مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال پنجم، شماره ۲، تابستان ۱۳۹۳؛ ص ۱۰۶-۹۳

یک مدل اعتماد تحمل‌کننده رفتار کاربران بدخواه

زهرا ناظمیان[۱]، محمّد عبداللهی ازگمی[۲*]

۱- دانشجوی کارشناسی ارشد ۲- دانشیار دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران

(دریافت: ۹۲/۱۰/۲۰، پذیرش: ۹۳/۰۶/۱۷)

چکیده

امروزه با وجود سازوکارهای دفاعی و روش‌های درستی‌یابی، درصدی از آسیب‌پذیری‌های امنیتی در سامانه‌ها باقی می‌ماند. بنابراین، محافظت از سامانه‌ها در برابر تمامی رفتارهای بدخواهانه و حملات امنیتی تقریباً غیرممکن است. اگر اقدامات لازم برای مقابله با تأثیرات طیف گسترده‌ای رفتارهای بدخواهانه بر روی سامانه به کار گرفته نشود، منجر به نفوذ و نقض ویژگی‌های امنیتی سامانه خواهند شد. سامانه‌های تحمل‌پذیر نفوذ برای افزایش امنیت سامانه‌ها و نرم‌افزارها مورد استفاده قرار می‌گیرند. در نظرگرفتن مفهوم اعتماد بین موجودیت‌ها می‌تواند نقش مهمی در افزایش امنیت در محیط‌های توزیع‌شده نظیر اینترنت ایفا نماید. اما، اعتماد هم مانند سایر راه‌حل‌های امنیتی در برابر حملات بدخواهانه، آسیب‌پذیر است. بنابراین ضرورت ایجاد روش‌هایی برای مقابله با رفتارهای بدخواهانه همچنان از اهمیت بالایی برخوردار است. در این مقاله رهیافتی مبتنی بر اعتماد برای تحمل‌پذیر کردن نرم‌افزارها در برابر نفوذ با رویکرد نسبی بودن مفهوم اعتماد ارائه شده است. از این‌رو، دقت مقادیر اعتماد کاربران به یکدیگر در کل سامانه افزایش یافته و این مقادیر به مقدار واقعی آن‌ها نزدیک‌تر شده است. هدف از ارائه این روش، حل چالش مطلق در نظرگرفتن اعتماد و مقاوم ساختن سامانه‌ها در برابر رفتارهای بدخواهانه با تشخیص و تعدیل نظرات واقعی و غیرواقعی کاربران است. نتایج حاصل از شبیه‌سازی روش پیشنهادی نشان می‌دهد که این روش، مجوز افزایش اعتماد ناعادلانه را به نفوذگران نمی‌دهد و در مقابل رفتارهای بدخواهانه و مخرب مقاوم است. همچنین افزودن مفهوم نسبی بودن به اعتماد و تشخیص کاربران بدخواه سبب بهبود روش پیشنهادی نسبت به روش‌های قبلی شده است.

کلید واژه‌ها: امنیت، اعتماد، رفتارهای بدخواهانه، تحمل‌پذیری نفوذ.

A Trust Model Tolerating the Behavior of Malicious Users

Z. Nazemian, M. Abdollahi Azgomi*

School of Computer Engineering, Iran University of Science and Technology

(Received: 10/01/2014; Accepted: 08/09/2014)

Abstract

Nowadays, in spite of the presence of defence mechanisms and verification methods, parts of the security vulnerabilities still remain in systems. Therefore, protection of systems against all malicious behaviors and security attacks is nearly impossible. If the required countermeasures are not employed against the impacts of malwares, they may lead to intrusion and the violation of system security policies. On the other hand, intrusion-tolerant systems are used to increase the security of systems and software. Consideration of the trust concept among the entities can play an important role to increase the security in distributed environments such as Internet. However, like other security mechanisms, trust is vulnerable to malicious attacks. Therefore, devising methods against malicious behaviors are very important. In this paper, a trust-based approach for tolerating software against intrusion with emphasis to the relativity of trust concept is presented. So that, the precision of trust values for users in the whole system is increased, such that these values are closed to real values. The goal of the proposed approach is to diminish the challenges of absolute trust in order to make systems resilient against malicious behaviors through detecting real and non-real ideas of users and balancing them. The simulation results show that the proposed approach does not allow intruders to increase trust values unfairly and it is resilient against malicious and destructive behaviors. Furthermore, the addition of relativity to trust concept and the detection of malicious users lead to the improvement of the recommended method, comparing to the existing methods.

Keywords: Security, Trust, Malicious Behaviors, Intrusion-Tolerance.

* Corresponding Author E-mail: azgomi@iust.ac.ir

۱. مقدمه

با گذشت زمان از آنجا که خطاها فقط شامل خطاهای غیرعمدی[1] نبوده و با وجود انواع تکنیک‌ها و سازوکارها همواره سامانه‌ها در برابر حملات پیشرفته و جدیدی قرار می‌گیرند و محافظت از آن‌ها در برابر تمامی حملات بدخواهانه[2] غیرممکن خواهد بود، به تدریج در دهه‌های اخیر مباحث مربوط به تحمل‌پذیری نفوذ[3] نیز مطرح شد؛ و به عنوان یک راه‌حل مؤثر برای ایجاد سامانه‌های امن به‌کار گرفته شد که بیانگر این موضوع است که علی‌رغم وجود حملات و خطرات بدخواهانه و عمدی[4]، سامانه با فعال‌سازی یک سازوکار قادر به جلوگیری از نفوذ و تولید یک سامانه امن در برابر خرابی[5] باشد [۱ و ۲]. سامانه‌های تحمل‌پذیر نفوذ به طور قابل ملاحظه‌ای برای افزایش امنیت نرم‌افزارها مورد استفاده قرار می‌گیرند و این سامانه‌ها در حال حاضر در برقراری امنیت نقشی کلیدی ایفا می‌کنند [۳]. مفهوم اعتماد[6] رویکردی است که اخیراً در این حوزه وارد شده است و اهمیت این مسئله را دوچندان کرده است. اعتماد یک مفهوم رایج در زندگی بشر است. همان‌طور که فناوری‌ها رشد می‌کنند و موقعیت‌های جدیدی را ایجاد می‌کنند، به موازات آن تهدیدهایی[7] وجود دارند که مانع رشد کامل و کارایی آن‌ها می‌شوند. سامانه‌های مبتنی بر اعتماد هم از این موضوع جدا نیستند و با رشد و استفاده از آن‌ها تهدیدهای جدیدی کارایی و امنیت این سامانه‌ها را به مخاطره می‌اندازند [۴].

امروزه افراد به راحتی می‌توانند از نقاط مختلف دنیا برای به اشتراک‌گذاری اطلاعات یا انجام تراکنش‌های گوناگون با هم در ارتباط باشند. در واقع میلیون‌ها کاربر از اینترنت برای به اشتراک گذاشتن اطلاعات و تجربه‌های خود استفاده می‌کنند. اینگونه محیط‌ها فضاهای بازی هستند که هرکس می‌تواند آزادانه وارد آن‌ها شده و محتوایی خاص را به اشتراک بگذارد که این امر سبب ایجاد چالش‌های فراوانی می‌شود. بدون وجود هیچ کنترلی در چنین محیط‌های توزیع‌شده، هرکس توانایی به اشتراک‌گذاری هرگونه محتوایی را دارد، بنابراین تعامل با کاربران ناشناس بدون هیچ کنترل مرکزی و ضمانتی به طور قابل توجهی خطر چنین تعاملاتی را افزایش می‌دهد. از آنجا که عوامل نفوذ و افراد فرصت‌طلب همیشه در کمین هستند و نوع حملات نیز دائماً در حال تغییرات است، با یک چالش پیچیده‌ای مواجه‌ایم. قرارگرفتن در معرض حمله‌های بدخواهانه و احتمال حذف، تغییر مکان یا وقوع خرابی یا نفوذ در سامانه‌های توزیع‌شده، قابلیت اعتماد به این سامانه‌ها را به ویژه در کاربردهای توزیع‌شده با نگرانی‌هایی همراه می‌کند. بنابراین ایجاد سازوکارهایی برای حفظ سطح مطلوب کارایی چنین سامانه‌هایی در مقابل انواع خطاها و نفوذهای عمدی از اهمیت بالایی برخوردار است. هدف از برقراری امنیت در مقابل انواع نفوذها این است که هیچ موجودیتی نتواند به صورت غیرمجاز و بر خلاف سیاست‌های امنیتی[8] خاص، به منابع یا اطلاعات یک سامانه دسترسی پیدا کند. هدف از ارائه این مقاله، فراهم‌سازی سطح قابل قبولی از سرویس در سامانه‌ها با فرض وجود رفتارهای بدخواهانه در محیط‌های توزیع‌شده و مقاوم کردن سامانه‌ها در برابر نفوذ با توجه به سازوکار اعتماد است. اگرچه فنون تحمل‌پذیری در سامانه‌ها راهکار مناسبی برای توسعه سامانه‌های تحمل‌پذیر نفوذ و مقابله با انواع خطاها هستند، اما مواردی مانند عمدی بودن حملات و آسیب‌پذیری‌ها که زمینه‌ساز بروز حمله‌های موفق هستند، ضرورت ایجاد راهکارهای مقاوم‌تری را نشان می‌دهند. مدیریت اعتماد و شهرت[9] یک راه‌حل جدید امنیتی در موقعیت‌هایی است که اطلاعات کافی در مورد سایر اعضای یک محیط نداریم. این در مورد محیط‌های توزیع‌شده و باز که افراد با سایر کاربران ناشناخته تعامل دارند، صدق کرده و باعث ایجاد خطرها و چالش‌های مختلفی می‌شود. در نتیجه کاربران در این محیط‌ها نیازمند سازوکارهایی هستند که قابلیت اعتماد کاربران دیگر را قبل از برقراری تعامل با آن‌ها بسنجند [۵]. در واقع هدف این مقاله پرداختن به بعضی رفتارهای بدخواهانه میان اعضای یک سامانه به صورت کلی و ارائه رهیافتی برای مقابله با آن‌ها در سامانه‌های مبتنی بر اعتماد است. در دهه‌های اخیر سامانه‌های نرم‌افزاری رشد چشم‌گیری داشته‌اند و موضوع امنیت در این سامانه‌ها روزبه‌روز گسترده‌تر و پیچیده‌تر شده است. در دهه‌های قبل تنها روش‌های تشخیص[10]، پوشش[11] و پیش‌بینی[12] نفوذ مطرح می‌شدند که تا حدودی در این زمینه مفید بودند، در حالی‌که در سال‌های اخیر این رویکرد تغییر کرده است [۶]. اگرچه تحقیقاتی که تاکنون انجام شده‌اند مسیرهای مجزایی را برای بررسی خود انتخاب کرده‌اند، اما مسائلی که باید حل شوند دارای ماهیت یکسانی هستند که یکی از آن‌ها حفظ کارکرد صحیح سامانه‌ها علی‌رغم روی دادن حوادث بد در آن‌ها است، که این حوادث بد، رفتارهای بدخواهانه[13] نام دارند و در نهایت منجر به نفوذ در سامانه می‌شوند. بنابراین وقوع نفوذ در فرآیند توسعه یک سامانه از یک طرف و نیازهای امنیتی شامل محرمانگی[14]، یکپارچگی[15] و دسترس‌پذیری[16] از طرف دیگر، ضرورت توجه به سازوکارهای تحمل‌پذیری نفوذ را مشخص می‌کند [۲ و ۷].

در مقاله حاضر به بعضی رفتارهای بدخواهانه میان اعضای یک سامانه به صورت کلی پرداخته شده است. در ادامه رهیافتی برای مقابله با آن‌ها در سامانه‌های مبتنی بر اعتماد ارائه شده است. در واقع

[1] Non-Deliberate Faults
[2] Malicious Attacks
[3] IT: Intrusion Tolerance
[4] Deliberate
[5] Failure
[6] Trust
[7] Threats

[8] Security Policies
[9] Reputation
[10] Detection
[11] Removal
[12] Forecasting
[13] Malicious Behaviors
[14] Confidentiality
[15] Integrity
[16] Availability

این سازوکار، تکمیل‌کننده سامانه‌های اعتمادی است که تاکنون ارائه شده‌اند و سعی در برطرف‌سازی نقاط ضعف و آسیب‌پذیری در آن‌ها و در نهایت مقاوم‌کردن این رهیافت‌ها در برابر رفتارهای بدخواهانه است. جزئیات این سازوکار در بخش روش تحقیق به طور کامل آورده شده است.

۱-۱. ارتباط امنیت و اعتماد

سازوکارهای امنیتی مرسوم معمولاً به محافظت سامانه‌ها و منابع آن‌ها در مقابل افراد بدخواه می‌پردازند. به این صورت که تنها افراد مجاز قادر به دستیابی منابع هستند. در حالت کلی، هدف از سازوکارهای امنیتی، محافظت در برابر حملات و رفتارهای بدخواهانه است. اما امروزه در بسیاری از مواقع لازم است افراد از خود در مقابل سامانه‌هایی که سرویس یا منابعی را ارائه می‌دهند، محافظت کنند که در این صورت مسئله معکوس می‌شود. فراهم‌کنندگان سرویس یا اطلاعات می‌توانند بدخواهانه عمل کنند؛ در حالی‌که سازوکارهای امنیتی مرسوم قادر به محافظت در مقابل چنین تهدیدهایی نیستند و با کمک سامانه‌های اعتماد و شهرت در مقابل می‌توانند در برابر این چنین تهدیدهایی محافظت به عمل آورند. تفاوت میان این دو رهیافت در ابتدا توسط راسموسن[1] و جانسون[2] مورد توجه قرار گرفت. آن‌ها از واژه «امنیت سخت»[3] برای سازوکارهای مرسوم مانند کنترل دسترسی و احراز هویت استفاده نمودند و از «امنیت نرم»[4] به عنوان سازوکارهای کنترل اجتماعی به صورت کلی مانند سامانه‌های اعتماد و شهرت یاد کرده‌اند. همین موضوع در برخی منابع با عنوان «اعتماد سخت»[5] و «اعتماد نرم»[6] به کار رفته است [۸ و ۹]. علاوه بر این در بسیاری از رهیافت‌های امنیتی، سطح تضمین امنیت[7] در سامانه مطرح می‌شود که نشان می‌دهد چقدر در برابر حملات و رفتارهای بدخواهانه مقاوم است و دیدی کلی از میزان اعتماد به سامانه را می‌رساند.

۱-۲. اهداف حمله در اعتماد

رفتارهای بدخواهانه یا خودخواهانه در نهایت منجر به حمله یا نفوذ در یک سامانه می‌شوند. مهاجم خودخواه، مقادیر اعتماد را برای منفعت خود تغییر می‌دهد، درحالی‌که مهاجم بدخواه، قصد کاهش میزان اعتماد بقیه عوامل یا ضربه‌زدن به دسترس‌پذیری کل سامانه و در نهایت نفوذ به آن را دارد. نفوذ در سامانه‌های مبتنی بر اعتماد ممکن است به صورت فردی یا به صورت تبانی گروهی باشد که تشخیص و مقابله با آن کار آسانی نیست. سامانه‌های مبتنی بر اعتماد در مقابل رفتارهای خودخواهانه و بدخواهانه آسیب‌پذیر هستند. حملات مختلفی در زمینه اعتماد مطرح است. به طور کلی کاربران بدخواه یا خودخواه با ارائه سرویس‌های نامطلوب، دادن بازخوردهای ناصادقانه، (کاذب) و توصیه‌های نادرست در مورد دیگران، اهداف متفاوتی را دنبال می‌کنند که در زیر به چند نمونه از این اهداف اشاره شده است:

۱- تهمت‌زدن[8] (بدخواهی): در این حمله، کاربر بدخواه مقدار اعتماد سایر کاربران را با بازخورد منفی ناعادلانه و کاذب کاهش می‌دهد. سامانه‌هایی که منبع بازخورد را احراز اصالت نمی‌کنند در برابر این حمله، آسیب‌پذیر هستند. زیرا اعتماد به بازخورد منفی، این حمله را تسهیل می‌کند. این حمله ممکن است به صورت فردی یا تبانی گروهی صورت گیرد که صورت تبانی گروهی آن مؤثرتر است و می‌تواند منجر به نفوذ در کل سامانه شود.

۲- خودبالابری[9] (خودخواهی): انگیزه مهاجم از این رفتار، افزایش ناعادلانه اعتماد به خود در برابر کل عوامل سامانه است. این رفتار نیز ممکن است به صورت فردی یا تبانی گروهی شکل گیرد. سامانه‌هایی که احراز اصالت داده‌ها و درستی آن‌ها را بررسی نمی‌کنند در برابر این حمله آسیب‌پذیر هستند. در واقع در حالت تبانی گروهی، تبانی‌کنندگان بدون برقراری هیچ ارتباطی، در مورد یکدیگر، بازخورد مثبت صادر می‌کنند و میزان اعتماد خود را افزایش می‌دهند.

۳- ضربه‌زدن به کل سامانه: ممکن است انگیزه مهاجم، خودخواهی یا بدخواهیِ سایر کاربران نباشد و تنها هدف وی ضربه‌زدن به درستی و جامعیت سامانه و در نهایت نفوذ به آن باشد. در واقع هر چه رفتارهای کاربرانِ بدخواه، غیرقابل تشخیص‌تر باشد، می‌تواند آسیب بیشتری به سامانه وارد نماید. با توجه به این‌که کاربر بدخواه کدام‌یک از رفتارها را دارد؛ چه اهدافی را دنبال می‌کند؛ آن را با چه الگوی رفتاری اجرا می‌کند و نحوه همکاری وی با سایر کاربران در راستای رفتار بدخواهانه خود چگونه است، می‌تواند منجر به انواع حملات علیه اعتماد شود [۱۰].

۱-۳. انواع حملات در زمینه اعتماد

در این بخش برخی از مهم‌ترین عوامل که سبب حمله و در نهایت نفوذ در زمینه اعتماد می‌شوند، معرفی خواهند شد [۱۰ و ۱۱].

۱- تبانیِ گروهی بدخواهانه برای افزایش اعتماد یکی از کاربران یا کاهش اعتماد به یکی از کاربران خارج از گروه: در این نوع از حمله به یک سامانه مبتنی بر اعتماد، کاربران بدخواه سعی در افزایش شهرت و اعتبار یکی از کاربران تبانی‌کننده دارند که از این راه برای کل کاربران منفعتی ایجاد کنند. در این نوع از حمله، تبانی‌کنندگان سعی

[1] Russmussen
[2] Janson
[3] Hard Security
[4] Soft Security
[5] Hard Trust
[6] Soft Trust
[7] Security Assurance Level
[8] Slandering
[9] Self Promoting

دارند با قدرت زیادی به تعامل با کاربر هدف بپردازند و بدون توجه به کیفیت خدمتی که وی ارائه می‌دهد به او میزان اعتماد کاذب و بالایی نسبت می‌دهند. این نوع از حمله سبب می‌شود تا میزان اعتماد یک کاربر بی‌دلیل، سریع و به طور ناعادلانه افزایش پیدا کند. حتی در بعضی موارد تبانی‌کنندگان همیشه سرویس بد ارائه می‌دهند و به سایر کاربران بدخواه، بیشترین مقدار اعتماد را اختصاص می‌دهند و برعکس به کاربرانی که درگیر تبانی نیستند بازخورد منفی و کم‌ترین مقدار اعتماد را اختصاص می‌دهند. نوع دیگر این حمله به این صورت است که تبانی‌کنندگان، یکی از کاربرانی را که عضو گروه تبانی‌کنندگان نیست، به عنوان قربانی، هدف می‌گیرند و با دادن بازخورد منفی با قدرت بالا، سعی در کاهش اعتبار وی دارند. هدف اصلی از این رفتارهای بدخواهانه، دادن بازخوردهای ناصادقانه و توصیه‌های نادرست مثبت و منفی در مورد یکی از اعضای گروه و در نهایت خودخواهی، بدخواهی و حتی ضربه‌زدن به کل سامانه است.

۲- کاربران بدخواه فردی: یکی از عوامل نفوذ در سامانه‌ها کاربران بدخواه فردی هستند که همواره سرویس بد ارائه می‌دهند. برای از بین‌بردن خطر این نفوذ باید رهیافت‌هایی را برای کاهش سطح اعتماد این عوامل در نظر گرفت و آن‌ها را به عنوان عامل بدخواه شناسایی و دسته‌بندی کرده و به تمام عوامل سامانه معرفی نمود. هدف اصلی از این نوع حمله، ضربه زدن به کل سامانه مبتنی بر اعتماد است. در نوع دیگری از این حمله ممکن است تبانی‌کنندگان همیشه سرویس خوب ارائه کنند که در این حالت جاسوس‌های بدخواه نامیده می‌شوند. در نتیجه میزان اعتماد بالایی دارند و به عوامل بدخواه هم حداکثر مقدار اعتماد را اختصاص می‌دهند. چون این عوامل از اعتبار و شهرت بالایی در کل مجموعه برخوردار هستند به سرعت سبب از بین رفتن کل سامانه می‌شوند.

۱-۴. دسته‌بندی روش‌های امنیتی مبتنی بر اعتماد بر اساس محیط کاربرد

به طور کلی روش‌های اعتمادی که تاکنون ارائه شده‌اند در چهار حوزه بر اساس محیط کاربردی آن‌ها تقسیم‌بندی شده‌اند [۱۲]:

شبکه‌های نظیر به نظیر
شبکه‌های مبتنی بر عامل‌ها[1]
شبکه‌های موردی[2]
شبکه‌های حسگر

علاوه بر این تقسیم‌بندی، شبکه‌های اجتماعی مبتنی بر وب[3]، شبکه‌های سیّار[4] و محیط‌های محاسبات فراگیر[5] نمونه‌هایی از این محیط‌ها هستند. به عنوان مثال روش‌های مبتنی بر اعتماد مطرح شده در برخی مراجع برای شبکه‌های اجتماعی مبتنی بر وب ارائه شده‌اند [۱۵- ۱۳]. روش‌های اعتماد ارائه شده در دیگر منابع برای شبکه‌های همتابه‌همتا طراحی شده‌اند [۱۶ و ۱۷]. در بسیاری از منابع نیز به بررسی روش‌های مبتنی بر اعتماد برای شبکه‌های حسگر و موردی پرداخته شده است [۱۸ و ۱۹].

۱-۵. دسته‌بندی روش‌های امنیتی مبتنی بر اعتماد بر اساس روش استنتاج اعتماد

همان‌طور که گفته شد روش‌های امنیتی مبتنی بر اعتماد را از منظرهای متفاوتی می‌توان دسته‌بندی کرد. یک دسته‌بندی بر اساس روش مورد استفاده برای محاسبه و استنتاج اعتماد است. همان‌طور که در بخش قبلی بیان شد، مسئله امنیت مبتنی بر اعتماد، در محیط‌های مختلفی مطرح است و تاکنون پنج روش برای محاسبه و استنتاج اعتماد پیشنهاد شده است. این روش‌ها، روش‌های فازی[6]، بیزی[7]، الهام‌گرفته از طبیعت[8]، تحلیلی[9] و روش‌های مورد استفاده در شبکه‌های اجتماعی و محیط‌های نامتجانس ابری هستند [۲۲-۲۰].

۱-۶. مروری بر پژوهش‌های امنیتی حوزه اعتماد

هدف اغلب این پژوهش‌ها، ارائه یک رهیافت مبتنی بر اعتماد با استفاده از شهادت‌ها یا تجربه‌های سایر کاربرانی است که در گذشته به صورت مستقیم یا غیرمستقیم با کاربر هدف (مورد نظر) در ارتباط بوده‌اند. در بعضی از موارد نیز از ترکیب این نظرها با استفاده از روش‌های محاسباتی برای تخمین میزان قابلیت اعتماد یک کاربر ناشناس استفاده می‌شود. در این روش‌ها منظور از گره، کاربران سامانه هستند. در ادامه به بررسی یکی از این روش‌ها پرداخته شده است.

روش اعتماد ویژه: هدف روش اعتماد ویژه[10]، افزایش امنیت در کل سامانه است. این امنیت می‌تواند توسط گره‌های بدخواه و یک‌سری از رفتارهای بدخواهانه که منجر به نفوذ می‌شوند، کاهش یابد [۱۶]. مقدار اعتماد محلی در این روش با C_{ij} نشان داده می‌شود، که بیانگر نظر گره i در مورد گره j بر اساس تجربه گذشته است. t_i مقدار اعتماد کلی است که تمام سامانه به i دارند. بر اساس تعاملاتی که i و j با هم دارند مقدار S_{ij} بیانگر میزان اعتماد محلی است و برابر تفاضل تراکنش‌های رضایت‌بخش[11] و نارضایت‌بخش[12] بین i و j است. در این رابطه، $Sat(i, j)$ بیانگر تعداد تراکنش‌های رضایت‌بخش و $unsat(i, j)$ بیانگر تعداد تراکنش‌های نارضایت‌بخش بین دو گره i و j است. این اعتماد محلی طبق رابطه (۱) محاسبه می‌شود:

[1] Agent-Base Environments
[2] Ad-hoc Networks
[3] Web-Based Social Networks
[4] Mobile Networks
[5] Pervasive Computing Environments
[6] Fuzzy
[7] Bayesian
[8] Bio-Inspired
[9] Analytic
[10] Eigen Trust
[11] Satisfy Transactions
[12] Unsatisfy Transactions

$$S_{ij} = Sat\ (i, j) - unsat\ \ (i, j) \quad (۱)$$

در این روش رابطه (۲) بـرای نرمـال‌سـازی مقـدار اعتمـاد محلـی در نظر گرفته شده است:

$$C_{ij} = \begin{cases} \dfrac{\max(S_{ij}, ۰)}{\sum_j \max(S_{ij}, ۰)} & if \quad \sum_j \max(S_{ij}, ۰) \neq ۰ \\ P_j & otherwise \end{cases} \quad (۲)$$

P_j بیان‌کننده مقادیر اعتمادی است که به صـورت پـیش‌فـرض بـه گره‌های از قبل قابل اعتماد داده شده است. هر گره سایر گره‌هـا را بر اساس C_{ij} انتخاب می‌کند. در این روش برای هر گره یـک بـردار اعتماد محلی تعریف می‌شود، به عنوان مثال C_i بردار اعتماد محلی گره i شامل تمام C_{ij}ها می‌شود. مقدار اعتماد کل گـره i بـر اسـاس مقادیر اعتماد محلی سایر گره‌ها به i محاسبه می‌شود. میزان تـأثیر اعتماد محلی هر گره، بر اساس اعتماد آن گره خواهد بود. مـاتریس C شامل تمـام بردارهـای C_i اسـت و بـه صـورت زیـر نمـایش داده می‌شود:

$$C = \begin{bmatrix} C_{11} & C_{12} & \dots & C_{1j} & \dots & C_{1n} \\ C_{21} & C_{22} & \dots & C_{2j} & \dots & C_{2n} \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ C_{i1} & C_{i2} & \dots & C_{ij} & \dots & C_{in} \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ C_{n1} & C_{n2} & \dots & C_{nj} & \dots & C_{nn} \end{bmatrix} \quad \overrightarrow{C_i} = \begin{bmatrix} C_{i1} \\ C_{i2} \\ \vdots \\ C_{i1} \\ \vdots \\ C_{in} \end{bmatrix} \quad (۳)$$

t_{ik} نشان‌دهنده مقدار اعتمادی است کـه i بـه k بـر اسـاس سـؤال از دوستان خود دارد. بردار t_{ik} به صورت رابطه (۴) تعریف می‌شود:

$$t_{ik} = \sum_j C_{ij} C_{jk} \quad (۴)$$

این روند می‌تواند با سؤال از دوستانِ دوستان ادامـه داشـته باشـد و در نتیجه i دید بیشتری پیدا کند. رابطه (۵) نشان‌دهنده این روند است:

$$\overrightarrow{t_i} = (C^T)\overrightarrow{C_i} \quad (۵)$$

پس از تکرار این پرس‌وجوها بعد از n بار رابطه (۵) بـه شـکل رابطـه (۶) تبدیل خواهد شد.

$$\overrightarrow{t_i}^{(n)} = (C^T)^n \overrightarrow{C_i} \quad (۶)$$

در واقع این روند باید تا زمان همگرایی[1] مقادیر ادامه پیدا کنـد. در این روش نشان داده شده اسـت کـه پـس از تعـداد گـام مشخصـی، الگوریتم حتماً همگرا خواهد شد. بنابراین، رابطه اعتماد محلی و کلی برای این‌که گره‌ها به صورت دائم گـره‌هـای بـدخواه را بـرای تعامـل انتخاب نکنند، به صورت رابطه (۷) تعریف می‌شود.

$$\overrightarrow{t}^{(k+1)} = (1-\alpha) C^T \overrightarrow{t}^{(k)} + \alpha \overrightarrow{P}$$
$$\overrightarrow{t}^{(۰)} = \overrightarrow{P} \quad (۷)$$

این روش تا حدی در برابر تهدیدهای گره‌های بـدخواه مقـاوم اسـت، چون گره‌هایی که سرویس بد ارائه می‌کنند، احتمـال انتخـاب شـدن کمتری دارند. در این روش، تشکیل جمع‌هـای بـدخواه، روی اعتمـاد کلی تأثیر چندانی ندارد. زیرا سامانه سعی می‌کند از راه گره‌های قابل اعتماد، جمع‌های بدخواه را از بین ببرد.

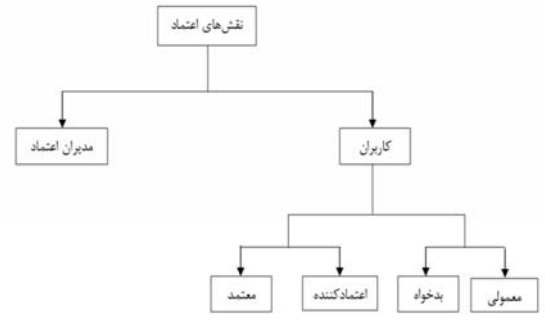
۲. روش تحقیق

در این رهیافت، مدل کلی در نظر گرفته شده برای سامانه، شامل سه جزء اصلی نقش‌های اعتماد، روابط اعتماد، ارزیابی و محاسبه اعتمـاد است. شکل (۱) نمای کلی اجزای اصلی را نشان می‌دهد. هر کـدام از این اجزا شامل زیربخش‌هایی هستند که در ادامه وظـایف هرکـدام از این زیربخش‌ها به صورت دقیق‌تر بیان خواهد شد.

شکل ۱. اجزای اصلی رهیافت پیشنهادی

۲-۱. نقش‌های اعتماد

نقش‌های اعتماد در این رهیافـت، شـامل کـاربران و مـدیران اعتمـاد هستند. برای هر کاربر، یک فایل سابقه و یک شناسه منحصر به فـرد در نظر گرفته می‌شود. فایل سابقه برای هر کاربر، شامل امتیازهای به دست آمده از روابط گذشته آن کاربر با سایر کاربران و مقادیر اعتماد محلی به دست آمده از این روابط اسـت. ایـن اطلاعـات در هـر بـازه زمانی، یک بار بـه‌روز مـی‌شـود. شـکل (۲) نقـش‌هـای اعتمـاد را در رهیافت پیشنهادی نشان می‌دهد.



شکل ۲. نقش‌های اعتماد

کاربران: همان‌طور که در قسمت قبل گفته شد، یکی از نقش‌هـای اعتماد در این رهیافت کاربران هسـتند. کـاربران از نظـر نـوع بـه دو دسته کاربران معمولی[2] و کاربران بـدخواه[3] در سـامانه تقسـیم‌بنـدی می‌شوند. در این سـامانه بـه هـر کـاربر از قبـل، یـک میـزان اعتمـاد

[1] Converge

[2] Usual Users
[3] Malicious Users

پیش‌فرض داده می‌شود تا در صورت عدم وجود روابط مستقیم و غیرمستقیم با سایر کاربران، مقدار اعتماد پیش‌فرض آن به عنوان مقدار اعتماد محلی در نظر گرفته شود.

کاربران بدخواه در سامانه، کاربرانی هستند که دائماً با توجه به نوع ارتباطی که با سایر کاربران دارند، هدف آن‌ها کاهش میزان امنیت کلی سامانه است. این کاربران می‌توانند از خود رفتارهای بدخواهانه متفاوتی که منجر به انواع حملات علیه اعتماد می‌شود، نشان دهند. اگر یک کاربر، بدخواه نباشد، معمولی در نظر گرفته می‌شود. کاربران معمولی، کاربرانی هستند که از خود رفتاری عادی نشان می‌دهند. در تقسیم‌بندی دیگری کاربران، از نظر روابط برقرار شده میان آن‌ها، به دو دسته اعتمادکننده و معتمد تقسیم می‌شوند.

مدیران اعتماد: از بین کاربران یک سامانه، با استفاده از یک تابع توزیع تصادفی، سه مدیر اعتماد برای هر کاربر انتخاب می‌شود. علاوه بر این، خود کاربران نباید نقشی در انتخاب مدیران اعتماد خود داشته باشند. وظیفه هر مدیر اعتماد، کنترل روابط مربوط به کاربرانی است که این کاربر، مدیر اعتماد آن‌ها است. در واقع در این رهیافت، هر کاربر می‌تواند مدیر اعتماد چند کاربر دیگر در نظر گرفته شود و به طور هم‌زمان هر کاربر، سه مدیر اعتماد دارد. در واقع در این بخش به منظور تحمل‌پذیرکردن رهیافت پیشنهادی، از افزونگی استفاده می‌شود. بدین ترتیب، این رهیافت از اکثریت آرا در بخش تصمیم‌گیری میزان اعتماد و نوع هر کاربر و از افزونگی در بخش نقش‌های اعتماد، برای تحمل‌پذیر کردن سامانه در برابر نفوذ استفاده می‌کند. در این سامانه، نقش‌های اصلی و پشتیبان (افزونه) دارای ویژگی‌های یکسانی هستند. بنابراین هر دو آسیب‌پذیری‌های مشابهی دارند، اما فرض می‌شود که پس از وقوع هر خرابی ناشی از یک حمله در بخشی از سامانه، از وقوع مجدد آن حمله روی نقش پشتیبان، از طریق محدودسازی آن حمله جلوگیری می‌شود. اگر برای هر کاربر در سامانه، سه مدیر اعتماد در نظر گرفته شود، اطلاعات اعتمادی هر کاربر به طور هم‌زمان، توسط چند مدیر اعتماد نگهداری می‌شود. نگهداری اطلاعات اعتمادی یک کاربر توسط مدیران اعتماد مختلف سبب می‌شود که یک مدیر اعتماد بدخواه که قصد تغییر دادن مقادیر اعتماد کاربران را دارد، در کل سامانه تأثیر زیادی نداشته باشد. در واقع با استفاده از افزونگی مدیران اعتماد، می‌توان از بروز بسیاری از حملات به سامانه جلوگیری کرد. از آنجا که هر کاربر در سامانه، یک شناسه منحصر به فرد دارد، بعد از انتخاب مدیران اعتماد، هر کاربر زمانی که اطلاع یافت که مدیران اعتماد وی، به طور تصادفی چه کاربرانی هستند، باید با استفاده از یک پیام، شناسه خود را برای مدیران اعتماد خود ارسال کند. وظیفه اصلی هر مدیر اعتماد، محاسبه میزان اعتماد کاربرانی است که به عنوان مدیر اعتماد آن‌ها تعیین شده است. مدیران اعتماد، بر اساس بازخوردهای (نظرات) مدیر کاربرانی که تا به حال با کاربر هدف (کاربری که می‌خواهید مقدار اعتماد سراسری آن را در کل سامانه محاسبه کنید) ارتباط داشته‌اند، میزان اعتماد محلی سایر کاربران را نسبت به کاربر هدف محاسبه می‌کنند. بعد از محاسبه مقدار اعتماد محلی، آن را در یک فایل سابقه که مربوط به هر کاربر در نظر گرفته شده است ثبت می‌کنند.

بنابراین وظایف مدیران اعتماد عبارتند از:

۱- مدیران اعتماد، بازخورد کاربران هدف را در کل سامانه ارائه می‌کنند و روابط رضایت و عدم رضایتی را که کاربران هدف با سایر کاربران داشته‌اند، امتیازدهی می‌کنند. مجموع این امتیازهای حاصل شده را در فایل مربوط به سابقه برای هر کاربر نگهداری می‌کنند. بر اساس این مقادیر، میزان اعتماد محلی هر کاربر (S_{ij}) به سایر کاربرانی که با آن‌ها در سامانه ارتباط داشته‌اند، طبق رابطه (۸) محاسبه می‌شود. برای در نظرگرفتن مقادیر نسبی اعتماد، به یک کاربر نظیر i بعد از برقراری ارتباط با کاربر دیگری نظیر j توسط مدیران اعتماد، امتیازی در بازه [۱و۰] به عنوان میزان رضایت یا عدم‌رضایت آن ارتباط از دیدگاه دو کاربر نسبت داده می‌شود. به عنوان مثال، اگر در یک ارتباط بین هر دو کاربر رضایتی کامل برقرار باشد با مقدار ۱ (tr(i,j)=1) و اگر میزان رضایتی وجود نداشته باشد، با مقدار ۰ (tr(i,j)=0) در محاسبات در نظر گرفته می‌شود. در نهایت مقدار اعتماد محلی که با توجه به میانگین مجموع امتیازهای نسبت داده شده به ارتباط‌های میان دو کاربر i و j به دست می‌آید، طبق رابطه (۸) محاسبه می‌شود

$$S_{ij} = \sum_{l=1}^{n} tr(i,j) = E\left(\sum_{l=1}^{n} Sat(i,j)\right) \qquad (۸)$$

که در این‌جا، n برابر با تعداد کل ارتباط‌های برقرار شده میان دو کاربر i و j است.

از آنجا که امتیازهای اختصاص داده شده به هر ارتباط در این رهیافت، در بازه [۱و۰] قرار دارد، در نتیجه میانگین این امتیازها که بیانگر مقدار اعتماد محلی حاصل شده بین هر دو کاربر در سامانه است هم در بازه [۱و ۰] قرار خواهد گرفت.

۲- تشخیص کاربران بدخواه با توجه به فایل سابقه مربوط به هر کاربر و کنترل روابط رضایت و عدم رضایت انجام شده توسط هر کاربر، از وظایف دیگر مدیران اعتماد است. در واقع مدیران اعتماد، وظیفه تشخیص کاربران بدخواه را با توجه به مجموع میانگین امتیازهای حاصل‌شده از روابط میان کاربران در سامانه، بر عهده دارند.

این رهیافت، بر پایه اکثریت آرا است. زمانی که مدیران اعتماد یک کاربر خاص، قصد محاسبه مقدار اعتماد کاربر هدف را دارند، برای این کار، نظر تمام کاربرانی را که تا آن لحظه با کاربر هدف ارتباط داشته‌اند، جویا می‌شوند. مدیران اعتماد بر اساس نظر آن کاربران و به عبارت دقیق‌تر بر اساس امتیازهای تخصیص داده‌شده به ارتباط‌های رضایت و عدم رضایت میان آن دو کاربر، میزان اعتماد محلی آن‌ها را با توجه به رابطه (۸) محاسبه می‌کنند. به طور فرض اگر کاربر i قبلاً با کاربر j در سامانه ارتباط داشته است، مدیران اعتماد کاربر i از مدیران اعتماد

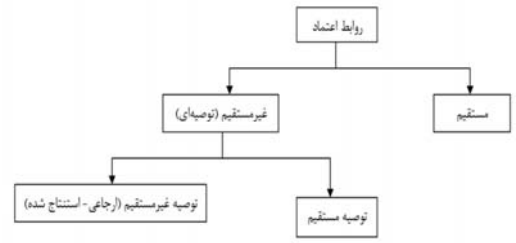
کاربر j مقدار امتیازهایی را که در ارتباط‌های رضایت و عدم رضایت بین دو کاربر به دست آمده است را جویا می‌شوند. اگر هیچ یک از کاربرانی که در نقش مدیران اعتماد هستند، بدخواه نباشند، تمام مقادیر بازگردانده شده توسط آن‌ها باید با یکدیگر سازگار باشند. اما اگر یکی از مدیران اعتماد، بدخواه باشد و به عبارتی قصد حمله به سامانه یا ایجاد نقص در بخشی از آن را داشته باشد؛ یا مقادیر امتیازهای نگهداری‌شده در فایل سابقه مربوط به هر کاربر و مقادیر اعتماد محلی را تغییر دهد یا اینکه مقادیر به دست آمده را اشتباه گزارش دهد، سبب می‌شود که نظرات مدیران اعتماد کاربر j با یکدیگر سازگار نباشند. در این حالت ناسازگاری، سامانه بر پایه اکثریت آرا عمل می‌کند. چون برای هر کاربر در سامانه، سه مدیر اعتماد در نظر گرفته شده، اگر نظر یکی از آن‌ها با دوتای دیگر سازگار نباشد، سامانه نظر آن مدیر اعتماد را مهم تلقی نمی‌کند و بر اساس نظر دو مدیر اعتماد دیگر مقدار اعتماد محلی را برای هر کاربر محاسبه می‌کند. این رهیافت در اغلب موارد درست کار می‌کند و با احتمال بسیار ناچیزی این امکان وجود دارد که همه یا اکثریت مدیران اعتماد هر کاربر، بدخواه باشند و مقادیر اعتماد محلی را تغییر دهند. زیرا مدیران اعتماد به صورت تصادفی با استفاده از یک تابع توزیع تصادفی انتخاب می‌شوند.

به طور کلی مدیران اعتماد برای هر کاربر، به عنوان یک عامل تأثیرگذار و مهم در این رهیافت ایفای نقش می‌کنند. کاربران بدخواه برای رسیدن به اهداف خود در سامانه، در بسیاری از موارد به سایر کاربران، بازخوردها و نظرات غیر واقعی و کاذب می‌دهند و از این طریق منجر به حمله و در نهایت نفوذ به سامانه می‌شوند. تشخیص کاربران بدخواه بر عهده مدیران اعتماد است. تصمیم‌گیری برای تشخیص بدخواه بودن کاربران نیز بر اساس اکثریت آرا انجام می‌شود. یعنی سامانه مورد نظر در صورتی با کاربر بدخواه برخورد می‌کند و نظر وی را در محاسبه مقدار اعتماد سراسری سایر کاربران اِعمال نمی‌کند که اکثریت مدیران اعتماد آن کاربر در مورد بدخواه بودن وی با هم توافق نظر داشته باشند. چون در این رهیافت برای هر کاربر، سه مدیر اعتماد در نظر گرفته شده، در صورتی یک کاربر به عنوان کاربر بدخواه تشخیص داده می‌شود که حداقل دو مدیر اعتماد آن در مورد بدخواه بودن وی توافق نظر داشته باشند. اگر مدیران اعتماد با استفاده از نتایج و شواهد موجود به این نتیجه برسند که یک کاربر، بدخواه است، در سازوکار محاسبه مقدار اعتماد سراسری برای کاربران سامانه، نظر کاربر بدخواه را اعمال نمی‌کنند.

بنابراین بدین صورت از بروز بسیاری از حملات علیه اعتماد و در نتیجه نفوذ به سامانه جلوگیری می‌شود. در ادامه چگونگی سازوکار تشخیص و محدودسازی نظر کاربران بدخواه در مورد میزان اعتماد سراسری هر کاربر به طور کامل شرح داده خواهد شد.

۲-۲. روابط اعتماد

در این رهیافت، روابط اعتماد در این سامانه به دو دسته روابط مستقیم و غیر مستقیم تقسیم می‌شوند. اعتماد مستقیم، به معنای میزان اعتمادی است که اعتماد کننده به معتمد بدون هیچ واسطه‌ای میان آن‌ها دارد. در حالی‌که در اعتماد غیر مستقیم یا مبتنی بر توصیه، میزان اعتماد هر کاربر بر اساس نظر یک کاربر سوم به معتمد تعیین می‌شود. چون در این رهیافت از اعتماد غیر مستقیم یا مبتنی بر توصیه برای محاسبه میزان اعتماد سراسری برای هر کاربر در سامانه استفاده می‌شود، بنابراین، این رهیافت مبتنی بر رابطه تعدی در اعتماد است. این رابطه تعدی می‌تواند در طول زنجیره‌های طولانی‌تری از کاربران در نظر گرفته شود (اعتماد ارجاعی- استنتاج شده - توصیه غیر مستقیم). به بیان دیگر در این سامانه، اعتمادکننده می‌تواند به صورت غیر مستقیم میزان اعتماد به کاربر سوم را با استفاده از توصیه‌های گروهی از کاربران معتمد به دست آورد. بنابراین محاسبه اعتماد در این حالت، با توجه به ترکیب چندین رابطه اعتماد مستقیم انجام می‌شود. به طور کلی در این رهیافت برای محاسبه میزان اعتماد محلی بین هر دو کاربر در سامانه، تمام روابط مستقیم و غیر مستقیم در نظر گرفته می‌شود و در انتها یک مقدار نهایی برای میزان اعتماد سراسری هر کاربر با توجه به این روابط، محاسبه می‌شود. شکل (۳) کلیه روابط به کار رفته در رهیافت پیشنهادی را نشان می‌دهد.



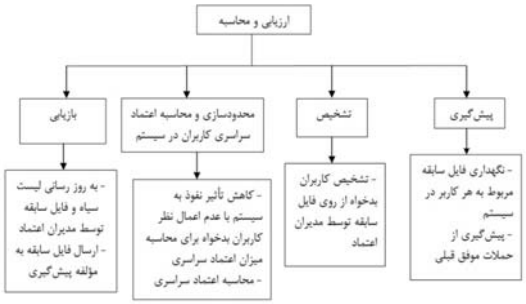
شکل ۳. روابط اعتماد

۲-۳. ارزیابی و محاسبه میزان اعتماد

این بخش، از چهار مؤلفه پیشگیری، تشخیص، محدودسازی و بازیابی برای تحمل‌پذیر کردن کل سامانه در برابر نفوذ استفاده می‌کند. شکل (۴) نمای کلی این بخش را نشان می‌دهد. در ادامه وظایف هر کدام از این مؤلفه‌ها به صورت دقیق‌تر بیان خواهد شد.

مؤلفه پیشگیری: این مؤلفه وظیفه پیشگیری از روی‌دادن حملاتی که توسط کاربران بدخواه در سامانه صورت می‌گیرد را بر عهده دارد. به عبارت دیگر این بخش از وقوع حملات موفق قبلی در سامانه جلوگیری می‌کند. فایل سابقه برای هر کاربر در سامانه در این بخش نگهداری می‌شود. این فایل حاوی اطلاعات به‌روز شده در مورد امتیازهای به دست آمده از روابط میان هر دو کاربر، مقادیر اعتماد محلی بین هر دو کاربر، نوع کاربر و به‌روزترین میزان اعتماد سراسری به آن کاربر از نظر سایر کاربران است. امتیازهای به دست آمده از روابط میان هر دو کاربر، شامل مجموع امتیازهای رضایت و عدم رضایت میان هر دو کاربر است. اگر هر کاربر توسط مدیران اعتماد از نظر نوع رفتار، مورد بررسی قرار بگیرد و به عنوان کاربر بدخواه

تشخیص داده شود، در لیست سیاه قرار می‌گیرد. مدیران اعتماد بعد از هر بازه زمانی، اطلاعات فایل سابقه مربوط به هر کاربر و لیست سیاه را به‌روز می‌نمایند. بنابراین این بخش با نگهداری فایل سابقه مربوط به هر کاربر از وقوع حملات موفق قبلی در سامانه جلوگیری می‌کند. علاوه بر این، سبب می‌شود تا در یک دوره یکسان مجدداً از کاربران بدخواهی که در لیست سیاه قرار گرفته‌اند، استفاده نشود تا از هرگونه سوء استفاده مجدد کاربران بدخواه در سامانه پیشگیری شود.



شکل ۴. نمای کلی بخش ارزیابی و محاسبه اعتماد

مؤلفه تشخیص: مرحله ابتدایی برای محاسبه میزان اعتماد سراسری بدون در نظر گرفتن نظر کاربران بدخواه سامانه توسط این مؤلفه انجام می‌شود. این مؤلفه به تشخیص کاربران بدخواه از روی اطلاعات فایل سابقه مربوط به هر کاربر می‌پردازد. در این مؤلفه برای تشخیص کاربران بدخواه، مدیران اعتماد هر کاربر باید قادر به بررسی فایل سابقه مربوط به هر کاربر باشند، تا با استفاده از آن فایل، کاربران بدخواه را در سامانه شناسایی کنند. بعد از محاسبه مقدار اعتماد محلی هر دو کاربر، مدیران اعتماد، به منظور تشخیص کاربران بدخواه در سامانه، از رابطه (۹) استفاده می‌کنند. آن‌ها با توجه به مقادیر اعتماد محلی که از روی میانگین روابط رضایت و عدم رضایت آن‌ها با سایر کاربران سامانه به دست می‌آیند و تعداد کل روابط انجام شده برای هر کاربر، به تشخیص کاربران بدخواه می‌پردازند. در این رابطه K تعداد کل کاربران در سامانه است. $n(S_{ij})$ تعداد کل روابط میان دو کاربر i و j است. در این مؤلفه یک مقدار آستانه (Th) برای تشخیص کاربران بدخواه در نظر گرفته می‌شود.

بعد از محاسبه این مقادیر، از روی فایل سابقه مربوط به هر کاربر، مقادیر حاصل از رابطه (۹) با مقدار آستانه مقایسه می‌شوند. اگر مقادیر به دست آمده از مقدار آستانه تعیین شده کمتر باشند، آن کاربر توسط مدیران اعتماد خود به عنوان یک کاربر بدخواه شناسایی و تشخیص داده می‌شود.

در واقع این رابطه برای تشخیص بدخواه بودن کاربر j به کار می‌رود و از روی میانگین روابط انجام گرفته بین کاربر j با سایر کاربران با توجه به نوع روابط آن‌ها به تشخیص نوع رفتار کاربر j در سامانه می‌پردازد.

$$M_j = \frac{1}{K-1}\left(\frac{\sum_{i=1}^{k-1} S_{ij}}{\sum_{i=1}^{k-1} n(S_{ij})}\right) \qquad (۹)$$

بعد از تشخیص کاربران بدخواه توسط رابطه فوق، مدیران اعتماد با توجه به رأی‌گیری اکثریت، در مورد رفتار کاربران در سامانه تصمیم‌گیری می‌کنند و اسامی کاربران بدخواه را در لیست سیاه قرار می‌دهند. در ادامه مدیران اعتمادِ هر کاربر از روی اطلاعات فایل سابقه هر کاربر، میزان اعتماد سراسری را برای آن کاربر محاسبه کرده و آن را دوباره در فایل سابقه مربوط به آن کاربر برای مراحل بعدی محاسبه، ثبت می‌کنند. همان‌طور که گفته شد وظیفه اصلی مدیران اعتماد، محاسبه میزان اعتماد محلی کاربران سامانه با توجه به امتیازهای حاصل‌شده برای هر رابطه، بر اساس نظراتی است که از کاربران دیگر در مورد آن‌ها دریافت می‌کنند. در صورت یکسان بودن نظرات تمامی مدیران اعتماد در مورد تشخیص یک کاربر بدخواه، آن کاربر به عنوان کاربر بدخواه تشخیص داده می‌شود. بنابراین سایر کاربران با توجه به لیست سیاه، تنها با کاربرانی در سامانه ارتباط برقرار می‌کنند که بیشترین میزان اعتماد به آن‌ها از دید تمام کاربران سامانه وجود دارد. بدین ترتیب با تشخیص کاربران بدخواه از بسیاری از حملات ناشی از رفتار آن‌ها که موجب کاهش امنیت سامانه می‌شوند، جلوگیری خواهد شد.

مؤلفه محدودسازی و محاسبه اعتماد سراسری کاربران در سامانه: در این رهیافت، محدودسازی به معنای عدم اِعمال نظر کاربران بدخواه برای محاسبه میزان اعتماد سراسری سایر کاربران در سامانه تعریف می‌شود. این تعریف از محدودسازی، منجر به محدودشدن تأثیر حملات کاربران بدخواه به زیرمجموعه‌هایی از سامانه می‌شود و در نهایت امکان دسترسی به حداقل سرویس‌های سامانه را در زمان حمله به سامانه فراهم می‌آورد.

این مؤلفه، با دریافت لیست سیاه از مؤلفه تشخیص، که وظیفه تشخیص کاربران بدخواه در سامانه را دارد، مانع از اعمال نظر کاربران بدخواه در مورد میزان اعتماد سراسری هر کاربر در سامانه می‌شود. در واقع این مؤلفه، سبب قطع ارتباط کاربران بدخواه با سایر کاربران در سامانه می‌شود. اجرای محاسبات مربوط به میزان اعتماد سراسری هر کاربر و عدم اِعمال نظرات کاربران بدخواه در سامانه بر عهده مدیران اعتماد است. این مؤلفه، مرحله اصلی برای محاسبه میزان اعتماد سراسری هر کاربر به منظور حفظ امنیت سامانه محسوب می‌شود. چگونگی محدودسازی نظرات کاربران بدخواه و محاسبه میزان اعتماد سراسری برای کاربران سامانه در ادامه توضیح داده خواهد شد.

مؤلفه بازیابی: مؤلفه بازیابی در سامانه مورد نظر شامل به‌روزرسانی اطلاعات مربوط به کاربران سامانه است. این مؤلفه پس از تشخیص کاربران بدخواه توسط مؤلفه تشخیص و محاسبه میزان اعتماد محلی و سراسری برای هر کاربر، انجام می‌شود و شامل به‌روزرسانی لیست سیاه و

فایل سابقه مربوط به هر کاربر است. در این مؤلفه، مدیران اعتماد، بعد از گذشت یک بازه زمانی مشخص، لیست سیاه و فایل سابقه مربوط به هر کاربر در سامانه را به‌روز می‌کنند و محتوای قبلی آن‌ها را به واحد پیشگیری ارسال می‌نمایند تا آن مؤلفه با نگهداری اطلاعات قدیمی مربوط به کاربران در سامانه، از بروز مجدد حملات قبلی و در نهایت نفوذ به سامانه توسط کاربران بدخواه جلوگیری نماید. در نهایت کاربران موجود در سامانه، برای برقراری ارتباط سازنده با سایر کاربران، می‌توانند از اطلاعات نگهداری شده در مؤلفه پیشگیری استفاده کنند. بعد از هر بازه زمانی مدیران اعتماد هر کاربر، نوع رفتار مربوط به هر کاربر را در سامانه گزارش می‌کنند. همان‌طور که در قسمت‌های قبل بیان شد، مدیران اعتماد با استفاده از اکثریت آرا برای هر کاربر تصمیم‌گیری می‌نمایند. اطلاعات مربوط به هر کاربر با اطلاعات جدید به‌روز می‌شوند. این اطلاعات، مربوط به فایل سابقه هر کاربر و لیست سیاه است. به طور کلی، وظیفه نگهداری اطلاعات فایل سابقه برای هر کاربر و پیشگیری از بروز حملات موفق قبلی در مؤلفه پیشگیری و تشخیص کاربران بدخواه در مؤلفه تشخیص، بر عهده مدیران اعتماد است. همچنین محاسبه میزان اعتماد سراسری کاربران از روی اطلاعات فایل سابقه در مؤلفه محدودسازی و محاسبه و به‌روزرسانی محتوای مربوط به فایل سابقه هر کاربر و لیست سیاه در مؤلفه بازیابی بر عهده آن‌ها است.

۲-۴. نرمال‌سازی مقادیر اعتماد محلی در سامانه

بعد از محاسبه مقادیر اعتماد محلی (S_{ij}) برای هر دو کاربر در سامانه، با توجه به امتیازهای حاصل‌شده از روابط میان آن‌ها، برای تجمیع مقادیر اعتماد محلی، نیاز داریم تا مقادیر نرمال‌سازی شوند. بنابراین برای هر دو کاربر i و j که در سامانه وجود دارند، یک میزان اعتماد محلی نرمال شده به نام C_{ij}، طبق رابطه (۱۰) تعریف می‌کنیم:

$$C_{ij}=\begin{cases}\dfrac{\max(S_{ij},0)}{\sum_j \max(S_{ij},0)} & if \quad \sum_j \max(S_{ij},0)\neq 0\\ P_j & otherwise\end{cases} \qquad (۱۰)$$

با نرمال‌سازی مقادیر اعتماد محلی تضمین می‌شود که تمامی مقادیر اعتماد محلی محاسبه شده در سامانه در بازه [۱و۰] خواهند بود. در واقع مخرج کسر به منظور نرمال‌سازی مقادیر اعتماد محلی به دست آمده، استفاده می‌شود. در این رابطه، صورت کسر بیانگر میزان اعتماد محلی مستقیمی است که از برقراری یک رابطه مستقیم میان دو کاربر در سامانه به وجود آمده است. در حالی‌که مخرج کسر بیانگر میزان اعتماد محلی غیرمستقیمی است که از مجموع کلیه روابط مستقیم و غیرمستقیم میان دو کاربر در سامانه حاصل شده است. به بیان دیگر در این رابطه صورت کسر میانگین مجموع وزن‌های یال مستقیم از یک گره (گره مبدأ) به گره دیگر (گره مقصد) در گراف در نظر گرفته می‌شود و مخرج کسر میانگین مجموع وزن یال‌های مستقیم و غیرمستقیم از گره مبدأ به گره مقصد در گراف است. اگر در گراف حاصل شده از روابط کاربران در سامانه، هیچ یال مستقیمی از گره مبدأ به گره مقصد وجود نداشته باشد، به این مفهوم است که دو کاربر در سامانه به یکدیگر اعتماد مستقیم ندارند و صورت کسر صفر می‌شود. در این شرایط اگر یال غیرمستقیم میان این دو گره وجود داشته باشد، مقدار اعتماد محلی نرمال شده صفر خواهد شد. مفهوم مقدار صفر در این حالت به این صورت است که در این مدل اهمیت زیادی به اعتماد غیرمستقیم در سامانه داده نمی‌شود و مقادیر اعتماد مستقیم نسبت به اعتماد غیرمستقیم اهمیت بیشتری دارند. در حالتی که هیچ یالی (مستقیم و غیرمستقیم) از گره مبدأ به مقصد وجود نداشته باشد، به این معنی است که کاربر i اصلاً کاربر دیگری را در سامانه نمی‌شناسد که با او ارتباط برقرار کند یا به هیچ کاربری در سامانه اعتماد ندارد. به بیان دیگر با هیچ کاربری در سامانه ارتباط برقرار نکرده است. در نتیجه مقدار اعتماد پیش‌فرض تعیین شده برای کاربر j (p_j) به عنوان مقدار اعتماد محلی نرمال شده بین i و j به دست می‌آید. یعنی کاربری که در یک سامانه هنوز ارتباطی با سایر کاربران برقرار نکرده است، ترجیح می‌دهد که بر اساس مقادیر اعتماد اولیه کاربران به آن‌ها اعتماد کند. هرچه اعتماد محلی نرمال‌شده به مقدار ۱ نزدیک‌تر باشد، میزان اعتماد میان دو کاربر بیشتر است. حداکثر میزان اعتماد محلی میان دو کاربر زمانی حاصل خواهد شد که تعداد روابط غیرمستقیم میان دو کاربر در سامانه کم باشد. چون این روابط منجر به اعتماد غیر مستقیم در سامانه می‌شوند و این نوع اعتماد در مقابل اعتماد مستقیم از اهمیت کمتری برخوردار است.

مقادیر اعتماد محلی C_{ij} نسبی هستند و یک مقدار مطلق به حساب نمی‌آیند. بنابراین اگر رابطه تساوی $C_{ik}=C_{ij}$ برقرار باشد، به این معنا است که در گراف حاصل از روابط کاربران در سامانه، از نظر گره i، مقدار اعتماد به گره‌های k و j یکسان در نظر گرفته می‌شود. در حالی که این تساوی به طور واضح مشخص نمی‌کند که آیا دو گره i و j در سامانه مقدار اعتماد بالایی در بین سایر گره‌ها دارند یا این‌که هر دو گره، بدخواه بوده و مقدار اعتماد پایینی دارند. در این رهیافت، برای هر کاربر در سامانه، یک بردار اعتماد محلی تعریف می‌شود. به عنوان مثال C_i بردار اعتماد محلی برای کاربر i است و شامل تمام مقادیر C_{ij} می‌شود. ماتریس C شامل تمام بردارهای C_i است و به صورت زیر نمایش داده می‌شود:

$$C=\begin{bmatrix} C_{11} & C_{12} & \dots & C_{1j} & \dots & C_{1n}\\ C_{21} & C_{22} & \dots & C_{2j} & \dots & C_{2n}\\ \vdots & \vdots & \dots & \vdots & \dots & \vdots\\ C_{i1} & C_{i2} & \dots & C_{ij} & \dots & C_{in}\\ \vdots & \vdots & \dots & \vdots & \dots & \vdots\\ C_{n1} & C_{n2} & \dots & C_{nj} & \dots & C_{nn}\end{bmatrix} \qquad \overrightarrow{C_i}=\begin{bmatrix} C_{i1}\\ C_{i2}\\ \vdots\\ C_{i1}\\ \vdots\\ C_{in}\end{bmatrix} \qquad (۱۱)$$

۲-۵. تجمیع مقادیر اعتماد محلی در سامانه به منظور محاسبه اعتماد سراسری هر کاربر

مقدار اعتماد سراسری برای هر کاربر در سامانه بر اساس مقادیر اعتماد محلی نرمال‌شده سایر کاربران به آن کاربر به‌دست می‌آید. برای محاسبه میزان اعتماد سراسری هر کاربر، از یک میانگین‌گیری وزن‌دار از تمامی مقادیر اعتماد محلی نرمال شده کاربران استفاده می‌شود:

$$t_{ik} = \sum_j C_{ij} C_{jk} \quad (۱۲)$$

در این رابطه t_{ik} نشان‌دهنده مقدار اعتمادی است که i به k بر اساس سؤال از دوستان وی دارد. همان‌طور که در قسمت بالا بیان شد، اگر ماتریس C را مجموعه مقادیر اعتماد محلی نرمال شده C_{ij} و t_i را برداری شامل تمام مقادیر t_{ik} در نظر گرفته شود، آن‌گاه می‌توان رابطه (۱۲) را به صورت زیر بیان کرد:

$$\vec{t_i} = C^T \vec{C_i} = \left(\sum_{j=1}^{n} C_{ij} C_{j1}, \ldots, \sum_{j=1}^{n} C_{ij} C_{jk}, \ldots, \sum_{j=1}^{n} C_{ij} C_{jn} \right) \quad (۱۳)$$

در این رابطه، C^T ترانهاده ماتریس C است. در واقع اگر بخواهیم روند محاسبه اعتماد، با پرسش از دوستان (از طریق یک واسطه) ادامه داشته باشد، این رابطه نشان دهنده این روند است. در ادامه اگر بخواهیم میزان اعتماد به کاربر i با پرسش از دوستان دوستان (از طریق دو واسطه) ادامه یابد و در نتیجه کاربر i دید کامل‌تری از سایر کاربران سامانه به دست آورد، رابطه (۱۳) به صورت زیر بیان می‌شود:

$$\vec{t_i}^{(2)} = (C^T)^2 . \vec{C_i} \quad (۱۴)$$

اگر این روند برای n کاربر در سامانه ادامه یابد، در نتیجه کاربر i دید کاملی بعد از n بار تکرار پیدا می‌کند و خواهیم داشت:

$$\vec{t_i}^{(n)} = (C^T)^n . \vec{C_i} \quad (۱۵)$$

در این الگوریتم، پس از تکرار این پرس‌وجوها (بعد از n بار) بردار مقدار اعتماد به دست آمده برای تمامی کاربران موجود در سامانه به یک بردار ویژه همگرا خواهد شد. به عبارتی مقادیر اعتماد سراسری پس از مقدار گام مشخصی به یک مقدار همگرا می‌شوند. در واقع این روند باید تا زمان همگرایی مقادیر به یک مقدار ثابت، ادامه پیدا کند. در این مدل نشان داده شده است که اگر مقدار n به اندازه کافی بزرگ باشد، بردار اعتماد t_i برای هر کاربر پس از تعداد گام مشخصی به یک مقدار همگرا خواهد شد. در نهایت رابطه محاسبه اعتماد سراسری کاربران، برای این‌که هر کاربر به صورت مداوم کاربران بدخواه را برای برقراری ارتباط انتخاب نکند، به صورت رابطه (۱۶) تعریف می‌شود:

$$\vec{t}^{(k+1)} = (1-\alpha) C^T \vec{t}^{(k)} + \alpha \vec{P} \quad (۱۶)$$

$$\vec{t}^{(\circ)} = \vec{P}$$

در این رابطه α مقداری ثابت بین صفر و یک در نظر گرفته می‌شود. P مقدار اعتماد پیش‌فرض است. بسط این رابطه به صورت زیر تعریف می‌شود:

$$t_i^{(k+1)} = (1-\alpha)(\beta_1 C_{1i} t_1^{(k)} + \ldots + \beta_n C_{ni} t_n^{(k)}) + \alpha P_i \quad (۱۷)$$

در این رابطه، k نشان‌دهنده تعداد واسطه‌ها است. $C_{1i}, C_{2i}, \ldots, C_{ni}$ مقادیر موجود در ماتریس C^T هستند. C_{1i} بیانگر مقدار اعتماد محلی است که کاربر ۱ به کاربر i در سامانه دارد. به طور کلی C_{ni} بیانگر مقدار اعتماد محلی نرمال شده‌ای است که کاربر n به کاربر i دارد. $t_1^{(k)}$ میزان اعتماد سراسری برای کاربر ۱ توسط کاربرانی است که با k واسطه از کاربر ۱ در سامانه قابل دسترس هستند. به همین ترتیب $t_n^{(k)}$ میزان اعتماد سراسری کاربر n توسط کاربرانی است که با k واسطه از کاربر n در سامانه، قابل دسترس هستند. ضریب β_j به منظور محدودسازی نظرات کاربران بدخواه برای محاسبه میزان اعتماد سراسری سایر کاربران در نظر گرفته شده است. این ضریب برای کاربران بدخواه صفر در نظر گرفته می‌شود. در عین‌حال اگر کاربری به عنوان یک کاربر بدخواه تشخیص داده نشود و در لیست سیاه قرار نگیرد، این ضریب برای آن به منظور محاسبه میزان اعتماد سراسری سایر کاربران در رابطه (۱۷) ۱ در نظر گرفته می‌شود. به عبارت دیگر، در این رهیافت، مجوز ارائه نظر هر کاربر در مورد میزان اعتماد سراسری سایر کاربران سامانه، به نوع رفتار و ارتباط‌های برقرار شده قبلی وی با توجه به اطلاعات نگهداری شده در فایل سابقه مربوط به وی بستگی دارد. با محدودکردن اِعمال نظر کاربران بدخواه در محاسبه میزان اعتماد سراسری سایر کاربران، از وقوع بسیاری از حملات توسط کاربران بدخواه در سامانه جلوگیری می‌شود. زیرا بسیاری از حملات روی داده علیه سامانه‌ها، نتیجه تأثیر توصیه نادرست و غیر واقعی کاربران بدخواه در مورد میزان اعتماد سایر کاربران است. علاوه بر این، هدف دیگر این رهیافت، استفاده از نظرات تمامی کاربران با توجه به نوع رفتار و سابقه آن‌ها در کل سامانه برای محاسبه میزان اعتماد سراسری کاربران است. به این ترتیب مقدار اعتماد سراسری حاصل‌شده برای هر کاربر در سامانه فقط محدود به اظهار نظر دوستان وی نمی‌شود و همین امر موجب می‌شود که دقت میزان اعتماد سراسری حاصل شده برای هر کاربر در سامانه افزایش یابد. در واقع به بیان دیگر، در محاسبه میزان اعتماد سراسری یک کاربر در سامانه، با توجه به نسبی بودن مفهوم اعتماد، تنها به بررسی نظرات کاربرانی که قبلاً با وی ارتباط داشته‌اند، بسنده نشده است. بنابراین مقدار اعتماد سراسری به مقدار واقعی آن‌ها نزدیک‌تر شده و اعتماد ارجاعی نیز برای محاسبه میزان اعتماد سراسری هر کاربر در نظر گرفته شده است. این رهیافت در برابر حملات فردی یک کاربر بدخواه مقاوم است، زیرا در مدل اعتماد ویژه، احتمال انتخاب کاربران بدخواه بسیار ناچیز است [۱۵]. محاسبات برای میزان اعتماد سراسری برای هر کاربر تا جایی ادامه پیدا می‌کند که تفاضل بین مقدار اعتماد سراسری به دست آمده برای یک کاربر با K واسطه و مقدار اعتماد سراسری به دست آمده برای همان کاربر با K+1 واسطه از مقدار ε کمتر باشد. زمانی که مدیران اعتماد یک کاربر با توجه به رابطه (۹) و از روی فایل سابقه برای آن کاربر به این توافق رسیدند که مقدار M برای آن کاربر از مقدار آستانه (Th) تعیین شده کمتر شده است، این کاربر را به عنوان کاربر بدخواه بر مبنای رأی‌گیری اکثریت تشخیص می‌دهند. الگوریتم محاسبه اعتماد سراسری برای هر کاربر تا جایی ادامه می‌یابد که مقادیر اعتماد سراسری برای آن به یک مقدار ثابت همگرا شوند.

۲-۶. کلیات روش شبیه‌سازی

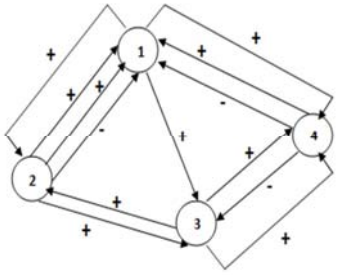
برای شبیه‌سازی از ابزار برنامه‌نویسی متلب استفاده کردیم و در ادامه به منظور نمایش کارایی رهیافت پیشنهادی، مدل اعتماد ویژه انتخاب شده است. این مدل، مدلی مبتنی بر اعتماد است که در بسیاری از نمونه‌ها، به عنوان مدل پایه و مدلی که در برابر رفتارهای بدخواهانه مقاوم است، در نظر گرفته شده است [۱۰، ۱۲، ۲۳ و ۲۴].

کامور و همکارانش، مدل اعتماد ویژه را به عنوان مدلی که در برابر برخی رفتارهای بدخواهانه مقاوم است، ارائه کرده‌اند [۱۶]. ما در شبیه‌سازی نشان خواهیم داد که هنوز مدل اعتماد ویژه در برابر بسیاری از رفتارهای بدخواهانه آسیب‌پذیر است و ما با رهیافت ارائه شده، مقاومت این مدل را در برابر رفتارهای بدخواهانه افزایش خواهیم داد.

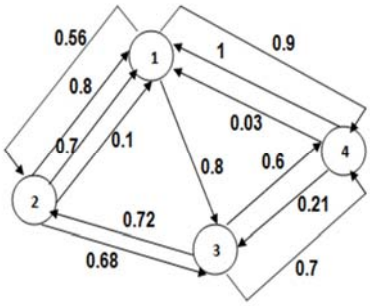
۳. نتایج و بحث

نمونه‌سازی رهیافت پیشنهادی: در این بخش، نمونه‌ای از رهیافت پیشنهادی با تعداد کاربر محدود مدل شده و در ادامه مورد ارزیابی قرار گرفته است. در انتها نیز نتایج آن به صورت نمودار برای مدل اعتماد ویژه و رهیافت پیشنهادی آورده شده است. شکل‌های (۵ و ۶) به ترتیب نمونه حاصل از برقراری ارتباط میان کاربران در یک سامانه را که به صورت گراف در نظر گرفته شده است، در مدل اعتماد ویژه و رهیافت پیشنهادی نشان می‌دهند. در هر دو شکل، هر گره به عنوان یک کاربر در سامانه فرض شده است. یال‌های هر گراف بیانگر ارتباط میان کاربران در سامانه هستند. چون این مدل برای چهار کاربر در سامانه در نظر گرفته شده است بنابراین اجرای مراحل مربوط به محاسبه میزان اعتماد سراسری برای هر کاربر توسط سایر کاربران ۱۶ بار تکرار شده است. علاوه بر این در هر بار اجرا برای همگرا شدنِ مقادیر محاسبه میزان اعتماد سراسری برای هر کاربر، مراحل محاسبه تا سه بار تکرار شده است تا نتایج با دقت بیشتری حاصل شوند. در شکل (۵) علامت روی هر یال بیانگر وزن آن است و نشان دهنده رضایت یا عدم رضایت روابط میان هر دو گره در گراف (کاربر در سامانه) است. تعداد روابط رضایت یا عدم رضایت بین هر دو کاربر به صورت مقادیر ورودی در نظر گرفته شده است. علامت مثبت نشان دهنده یک ارتباط رضایت و علامت منفی نشان دهنده یک ارتباط عدم رضایت میان هر دو کاربر است. در شکل (۶) وزن روی هر یال بیانگر امتیاز حاصل از برقراری ارتباط میان هر دو کاربر است. این مقادیر نیز به صورت مقادیر ورودی و در بازه [۱و۰] در نظر گرفته شده‌اند. هر چه وزن یال‌ها بیشتر باشند، میزان رضایت‌مندی هر دو کاربر از آن ارتباط بیشتر است. علاوه بر این برای انجام محاسبه، مقادیر اولیه اعتماد برای هر کاربر در هر دو مدل به صورت مقادیر ورودی در نظر گرفته شده است.

در ادامه، محاسبه به منظور به دست آوردن اعتماد سراسری برای هر کاربر در گراف شکل (۵) در مدل اعتماد ویژه، طبق رابطه (۷) انجام می‌گیرد. در رهیافت پیشنهادی نیز این محاسبات به منظور به دست آوردن اعتماد سراسری برای هر کاربر در گراف شکل (۶) طبق روابط (۹ و ۱۷) انجام می‌شود. مقادیر به دست آمده برای اعتماد سراسری برای هر دو مدل در شکل (۷) آورده شده است. ستون اول مربوط به ارتباط بین هر گره با سایر گره‌ها است. ستون دوم مربوط به مقادیر اعتماد سراسری در مدل اعتماد ویژه و ستون سوم مربوط به مقادیر اعتماد سراسری در رهیافت پیشنهادی است. شکل‌های (۱۱-۸) نمودارهای مربوط به هر دو مدل را برای میزان اعتماد سراسری هر کاربر توسط مقادیری که سایر کاربران به آن‌ها اختصاص داده‌اند، نشان می‌دهند. در این نمودارها EigenTrust و proposed به ترتیب مربوط به مقادیر حاصل از مدل اعتماد ویژه و رهیافت پیشنهادی است.



شکل۵. گراف حاصل از برقراری ارتباط میان کاربران سامانه در مدل اعتماد ویژه

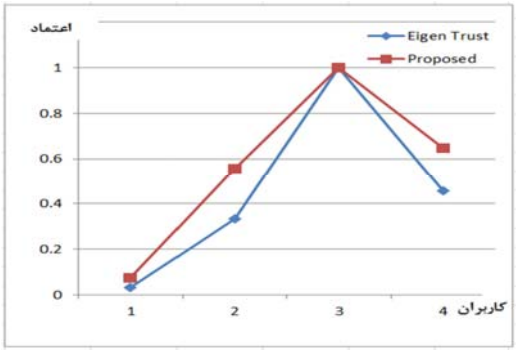


شکل ۶. گراف حاصل از برقراری ارتباط میان کاربران سامانه در رهیافت پیشنهادی

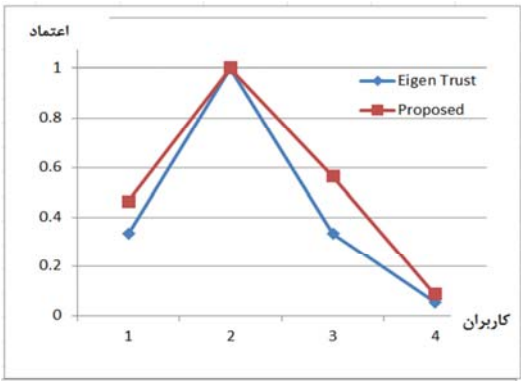
	A	B	C
1	1x1	1	1
2	1x2	0.397213	0.621351
3	1x3	0.456765	0.623465
4	1x4	0.213876	0.399113
5	2x1	0.333333	0.463557
6	2x2	1	1
7	2x3	0.333333	0.564337
8	2x4	0.054765	0.085432
9	3x1	0.032456	0.073786
10	3x2	0.333333	0.556701
11	3x3	1	1
12	3x4	0.456234	0.646876
13	4x1	0.567125	0.902345
14	4x2	0.054678	0.175821
15	4x3	0.36444	0.53442
16	4x4	1	1

شکل ۷. مقادیر به دست آمده برای میزان اعتماد سراسری در هر دو مدل

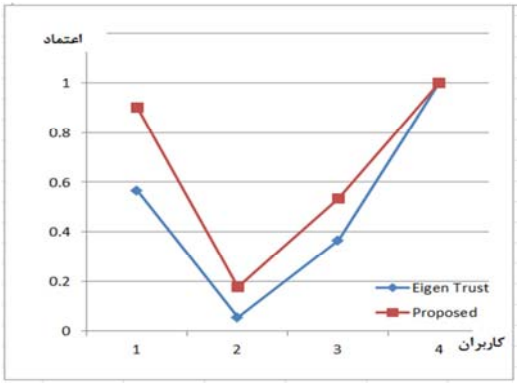
شکل ۸. مقدار اعتماد سراسری گره‌ها از نظر گره ۱ در هر دو مدل



شکل ۱۰. مقدار اعتماد سراسری گره‌ها از نظر گره ۳ در هر دو مدل



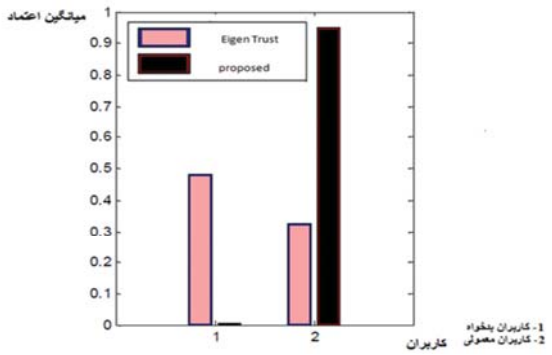
شکل ۹. مقدار اعتماد سراسری گره‌ها از نظر گره ۲ در هر دو مدل



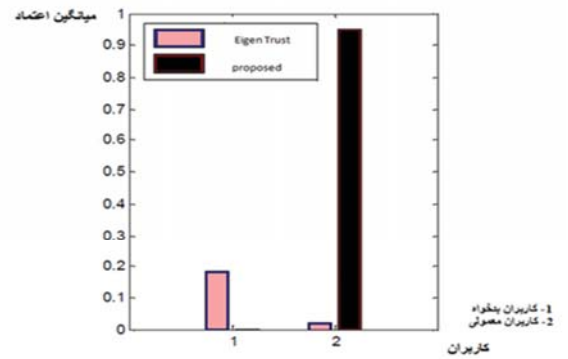
شکل ۱۱. مقدار اعتماد سراسری گره‌ها از نظر گره ۴ در هر دو مدل

همان‌طور که مشاهده می‌شود نتایج حاصل شده از این نمونه‌سازی برای مقدار اعتماد سراسری در رهیافت پیشنهادی نسبت به مدل اعتماد ویژه بهبود یافته است. با توجه به نمودارها در نظر گرفتن مقادیر نسبی برای میزان رضایت‌مندی روابط که منجر به نسبی شدن مفهوم اعتماد میان هر دو کاربر می‌شود، در مقایسه با مطلق در نظر گرفتن این مقادیر در مدل اعتماد ویژه دقت محاسبات را افزایش داده است. چون در نهایت مقادیر اعتماد سراسری برای هر دو کاربر از روی مقادیر اعتماد محلی میان آن دو کاربر حاصل می‌شوند، بنابراین، نسبی کردن این مقادیر برای محاسبه مقدار اعتماد سراسری از اهمیت بالایی برخوردار است. طبق رابطه (۹) (تشخیص کاربران بدخواه)، چون در این نمونه هر چهار کاربر موجود در سامانه کاربران معمولی هستند، بنابراین طبق نمودارهای حاصل شده، میزان اعتماد سراسری برای آن‌ها نسبت به مدل اعتماد ویژه افزایش یافته است.

شبیه‌سازی رهیافت پیشنهادی: برای شبیه‌سازی رهیافت پیشنهادی، به طور کلی دو نوع کاربر معمولی و بدخواه در نظر گرفته شده است. تعداد کل کاربران و درصد کاربران بدخواه نیز هر بار متفاوت است و از طریق ورودی دریافت می‌شوند. برای نمونه تعداد کاربران را ۵۰ در نظر گرفتیم و درصد کاربران بدخواه را برابر با ۱۰٪ و ۴۰٪ قرار دادیم. شکل‌های (۱۲ و ۱۳) میانگین مقادیر اعتماد کاربران (معمولی و بدخواه) را در سامانه هنگامی‌که میزان اعتماد سراسری توسط مدل اعتماد ویژه محاسبه می‌شود با حالتی که میزان اعتماد سراسری توسط رهیافت پیشنهادی محاسبه می‌شود، مقایسه می‌کند.



شکل ۱۲. میانگین مقدار اعتماد سراسری کاربران معمولی و بدخواه (تعداد کاربران: ۵۰، درصد کاربران بدخواه: ۱۰)



شکل ۱۳. میانگین مقدار اعتماد سراسری کاربران معمولی و بدخواه (تعداد کاربران: ۵۰، درصد کاربران بدخواه: ۴۰)

تحلیل نتایج نمودارهای شکل (۱۲ و ۱۳) به شرح زیر است:

۱- در شبیه‌سازی مربوط به رهیافت پیشنهادی، با اضافه کردن اعتماد ارجاعی، کاربران بدخواه قادر به بالابردن ناعادلانه میانگین میزان اعتماد سراسری خود نشده‌اند و میزان اعتماد سراسری آن‌ها در مقایسه با مدل اعتماد ویژه کاهش یافته است. این مطلب در نمودارهای مربوط به رهیافت پیشنهادی در مقایسه با مدل اعتماد ویژه به طور واضح مشخص است.

۲- میانگین اعتماد سراسری برای کاربران معمولی افزایش یافته است. این مطلب بیانگر این است که کاربران بدخواه در سامانه نتوانسته‌اند مقدار اعتماد سراسری خود را به طور ناعادلانه و کاذب افزایش دهند. در واقع دلیل این امر به این شرح است که با کاهش میانگین اعتماد سراسری کاربران بدخواه، احتمال انتخاب شدن کاربرانی با رفتار عادی به عنوان کاربر انتخابی برای برقراری ارتباط بیشتر می‌شود و افزایش این احتمال، متناظر با افزایش میانگین اعتماد سراسری است.

۳- با توجه به رابطه (۱۰) اگر در گراف حاصل شده از روابط کاربران در سامانه، هیچ یال مستقیمی از گره مبدأ به گره مقصد وجود نداشته باشد، به این مفهوم است که دو کاربر در سامانه به یکدیگر اعتماد مستقیم ندارند و صورت کسر صفر می‌شود. در این شرایط اگر یال غیر مستقیم میان این دو گره وجود داشته باشد، مقدار اعتماد محلی نرمال‌شده صفر خواهد شد. مفهوم مقدار صفر در این حالت به این صورت است که در این مدل اهمیت زیادی به اعتماد غیر مستقیم در سامانه داده نمی‌شود و مقادیر اعتماد مستقیم نسبت به اعتماد غیر مستقیم اهمیت بیشتری دارند. در حالتی که هیچ یالی (مستقیم و غیر مستقیم) از گره مبدأ به مقصد وجود نداشته باشد، به این معنی است که کاربر اصلاً کاربر دیگری را در سامانه نمی‌شناسد که با او ارتباط برقرار کند یا به هیچ کاربری در سامانه اعتماد ندارد. به بیان دیگر با هیچ کاربری در سامانه ارتباط برقرار نکرده است. در نتیجه مقدار اعتماد پیش‌فرض تعیین‌شده برای گره مقصد به عنوان مقدار اعتماد محلی نرمال شده بین دو گره به دست می‌آید.

۴. نتیجه‌گیری

در این مقاله یک رهیافت مبتنی بر اعتماد برای تحمل‌پذیر کردن سامانه در برابر نفوذ با هدف مقاوم بودن در برابر رفتارهای بدخواهانه ارائه شد. در این رهیافت با استفاده از روش‌های مبتنی بر شهرت، از تحلیل‌های ریاضی به منظور استنتاج اعتماد برای پیش‌بینی رفتار آینده استفاده شده است. هدف اصلی این رهیافت، حل چالش مطلق در نظر گرفتن اعتماد است. زیرا اِعمال یک میزان اعتماد مطلق برای هر کاربر در یک سامانه، سبب عدم بازتاب صحیح شرایط روی‌داده در فرآیند تصمیم‌گیری می‌شود. استفاده از نظرات تمامی کاربران برای تخمین میزان اعتماد سراسری به هر کاربر در سامانه، از اهداف دیگر این رهیافت است. این روش با حذف نظرات کاربران بدخواه در محاسبه میزان اعتماد سراسری برای هرکاربر، ضمن انعکاس درست شرایط رخ داده در سامانه سبب افزایش امنیت و کارایی در کل سامانه شده است. همان‌طور که مشاهده شد افزودن مفهوم نسبی بودن به اعتماد و تشخیص کاربران بدخواه با توجه به میانگین امتیاز حاصل شده از روابط رضایت‌بخش میان آن‌ها سبب بهبود رهیافت پیشنهادی نسبت به مدل اعتماد ویژه شده است. همچنین عدم اِعمال نظر کاربران بدخواه در مورد میزان اعتماد سراسری کاربران در یک سامانه سبب افزایش دقت در مقادیر اعتماد سراسری برای هر کاربر در رهیافت پیشنهادی شده است.

۵. مراجع

[1] Kuo, Z.; Fei, R.; Jianfeng, C.; Liang, Hu. "Surveys on the Intrusion Tolerance System"; Computer Communications and Networking 2009, 25, 90-97.

[2] Verssimo, P. E.; Neves, N. F.; Correia, M. P. "Intrusion-Tolerant Architectures: Concepts and Design"; Architecting Dependable Systems 2003, 8, 3-36.

[3] Bessani, A. N. "From Byzantine Fault Tolerance to Intrusion Tolerance"; In Proc. of the 41st Int. Conf. on Dependable Systems and Networks, Hong Kong, China 2011, 15-18.

[4] Josang, A.; Golbeck, J. "Challenges for Robust Trust and Reputation Systems"; In Proc. of the 5th Int. Workshop on Security and Trust Management (SMT), Saint Malo, France 2009, 45-76.

[5] Schryen, G.; Volkamer, M.; Ries, S.; Mahbub Habib, S. "A Formal Approach Towards Measuring Trust in Distributed Systems"; In Proc. of the ACM Symposium on Applied Computing, New York, NY, USA 2011, 1739-1745.

[6] Mukhopadhyay, I.; Chakraborty, M.; Chakrabarti, S. "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems"; J. Inform. Secure. 2011, 2, 28-38.

[7] Patel, A.; Qassim, Q.; Wills, C. "A Survey of Intrusion Detection and Prevention Systems"; Information Management & Computer Security 2010, 18, 277-290.

[8] Josang, A.; Ismail, R.; Boyd, C. "A Survey of Trust and Reputation Systems for Online Service Provision"; Decision Support Systems 2007, 43, 618-644.

[9] Nagarajan, A.; Varadharajan, V. "Dynamic Trust Enhanced Security Model for Trusted Platform Based Services"; Future Generation Computer Systems 2011, 27, 564-573.

[10] Marmol, F. G.; Mart, G. "Security Threats Scenarios in Trust and Reputation Models for Distributed Systems"; Computers & Security 2009, 28, 545-556.

[11] Hoffman, K.; Zang, D.; Nita-Rotaru, C. "A Survey of Attack and Defence Techniques for Reputation Systems"; ACM Computing Surveys (CSUR) 2009, 42, 121-146.

[12] Marmol, F. G.; Perez, G. M. "Towards Pre-Standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems"; Computer Standards & Interfaces 2010, 32, 185-196.

[13] Golbeck, J. "Computing and Applying Trust in Web-Based Social Networks"; Comput. Sci. 2005, 24, 120-135.

[14] Josang, A.; Hayward, R.; Pope, S. "Trust Network Analysis with Subjective Logic"; In Proc. of the 29th Int. Australasian Conf. on Computer Science (ACSC), Hobart, Australia 2006, 85-94.

[15] Artz, D.; Gil, Y. "A Survey of Trust in Computer Science and the Semantic Web"; Web Semantics: Services and Agents on the World Wide Web 2007, 5, 58-71.

[16] Kamvar, S. D.; Schlosser, M. T.; Molina, H. G. "The Eigen Trust Algorithm for Reputation Management in P2P Networks"; In Proc. of the 12th Int. Conf. on World Wide Web, Budapest, Hungary 2003, 640-651.

[17] Griffiths, N.; Chao, K.; Younas, M. "Fuzzy Trust for Peer-to-Peer Systems"; In Proc. of the Int. Conf. on Distributed Computing Systems, Genova, Italy 2006, 61-73.

[18] Yu, Y.; Li, K.; Zhou, W.; Li, P. "Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures"; J. Comput. 2012, 35, 867-880.

[19] Theodorakopoulos, G.; Baras, J. S. "Trust Evaluation in Ad-Hoc Networks"; In Proc. of the 3rd ACM workshop on Wireless Security, Philadelphia, PA, USA 2004, 1-10.

[20] Tajeddine, A.; Kayssi, A.; Chehab, A.; Artail, H. "Fuzzy Reputation-Based Trust Model"; Soft Computing 2011, 11, 345-355.

[21] Schmidt, S.; Steele, R.; Dillon, T. S.; Chang, E. "Fuzzy Trust Evaluation and Credibility Development in Multi-Agent Systems"; Soft Computing 2012, 7, 492-505.

[22] Guo, Q.; Sun, D.; Chang, G.; Sun, L.; Wang, X. "Modeling and Evaluation of Trust in Cloud Computing Environments"; In Proc. of the 3th Int. Conf. in Advanced Computer Control (ICACC), Harbin, China 2011, 112-116.

[23] Srivatsa, M.; Xiong, L.; Liu, L. "Trust Guard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks"; In Proc. of the 14th Int. Conf. on World Wide Web, New York, NY, USA 2005, 422-431.

[24] Liu, X.; Datta, A.; Rzadca, K. "Trust Beyond Reputation: A Computational Trust Model Based on Stereotypes"; Electronic Commerce Research and Applications 2012, 30-46.