEE*, ٤٦٥-٤۸۰.
٦. Sun, F., Xu, L., Su, Z. (۲۰۱٤). Detecting logic vulnerabilities in e-commerce applications. *NDSS*.
۷. Jiang, C., Song, J., Liu, G., Zheng, L., Luan, W. (۲۰۱۸). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. *IEEE Internet of Things Journal*, ٥(٥), ۳٦۳۷-۳٦٤۷.
۸. Pellegrino, G., Balzarotti, D. (۲۰۱٤). Toward black-box detection of logic flaws in web applications. *NDSS*.
۹. Sudhodanan, A., Armando, A., Carbone, R., Compagna, L. (۲۰۱٦). Attack patterns for black-box security testing of multi-party web applications. *NDSS*.
۱۰. Hirschberger, D., Mladenov, D., Mainka, M., Schwenk, J. (۲۰۱٦). Bachelor thesis cashier-as-a-service based webshops overview and steps towards security testing.
۱۱. Maatoug, G., Dadeau, F., Rusinowitch, M. (۲۰۱٤). Model-based vulnerability testing of payment protocol implementations. *HotSpot'14-2nd Workshop on Hot Issues in Security Principles and Trust, affiliated with ETAPS 2014.*
۱۲. Chen, E., Chen, S., Oadeer, S., Wang, R. (۲۰۱٤). A practical approach to protocol-agnostic security for multiparty online services. *MSR-TR*.
۱۳. Xing, L., Chen, Y., Wang, X., Chen, S. (۲۰۱۳). Integuard: Toward automatic protection of third-party web service integrations. *NDSS*.
۱٤. Fung, A., Cheung, K., Wong, T. (۲۰۱۲). Faith: Scanning of rich web applications for parameter tampering vulnerabilities. *Tech. Rep.*
۱٥. Fung, P., Wang, T., Cheung, K., Wong, T. (۲۰۱٤). Scanning of real-world web applications for parameter tampering vulnerabilities. *Proceedings of the 9th ACM symposium on Information, computer and communications security, ACM*, ۳٤۱-۳٥۲.
۱٦. McGraw, G., Viega, J. (۲۰۰۲). Building secure software. *RTO/NATO Real-Time Intrusion Detection Symp.*
۱۷. Jensen, K., Kristensen, L. (۲۰۰۹). Kristensen, Coloured Petri nets: modelling and validation of concurrent systems. *Springer Science & Business Media.*
۱۸. Jensen, K., Rozenberg, G. (۲۰۱۲). Rozenberg, High-level Petri nets: theory and application. *Springer Science & Business Media.*

۱۹. Jensen, K. (۲۰۱۳). Coloured Petri nets: basic concepts, analysis methods and practical use. *Springer Science & Business Media*, vol. ۱.