وارسی استحکام سامانه‌های اعتماد

امیر جلالی بیدگلی[1] و بهروز ترک لادانی[2]

[1] دانشجوی دکتری گروه مهندسی نرم افزار، دانشکده کامپیوتر، دانشگاه اصفهان، اصفهان
amirjalali@eng.ui.ac.ir

[2] دانشیار گروه مهندسی نرم افزار، دانشکده کامپیوتر، دانشگاه اصفهان، اصفهان
ladani@eng.ui.ac.ir

چکیده

اعتماد و شهرت، مفاهیمی شناخته‌شده در علوم اجتماعی هستند که امروزه در قالب سامانه‌های اعتماد، کاربردهای روزافزونی در علوم رایانه و ارتباطات پیدا کرده‌اند. این سامانه‌ها با ارائهٔ مدلی محاسباتی و بر پایه مجموعه‌ای از تجربیات و توصیه‌ها، مقادیر اعتماد (یا شهرت که نوع خاصی از اعتماد است) را محاسبه می‌کنند. این مقادیر به موجودیت‌ها در شناسایی و سپس منزوی ساختن موجودیت‌های غیردرست‌کار جامعه یاری می‌رساند. انتظار بر آن است که مقادیر اعتماد، میزان درست‌کاری هر موجودیت را نمایش دهد که درنتیجه یک موجودیت با اعتماد پایین با احتمال بالایی یک موجودیت بدخواه یا خودخواه خواهد بود. از سامانه‌های اعتماد به‌عنوان مهم‌ترین ابزار در نسل جدید روش‌های امنیتی به نام امنیت نرم نام برده‌اند. باوجود کاربردهای گسترده، این سامانه‌ها در مقابل برخی حملات آسیب‌پذیر هستند. این حملات دنباله‌ای از رفتارهای گمراه‌کننده و ریاکارانه توسط موجودیت‌های بدخواه هستند که قادر به فریب مدل محاسبه اعتماد و درنتیجه افزایش یا کاهش مقادیر اعتماد به نفع حمله‌کنندگان خواهد بود. یک سامانه اعتماد آسیب‌پذیر، نه تنها ابزار تصمیم‌یار مناسبی برای موجودیت‌ها نیست؛ بلکه ممکن است به ابزاری در دست حمله‌کنندگان جهت افزایش قدرت حملاتشان تبدیل شود، از این رو لازم است پیش از استفاده از یک سامانه، استحکام آن دربرابر حملات ارزیابی گردد. این مقاله به مرور و بررسی حملات اعتماد و روش‌های موجود در ارزیابی استحکام سامانه‌های اعتماد در برابر آنها می‌پردازد. شبیه‌سازی و وارسی صوری، دو بستر اصلی جهت ارزیابی استحکام سامانه‌های اعتماد است. شبیه‌سازی که روش غالب در اکثر پژوهش‌هاست، روش تخمینی است که در هر بار تنها قادر است چند مسیر اجرا را از سامانه بررسی کند. در مقابل در روش‌های وارسی صوری، کل فضای حالت اجرای مدل جهت بررسی دارا بودن ویژگی‌های امنیتی مورد نظر پوشش داده می‌شود؛ از این رو نتایج به‌دست آمده با این روش‌ها دقیق و قابل اثبات است. با وجود مزیت‌های فراوان روش‌های صوری بر روش‌های شبیه‌سازی، پژوهش‌های مرتبط با وارسی استحکام سامانه‌های اعتماد هنوز ناقص و در مراحل نخستین پژوهش هستند، هرچند این پژوهش‌ها در سال‌های اخیر رشد خوبی داشته‌اند. در این مقاله این پژوهش‌ها در کنار روش‌های مبتنی بر شبیه‌سازی مرور و معایب و مزایای هر یک بررسی می‌شود.

واژگان کلیدی: اعتماد، شهرت، سامانه‌های اعتماد، حمله، استحکام، وارسی، شبیه‌سازی.

۱- مقدّمه

امروزه با توسعه فناوری ارتباطات و اینترنت، محیط‌های الکترونیکی می‌توانند بستر ارتباطی بین هزاران فرد یا سامانهٔ رایانه‌ای باشند که با گسترش مفاهیمی مانند شبکه‌های اجتماعی و خدمات الکترونیکی روزبه‌روز بر پیچیدگی آنها نیز افزوده می‌شود. افراد یا موجودیت‌ها در این‌گونه سامانه‌ها اغلب نیازمند ارتباط و همکاری با یکدیگر هستند؛ درحالی‌که نسبت به یکدیگر دانش یا شناخت قبلی و کافی ندارند و ممکن است برخی از موجودیت‌های حاضر در سامانه، رفتار خودخواهانه یا بدخواهانه‌ای را در پیش بگیرند. اعتماد[1] و شهرت[2] مفاهیمی آشنا در علوم اجتماعی است که پایه‌های ارتباطی، جوامع انسانی را شکل می‌دهند. در سال‌های اخیر این مفاهیم با عنوان سامانه‌های اعتماد و شهرت[3] در بسیاری

[1] Trust
[2] Reputation
[3] Trust and Reputation Systems

از حوزه‌های علوم رایانه و ارتباطات کاربرد یافته‌اند. اعتماد کمیتی است که نشان‌دهنده باور یک فرد به فرد دیگر در انجام رفتار مورد نظر وی است. شهرت در مقابل، تجمیع نظرات کل جامعه درباره رفتار یک موجود است. بنابراین شهرت را نیز می‌توان نوعی از اعتماد دانست که محاسبه آن نه توسط یک فرد بلکه توسط جامعه صورت می‌گیرد. به همین جهت سامانه‌های اعتماد و شهرت را می‌توان به‌طور عام سامانه‌های اعتماد نامید. هدف از سامانه‌های اعتماد ارائه مدلی جهت محاسبه اعتماد و سپس به‌کارگیری آن در تعاملات و تراکنش‌های بین موجودیت‌های سامانه است. محاسبهٔ اعتماد در این سامانه‌ها با استفاده از تجربیات مستقیم گذشته و همچنین مجموعه نظرات و توصیه‌های دریافت‌شده (تجربیات غیرمستقیم) انجام می‌پذیرد. مقدار اعتماد محاسبه‌شده، معیاری جهت پیش‌بینی رفتار آیندهٔ هر موجودیت فراهم می‌آورد که می‌تواند در تصمیم‌گیری عضوهای سامانه یاری‌رسان باشد.

کاربرد سامانه‌های اعتماد در سامانه‌های رایانه‌ای و ارتباطی روزبه‌روز در حال گسترش است. همان‌طور که اشاره شد، این سامانه‌ها به موجودیت‌های محیط اجازه می‌دهند که براساس تجارب خود و دیگران، درست‌کاری سایر اعضا را پیش‌گویی کنند و براساس آن بهترین عضو را جهت همکاری یا درخواست خدمت شناسایی نمایند. به‌عنوان نمونه در شبکه‌های نظیر به نظیر[1] برای اشتراک منابع و یا در محیط‌های محاسباتی مشبک[2] برای انتخاب گره همکار، هر گره از سامانه در نتیجه تراکنش‌هایی که با دیگر گره‌ها انجام می‌دهد، تجربه‌ای به دست می‌آورد که می‌تواند راهنمای وی در انتخاب گره‌های دیگر جهت انجام تراکنش‌های پیش رو باشد. درصورتی‌که تجربهٔ قبلی نشان‌دهنده رفتار خصمانهٔ یک گره (مانند ارسال فایل‌های آلوده به ویروس در شبکه‌های نظیر به نظیر، یا عدم پایبندی یک گره به تعهدات زمانی در محیطهای محاسباتی مشبّک) باشد، برای جلوگیری از آسیب‌های بیشتر می‌توان از انجام تراکنش‌های جدید با وی خودداری کرد. سامانه‌های اعتماد چکیده تجارب گذشته را در قالب کمیّتی مقایسه‌پذیر با عنوان اعتماد در اختیار موجودیت‌های سامانه قرار می‌دهند. این قابلیت موجب شده، سامانه‌های اعتماد در هر محیط که نیاز به همکاری و تعامل دو به دو بین موجودیت‌هاست، کاربرد داشته باشند. از این رو سامانه‌های اعتماد به‌عنوان دسته بسیار مهمی از سامانه‌های تصمیم‌یار در بسیاری از حوزه‌ها مانند خدمات برخط[3] و تجارت الکترونیکی [۱-۳]، وب معنایی[4] [۴-۶]، شبکه‌های اجتماعی[5] [۷]، ارتباطات بی‌سیم[6] [۸, ۹]، سامانه‌های چندعامله[7] [۱۰]، شبکه‌های اقتضایی[8] [۱۱-۱۳] و محاسبات مشبک [۱۴, ۱۵] کاربرد دارند. علاوه‌براین نمونه‌ها، سادگی و کارآیی سامانه‌های اعتماد موجب شده که روزبه‌روز کاربردهای جدیدی از آنها ارائه شود. به‌عنوان مثال می‌توان به پژوهش‌هایی که در زمینه استفاده از اعتماد در سامانه‌های تشخیص نفوذ[9] [۱۶و۱۷] و تشخیص هرزنامه‌ها[10] [۱۸] انجام شده، اشاره کرد.

سامانه‌های اعتماد همچنین محبوبیت قابل توجهی در پایگاه‌های ارائه دهنده خدمات اینترنتی یافته‌اند و توسط بسیاری از شرکت‌های بزرگ مانند eBay، Amazon، Alibaba، Yahoo، YouTube، Yelp، Epinions و CouchSurfing استفاده شده‌اند. Xu و همکاران در پژوهش خود [۱۹] نشان دادند مفاهیم شهرت و اعتماد چنان در سایت‌های خرید و فروش برخط مانند eBay، Amazon و Alibaba نهادینه و کاربردی شده‌اند که میزان سودآوری هر کاربر در آنها به‌طورکامل وابسته به مقادیر محاسبه‌شدهٔ شهرت وی است. این مسئله موجب ظهور تجارت غیرقانونی جدیدی شده است که در آن یک کاربر می‌تواند با پرداخت پول میزان شهرت خود را به‌صورت غیرواقعی در یک روز تا صدها برابر افزایش دهد. تجربیات ارائه‌شده در این پژوهش نشان داد در سال ۲۰۱۵ حداقل یازده‌هزار کاربر تقلبی با هدف افزایش غیرقانونی شهرت در این پایگاه‌های معروف برخط مشغول هستند که تراکنش‌های مالی آن بالغ بر ۲۲۰۰۰۰ عدد، حجم مالی ۶،۷۰۰،۰۰۰ دلار و سودآوری ۷۰،۰۰۰ دلار در سال می‌شود، درحالی‌که سامانه‌های اعتماد تعبیه‌شده تنها قادر به شناسایی و حذف ۲/۲٪ از آنها می‌شوند.

سامانه‌های اعتماد گذشته از کاربردهای روزافزون، به‌عنوان مهم‌ترین ابزار در *امنیت نرم*[11] [۱, ۲۰, ۲۱] شناخته می‌شوند. امنیت نرم به نسل جدیدی از روش‌های امنیتی

[1] Peer-to-peer network
[2] Grid Computing

[3] Online Services
[4] Semantic Web
[5] Social Networks
[6] Wireless Communications
[7] Multi-Agent Systems
[8] Ad-hoc Network
[9] Intrusion Detection Systems
[10] Spam
[11] Soft Security

اشاره می‌کند که در آن به جای استفاده از روش‌های سنتی، از هنجارهای اجتماعی جهت کنترل سامانه استفاده شود. در مقابل امنیت نرم، *امنیت سخت*[1] تعریف می‌شود که به مجموعه روش‌های سنتی امنیتی مانند روش‌های رمزنگاری و کنترل دسترسی اطلاق می‌شود. اعتماد مهمترین هنجار اجتماعی شناخته‌شده در امنیت نرم است. کاربرد و توسعه روزافزون وسایل ارتباطی و الکترونیکی باعث شده تا امنیت سخت به‌تنهایی پاسخ‌گوی نیازهای آتی نباشد؛ که این موضوع بیش از پیش بر اهمیت سامانه‌های اعتماد می‌افزاید.

باوجود کاربردهای روزافزون سامانه‌های اعتماد، این سامانه‌ها ممکن است نسبت به برخی از حملات آسیب‌پذیر باشند. در این حملات، حمله‌کننده با استفاده از دنباله‌ای از رفتارهای گمراه‌کننده، سعی در فریب مدل محاسبه اعتماد دارد؛ به‌نحوی که میزان اعتماد محاسبه‌شده، به نفع وی، کمتر یا بیشتر از مقدار واقعی باشد. البته باید توجه داشت که سامانه‌های اعتماد در اصل، با هدف شناسایی و منزوی‌کردن موجودیت‌های بدخواه یا خودخواه ارائه شده‌اند. ابزار مورد استفاد سامانه در این هدف، میزان اعتماد محاسبه‌شده است که هرچه کمتر باشد، احتمال بدخواهی یک موجودیت بیشتر است؛ اما حمله‌کنندگان را در این سامانه‌ها می‌توان دسته‌ای از موجودیت‌های بدخواه تعریف کرد که هوشمندانه به فریب و دستکاری مقادیر اعتماد اقدام می‌کنند و درنتیجه نه تنها سامانه قادر به شناسایی آنها نخواهد بود، بلکه ممکن است به ابزاری جهت تقویت حمله تبدیل شود. استحکام[2] یک سامانه اعتماد توانایی محاسبه صحیح مقادیر اعتماد در هر شرایطی حتی شامل وجود حمله‌کنندگان در محیط است. همان‌طور که در این پژوهش نشان داده می‌شود، یک سامانه غیرمستحکم نه تنها ابزار تصمیم‌یار مناسبی برای موجودیت‌ها نیست، بلکه حتی ممکن است آسیب واردشده به سامانه بیش از حالتی باشد که در آن هیچ ابزار تصمیم‌یاری موجود نیست؛ از این‌رو ارزیابی استحکام سامانه‌های اعتماد علیه حملات، چالش مهمی است که لازم است پیش از استفاده از این سامانه‌ها بررسی شود.

چالش اعتبارسنجی استحکام سامانه‌های اعتماد به دفعات در مقالات مورد اشاره واقع شده است. به‌عنوان نمونه Jøsang در مقالهٔ خود [۲۲] با انتقاد از وضعیت موجود، سه روش را برای نیل به این هدف پیشنهاد می‌دهد: ۱) ارزیابی و آزمایش سامانه در محیط واقعی و شامل حمله‌کنندگان، ۲) ارزیابی توسط فرد یا گروه سومی که انگیزه‌ای جهت برترنشان دادن سامانه نداشته باشند، و ۳) ارائه یک روش ارزیابی جامع و قابل قبول. مشخص است که دو روش پیشنهادی نخست امکان اجرا در همه شرایط را ندارند. ارائهٔ یک روش ارزیابی جامع و اثبات‌پذیر می‌تواند راه حلی برای این چالش باشد.

در حال حاضر، مهم‌ترین روش ارزیابی سامانه‌های اعتماد، شبیه‌سازی موردی آنها است. در این روش، یک سامانه نمونه به همراه حمله یا حملات خاصی، مدل و سپس شبیه‌سازی می‌شوند. این روش گذشته از آنکه ممکن است به علت انگیزه و اشتباهات فردی، اعتبار و صحت کافی را نداشته باشد، نمی‌تواند به‌عنوان ابزار جامعی جهت ارزیابی امنیتی سامانه‌های اعتماد استفاده شود؛ چون نه تنها روش‌ها و الگوریتم‌های یکسان و قابل اثباتی جهت مدل‌سازی و شبیه‌سازی استفاده نشده است، بلکه حتی تعریف دقیق و جامعی از مفاهیم استحکام و حمله نیز وجود ندارد. گذشته از آن، شبیه‌سازی روشی تخمینی است که نتایج حاصل ممکن است دارای خطا باشند؛ زیرا این روش قادر به بررسی تمام مسیرهای ممکن از اجرای سامانه نیست و نتایج آن تنها از بررسی چند مسیر اجرای نمونه حاصل می‌شود.

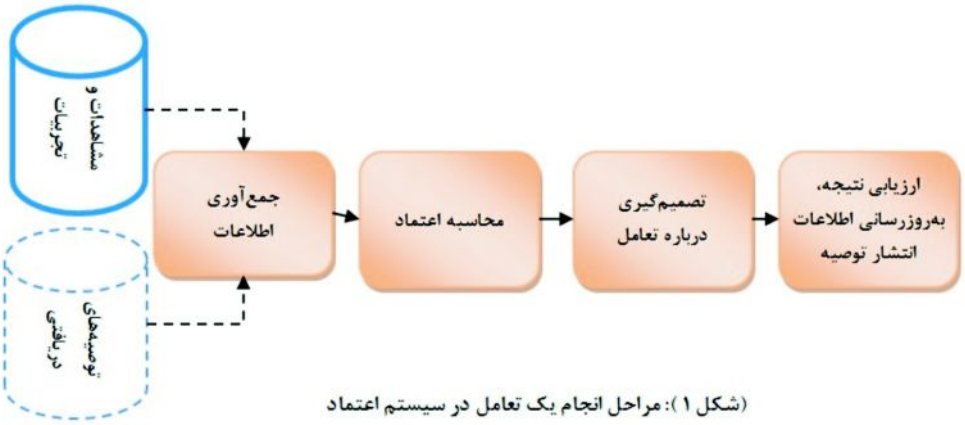
در این مقاله روش‌های موجود در ارزیابی استحکام سامانه‌های اعتماد با تأکید بر وارسی صوری و مزایای آن مرور می‌شوند. مقاله به‌صورت زیر ادامه می‌یابد. در بخش دوم، سامانه‌های اعتماد، مفاهیم و چارچوب‌های متداول مرور می‌شوند. چالش‌های امنیتی سامانه‌های اعتماد با مروری بر مهم‌ترین انواع حملات در بخش سوم ارائه می‌شود. نتایج و پژوهش‌های موجود در زمینه ارزیابی استحکام سامانه‌های اعتماد در بخش چهارم معرفی می‌شوند. بخش پنجم، چکیده‌ای از روش‌های وارسی صوری در این حوزه را مرور می‌کند و درنهایت مقاله در بخش ششم و هفتم به‌ترتیب با بررسی چالش‌های موجود و نتیجه‌گیری خاتمه می‌یابد.

۲- سامانه‌های اعتماد

با وجود پژوهش‌های فراوانی که در زمینهٔ اعتماد انجام شده، تعریف جامع و مورد اجماعی در مقالات برای این مفاهیم ارائه نشده است. به‌عنوان نمونه Gumbertta تعریف زیر را از اعتماد ارائه داده است:

«درجهٔ خاصی از احتمال ذهنی که در آن، پیش از انجام

[1] Hard Security
[2] Robustness



(شکل ۱): مراحل انجام یک تعامل در سیستم اعتماد

رفتار خاصی و مشاهده آن، اعتمادکننده باور دارد که معتمد، رفتار مورد نظر را انجام می‌دهد.» [۲۳]

اعتماد همچنین به‌صورت زیر تعریف شده است:

«عقیده‌ای مبنی بر این‌که معتمد رفتار قابل اتکا، قابل اعتماد و امنی را در زمینهٔ خاصی نشان می‌دهد.» [۲۴]

اما شاید بهترین تعریف برای اعتماد را تعریف زیر دانست:

«اعتماد یک فرد (اعتمادکننده) به فرد دیگر (معتمد) به حالت ذهنی اطلاق می‌شود که در آن اعتمادکننده عقیده دارد معتمد، خدمت مشخصی را به خوبی برای وی انجام می‌دهد و انتظار دارد که معتمد آن خدمت را طبق نظر او انجام دهد و همچنین این خطر را خواهد پذیرفت که ممکن است معتمد طبق انتظار وی رفتار نکند.» [۲۵]

اعتماد یک حدس کورکورانه و یا انتخاب تصادفی نیست؛ بلکه شامل تحلیل دانش موجود و تجربیات کسب‌شده جهت پیش‌بینی رفتار آینده هر موجود است. در پژوهش‌ها روش‌های مختلفی جهت محاسبه اعتماد ارائه شده است؛ اما تمام آنها در برخی خصوصیات مشترک هستند. نخست آن‌که اعتماد کمیّتی غیریکنواخت و پویا در زمان است و تعامل و تجربه بیشتر می‌تواند اعتماد به یک موجود را کاهش یا افزایش دهد. دوم آنکه اعتماد وابسته به زمینه[1] است. شما ممکن است به یک فرد در زمینهٔ دندانپزشکی اعتماد داشته باشید؛ اما به وی در زمینهٔ تعمیر ماشین اعتماد نداشته باشید.

سامانه‌های اعتماد دسته‌ای از سامانه‌های تصمیم‌یار هستند که با به‌کارگیری روش‌های محاسبه اعتماد، موجودیت‌های محیط را در برقراری رابطه و همکاری بهتر با یکدیگر یاری می‌رسانند. مقادیر محاسبه‌شده اعتماد در هر زمینه، به‌طورعمومی نشان‌دهنده میزان درست‌کاری موجودیت در آن زمینه است. بنابراین اعضا در یک محیط می‌توانند با مقایسهٔ این مقادیر، موجودیت‌های خودخواه یا بدخواه را شناسایی و با خودداری از برقراری ارتباط با آنها، این موجودیت‌ها را از محیط طرد و منزوی کنند.

یک سامانه اعتماد حداقل از دو نوع موجودیت تشکیل می‌شود: خدمت‌دهندگان[2] و امتیازدهندگان[3] [۲۱, ۲۲, ۲۶]. البته یک موجودیت ممکن است در هر دو نقش ظاهر شود. ارائه‌دهندگان خدمت خدمات مورد نیاز محیط را ارائه می‌دهند و امتیازدهندگان (که اغلب مشتریان یا دریافت‌کنندگان خدمت هستند) با بررسی خدمت‌های انجام‌شده، به هر یک امتیازی را انتساب می‌دهند. مجموعه امتیازهای کسب شده توسط هر خدمت‌دهنده مبنای محاسبه مقدار اعتماد وی در زمینه خدمت‌رسانی اوست.

شکل ۱ مراحل انجام یک تعامل در سامانه اعتماد را نشان می‌دهد. مستقل از جزئیات هر سامانه، انجام یک تعامل از چهار گام کلی تشکیل شده است. گام نخست جمع‌آوری اطلاعات لازم جهت محاسبه اعتماد است. این اطلاعات در سامانه‌های اعتماد متمرکز، می‌تواند در یک سرویس‌دهنده ذخیره شود. برخلاف سامانه‌های متمرکز، در سامانه‌های توزیع‌شده هر موجودیت اغلب تنها به اطلاعات، تجربیات و مشاهده‌های مستقیم خود دسترسی دارد. در این سامانه‌ها از مفهومی با عنوان توصیه[4] برای دسترسی به دانش لازم استفاده می‌شود. توصیه نظر یک عضو درباره اعتمادپذیری عضو دیگر است که در محیط منتشر می‌شود. توصیه به‌طورعمومی خلاصه‌ای از تجربیات و دانش یک عضو است که در اختیار سایرین قرار می‌گیرد. هر موجودیت برای افزایش دانش و محاسبه دقیق‌تر اعتماد، لازم است

[1] Context

[2] Service Providers
[3] Raters
[4] Recommendation

توصیه‌های منتشرشده را نیز لحاظ نماید.

دومین گام از یک سامانه اعتماد، محاسبه اعتماد براساس اطلاعات جمع‌آوری‌شده است. روش‌های مختلفی جهت محاسبهٔ اعتماد، در مقالات ارائه شده است. برخی از روش‌ها مانند روش استفاده‌شده توسط eBay به‌سادگی با جمع امتیازها، شهرت را محاسبه می‌کند [۲۷]. در این روش هر امتیاز یک مقدار عددی ۱-، ۰ یا ۱ است و شهرت هر فروشنده برابر با جمع تمام امتیازهاست. میانگین‌گیری نیز جزء روش‌های مطرح در سامانه‌های اعتماد هستند؛ به‌عنوان نمونه REGRET [۲۸, ۲۹] و Core [۳۰] با استفاده از میانگین وزن‌دار امتیازات، اعتماد به هر فرد را محاسبه می‌کند. برخی دیگر از روش‌ها، با نگاشت مسئله محاسبه اعتماد به سایر دامنه‌ها، از روش‌های استفاده شده برای حل مسائل در آن دامنه برای محاسبه اعتماد استفاده کرده‌اند؛ به‌عنوان نمونه EigenTrust [۳۱] با معادل دانستن شهرت با رتبه‌بندی، از الگوریتم PageRank [۳۲] برای محاسبه شهرت استفاده می‌کند. PageRank الگوریتمی است که توسط Google جهت رتبه‌بندی سایت‌ها به کار می‌رود. مدل ارائه‌شده توسط Yu و Singh [۳۳] با نگاشت مسئله اعتماد به فضای عقیده، از تئوری Dempster-Shafer [۳۴] سود جسته است. مدل شهرت Beta [۳۵] به‌عنوان آخرین نمونه، توزیع احتمالی رفتار هر فرد را منطبق بر توزیع بتا فرض می‌کند و درنتیجه شهرت وی را برابر با امید ریاضی این توزیع تعریف می‌کند. مستقل از روش استفاده‌شده، خروجی گام دوم از سامانه اعتماد، مقدار محاسبه‌شده اعتماد است که ممکن است کمیّتی پیوسته (مانند بازه صفر تا یک)، گسسته (مانند اعداد صحیح)، دوتایی[1] (مانند قابل اعتماد یا غیرقابل اعتماد) و یا کیفی[2] (مانند قابل اعتماد و بسیار قابل اعتماد) باشد.

در گام سوم، موجودیت‌های جامعه از مقادیر محاسبه‌شده اعتماد برای گرفتن تصمیم‌های لازم یاری می‌جویند. این تصمیم‌ها شامل «چه کسی بهترین فرد برای انجام تعامل است؟» و «آیا با موجودیت x تعامل انجام شود؟» هستند. به‌عنوان نمونه خدمت‌گیرندگان[3] از این مقادیر برای انتخاب بهترین خدمت‌دهنده استفاده می‌کنند. همچنین موجودیت‌ها می‌توانند برای همکاری یا عدم همکاری با یک موجودیت خاص از این مقادیر استفاده کنند. موجودیت‌های دارای اعتماد پایین با احتمال بیشتری نسبت به سایرین ممکن است خودخواه یا بدخواه باشند که در این صورت عدم همکاری با آنها به انزوای ایشان می‌انجامد. پس از انجام هر تعامل و همکاری در سامانه، تعامل انجام‌شده ارزیابی و به آن امتیازی داده می‌شود. آخرین گام از سامانه اعتماد، به‌روزرسانی اطلاعات با استفاده از امتیاز داده‌شده و درصورت نیاز انتشار توصیه‌های جدید است. امتیاز و توصیه‌های منتشرشده، درحقیقت دانش جدیدی است که از موجودیت‌های درگیر تعامل کسب شده و می‌تواند به محاسبه دقیق‌تر مقادیر اعتماد در تعاملات آینده کمک کند.

[1] Binary
[2] Qualitative
[3] Clients

۳- چالش‌های امنیتی سامانه‌های اعتماد

برای تبیین چالش‌های امنیتی در سامانه‌های اعتماد، در ابتدا مثال نمونهٔ زیر را بررسی می‌کنیم. سامانه شهرت Beta [۳۵] را در نظر بگیرید. این سامانه مقدار شهرت هر موجودیت را به‌صورت زیر محاسبه می‌کند:

$$\frac{r+1}{s+r+2} \quad (۱)$$

که در آن r تعداد خدمات رضایت‌بخش و s تعداد خدمات غیررضایت‌بخش انجام‌شده توسط موجودیت است. برای یک تازه‌وارد به سامانه، مقادیر این دو شمارنده، صفر و درنتیجه مقدار پیش‌فرض شهرت برابر با ۰,۵ است. اکنون سامانه‌ای را بر پایه شهرت Beta در نظر بگیرید که در آن اعضا بر اساس میزان شهرت یکدیگر با هم همکاری می‌کنند. در این سامانهٔ فرضی، اعضا از همکاری با موجودیت‌هایی که مقدار شهرت آنها کمتر از ۰,۵ باشد، با هدف منزوی کردن آنها خودداری می‌کنند؛ چون تصور آن است که این مقدار نشان‌دهنده یک موجودیت غیر قابل اعتماد است. فرض کنید X یک عضو نمونه در این سامانه است که از سازوکار محاسبهٔ شهرت و تاثیر آن بر روی همکاری بین اعضا مطلع است. X با این دانش قصد دارد رفتار غیر رضایت‌بخشی از خود نشان دهد و با وجود آن از منزوی‌شدن خود در سامانه جلوگیری کند. وی در ۱۰ همکاری نخست رفتار رضایت‌بخشی از خود نشان می‌دهد و شهرت خود را به مقدار $\frac{11}{12}$ می‌رساند. در این حالت، X همکاری‌های غیررضایت‌بخش خود را آغاز می‌کند و به مدت ۱۰ تراکنش بعدی ادامه می‌دهد. مقدار شهرت وی در این مدت کاهش یافته و دوباره به ۰,۵ می‌رسد. X با علم به اینکه ادامه این رفتار موجب منزوی‌شدن وی خواهد شد، دوباره رفتار رضایت‌بخش خود را از سر می‌گیرد و همین چرخه را تکرار می‌کند. این رفتار X به سامانه اجازه شناسایی وی به‌عنوان یک موجودیت غیرقابل اعتماد را نمی‌دهد،

درحالیکه عامدانه نیمی از تراکنش‌ها را به‌صورت غیررضایت‌بخش انجام می‌دهد و می‌تواند تا ابد به سوء استفاده از سامانه بدون شناسایی ادامه دهد.

مثالی که در بالا ذکر شد، نمونه ساده‌ای از رفتارهای گمراه‌کننده‌ای است که موجب فریب سامانه‌های اعتماد می‌شود. این رفتارها که در واقع حمله علیه سامانه‌های اعتماد هستند، مهمترین چالش امنیتی این سامانه‌ها محسوب می‌شوند. حملات به سامانه‌های اعتماد بر خلاف حملات سنتی شکستن قوانین و یا نفوذ به سرورها نیستند، بلکه دنباله‌ای از رفتارهای ریاکارانه هستند که به گمراه شدن سامانه می‌انجامد. این حملات نه تنها سامانه را در دستیابی به هدف خود که شناسایی موجودیت‌های خودخواه و بدخواه است، باز می‌دارد، بلکه ممکن است ابزاری شود که حمله‌کنندگان از آن برای ارتقاء قدرت حملاتشان استفاده کنند. قابلیت اطمینان به یک سامانه اعتماد وابسته به میزان استحکام آن در برابر چنین حملاتی است. یک سامانه مستحکم، سامانه‌ای است که بتواند در هر شرایطی (شامل وجود حمله‌کنندگان) مقادیر اعتماد را به‌درستی محاسبه کند.

حملات مختلفی تاکنون برعلیه سامانه‌های اعتماد ارائه شده‌اند که برخی ساده و برخی بسیار پیچیده‌اند. حملات پیچیده اغلب شامل گروهی از حمله‌کنندگان می‌شود که با هماهنگی کامل با یکدیگر هر یک بخشی از حمله را اجرا می‌کنند. حمله‌کنندگان با ترکیب رفتارهای مختلف، سعی می‌نمایند، حداکثر ضربه را به سامانه بزنند. شناسایی این گونه حملات برای سامانه بسیار مشکل است. در این بخش برخی از مهم‌ترین حملات مطرح در سامانه‌های اعتماد معرفی می‌شوند. البته حملات اعتماد تنها محدود به موارد اشاره‌شده نیست، و موارد انتخاب‌شده تنها مهم‌ترین و پرارجاع‌ترین حملات در پژوهش‌هاست.

۳-۱- حمله روشن-خاموش

حملهٔ روشن-خاموش که به رفتار متناقض[1] و حملهٔ خیانت[2] نیز معروف است [۳۶-۳۸]، به حملاتی اشاره دارد که در آنها حمله‌کننده برای مدتی رفتار درست‌کارانه‌ای در پیش می‌گیرد تا اعتماد سایرین را جذب و پس از آن رفتار غیردرست‌کارانهٔ خود را آغاز کند. به‌عنوان نمونه در تجارت الکترونیکی یک فروشنده ممکن است برای مدت زمان کوتاهی تراکنش‌های کم‌ارزش را با بهترین کیفیت انجام دهد، تا بتواند با کسب اعتماد، خریداران را برای تراکنش‌هایی با حجم مالی بالاتر جذب کند و سپس به فریب و کلاه‌برداری در این تراکنش‌ها که برای وی سود سرشاری خواهد داشت، بپردازد. پس از دوره‌ای از رفتار غیردرست‌کارانه، حمله‌کننده می‌تواند برای بازیابی اعتماد ازدست‌رفته دوباره به رفتار درست‌کارانه روی آورد. چرخهٔ تبدیل از یک موجود درست‌کار به غیردرست‌کار و به‌عکس به‌عنوان حملهٔ روشن-خاموش شناخته می‌شود.

۳-۲- حملهٔ تازه‌وارد

اعتماد یک حمله‌کننده ممکن است به‌علت انجام طولانی مدت رفتار غیردرست‌کارانه به‌حدی کاهش یافته باشد که بازیابی آن برای حمله‌کننده مقدور نباشد. در این حالت وی می‌تواند با ایجاد یک شناسه جدید برای خود دوباره به‌عنوان یک تازه وارد در سامانه شناسایی شود. این فرآیند که به حمله تازه وارد یا حمله عیب‌پوشی[3] معروف است [۳۷, ۳۹]، به حمله‌کننده اجازه می‌دهد با حذف سابقه بد خود، دوباره رفتار غیردرست‌کارانهٔ خود را ادامه دهد.

۳-۳- حملهٔ Sybil

حمله Sybil [۴۰] هنگامی اتفاق می‌افتد که حمله‌کننده تعداد زیادی شناسه جعلی ایجاد و با استفاده از آنها حملات گروهی و هماهنگ‌شده‌ای را در سطح سامانه اجرا کند. در این حالت علاوه‌بر تقویت حملات، هویت اصلی حمله‌کننده نیز مخفی می‌ماند و درصورت شناسایی و طردشدن هر یک از شناسه‌ها، وی به‌سادگی می‌تواند با ایجاد شناسهٔ جدید حمله را ادامه دهد. استفاده از سازوکارهای امنیتی جهت جلوگیری از ایجاد شناسه‌های جعلی یا تکراری، می‌تواند راه‌کاری برای جلوگیری از حملات Sybil و تازه وارد باشد. Sybil نام قهرمان رمانی به همین نام است که مبتلا به عارضهٔ چندشخصیتی بوده و خود را در شانزده شخصیت جداگانه تصور می‌کند.

۳-۴- حملهٔ توصیهٔ غیرصادقانه

توصیهٔ غیرصادقانه[4] [۳۷] شامل ارزیابی غیرصادقانهٔ یک خدمت و درنتیجه انتساب امتیاز دروغین یا انتشار توصیهٔ

[1] Inconsistent Behavior
[2] Betrayal Attack
[3] Whitewashing Attack
[4] Dishonest Recommendation

نادرست است. این داده‌ها به‌عنوان اطلاعات غلط واردشده به سامانهٔ اعتماد، موجب محاسبهٔ اشتباه اعتماد به نفع حمله‌کننده خواهد شد. در پژوهش‌ها چندین زیرنوع از این حمله مطرح شده است که مهم‌ترین آنها بدنام‌کردن و خوشنام‌کردن است [۲۱, ۴۱]. علاوه‌بر این دو نوع، توصیه‌های کورکورانه (بی‌دقت) نیز در برخی از پژوهش‌ها پیشنهاد شده است [۳۷]. در سامانه‌هایی که یک موجودیت مجبور به ارزیابی خدمت است و یا برای آن پاداش دریافت می‌کند، ممکن است به ارائهٔ ارزیابی بدون دقت و یا حتی تصادفی اقدام کند. حملات توصیهٔ غیرصادقانه می‌تواند به‌صورت فردی یا گروهی اجرا شود.

۳-۵- حملهٔ تمایز

در حملات تمایز[1] [۲۲]، حمله‌کننده رفتار متناقضی را با افراد مختلف در سامانه در پیش می‌گیرد. به‌عنوان نمونه وی ممکن است با گروه کوچکی از افراد رفتار غیردرست‌کارانه داشته باشد، درحالی‌که برای مابقی سامانه درست‌کار باشد. این حمله می‌تواند نتایج مختلفی داشته باشد. نخست آنکه اگر تعداد افراد گروه نخست (افرادی که حمله‌کننده با آنها رفتار غیردرست‌کارانه داشته است) کم بوده و یا رأی آنها در سامانه وزن پایینی داشته باشد. حمله‌کننده می‌تواند بدون از دست دادن اعتماد به رفتار خود ادامه دهد. گذشته از آن، اگر سامانه از سازوکاری برای شناسایی توصیه‌های غیرصادقانه استفاده کند، ممکن است توصیه‌های منتشرشده توسط این گروه را غیرصادقانه ارزیابی کرده و از محاسبه خارج کند. این امر خود به بالابردن اعتماد به حمله‌کننده کمک می‌کند.

۳-۶- حمله عدم تعادل ارزش

در برخی از سامانه‌ها خدمات ارائه‌شده ارزش‌های متفاوتی دارند. یک سامانه اعتماد ممکن است این تفاوت ارزش را در امتیازها و محاسبه اعتماد لحاظ نکند؛ در این حالت حمله‌کننده می‌تواند با اجرای درست‌کارانه خدمات باارزش پایین و اجرای غیردرست‌کارانه خدمات باارزش بالا به سودی بیش از حد معمول دست یابد، بدون آنکه کاهش قابل توجهی در اعتماد داشته باشد. این رفتار به‌عنوان حمله عدم تعادل ارزش[2] [۲۱, ۲۲, ۴۲] شناخته می‌شود و جهت جلوگیری از آن کافی است وزن هر امتیاز وابسته به ارزش خدمت باشد.

۳-۷- حملهٔ تأخیر شهرت

در سامانه‌های توزیع‌شده، ممکن است تأخیری بین انجام یک رفتار غیردرست‌کارانه و انتشار آن در محیط وجود داشته باشد. حمله‌کننده می‌تواند با سوءاستفاده از این تأخیر، قبل از مطلع‌شدن سایرین، رفتار غیردرست‌کارانهٔ خود را ادامه دهد. این حمله که به تأخیر شهرت[3] [۲۲, ۴۲, ۴۳] معروف است، به‌طورعمومی به علت تأخیر در انتشار توصیه‌ها، در محیط‌های توزیع‌شده مانند شبکه‌های حس‌گر بی‌سیم است.

۳-۸- حملهٔ نوسان

در حملهٔ نوسان[4] [۴۴]، حمله‌کنندگان به دو گروه تقسیم می‌شوند. یک گروه رفتارهای غیردرست‌کارانه در پیش گرفته، درحالی‌که گروه دیگر رفتار درست‌کارانه از خود نمایش می‌دهد. گروه دوم که توانسته اعتماد سایرین را جلب کند با انتشار توصیه‌های نادرست سعی در خوشنام‌کردن گروه نخست می‌نماید. این فرآیند از کاهش سریع اعتماد به گروه غیردرست‌کار جلوگیری کرده و اجازه می‌دهد آنها مدت زمان طولانی‌تری را به رفتار خود ادامه دهند. هنگامی که دیگر ادامهٔ رفتار غیردرست‌کارانه ممکن نباشد، نقش دو گروه جابه‌جا می‌شود؛ شناسایی این حمله که یک حملهٔ گروهی است، بسیار مشکل است.

۳-۹- حمله RepTrap

در بسیاری از سامانه‌ها با تابعیت از رأی اکثریت، توصیه‌های نادرست شناسایی و پالایش می‌شوند، به این معنی که توصیه با مجموع بیشترین وزن، توصیهٔ درست در نظر گرفته شده و ملاک نادرستی بقیهٔ توصیه‌ها میزان اختلاف آنها با این توصیه است. وزن هر توصیه تابعی از میزان اعتماد به توصیه‌کننده است. در این‌گونه سامانه‌ها، حمله‌کنندگان می‌توانند با انتخاب هوشمندانه، موجودیت‌هایی که می‌توانند در آنها قانون اکثریت را بشکنند، نه تنها در بدنام‌کردن هدف خود موفق باشند، بلکه با شناساندن سایرین به‌عنوان اقلیت، وزن توصیه‌های آنان را نیز کاهش دهند. موجودیت‌های هدف که در این حمله *دام* (Trap) نامیده می‌شوند، موجودیت‌هایی هستند که حمله‌کنندگان قادرند توصیه‌های

[1] Discrimination Attacks
[2] Value Imbalance Attack
[3] Reputation Lag Attack
[4] Oscillation Attack

خود را در ارتباط با ایشان غالب (با بیشترین وزن) نمایند. حمله‌کنندگان یکی پس از دیگری با انتخاب دام‌های مختلف حملهٔ خود را گسترش می‌دهند. این فرایند به‌عنوان حملهٔ RepTrap [۴۵, ۴۶] نامیده می‌شود.

۴- ارزیابی استحکام سامانه‌های اعتماد با استفاده از شبیه‌سازی

حملات اعتماد، چالش امنیتی مهمی هستند که استحکام و کارآیی سامانه‌های اعتماد را نشانه رفته‌اند. پژوهش‌های مختلفی در زمینهٔ ارزیابی امنیتی این سامانه‌ها انجام شده است. همان‌طور که پیشتر اشاره شد، دو بستر اصلی جهت ارزیابی این سامانه‌ها شبیه‌سازی و وارسی هستند. در این بخش سعی شده تا مهم‌ترین پژوهش‌های انجام‌شده در بستر شبیه‌سازی مرور شوند. این پژوهش‌ها را می‌توان در سه دسته تقسیم کرد:

۱) پژوهش‌هایی که بدون ذکر صریح یک روش ارزیابی یا جزییات آن تنها به ارائه نتایج پرداخته‌اند.
۲) پژوهش‌هایی که سعی در ارائهٔ یک روش ارزیابی داشته‌اند.
۳) پژوهش‌هایی که جهت سهولت کار سایر پژوهش‌گران، ابزاری جهت ارزیابی سامانه‌های اعتماد و شهرت معرفی کرده‌اند.

در ادامه این سه دسته به‌ترتیب مرور و معرفی می‌شوند.

۴-۱- ارزیابی‌ها و نتایج منتشرشده

با توجه به اهمیت حملات در سامانه‌های اعتماد، پژوهش‌های بسیاری برای بررسی استحکام سامانه‌های موجود در مقابل حملات و انتشار نتایج آن ارائه شده است. این مقالات خود به دو گروه قابل تقسیم هستند: مقالات با دامنهٔ بررسی محدود و دامنهٔ فراگیر. دسته نخست، پژوهش‌هایی را شامل می‌شوند که تنها محدود به حمله، سامانه یا محیط خاصی هستند. به‌عنوان نمونه Shi [۴۷]، Chen [۴۸] و Perrone [۴۹] حمله روشن-خاموش را در شبکه‌های حس‌گر بی‌سیم بررسی کرده‌اند و یا توصیه‌های غیرصادقانه به عنوان یکی از حملات مهم در مقالات به صورت مجزا بررسی شده است [۵۰-۵۳]. برخی از مقالات به معرفی و تحلیل حملات جدید مانند RepTrap [۴۵, ۴۶]، RepHi [۵۴]، حمله تناوب (Oscillation) [۴۴] و Sybil [۴۰, ۵۵] پرداختند. دسته‌ای از مقالات تنها یک سامانه یا محیط خاص را مورد مطالعه قرار داده‌اند. بررسی سامانه شهرت Beta [۵۶]، PageRank [۵۷] نمونه‌هایی از این مقالات هستند. سامانه‌های تجاری مانند eBay توجه بسیاری از مقالات را به خود جلب کرده‌اند [۵۸-۶۰]. این موارد تنها نمونه‌هایی از این گروه از پژوهش‌ها هستند که با وجود فراوانی نسبی آنها، نتایج به دست آمده موردی بوده و قابل توسعه به سایر حملات یا سامانه‌ها نیستند.

دستهٔ دوم از پژوهش‌های این بخش، مقالاتی هستند که با هدف رسیدن به نتایج فراگیرتر، مستقل از سامانه یا حملهٔ خاص به بررسی بازهٔ گسترده‌تری از چالش‌ها پرداخته‌اند. Hoffman [۳۹] با در نظرگرفتن شباهت‌ها و تفاوت‌ها، یک طبقه‌بندی برای سامانه‌های اعتماد ارائه کرده و سپس استحکام آنها را علیه ۲۵ حملهٔ شناخته‌شده بررسی و مقایسه کرده است. Jøsang [۲۲] و Mármol [۶۱, ۶۲] نیز به روش مشابه، حملات را بررسی و دسته‌بندی کرده‌اند. Noorian [۶۳] با معرفی ویژگی‌هایی که آنها را خصیصه‌های نرم و سخت[1] نامیده، چارچوبی چندبعدی برای مقایسهٔ سامانه‌های اعتماد ارائه داده است. کار مشابهی نیز توسط Vavilis و همکاران با هدف دسته‌بندی نیازمندی‌های سامانه‌های اعتماد ارائه شده است [۶۴]. Koutrouli [۳۷] و Sun [۳۶] به مرور حملات مطرح و روش‌های مقابله با آنها پرداخته‌اند و سپس با بررسی روش‌های استفاده‌شده در سامانه‌های اعتماد، استحکام هر یک را ارزیابی کرده‌اند.

مقالات ذکرشده در اینجا تنها بخشی از مقالاتی هستند که به بررسی و ارزیابی حملات در سامانه‌های اعتماد پرداخته‌اند، هرچند که این مقالات روش و چارچوب ارزیابی خود را ذکر نکرده‌اند و تنها به ارائهٔ نتایج پرداخته‌اند. ارزیابی‌های ارائه‌شده اغلب کیفی بوده و به‌طورعمومی تنها به بررسی وجود داشتن یک سازوکار دفاعی یا ویژگی خاص اکتفا کرده‌اند (مانند [۳۹, ۶۳]). مقالات محدودی به ارائه نتایج عینی و عملی پرداخته‌اند، که در اغلب آنها نیز ذکری از جزئیات روش ارزیابی نشده است و تنها به ذکر استفاده از شبیه‌سازی یا مجموعهٔ دادهٔ خاصی اکتفا کرده‌اند. به‌عنوان نمونه در [۳۹] از عبارات «نیمه‌مستحکم» و «به‌طورکامل مستحکم» استفاده شده است که تعریف دقیقی از آنها ارائه نشده است. حتی مفاهیم اصلی مانند «مستحکم» و «آسیب‌پذیر» نیز بدون تعریف دقیق استفاده شده است [۶۲]. ابهام در تعاریف مفاهیم و حملات و همچنین

[1] Soft and Hard Features

روش‌های ارزیابی سبب شده حتی برخی از نتایج ارائه‌شده در مقالات با یکدیگر همخوانی نداشته باشند. به‌عنوان نمونه در مقاله Kerr و Cohen [۶۵] استحکام مدل Beta بیش از TRAVOS [۶۶] ارزیابی شده است، حال آنکه Zhang و همکاران در پژوهش خود [۴۱] نتیجه‌ای به‌طورکامل مخالف ارائه کرده‌اند. به‌عنوان نمونه‌ای دیگر، در یک مقاله استحکام سامانه‌های PowerTrust [۶۷] و EigenTrust [۳۱] معادل ارزیابی شده‌اند [۶۲]، درحالی‌که در دیگری PowerTrust سامانه مستحکم‌تری معرفی شده است [۳۹]. در آخر لازم است اضافه شود که اختلاف در تعاریف و عدم وجود روش استانداردی برای ارزیابی، اجازهٔ مقایسهٔ دقیق نتایج پژوهش‌ها را نمی‌دهد.

۴-۲- روش‌ها و معیارهای ارزیابی

در این بخش روش‌ها و معیارهای ارائه‌شده در پژوهش‌ها جهت ارزیابی سامانه‌های اعتماد مرور می‌شوند. روش‌های مورد اشاره در این بخش همگی در بستر شبیه‌سازی انجام می‌شوند (که همان‌طور که ذکر شد روش غالب در پژوهش‌هاست). به‌طورتقریبی تمامی این روش‌ها، سامانه را به‌صورتی محیطی شامل تعدادی گره درست‌کار و حمله‌کننده فرض می‌کنند که در آن هر گره درگیر همکاری یا انجام تراکنش با سایرین است [۳۶, ۳۸, ۴۱, ۴۲, ۶۸-۷۲]. محیط مجهز به یک سامانه محاسبهٔ اعتماد است که در تصمیم‌گیری صحیح و شناسایی حمله‌کنندگان به موجودیت‌های درست‌کار یاری می‌رساند. حمله‌کنندگان به دو صورت تصادفی و یا دارای نقشه مدل شده‌اند: در روش نخست، حمله‌کنندگان به‌صورت موجودیت‌های تصادفی تعریف می‌شوند که احتمال شکستن هنجارهای سامانه توسط آنها منطبق بر یک توزیع احتمالی است. به عنوان نمونه در پژوهش ارائه‌شده توسط Kerr [۴۲]، یک حمله‌کننده ممکن است با احتمال ۵۰٪ در یک تراکنش دیگری را فریب دهد. در روش دوم، حمله‌کنندگان نقشه حملهٔ از پیش تعیین شده دارند؛ که مشخص می‌کند در هر لحظه چگونه رفتار نمایند. به عنوان نمونه یک حمله‌کننده اگر به اعتمادی پایین‌تر از آستانه مشخص شده برسد، اقدام به ایجاد شناسهٔ جدیدی برای خود خواهد کرد.

گذشته از استفاده از بستر شبیه‌سازی برای ارزیابی، پژوهش‌ها نیازمند معیاری جهت بررسی نتایج و اندازه‌گیری استحکام سامانه هستند. در برخی از پژوهش‌ها این معیار به‌صورت کیفی (مستحکم، نیمه مستحکم و ضعیف) بیان شده است [۳۹, ۶۲]، حال آنکه در خود این مقالات نیز اذعان شده است که استحکام سامانه‌های اعتماد کیفی نبوده، بلکه کمّی[1] است.

مقالات مورد توجه به‌طورعمومی معیار کمّی و قابل مقایسه‌ای برای استحکام تعریف کرده‌اند. به‌عنوان نمونه برخی، تعداد تراکنش‌های موفق (درست‌کارانه) انجام‌شده را به‌عنوان معیار استحکام یک سامانه اعتماد در نظر گرفته‌اند [۶۹, ۷۳]. البته این معیار، معیار صحیحی نیست؛ چون حالات بسیاری را می‌توان تصور کرد که در آنها هدف حمله‌کننده انجام خدمت بدخواهانه نیست (مانند توصیه غیرصادقانه).

معیار دیگری که توسط مقالات تعریف و استفاده شده است، حداکثر تعداد حمله‌کنندگانی است که یک سامانه می‌تواند تحمل کند [۶۹]. گذشته از مبهم بودن مفهوم استفاده شده، این معیار وابسته به شرایط سامانه مانند تعداد موجودیت‌های درست‌کار، توزیع احتمالی رفتارها و همچنین تعریف آستانه تحمل یک سامانه است.

انحراف[2] در محاسبه مقادیر اعتماد نیز یکی دیگر از معیارهای اندازه‌گیری استحکام است [۳۶, ۶۹]. در این معیار سامانه یک‌بار بدون وجود حمله‌کنندگان و بار دیگر با وجود حمله‌کنندگان، شبیه‌سازی می‌شود و میانگین مقادیر اعتماد در هر حالت محاسبه می‌شود. معیار استحکام یک سامانه اختلاف بین این دو میانگین است که هر چه کوچکتر باشد، نشان‌دهندهٔ استحکام بیشتر سامانه است. این معیار هنگامی صحیح است که هدف حمله‌کننده تنها بدنام‌کردن یک موجودیت درست‌کار باشد. معیار مشابهی نیز توسط Jelenc و همکاران [۷۰] با نام دقت (Accuracy) استفاده شده است. در راهکار ارائه‌شده توسط ایشان، پیش از شبیه‌سازی، برای هر موجودیت مقدار واقعی توانایی وی تعیین شده و سپس مقادیر محاسبه‌شدهٔ اعتماد با توانایی ذاتی آنها مقایسه می‌شود. یک سامانه، هنگامی مستحکم است که مقادیر اعتماد به‌طوردقیق برابر با توانایی ذاتی افراد باشد. در این رویکرد رفتار هر فرد تابعی از توانایی وی است؛ در نتیجه روش پیشنهادشده توانایی مدل‌سازی حمله‌کنندگان هوشمند را ندارد. یک حمله‌کنندهٔ هوشمند می‌تواند بر حسب منفعت خود، رفتار درست‌کارانه یا بدخواهانه در پیش گیرد. البته این پژوهش معیار دیگری نیز با عنوان مطلوبیت

[1] Quantitative
[2] Bias

(Utility) معرفی می‌کند که با مقایسهٔ گرهٔ انتخاب‌شده جهت همکاری با بهترین گرهٔ ممکن به دست می‌آید. این معیار در صورتی بیشینه است که در هر تراکنش بهترین گرهٔ ممکن برای همکاری انتخاب شود. معیار مطلوبیت نیز از مفهوم توانایی ذاتی سود برده و بنابراین از مشکلی که در بالا ذکر شده رنج می‌برد.

Zhang و همکاران جهت بررسی حملات توصیه‌های غیرصادقانه، معیار استحکام یک سامانه اعتماد را اختلاف تعداد تراکنش‌های انجام‌شده توسط حمله‌کنندگان با تعداد تراکنش‌های انجام‌شده توسط درست‌کاران تعریف کرده‌اند [۴۱]. مقدار این معیار مستقل از کیفیت انجام خدمت است. درصورتی‌که یک حمله‌کننده برای مدتی تصمیم به انجام رفتار درست‌کارانه داشته باشد، معیار استحکام سامانه برابر با هنگامی است که وی رفتار بدخواهانه انجام می‌دهد. در این حالات معیار بالا فاقد اعتبار است.

MDP (Malicious Detection Performance) معیار دیگری است که برای استحکام سامانه‌های اعتماد تعریف شده است [۳۸, ۷۲, ۷۳]. فرض کنید D_i تعداد گره‌هایی باشد که گره i را به‌عنوان گرهٔ غیرقابل اعتماد شناسایی کرده باشند و M مجموعهٔ همهٔ حمله‌کنندگان باشد، آنگاه MDP به‌صورت زیر تعریف می‌شود:

$$\frac{\sum_{i\in M} D_i}{|M|} \qquad (۲)$$

این معیار به روش مشابه، مثبت کاذب[1] را نیز تعریف کرده است:

$$\frac{\sum_{i\in G} D_i}{|G|} \qquad (۳)$$

که در آن G مجموعه گره‌های درست‌کار است. استفاده از این معیار نیازمند تعریف مفهوم «غیرقابل اعتمادبودن» است که در برخی سامانه‌ها ممکن نیست. گذشته از این، حمله‌کننده می‌تواند با وجود انجام حملات، رفتار درست‌کارانه در پیش بگیرد (مانند حملات بدنام‌کردن). در این حالت معیار MDP کارآیی خود را از دست می‌دهد.

آخرین و البته مهم‌ترین معیار استفاده‌شده بر اساس پاداش دریافت‌شده توسط حمله‌کنندگان است [۴۲, ۶۵, ۶۹, ۷۴, ۷۵]. این معیار با الگوگرفتن از نظریه بازی‌ها، برای هر رفتار در سامانه پاداش و هزینه تعریف کرده است. استحکام یک سامانه وابسته به پاداش دریافت‌شده توسط حمله‌کنندگان است. در معیار پیشنهادشده، انگیزهٔ حمله‌کنندگان کسب بیشینهٔ سود تعریف می‌شود، بنابراین معیار بالا برخلاف سایر معیارها، امکان مدل‌سازی حالاتی را فراهم می‌آورد که در آن حمله‌کننده برای کسب سود بیشتر مجبور به رفتار درست‌کارانه می‌شود.

۴-۳- ابزارهای ارائه‌شده

گذشته از روش‌های موردی استفاده‌شده در مقالات، تنها راه قابل استفاده برای ارزیابی و مقایسهٔ استحکام سامانه‌های اعتماد، ابزارهای ارائه‌شده برای این منظور هستند. هرچند همهٔ این ابزارها مبتنی بر روش‌های شبیه‌سازی هستند. در این بخش مهم‌ترین ابزارهای ارائه‌شده در مقالات بررسی و مرور می‌شوند.

ART[2] [۷۵] مهم‌ترین و معروف‌ترین ابزار معرفی‌شده برای بررسی سامانه‌های اعتماد است. در این ابزار، سامانه اعتماد در یک محیط خرید و فروش قطعات هنری فرض شده است که در آن عامل‌ها از مقادیر اعتماد محاسبه‌شده، جهت تصمیم‌گیری برای خرید یا فروش یک قطعهٔ هنری استفاده می‌کنند. عامل‌ها در این محیط به دنبال افزایش سود خود بوده و ممکن است اقدام به فریب و کلاه‌برداری در معاملات کنند. ابزار با شبیه‌سازی این محیط و تخمین شناسایی عامل‌های فریب‌کار، امکان ارزیابی سامانه را فراهم می‌آورد. با وجود محدودیت‌های این ابزار که استفاده از آن را در بسیاری از مطالعات غیرممکن می‌سازد [۶۵, ۷۶]، این ابزار به‌عنوان یک تجربهٔ موفق در این زمینه بوده است. البته توسعه و پشتیبانی این ابزار از سال ۲۰۰۸ متوقف شده است.

TREET[3] ابزار دیگری است که به‌منظور غلبه بر محدودیت‌های ART ارائه شده است [۶۵]. ساختار این ابزار مشابه با ART بوده و با الگوگرفتن از آن سعی کرده تا با حفظ مزایا، محدودیت‌های موجود را برطرف سازد. این ابزار با اقبال چندانی مواجه نشد. پژوهش دیگری نیز از روش مشابه برای ارزیابی اعتماد در شبکه‌های نظیر به نظیر سود برده است [۷۷]، هرچند که نسخهٔ اجرایی ابزار، پیاده‌سازی نشده و یا در دسترس عموم قرار نگرفته است.

TRMSim-WSN[4] [۷۸] ابزاری دیگری است که با هدف ارزیابی سامانه‌های اعتماد در شبکه‌های حس‌گر بی‌سیم ارائه شده است. این ابزار چارچوبی برای شبیه‌سازی اعتماد در زبان Java ارائه کرده است که قابلیت ارزیابی و

[1] False Positive

[2] Agent Reputation and Trust Testbed

[3] Trust and Reputation Experimentation and Evaluation Testbed

[4] Trust and Reputation models Simulator for Wireless Sensor Networks

مقایسهٔ سامانه‌های مختلف را دارد. برخی سامانه‌ها و حملات از پیش در این ابزار تعبیه شده است که مدل‌ساز می‌تواند با دست‌کاری تنظیمات، نتایج شبیه‌سازی را مشاهده و مقایسه کند. افزودن سامانه یا حملهٔ جدید به ابزار، نیازمند کدنویسی و ارث‌بری از طبقه‌های پایه‌ای است که به همین منظور طراحی شده است.

ATB[1] [۷۰] آخرین ابزاری است که در این بخش معرفی می‌شود. این ابزار دو بهبود قابل توجه در این زمینه داشته است. نخست آنکه با تعریف دقیق سامانه و مفاهیم اعتماد، برخلاف پژوهش‌های قبلی ابهام تعاریف را از بین برده است. دوم آنکه ابزار ارائه‌شده با جداسازی محاسبهٔ اعتماد از فرآیند تصمیم‌گیری عامل‌ها، قادر است تنها به ارزیابی محاسبهٔ اعتماد مستقل از فرآیند تصمیم‌گیری بپردازد. البته با وجود نقاط قوت روش پیشنهادی، ابزار توانایی مدل‌سازی کامل حملات را ندارد. این ابزار دو معیار دقت و مطلوبیت را نیز جهت ارزیابی معرفی کرده که در بخش قبل مرور شد.

۵- چالش‌های موجود در ارزیابی سامانه‌های اعتماد

در بین پژوهش‌های فراوانی که در حیطهٔ ارزیابی امنیتی سامانه‌های اعتماد انجام شده است، مقالات به‌طورعمومی به بیان نتایج و نه روش پرداخته‌اند. معدود روش‌های ارائه‌شده نیز یا خاص‌منظوره هستند و یا از پشتوانهٔ تئوری قابل قبولی برخوردار نیستند. به‌طورتقریبی تمام ارزیابی‌های انجام‌شده از طریق شبیه‌سازی و بخش عمده آن توسط خود ارائه‌دهندگان مدل‌های اعتماد انجام شده است. ارزیابی یک مدل توسط ارائه‌دهندگان آن، ممکن است مطالعات و نمونه‌هایی را در برگیرد که نقص‌های مدل ارائه‌شده را بپوشاند و آن را برتر از آنچه به‌طورواقعی هست، نمایش دهد. این مشکل در مقالات نیز اشاره شده است [۲۲, ۷۹].

در شبیه‌سازی‌های انجام‌شده در پژوهش‌ها، حمله‌کنندگان به‌صورت بسیار ساده و پیش‌پا افتاده مدل‌سازی شده‌اند. حمله‌کنندگان اغلب رفتار ثابت و از پیش تعریف‌شده‌ای را انجام می‌دهند و یا در بهترین حالت به‌صورت یک موجود تصادفی و با احتمال رفتار غیردرست‌کارانه مدل شده‌اند. در این نوع مدل‌سازی، حمله‌کنندگان فاقد اراده و هوشمندی لازم هستند، درنتیجه نتایج ارزیابی‌ها محدود و غیرقابل تعمیم است. حتی با بررسی مجموعه‌ای از حملات شناخته‌شده و یا موجودیت‌های تصادفی نیز نمی‌توان استحکام یک سامانه را استنتاج کرد.

صرف نظر از مشکلات بالا، شبیه‌سازی موردی به ذات، دارای مشکلاتی است که سبب می‌شود استفاده و اجرای چندباره آن توسط سایر پژوهش‌گران به‌سادگی میسر نباشد. تعاریف مبهم، تنوع روش‌ها و ابزارها و عدم وجود معیاری مشترک بین پژوهش‌ها، سبب شده است تا مقایسهٔ شبیه‌سازی‌های انجام‌شده با یکدیگر امکان‌پذیر نباشد. اختلاف در برخی نتایج ارائه‌شده توسط مقالات، خود مؤید این نکته است. همچنین شبیه‌سازی خود روشی تخمینی است که تنها مسیرهای اجرایی محدود را می‌تواند تخمین (و نه تحلیل و اثبات) نماید.

Josang در مقالات خود [۲۲, ۷۹] به‌صراحت به این مشکل اشاره کرده است:

> *« ارزیابی مدل‌های اعتماد و شهرت شبیه به ارزیابی روش‌های امنیتی است. پژوهش‌گر برای ارائهٔ یک روش امنیتی جدید در کنفرانس‌های علمی لازم است آن را با استفاده از روش‌های استاندارد ارزیابی کند و تنها مقالاتی در چنین کنفرانس‌هایی پذیرفته می‌شود که روش خود را در مقابل حملات استاندارد ارزیابی کرده باشند. ... مدل‌های اعتماد و شهرت نیز به همین ترتیب پیش از ارائه می‌بایست با روش‌های قابل قبول ارزیابی و بررسی شوند... یک پیش‌نیاز مهم برای ارزیابی مدل‌های اعتماد، داشتن روش‌های مورد اطمینان برای ارزیابی است.»* [۲۲]

وی در ادامه به مشکلات روش‌های فعلی پرداخته و آنها را ناکافی و ناکارآمد دانسته و اشاره کرده که هیچ یک از روش‌های کنونی را نمی‌توان روش کامل و جامعی برای ارزیابی دانست. او مهم‌ترین پیش‌نیاز اعتبارسنجی سامانه‌های اعتماد را داشتن روشی مورد اطمینان برای این منظور می‌داند و سه راهکار کلی را برای این منظور پیشنهاد می‌دهد:

۱. **آزمایش تجربی**: صحت و استحکام سامانه‌های اعتماد را می‌توان از طریق پیاده‌سازی و آزمایش آنها در محیط‌های واقعی بررسی کرد. البته این محیط‌ها می‌بایست شامل گره‌های مستعد حمله نیز باشند، چون بررسی استحکام نیازمند حملات است. البته به این منظور نباید به یک محیط و یا

[1] Alpha TestBed

حمله خاص بسنده کرد. به‌منظور اطمینان لازم است محیط‌های مختلف و متفاوتی برای آزمایش انتخاب شود.

۲ . **ارزیابی توسط فرد بی‌طرف**: اگر فرد سومی که هیچ علاقه‌ای به شکست یا موفقیت سامانه مورد بررسی ندارد، با روش‌های تئوری، سامانه اعتماد را ارزیابی کند، نتایج وی می‌تواند در مجامع علمی قابل قبول باشد. Jøsang اشاره می‌کند که این‌گونه ارزیابی‌ها بسیار ارزشمند است.

۳ . **تولید یک روش اعتبارسنجی جامع**: به‌عنوان آخرین راهکار، Jøsang ذکر می‌کند درصورتی‌که روش استاندارد و قابل قبولی برای اعتبارسنجی سامانه‌های اعتماد تولید شود که صحت آن به‌صورت صوری و یا عملی اثبات شده باشد، می‌توان از آن برای اعتبارسنجی استفاده کرد. وی بیان می‌کند که فقط در این حالت نویسنده و طراح یک مدل، مجاز است که خود مدل خود را ارزیابی کند و نتایج می‌تواند قابل قبول باشد.

درعمل دو راهکار اول، امکان‌پذیر نیست؛ اما به راهکار سوم با ارائه روشی فراگیر و با پشتوانه تئوری کافی می‌توان دست یافت. خصوصیات و مزایای منحصر به فرد روش‌های وارسی صوری، این روش‌ها را به‌عنوان بهترین بستر برای ارائه یک روش جامع و فراگیر جهت ارزیابی استحکام سامانه‌های اعتماد معرفی می‌کنند.

۶- وارسی صوری استحکام سامانه‌های اعتماد

باید توجه داشت که شبیه‌سازی که اکنون روش مطرح در ارزیابی استحکام سامانه‌های اعتماد است، تنها می‌تواند رفتار یک سامانه را تنها در مسیرهای اجرای محدود یا تصادفی بررسی کند. شبیه‌سازی به‌عنوان یک روش تخمینی مطرح می‌شود به این معنی که نتایج می‌تواند دارای خطا باشد. در مقابل روش‌های وارسی صوری، قادر هستند با بررسی تمام مسیرهای ممکن اجرای سامانه، نتایج حاصل را تضمین کند. این روش‌ها دقیق و بدون خطا بوده و نتایج آن قابل اثبات هستند. با گسترش استفاده از سامانه‌های اعتماد (به‌ویژه در برخی از محیط‌های حساس)، نیاز به ارائهٔ روش‌های وارسی صوری در ارزیابی این سامانه‌ها روزبه‌روز بیشتر احساس می‌شود.

پژوهش‌های انجام‌شده در زمینه وارسی صوری استحکام سامانه‌های اعتماد، محدود و در مراحل نخستین هستند، هرچند روند رو به افزایش آنها در سال‌های اخیر نشان از توجه پژوهش‌گران به این چالش است. مؤلّفان این مقاله در پژوهش قبلی خود [۸۰] نشان داده‌اند که یک سامانه اعتماد را می‌توان با استفاده از شبکه‌های پتری رنگی[1] [۸۱] مدل کرد. در روش ارائه‌شده مقادیر اعتماد به‌عنوان نشانه‌های رنگی[2]، موجودیت‌ها به‌عنوان محل[3] و تراکنش بین موجودیت‌ها به‌عنوان انتقال[4] توصیف شده‌اند. هرچند روش ارائه‌شده اولیه بوده و قابل توسعه به سامانه‌های اعتماد در حالت کلی نیست. پژوهش دیگری نیز از شبکه‌های پتری برای مدل‌سازی صوری و سپس به‌دست آوردن مقدار بهینه طول زنجیره اعتماد در شبکه‌های متحرک اقتضایی سود جسته است [۸۲].

برخی از پژوهش‌ها با استفاده از ابزار PRISM[5] [۸۳] (که یک ابزار برای وارسی احتمالی مدل‌هاست)، به تعریف و سپس وارسی سامانه‌های اعتماد پرداخته‌اند [۵۶, ۸۴]. به این منظور یک سامانه اعتماد با استفاده از چارچوب ریاضی MDP[6] مدل شده است که در آن موجودیت‌های سامانه به‌صورت ماژول[7]، مقادیر اعتماد به‌عنوان متغیر و تراکنش بین موجودیت‌ها به دستور[8] نگاشت می‌شوند؛ سپس ویژگی‌های مورد نظر جهت وارسی با استفاده از منطق زمانی احتمالی[9] توصیف و مدل علیه آنها وارسی می‌شود. جلالی و همکارش [۵۶] همچنین از مفهوم پاداش[10] جهت توصیف بهتر ویژگی‌ها سود جسته‌اند. این پژوهش‌ها اگر چه نشان می‌دهد وارسی احتمال مدل می‌تواند در بررسی استحکام سامانه‌های اعتماد کاربرد داشته باشد، اما روش‌های ارائه‌شده محدود به مسائل ساده بوده و به‌عنوان یک روش عمومی وارسی استحکام قابل ارائه نیست. همچنین محدودیت‌های منطق وارسی احتمالی موجب شده تا روش‌ها فاقد قابلیت اندازه‌گیری قدرت یک حمله باشند و تنها به بررسی وجود یا احتمال برخی گزاره‌های منطقی محدود شوند.

Sassone و همکاران [۸۵] معیاری کمّی جهت مقایسهٔ دو

[1] Coloured Petri Nets
[2] Coloured Tokens
[3] Place
[4] Transition
[5] Probabilistic Symbolic Model Checker
[6] Markov Decision Process
[7] Module
[8] Command
[9] pCTL
[10] Reward

سامانه اعتماد بر پایهٔ قضیه بیز[1] ارائه داده‌اند. اساس این روش محاسبه مقدار $\mathcal{A}(y|X)$ است که به معنای احتمال مشاهده رفتار y توسط یک موجودیت به شرط آنکه تاریخچه رفتارهای قبلی وی X باشد. این احتمال توسط مدل محاسبه اعتماد $\mathcal{A}$ محاسبه می‌شود. پژوهش سپس با سودجستن از تئوری اطلاعات[2]، روشی برای مقایسه توزیع احتمالی به دست آمده از هر مدل با دیگری ارائه داده است. از آنجا که پایه روش ارائه‌شده قضیه بیز است، این روش برای مدل‌های محاسبه اعتماد مانند بتا مناسب است و نمی‌توان آن را برای هر مدلی استفاده کرد. همچنین در روش ایشان از سایر متغیرهای دیگر مانند توصیه صحبتی نشده است و به‌علاوه این روش توانایی در نظر گرفتن حمله را ندارد.

Herrmann [۸۶] از منطق زمانی اعمال[3] (TLA) سود جسته و با اضافه‌کردن مفاهیم لازم جهت محاسبه اعتماد، روش را جهت مدل‌سازی صوری سامانه‌های اعتماد بسط داده است. رویکرد به کار رفته مبتنی بر تعریف شئ‌گرای دنباله‌ای از فرآیندها و توصیف صوری آنهاست. این روش جهت پیاده‌سازی منطق ذهنی [۸۷] استفاده شده است. مشکل اساسی روش ارائه‌شده آن است که به‌سادگی قابل توسعه به سایر سامانه‌های اعتماد نیست و همچنین فاقد قابلیت مدل‌سازی حمله و حمله‌کننده است.

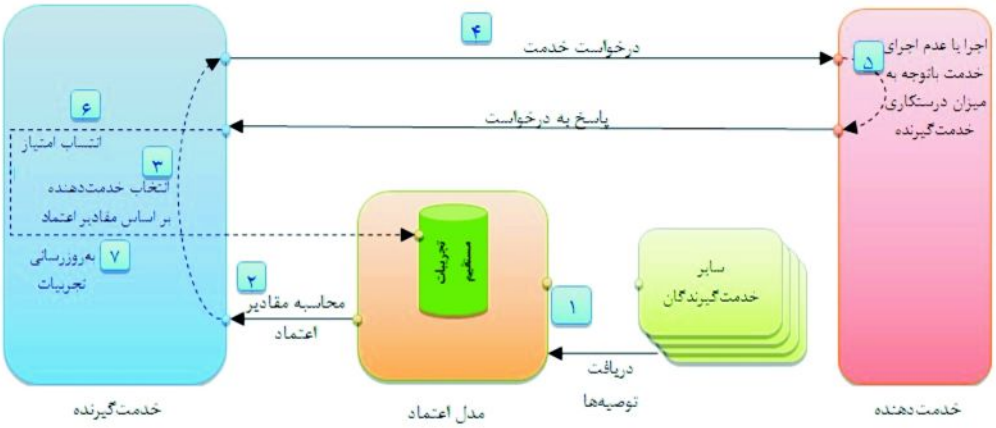
Muller [۸۸] یک چارچوب صوری برای تعریف اعتماد و روابط آن در یک محیط ارائه داده است. هدف وی از این چارچوب بیان دقیق و خوش‌ساخت سامانه اعتماد به‌گونه‌ای است که امکان استنتاج در آن فراهم باشد. وی جهت نمایش این توانایی، به بررسی برخی سامانه‌های نمونه و اثبات برخی گزاره‌ها در آنها پرداخته است. روش وی هرچند شامل توصیف صوری سامانه اعتماد است، اما همان‌طور که اشاره‌شده هدف از آن تعریف دقیق سامانه و نه وارسی علیه حملات بوده است. به همین جهت روشی جهت توصیف حمله ارائه نداده است. گذشته از آن مقدار اعتماد در این روش به‌صورت دوتایی (قابل اعتماد و غیر قابل اعتماد) مدل شده است که با واقعیت اکثر سامانه‌ها مطابقت ندارد. آخر آنکه این روش فاقد هر الگوریتم وارسی خودکار بوده و مفهوم زمان نیز در آن در نظر گرفته نشده است.

Muller و همکاران [۸۹] در پژوهش دیگری، با الگوگرفتن از شباهت بین استحکام سامانه‌های اعتماد و امنیت سامانه‌های رایانه‌ای، به تعریف نمادین سامانه اعتماد و استحکام آن پرداخته‌اند. با وجود ارائه مناسب تئوری لازم، به‌نظر می‌رسد روش ارائه‌شده به‌علت پیچیدگی بیش از حد، درعمل قابل استفاده نیست. این پژوهش هیچ مطالعهٔ موردی را نیز ارائه نداده است.

Wang و همکاران [۹۰] با استفاده از مفاهیم تئوری اطلاعات، بی‌نظمی و نشت اطلاعات نشان دادند که توصیه‌ای در سامانه اعتماد بد محسوب می‌شود که نشت اطلاعاتی کمی داشته باشد؛ سپس با در نظر گرفتن این مفهوم بدترین توصیه ممکن در یک سامانه اعتماد را محاسبه و اثبات کردند. ایشان همچنین با بررسی این توصیه در مدل‌های مختلف، روش جدیدی برای محاسبهٔ اعتماد جهت بهبود نقاط ضعف ارائه داده‌اند. نویسندگان در پژوهش دیگری [۹۱] با توسعهٔ روش قبلی، امکان بررسی نشت اطلاعات در حملات گروهی را نیز بررسی کرده‌اند و با استفاده از آن به مقایسه چهار دسته حمله اصلی در حملات گروهی توصیه‌های دروغین پرداخته‌اند. روش ایشان تنها حملات ارزیابی غیرصادقانه خدمت را در بر می‌گیرد و به سایر حملات مانند اجرای غیردرست‌کارانه خدمت قابل توسعه نیست. به‌علاوه رفتار حمله‌کننده در آن به‌صورت احتمالی توصیف‌شده است. مفهوم زمان نیز در این روش مدل نشده است که در نتیجه آن، متغیرهای وابسته به زمان مانند تاریخچه رفتار موجودیت‌ها از مدل حذف شده است. علاوه‌بر آن، این امر سبب شده است تا امکان بررسی دنباله‌ای از توصیه‌های دروغین فراهم نباشد. درعمل ممکن است یک حمله‌کننده با انتشار دنباله‌ای از توصیه‌های دروغین به هدف خود نائل آید، حال آنکه این روش فاقد قابلیت مدل‌سازی چنین حالتی است.

Aldini [۹۲] با توسعهٔ پژوهش قبلی خود [۸۴]، روشی صوری بر پایهٔ جبر فرآیندی[4] برای مدل‌سازی و وارسی سامانه‌های اعتماد ارائه داده است. این روش، روش کامل‌تری نسبت به روش‌های قبل از خود محسوب می‌شود. در این روش هر موجودیت به‌صورت یک فرایند مستقل توصیف شده که قابلیت تعامل با سایر فرآیندها را دارد؛ سپس با ترجمه این توصیف به سامانه تراکنش برچسب‌گذاری‌شده[5]، فضای حالت سامانه مدل می‌شود. پژوهش نشان می‌دهد که مدل حاصل، نمونه‌ای از سامانه انتقال کریپک[6] است و امکان وارسی با منطق زمانی را دارد. این روش اگر چه مبنای تئوری خوبی دارد، اما فضای حالت

[1] Bayes' theorem
[2] Information Theory
[3] Temporal Logic of Actions
[4] Process Algebra
[5] Labeled Transition System
[6] Kripke Transition System



(شکل ۲): نقش و نحوه تعامل خدمت‌دهندگان، خدمت‌گیرندگان و مدل محاسبه اعتماد با یکدیگر

و پیچیدگی آن بیش از حدی به‌نظر می‌رسد که درعمل قابل استفاده باشد. پژوهش نیز خود نمونهٔ اجراشده‌ای از آن را ارائه نداده است. مدل‌سازی نحوهٔ محاسبه اعتماد در این روش ساده‌انگارانه است. به‌عنوان نمونهٔ اعتماد تنها تابعی از مقدار قبلی آن و مشاهدهٔ اخیر در نظر گرفته شده است که درعمل قابلیت توصیف بسیاری از مدل‌های محاسبه اعتماد را که به تاریخچه کامل رفتار نیازمند هستند، ندارد. این امر از سوی دیگر با افزودن جدول اعتماد به فضای حالت، سامانه را مستعد انفجار فضای حالت کرده است. همچنین روش پیشنهادی فاقد معیاری جهت اندازه‌گیری قدرت حمله و استحکام سامانه است و تنها قابلیت بررسی برخی گزاره‌های منطقی تعریف شده را دارد.

جلالی و همکارش (مؤلفان این مقاله) در [۹۳, ۹۴] با تکمیل پژوهش‌های پیشین خود، روشی جهت وارسی استحکام سامانه‌های اعتماد در برابر حملات ارائه داده‌اند. روش پیشنهادی شامل چارچوب صوری به نام TRAP است که قابلیت مدل‌سازی سامانه اعتماد به همراه موجودیت‌های حمله‌کننده، توانایی‌ها و اهداف ایشان را دارد. در این سامانه اعتماد به‌صورت محیطی شامل مجموعه‌ای خدمت‌دهندگان و خدمت‌گیرندگان مدل شده است که به انجام تراکنش با یکدیگر می‌پردازند. هر خدمت‌دهنده و خدمت‌گیرنده ممکن است درست‌کار و یا حمله‌کننده باشد. جهت شناسایی موجودیت‌های حمله‌کننده، محیط به یک مدل محاسبه اعتماد مجهز شده است. مقادیر محاسبه‌شده توسط این مدل در اختیار موجودیت‌ها قرار گرفته و آنها جهت تصمیم‌گیری و شناسایی حمله‌کنندگان از این مقادیر استفاده می‌کنند.

شکل ۲ نحوهٔ تعامل خدمت‌دهندگان و خدمت‌گیرندگان و نقش مدل محاسبه اعتماد در این تعامل را نشان می‌دهد.

TRAP قادر است یک سامانه اعتماد را در سه بخش به‌صورت نمادین مدل کند که به‌ترتیب شامل مدل محاسبهٔ اعتماد، مدل موجودیت‌های درست‌کار و مدل حمله‌کنندگان است. رفتار پویای مدل TRAP به واسطه ترجمه آن به چارچوب ریاضی POMDP تعریف شده است. این چارچوب جهت مدل‌سازی تصمیم‌گیری یک عامل در محیط احتمالی و با مشاهدات محدود استفاده می‌شود. در ترجمه بین TRAP و این چارچوب، حمله‌کنندگان در نقش عامل‌هایی ظاهر می‌شوند که قصد انتخاب بهترین فعالیت جهت آسیب‌رساندن حداکثری به سامانه را دارند؛ درحالی‌که ممکن است مشاهدات آنها از محیط و تراکنش‌های آن به‌صورت محدود باشد. حمله‌کنندگان به‌ازای هر فعالیت غیردرست‌کارانه پاداش دریافت می‌کنند که مجموع این پاداش‌ها نشان‌دهنده موفقیت ایشان در فرآیند حمله است. براساس مقدار پاداش دریافت‌شده در طی یک حمله و نسبت آن به پاداش حداکثر و پاداش عادی (بدون اجرای حمله)، معیاری جهت اندازه‌گیری استحکام یک سامانه اعتماد ارائه شده است که هر چه پایین‌تر باشد، نشان‌دهنده موفقیت بیشتر حمله‌کنندگان در نیل به اهدافشان است و آسیب‌پذیری بیشتر سامانه را نشان می‌دهد. در پژوهش اثبات شده است که معیار پیشنهادی در درازمدت مستقل از تعداد مراحل اجرای سامانه بوده و به مقداری ثابت همگراست. این خصوصیت از آن جهت حائز اهمیت است که وارسی صوری، مستعد انفجار فضای حالت است و در بسیاری

از مطالعات بررسی عملی یک سامانه در تعداد مراحل بالا امکان‌پذیر نیست. خصوصیت اثبات‌شده نشان می‌دهد وارسی یک سامانه در کوتاه‌مدت می‌تواند استحکام آن را در درازمدت نیز نمایش دهد. همچنین در روش پیشنهادی برای نخستین‌بار مفهوم بدترین حمله ممکن علیه یک سامانه (که مهم‌ترین مزیت روش‌های صوری است) تعریف و محاسبه شده است. در این پژوهش‌ها همچنین با معرفی دو ابزار RepSyFire [۹۵] و TruSyFire [۹۶] به‌ترتیب جهت وارسی سامانه‌های محاسبه شهرت و سامانه‌های محاسبه اعتماد، امکان استفاده عملی از روش پیشنهادی را در اختیار سایر پژوهش‌گران قرار داده است.

۷- نتیجه‌گیری

در این مقاله حملات اعتماد، به‌عنوان مهم‌ترین چالش امنیتی سامانه‌های اعتماد بررسی شدند. حملات اعتماد، دنباله‌ای از رفتارهای ریاکارانه با هدف گمراه‌سازی سامانه اعتماد هستند که تهدیدی برای استحکام و قابلیت اطمینان سامانه محسوب می‌شوند. پس از مروری بر حملات شناخته‌شده، پژوهش‌های انجام‌شده با هدف ارزیابی امنیتی سامانه‌های اعتماد بررسی شدند. شبیه‌سازی و وارسی، دو بستر اصلی در روش‌های ارزیابی هستند. پژوهش‌های بسیاری نیز در زمینه ارزیابی استحکام سامانه‌های اعتماد با استفاده از شبیه‌سازی منتشر شده است؛ اما به‌اختصار همه این موارد از چند جهت ضعف دارند. نخست آنکه در ارزیابی‌های انجام‌شده حمله‌کنندگان به‌طورعمومی شخصیت‌های ساده و یا ثابتی دارند و بر اساس یک نقشهٔ از پیش تعریف‌شده و بدون هوشمندی عمل می‌کنند و یا در بهترین حالت، رفتارهای احتمالی دارند. مشکل دوم و مهم‌تر آن است که شبیه‌سازی هرچند روش شناخته‌شده و در دسترسی است، اما خود با محدودیت‌هایی همراه بوده که امکان مقایسه، اثبات و تضمین نتایج را فراهم نمی‌آورد. در مقابل، روش‌های وارسی، روش‌های تحلیل دقیق سامانه هستند که بررسی صحّت سامانه را در همهٔ مسیرهای اجرای ممکن تضمین می‌کند. پژوهش‌های انجام‌شده در زمینه وارسی صوری استحکام سامانه‌های اعتماد، هرچند در سال‌های اخیر رو به رشد بوده‌اند، اما در مراحل نخستین پژوهش هستند و استفاده از آنها در حال حاضر هنوز فراگیر نشده است، هرچند با توجه به اهمیت سامانه‌های اعتماد، نیاز به چنین روشی وجود داشته و در پژوهش‌ها نیز مورد اشاره قرار گرفته است. این روش‌ها به همراه نقاط ضعف و قوت هر یک در این مقاله مرور و بررسی شده‌اند.

۸- مراجع

[1] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, pp. 618-644, 2007.

[2] J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models," Artificial Intelligence Review, vol. 24, pp. 33-60, 2005.

[3] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), 2007, pp. 25-25.

[4] D. Artz and Y. Gil, "A survey of trust in computer science and the Semantic Web," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 5, pp. 58-71, 2007.

[5] Y. Zhang, H. Chen, and Z. Wu, "A social network-based trust model for the semantic web," presented at the Proceedings of the Third international conference on Autonomic and Trusted Computing, 2006.

[6] J. Golbeck, "Trust on the world wide web: a survey," Foundations and Trends in Web Science, vol. 1, pp. 131-197, 2006.

[7] F. Gomez Marmol, M. Gil Perez, and G. Martinez Perez, "Reporting Offensive Content in Social Networks: Toward a Reputation-Based Assessment Approach," Internet Computing, IEEE, vol. 18, pp. 32-40, 2014.

[8] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proceedings of the IEEE, vol. 98, pp. 1755-1772, 2010.

[9] M. C. Fernandez-Gago, R. Roman, and J. Lopez, "A survey on the applicability of trust management systems for wireless sensor networks," in Third International Workshop on Security, Privacy and Trust in

Pervasive and Ubiquitous Computing (SECPerU), 2007, pp. 25-30.

[10] I. Pinyol and J. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems :a review," Artificial Intelligence Review, vol. 40, pp. 1-25, 2013/06/01 2013.

[11] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," Communications Surveys & Tutorials, IEEE, vol. 13, pp. 562-583, 2011.

[12] G .Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 318-328, 2006.

[13] H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," Security & Privacy, IEEE, vol. 2, pp. 28-39, 2004.

[14] E. Cody, R. Sharman, R. H. Rao, and S. Upadhyaya, "Security in grid computing: A review and synthesis," Decision Support Systems, vol. 44, pp. 749-764, 2008.

[15] J. D. Sonnek and J. B. Weissman" ,A quantitative comparison of reputation systems in the grid," in Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, 2005, pp. 242-249.

[16] M. G. Pérez, J. E. Tapiador, J. A. Clark, G. M. Pérez, and A. F. S. Gómez, "Trustworthy placements: Improving quality and resilience in collaborative attack detection," Comput. Netw., vol. 58, pp. 70-86, 2014.

[17] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Trust Management and Admission Control for Host-Based Collaborative Intrusion Detection," J. Netw. Syst. Manage., vol. 19, pp. 257-277, 2011.

[18] D. N. Yost, "Email Filtering Using Relationship and Reputation Data," ed: Go-ogle Patents, 2010.

[19] H. Xu, D. Liu, H. Wang, and A. Stavrou, "E-commerce Reputation Manipulation: The Emergence of Reputation-Escalation-as-a-Service," presented at the 24th International World Wide Web Conference (WWW 2015), Italy, 2015.

[20] L. Rasmusson and S. Jansson, "Simulated social control for secure Internet commerce," in Proceedings of the 1996 workshop on New security paradigms, Lake Arrowhead, California, United States, 1996, pp. 18-25.

[21] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards Robust and Effective Trust Management for Security: A Survey," in The 13th IEEE International Conference on Trust ,Security and Privacy in Computing and Communications (IEEE TrustCom-14), Beijing, China, 2014.

[22] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in the 5th International Workshop on Security and Trust Management (STM 2009 ,(Saint Malo, France, 2009, pp. 60-64.

[23] D. Gambetta, Trust: Basil Blackwell, Oxford, 1990.

[24] T. Grandison and M. Sloman, "A survey of trust in internet applications," Communications Surveys & Tutorials, IEEE, vol. 3, pp. 2-16, 2000.

[25] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organiz-ational trust," Academy of management review, vol. 20, pp. 709-734, 1995.

[26] L. Liu and W. Shi, "Trust and reputation management," Internet Computing, IEEE, vol. 14, pp. 10-13, 2010.

[27] eBay. Feedback scores, stars, and your reputation. Available: http://pa-ges.ebay.com/help/feedback/scores-reputation.html, (Accessed: 2014 Sep.).

[28] J. Sabater and C. Sierra, "Social ReGreT, a reputation model based on social relations," ACM SIGecom Exchanges, vol. 3, pp. 44-56, 2001.

[29] J. Sabater and C. Sierra, "REGRET: reputation in gregarious societies," in Proceedings of the fifth international conference on Autonomous agents, Montreal, Quebec, Canada, 2001, pp. 194-195.

[30] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Advanced Communications and Multimedia Security IFIP, Slovenia, 2002, pp. 107-121.

[31] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina" ,The eigentrust algorithm for reputation management in p2p networks," in Proceedings of the 12th international conference on World Wide Web, Budapest, Hungary, 2003, pp. 640-651.

[32] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank citation ranking: Bringing order to the web," 1999.

[33] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in Proc. of the first international joint conference on Autonomous agents and multiagent systems: part 1, Bologna, Italy, 2002 ,pp. 294-301.

[34] H. E. Kyburg Jr, "Bayesian and non-Bayesian evidential updating," Artificial Intelligence, vol. 31, pp. 271-293, 1987.

[35] A. Jøsang and R. Ismail, "The beta reputation system," in Proceedings of the 15th Bled Electronic Commerce Conference, 2002, pp. 41-55.

[36] Y. L. Sun and Y. Liu, "Security of Online Reputation Systems: Evolution of Attacks and Defenses," vol. 29, pp. 87-97, 2012.

[37] E. Koutrouli and A. Tsalgatidou, "Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers," Computer Science Review, vol. 6, pp. 47-70, 2012.

[38] Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, "Attacks on trust evaluation in distributed networks," in Information Sciences and Systems, 2006 40th Annual Conference on, 2006, pp. 1461-1466.

[39] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surv., vol. 42, pp. 1-31, 2009.

[40] J. Douceur, "The sybil attack," in Peer-to-Peer Systems .vol. 2429, ed: Springer Berlin / Heidelberg, 2002, pp. 251-260.

[41] L. Zhang, S. Jiang, J. Zhang, and W. K. Ng, "Robustness of Trust Models and Combinations for Handling Unfair Ratings," Trust Management VI, vol. 374, pp. 36-51, 2012.

[42] R. Kerr and R. Cohen, "Smart cheaters do prosper: defeating trust and reputation systems," in The 8th International Conference on Autonomous Agents and Multiagent Systems, Budapest, Hungary, 2009, pp. 993-1000.

[43] P. Herbig and J. Milewicz, "The relationship of reputation and credibility to brand success," Journal of Consumer Marketing, vol. 12, pp. 5-10, 1995.

[44] M. Srivatsa, L. Xiong, and L. Liu, "TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks," in Proceedings of the 14th international conference on World Wide Web, 2005, pp. 422-431.

[45] Y. Yang, Q. Feng, Y. Sun, and Y. Dai, "Reputation trap: An powerful attack on reputation system of file sharing p2p environment," in the 4th International Conference on Security and Privacy in Communication Networks, Istanbul, Turkey, 2008.

[46] Y. Yang, Q. Feng, Y. L. Sun, and Y. Dai, "Reptrap: a novel attack on feedback-based reputation systems," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008, p. 8.

[47] P. Shi and H. Chen, "RASN: Resist on-off Attack for Wireless Sensor Networks," in Proceedings of the 2012 International Conference on Computer Application and System Modeling, 2012.

[48] S. Chen, Y. Zhang, P. Liu ,and J. Feng, "Coping with Traitor Attacks in Reputation Models for Wireless Sensor Networks," 2010, pp. 1-6.

[49] L. F. Perrone and S. C. Nelson, "A study of on-off attack models for wireless ad hoc

networks," in 1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks,, 2006, pp. 1-10.

[50] Y.-F. Yang, Q.-Y. Feng, Y. Sun, and Y.-F. Dai, "Dishonest Behaviors in Online Rating Systems: Cyber Competition, Attack Models, and Attack Generator," Journal of Computer Science and Technology, vol. 24, pp. 855-867, 2009.

[51] S. Chen, Y. Zhang, Q. Liu, and J. Feng, "Dealing with dishonest recommendation: The trials in reputation management court," Ad Hoc Networks.

[52] Y. Yang, Y. L. Sun, S. Kay, and Q. Yang, "Defending online reputation systems against collaborative unfair raters through signal modeling and trust," in Proceedings of the 2009 ACM symposium on Applied Computing, 2009, pp. 1308-1315.

[53] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, and M. Gonçalves, "Detecting spammers and content promoters in online video social networks," in Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval, Boston, USA, 2009, pp. 620-627.

[54] J. Feng, Y. Zhang, S. Chen, and A. Fu, "RepHi: A novel attack against P2P reputation systems," in Computer Communications Workshops (INFOCOM WKSHPS), 2011, pp. 1088-1092.

[55] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the sybil attack," University of Massachusetts Amherst, Amherst ,MA, 2006.

[56] A. J. Bidgoly and B. T. Ladani, "Quantitative verification of beta reputation system using PRISM probabilistic model checker," in Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on, 2013, pp. 1-6.

[57] A. Clausen, "The cost of attack of PageRank," in Proceedings of The International Conference on Agents Web Technologies and Internet Commerce (IAWTIC'2004), Gold Coast, 2004.

[58] F. Dini and G. Spagnolo, "Buying reputation on eBay: Do recent changes help?," International Journal of Electronic Business, vol. 7, pp. 581-598, 2009.

[59] P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood, "The value of reputation on eBay: A controlled experiment," Experimental Economics, vol. 9, pp. 79-101, 2006.

[60] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," The Economics of the Internet and E-Commerce, vol. 11, pp. 127-157, 2002.

[61] F. Gómez Mármol and G. Martínez Pérez, "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems," Computer Standards and Interfaces, vol. 32, pp. 185-196, 2010.

[62] F. G. Mármol and G. M. Pérez, "Security threats scenarios in trust and reputation models for distributed systems," Computers and Security, vol. 28, pp. 545-556, 2009.

[63] Z. Noorian and M. Ulieru, "The state of the art in trust and reputation systems: A framework for comparison," Journal of theoretical and applied electronic commerce research ,vol. 5, pp. 97-117, 2010.

[64] S. Vavilis, M. Petković, and N. Zannone, "A reference model for reputation systems," Decision Support Systems, vol. 61, pp. 147-154, 5// 2014.

[65] R. Kerr and R. Cohen, "TREET: the Trust and Reputation Experimentation and Evaluation Testbed," Electronic Commerce Research, vol. 10, pp. 271-290, 2010.

[66] W. T. L. Teacy, J. Patel, N. Jennings, and M. Luck, "TRAVOS: Trust and Reputation in the Context of Inaccurate Information Sources," Autonomous Agents and Multi-Agent Systems, vol. 12, pp. 183-198, 2006.

[67] A. Rahbar and O. Yang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 460-473, 2007.

[68] Y. L. Sun and Y. Yang, "Trust establishment in distributed networks: Analysis and modeling," in Communications, 2007. ICC'07. IEEE International Conference on, 2007, pp. 1266-1273.

[69] A. Schlosser, M. Voss, and L. Brückner, "On the simulation of global reputation systems," Journal of Artificial Societies and Social Simulation, vol. 9, 2006.

[70] D. Jelenc, R. Hermoso, J. Sabater-Mir, and D. Trček, "Decision making matters: A better way to evaluate trust models," Knowledge-Based Systems, vol. 52, pp. 147-164, 2013.

[71] R. de Oliveira Albuquerque, F. F. Cohen, J. Mota, and R. T. de Sousa, "Analysis of a Trust and Reputation Model Applied to a Computational Grid Using Software Agents," in Convergence and Hybrid Information Technology, 2008. ICHIT '08. International Conference on, 2008, pp. 196-203.

[72] Y. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in IEEE INFOCOM, 2006, pp. 230-236.

[73] Y. Sun, Z. Han, and K. J. R .Liu, "Defense of trust management vulnerabilities in distributed networks," Communications Magazine, IEEE, vol. 46, pp. 112-119, 2008.

[74] R. Kerr and R. Cohen, "An experimental testbed for evaluation of trust and reputation systems," Trust Management III, pp. 252-266, 2009.

[75] K. K. Fullam, T. B. Klos, G. Muller, J. Sabater, A. Schlosser, Z. Topol, et al., "A specification of the Agent Reputation and Trust (ART) testbed: experimentation and competition for trust in agent societies," in Proc. of the 4th international joint conference on Autonomous agents and multiagent systems, The Netherlands, 2005, pp. 512-518.

[76] P. Chandrasekaran, "A Testbed for Evaluating Computational Trust Models," Carleton University, 2012.

[77] P. Chandrasekaran and B. Esfandiari, "A Model For A Testbed For Evaluating Reputation Systems," 2011, pp. 296-303.

[78] F. G. Marmol and G. M. Perez, "TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks," in Communications, 2009. ICC '09. IEEE International Conference on, 2009, pp. 1-5.

[79] A. Jøsang, "Robustness of Trust and Reputation Systems: Does it Matter?," in International Conference on Trust Management (IFIPTM 2012). Surat, India, 2012, pp. 253-262.

[80] A. Jalaly Bidgoly and B. Tork Ladani, "Trust modeling and verification using Colored Petri Nets," in 8th International ISC Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 2011, pp. 1-8.

[81] K. Jensen, Coloured Petri nets: basic concepts, analysis methods and practical use vol. 1: Springer Science & Business Media, 2013.

[82] J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," Journal of Network and Computer Applications, vol. 35, pp. 1001-1012 ,2012.

[83] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM 4.0: Verification of probabilistic real-time systems," in Computer Aided Verification, 2011, pp. 585-591.

[84] A. Aldini, "Formal Approach to Design and Automatic Verification of Cooperation-Based Networks," International Journal On Advances in Internet Technology, vol. 6, pp. 42-56, 2013.

[85] V. Sassone, K. Krukow, and M. Nielsen, "Towards a formal framework for computational trust," in Formal Methods for Components and Objects, 2007, pp. 175-184.

[86] P. Herrmann, "Temporal Logic-Based Specification and Verification of Trust Models Trust Management." vol. 3986, K. Stølen, W. Winsborough, F. Martinelli, and

F. Massacci, Eds., ed: Springer Berlin / Heidelberg, 2006, pp. 105-119.

[87] A Jøsang, "Subjective logic," Book Draft, 2011.

[88] T. Muller, "Semantics of Trust," in Formal Aspects of Security and Trust, 2011, pp. 141-156.

[89] T. Muller, Y. Liu, S. Mauw, and J. Zhang, "On robustness of trust systems," in 8th International Conference on Trust Management (IFIPTM'14), Singapore, 2014, pp. 44-60.

[90] D. Wang, T. Muller, A. A. Irissappane, J. Zhang, and Y. Liu, "Using information theory to improve the robustness of trust systems," in Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, 2015, pp. 791-799.

[91] D. Wang, T. Muller, J. Zhang, and Y. Liu, "Quantifying Robustness of Trust Systems against Collusive Unfair Rating Attacks Using Information Theory," in Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, 2015, pp. 1997-1998.

[92] A. Aldini, "Modeling and verification of trust and reputation systems," Security and Communication Networks, 2015.

[93] A. Jalaly Bidgoly and B. Tork Ladani, "Modelling and Quantitative Verification of Reputation Systems Against Malicious Attackers," The Computer Journal, vol. 58, pp. 2567-2582, 2015.

[94] A. Jalaly Bidgoly and B. Tork Ladani, "Modeling and Quantitative Verification of Trust Systems against Malicious Attackers," The Computer Journal, Accepted, In Press.

[95] RepSyFire: Reputation System Verifier. Available: http://eng.ui.ac.ir/~ladani/CTLab, (Accessed: 2015).

[96] TruSyFire: Trust Systems Verifier. Available: http://eng.ui.ac.ir/~ladani/CTLab, (Accessed: 2015.(

امیر جلالی بیدگلی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر (نرم افزار) به ترتیب در سال ۱۳۸۵ در دانشگاه کاشان و ۱۳۸۸ در دانشگاه علم و صنعت ایران به پایان رساند و هم‌اکنون دانشجوی دکترای مهندسی کامپیوتر (نرم‌افزار) در دانشکده کامپیوتر دانشگاه اصفهان است. زمینه‌های تحقیقاتی مورد علاقه وی مشتمل بر اعتماد محاسباتی، امنیت نرم‌افزار، توصیف و وارسی صوری و مدلسازی و شبیه‌سازی است. از وی مقالاتی در مجلات و کنفرانس‌های داخلی و بین‌المللی در حوزه‌های فوق به چاپ رسیده است.

بهروز ترک لادانی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر (نرم افزار) به ترتیب در سال ۱۳۷۵ در دانشگاه اصفهان و ۱۳۷۷ در دانشگاه صنعتی امیر کبیر به پایان رساند و سپس مدرک دکترای خود را در سال ۱۳۸۳ در رشته مهندسی کامپیوتر (سیستم های نرم افزاری) از دانشگاه تربیت‌مدرس اخذ نمود. وی از سال ۱۳۸۴ به عضویت هیئت علمی دانشگاه اصفهان درآمد و هم اکنون دانشیار گروه مهندسی نرم افزار این دانشگاه است. ایشان همچنین عضو پیوسته انجمن رمز ایران بوده و در حال حاضر عضو شورای اجرایی و نماینده این انجمن در دانشگاه اصفهان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه دکتر لادانی مشتمل بر توصیف و وارسی صوری امنیت، پروتکل های رمزنگاری، اعتماد محاسباتی و امنیت نرم افزار است.