سال دوازدهم، شماره‌های ۴۵ و ۴۶، پاییز و زمستان۱۳۹۹

صص: ۵۳_۷۰

دو فصلنامه علمی

فناوری اطلاعات و ارتباطات ایران

یک مدل کنترل دسترسی برای شبکه های اجتماعی آنلاین از طریق ارتباطات کاربربه‌کاربر

[*]محمدجواد پیران [**]محمود دی‌پیر

[*]دانشجوی دکتری، دانشگاه آزاد اسلامی واحد علوم و تحقیقات

[**]محمود دی‌پیر، دانشیار، دانشگاه هوایی شهید ستاری

تاریخ دریافت ۱۳۹۹/۰۱/۱۵ تاریخ پذیرش ۱۳۹۹/۰۹/۲۹

نوع مقاله: پژوهشی

چکیده

با فراگیر شدن شبکه‌های اجتماعی و رشد افزون اطلاعات به اشتراک‌گذاری شده در آن‌ها، کاربران این شبکه‌ها در معرض تهدیدهای بالقوه‌ی امنیت و حریم خصوصی داده‌ها قرار دارند. تنظیمات حریم‌خصوصی گنجانده‌شده در این شبکه‌ها به کاربران کنترل کاملی در جهت مدیریت و خصوصی‌سازی دسترسی به اطلاعات اشتراکی‌شان توسط کاربران دیگر نمی‌دهد. در این مقاله به کمک مفهوم گراف اجتماعی، یک مدل جدید کنترل دسترسی کاربربه‌کاربر پیشنهاد شد که امکان بیان سیاست‌های حریم شخصی و کنترل دسترسی دقیق‌تر و حرفه‌ای‌تری را برحسب الگو و عمق روابط میان کاربران در شبکه‌های اجتماعی فراهم می‌کند. در این مقاله با به‌کارگیری روش شاخصه‌ای منظم، روابط غیرمستقیم در میان کاربران موردبررسی و تحلیل قرارگرفته و سیاست‌های دقیق‌تری نسبت به مدل‌های قبلی ارائه‌شده است. ارزیابی نتایج نشان داد، در مورد ۱۰ همسایه برای هر کاربر، تجمع احتمال یافته‌های یک مسیر واجد شرایط، به ترتیب برای سه حلقه شمارنده اول برابر ۱، ۱۰/۵ و ۶۷/۳ درصد است، و نهایتاً برای شمارنده چهارم به ۱۰۰ درصد می‌رسد که با افزایش مشخصه شمارشی تعریف‌شده، زمان اجرای متوسط الگوریتم پیشنهادی و سایر الگوریتم‌های ارائه‌شده در روش‌های قبلی افزایش می‌یابد اما برای حدود بالاتر مشخصه شمارشی، الگوریتم پیشنهادی بهتر از الگوریتم‌های قبلی عمل می‌کند.

واژگان کلیدی: شبکه‌های اجتماعی، امنیت شبکه، حریم خصوصی، حلقه شمارنده، امنیت داده‌ها.

نویسنده مسئول: محمد جواد پیران mohamadjavadpiran@gmail.com

۱-مقدمه

شـــبکه‌های اجتماعی در زندگی روزانه نقش قابل‌توجهی داشـــته و شـــکل ارتباطات تعاملی و به اشـــتراک‌گذاری اطلاعات را در میان مردم تغییر داده‌اند. کاربران حجم گسترده‌ای از اطلاعات خود را در شبکه‌های اجتماعی آنلاین با اهداف مختلفی به اشتراک می‌گذارند. به اشـــتراک‌گذاری اطلاعات و ارتباط میان کاربران که مبتنی بر ارتباطات اجتماعی است تحت عنوان روابط[۱] تعریف می‌شود [۱]. با توجه به این‌که بیشـــتر کاربران باهدف ارتباط با افراد و مخاطبان شناخته‌شده‌ی خود به شبکه‌های اجتماعی آنلاین می‌پیوندند، آن‌ها اغلب اطلاعات حساس یا خصوصی زیادی را در مورد خود منتشر کرده و به اشتراک می‌گذارند. با توجه به شهرت شبکه‌های اجتماعی آنلاین و رشـد انفجاری اطلاعات به اشـتراک‌گذاری شـده در آن‌ها، کاربران شـــبکه‌های اجتماعی آنلاین در معرض تهدیدات بالقوه‌ی امنیت و حریم خصـــوصـــی داده‌های خود قرار دارند. بنابرین جرائم مرتبط با حریم خصـوصـی و امنیت در شـبکه‌های اجتماعی آنلاین توجه تعداد زیادی از رســـانه‌ها و جوامع تحقیقاتی را به خود جلب کرده اســـت[۲و۱]. این رخدادها نشـــان‌دهنده‌ی ضـــرورت کنترل دســـترســـی مؤثر اســـت که موجب محافظت از داده‌ها نســـبت به دسترسی نامشخص و تأیید نشده در شبکه‌های اجتماعی آنلاین می‌گردد [۳].

کنترل دســـترســـی در شـــبکه‌های اجتماعی آنلاین نشـــان‌دهنده مشخصات و خصوصیات منحصربه‌فرد متعددی نسبت به کنترل دسـترسـی معمول می‌باشـد. در کنترل دسـترسـی اجباری و نقش محور، یک سیاست کنترل دسترسی سیستم گسترده توسط مدیر امنیت لحاظ می شود. در کنترل دسترسی اختیاری، مالک و ناشر منبع سیاست کنترل دسترسی را تعریف می‌کند. در سیستم‌های شـــبکه‌های اجتماعی آنلاین کاربران انتظار دارند تا دســـترســـی را نســـبت به منابع و فعالیت‌های مرتبط خودتنظیم کنند؛ بنابراین دســـترســـی به اطلاعات در شـــبکه‌های اجتماعی آنلاین در معرض سیاست‌های تعیین شده از سوی کاربر قرار دارد [۴]. به‌جز مالک اطلاعات منبع، برخی از کاربران مرتبط نیز ممکن اســـت کنترل نمایش اطلاعات منبع یا کاربر را در اختیار داشـــته باشـــند. جهت ممانعت کاربران از دســـترســـی به محتوای ناخواســـته یا نامناســـب، سیاست‌های تعیین شده از سوی کاربر که موجب ارائه نحوه‌ی در نظر گرفتن اطلاعات دسترسی موردنیاز کاربران است به کار گرفته می شوند؛ بنابراین بایستی سیستم این سیاست‌های نسبی را از سـوی کاربران در دسـترس و کاربران هدف همراه باسـیاسـت‌های تعیین‌شده‌ی سیستم جمع‌آوری کرده و آن‌ها را برای تصمیم‌گیری در مورد کنترل جمعی آگاه کند. در شـــبکه‌های اجتماعی آنلاین دسترسی به منابع به‌طورمعمول بر اساس روابط بین دسترسی کاربر و کنترل کاربر در گراف اجتماعی کنترل می‌شود. این نوع از کنترل دســـترســـی رابطه محور، وجود یک رابطه خاص یا مجموعه‌ای از روابط را بین کاربران در نظر گرفته و سیاست‌های کنترل دسترسی را برحسب این روابط کاربر با کاربر[۲] بیان می‌کنند[۵].

در این مقاله یک مدل کنترل دسترسی رابطه محور کاربربه‌کاربر جدید پیشـــنهاد می‌شـــود که امکان بیان ســـیاســـت‌های کنترل دسترسی دقیق‌تر و حرفه‌ای‌تری را برحسب الگو و عمق روابط میان کاربران در شـــبکه فراهم می‌کند. نوع الگو، بیان‌کننده الگوی انواع روابط موجود در مسـیر رابطه از کاربر در دسـترس به سـمت کاربر هدف است. در این تحقیق یک روش شاخصه‌ای منظم از کاراکترها را به کار گرفته و علائم کمی نیز جهت بیان مسـیر رابطه مورداسـتفاده قرار می‌گیرند که نشـان‌دهنده روابط غیرمسـتقیم در میان کاربران اســـت. اســـتفاده از رابطه مبتنی بر عبارات منظم و روابط چندگانه به ما توانایی لازم را در جهت ارائه ســـیاســـت‌های مشخص می دهد که این قابلیت در مدل‌های قبلی وجود نداشت و با توجه به اطلاعات ما، این مدل به‌عنوان اولین مدل کنترل دســـترســـی رابطه‌ای برای شـــبکه‌های اجتماعی آنلاین با این قابلیت شـــناخته می‌شـــود. در ادامه در قســـمت۱، مروری بر مهم‌ترین پژوهش‌های صـــورت گرفته در خصـــوص کنترل دســـترســـی برای شبکه‌های اجتماعی آنلاین انجام شده است؛ سپس در قسمت۲، روش پیشنهادی بیان می‌شود. ارزیابی نتایج در قسمت۳ انجام‌شده و درنهایت قســـمت۴ به نتیجه‌گیری و قســـمت ۵ به پیشـــنهادهایی جهت پژوهش محققین آتی پرداخته است.

۲-مروری بر پیشینه‌ی پژوهش

رنجبر، مومن زاده و ارفعی‌نیا، در پژوهشـــی با عنوان مدل کنترل دسترسی در شبکه‌های اجتماعی، با یک تکنیک کنترل دسترسی

[۱] Relationships

[۲] User-to-User

مؤثر پیشنهاد گردید تا مجاز یا غیر مجاز بودن درخواست دسترسی به منابع مشترک را با توجه به شرایط طرفین چندگانه تعیین نمایند [۶]. روش کنترل دسترسی پیشنهادی برای تجزیه و تحلیل حفظ حریم خصوصی کاربر به کاربر می‌رود. یکی از مشکلات شبکه‌های اجتماعی که کاربران با آن روزانه رو به ر و می‌شوند افراد ناشناسی که برای سوء استفاده از اطلاعات شخصی کاربران منبع به آن‌ها درخواست دوستی می‌دهند و اکثر کاربران منبع بدون هیچ اطلاعاتی راجع به درخواست دهنده ندانسته درخواست را قبول می‌کنند که این امر باعث آسیب‌پذیری می‌شود. مکانیسم‌های امنیتی موجود در شبکه‌های اجتماعی نمی‌تواند به طور مؤثر از اطلاعات خصوصی کاربران محافظت کند. در پژوهش مذکور مدلی ارائه شد که در صد آ سیب‌پذیری کاربران شبکه‌های اجتماعی را کمتر می‌کند. مدل ارائه شده با گذاشتن یک قانون به نام قانون دو ست م شترک که باعث زیاد شدن اعتماد بین کاربر منبع و کاربر درخواست‌دهنده در شبکه اجتماعی می شود. به طوری که اگر تعداد دوستان مشترک بین کاربر منبع و کاربر درخواست دهنده زیاد باشد آن درخواست در قسمت درخواست‌های قابل اعتماد قرار می‌گیرد و اگر تعداد دوستان مشترک کم باشد آن درخواست در قسمت درخواست‌های غیرقابل اعتماد قرار می‌گیرند. بنابراین کاربر منبع متوجه می‌شود که چه کاربرانی قابل اعتماد هستند و چه کاربرانی غیرقابل اعتماد می‌باشند. اما در آخر خود کاربر منلع تصمیم می‌گیرد که چه درخواست‌هایی را قبول کند و یا چه درخواست‌هایی را رد کند.

چنگ و همکاران در تحقیقی به بررسی تصمیم برای استفاده از یک شبکه اجتماعی آنلاین به‌صورت کنش اجتماعی عمدی مفهوم‌سازی و تأثیر نسبی سه مد فرآیندهای نفوذ و تأثیر اجتماعی (رعایت و تطابق درونی سازی و شناسایی) بر کاربرد کنش اجتماعی عمدی (قصد جمعی) موردبرر سی قراردادند. نتایج برر سی بر روی تحقیق تجربی کاربران فیس بوک (تعداد افراد= ۳۸۹ نفر) نشان داد، قصد جمعی برای استفاده از سایت شبکه اجتماعی بر طبق هنجار ذهنی و هو یت اجتماعی تعیین می‌گردد. به‌علاوه هو یت اجتماعی ساختار نهفته درجه دومی است که از مؤلفه‌های درجه اول شناختی ارزیابی و عاطفی تشکیل شده ا ست[۷]. سوریانی و همکاران در مقاله ای به برخی از پژوهش‌ها و تحقیقات انجام‌شده پیرامون اطلاعات سایت‌های شبکه اجتماعی با مرور برخی از کاربردهای جذابی که این اطلاعات را مورد تحلیل قرار می‌دهند را معرفی نمود ند [۸]. این امر منجر به معرفی تعدادی بخش های پژوهشی جدید برای محققین گردید. با مرور تحقیق سوریانی و همکاران، طبقه‌بندی عناوین پژوهشی در مورد شبکه‌های اجتماعی آنلاین مطرح گردید. این طبقه‌بندی شامل ۱۷ زیر عنوان یا زیر بخش تحقیقاتی بود که به همراه برخی تحقیقات انجام‌شده در این زیر بخش‌ها معرفی‌شده است. بر طبق پیامدهای (جزئی قابل‌توجه و بعضاً فجیع) ارتباط اطلاعات شخصی و خصوصی یکی از بخش‌های پژوهشی که محققین روی آن بسیار پژوهش کرده‌اند حریم خصوصی در شبکه‌های اجتماعی آنلاین می‌باشد. بعد از ارائه کلیاتی پیرامون زیر بخش‌های پژوهشی مختلف سایت‌های شبکه اجتماعی بر زیر بخش حفاظت از حریم خصوصی در شبکه‌های اجتماعی تأکید بیشتری کرده و جنبه‌های مختلفی از آن به همراه طبقه‌بندی این جنبه‌ها را معرفی نمودند. یانگ و همکاران تلاشی بر تدوین سامانه‌های توصیه‌گر کاملاً پیش‌برنده رتبه‌بندی / بازخورد چرخه محور انجام دادند که بر استنتاج چرخه‌های صداقت اجتماعی با مقوله خاص تمرکز می‌کند و از داده رتبه‌بندی فعلی همراه با داده شبکه اجتماعی گرفته‌شده است. چندین وار یانس مختلف مرتب‌شده دوستان با چرخه‌های مبتنی بر سطوح تخصصی استنباط شده آن‌ها را طرح‌ریزی می‌کند. از طریق آزمایش‌های صورت گرفته بر داده‌های عمومی موجود شرح می‌دهد که الگوهای پیشنهادی چرخه محور می‌تواند از اطلاعات صداقت اجتماعی کاربر که به‌دقت بی شتر منتج می شود را موردا ستفاده بهتر قرار دهد [۹]. ساردو و هم‌کاران یک چارچوب تجربی را پیشنهاد کرده‌اند که با این چارچوب پروفایل جعلی در لیست دوستان امکان‌پذیر است بااین‌حال این چارچوب به سایت شبکه‌ی اجتماعی خاصی به نام فیس‌بوک محدودشده است. این چارچوب داده‌ها را از لیست دوستان استخراج می‌کند و آن را برای طبقه‌بندی آن‌ها به‌عنوان داده های واقعی یا جعلی مورداستفاده قرار می‌د هد و از رو ند یادگیری ما شین نظارت شده و تحت نظارت ا ستفاده می‌کند [۱۰]. یانگ و همکاران در مقاله ای، پروفایل ده میلیون کاربر از بزرگ‌ترین میکروبلاگ کشور چین و تعداد ۴۱میلیون پروفایل تویتر به‌طور تجربی مطالعه شدند. بامطالعه توپولوژی اع ضا به این ویژگی پایدار پی بردند که کاربران تابع انتشار اطلاعات مطلوب برحسب حداقل زمان تکثیر دست هستند. سپس این دلیل را از دیدگاه تئوریکی بررسی کرده و پی بردند که ساختار شبکه به حداقل انتشار

اطلاعات برحسب حداقل زمان تکثیر وابسته است. این مطالعه کارایی انتشار اطلاعات در میکروبلاگ شبکه‌های اجتماعی آنلاین را نشان می‌دهد. این کارایی با انجام آزمایش های تجربی تحلیل تئوریکی و شبیه سازی عددی تائید می شود[۱۱]. لایت و همکاران در مقاله ای به یکی از روش‌های نظریه‌پردازی درباره تجربه افراد از سایت‌های شبکه اجتماعی به مفهوم قطع ارتباط پرداختند. با معرفی و توسعه یک دیدگاه مبتنی بر قطع ارتباط نشان دادند که استراتژی‌های قطع ارتباط توقف و جلوگیری جزء الزامات عملیاتی کاربران و صاحبان سایت‌هایی نظیر فیس‌بوک است. درواقع پژوهش آن‌ها اثبات کرد که قطع ارتباط در این محیط ها را نباید فقط به‌عنوان رو شی برای مقاومت در برابر این سایت‌ها و ترک آن‌ها در نظر گرفت بلکه این قطع ارتباط می‌تواند به‌عنوان یک عامل تسهیل گر اجتماعی اقتصادی نیز عمل کند [۱۲].

با برر سی پی شینه‌ی پژوهش، یک مدل کنترل د ستر سی رابطه محور کاربربه‌کاربر جدید برای شبکه‌های اجتماعی آنلاین پی شنهاد شده است که امکان بیان سیاست‌های کنترل د سترسی دقیق‌تر و حرفه‌ای‌تری را برحسب الگو و عمق روابط میان کاربران در شبکه را فراهم می‌کند. سیاست‌های کنترل دسترسی در مورد کاربران و منابع برحسب اقدام ثبت‌شده انواع روابط، نقطه شروع ارزیابی و تعداد جهش‌ها در مسیر تشکیل‌شده‌اند. روش پیشنهادی، شاخصه‌ای منظم از کاراکترها را به کار گرفته و از علائم کمی جهت بیان مسیر رابطه استفاده می‌کند که نشان‌دهنده روابط غیرمستقیم در میان کاربران می‌باشند. استفاده از رابطه مبتنی بر عبارات منظم و روابط چندگانه موجب توانایی ارائه سیا ست‌های م شخص نسبت به مدل‌های انجام‌شده در کارهای پیشین می‌گردد. این مدل به‌عنوان اولین مدل کنترل دسترسی رابطه‌ای برای شبکه‌های اجتماعی آنلاین با این قابلیت شناخته می‌شود.

۳- روش پیشنهادی

در این قسمت به بیان مفاهیم پایه و سپس روش پیشنهادی پرداخته‌شده است.

۳-۱ اصول مقدماتی

مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر[۳] که توسط چنگ و همکاران معرفی‌شده است[۷]، روابط کاربر به کاربر[۴] در شبکه‌های اجتماعی آنلاین[۵] را به‌منظور صدور مجوز[۶] دریافت کرده و یک‌زبان تعیین خط‌مشی[۷] مبتنی بر عبارات منظم[۸] تعریف می‌کند. ابتدا مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر را که مدل پیشنهادی ما بر اساس آن است به‌طور خلاصه بیان می‌کنیم.

۳-۱-۱ علامت‌های پایه

علامت $\Sigma = \{\sigma_1.\sigma_2.\dots.\sigma_n.\sigma_1^{-1}.\sigma_2^{-1}.\dots.\sigma_n^{-1}\}$ در مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر ، مجموعه‌ای از انواع روابط را مشخص می‌کند. با در نظر گرفتن یک رابطه از نوع $\sigma_i \in \Sigma$، معکوس رابطه به صورت $\sigma_i^{-1} \in \Sigma$ خواهد بود. یک اقدام[۹] دارای یک فرم فعال و یک فرم منفعل است، که به ترتیب با اقدام و اقدام$^{-1}$ نشان داده می‌شوند. اگر "آلیس" بتواند "باب" را پوک (یک اصطلاح در شبکه های اجتماعی)[۱۰] کند، از دیدگاه "آلیس" عملکرد پوک ولی از دیدگاه "باب" پوک$^{-1}$ خواهد بود.

۳-۱-۲ اجزای مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر

اجزای این مدل در شکل (۱)، نشان داده‌شده است. کاربر در حالی دسترسی[۱۱] نشان‌دهنده یک کاربر فعال است که درخواست دسترسی به یک هدف را دارد و حامل خط‌مشی‌های کاربر در حال دسترسی[۱۲] است. هر اقدام نشان‌دهنده عملیاتی است که توسط یک کاربر در حال دسترسی در برابر یک هدف آغازشده است. یک عملکرد برای کاربر در حال دستر سی به صورت اقدام و برای هدف به‌صورت اقدام$^{-1}$ نشان داده می‌شود. اهداف می‌توانند کاربران هدف[۱۳] باشند (به‌عنوان‌مثال، یک کاربر، کاربر دیگر را پوک کند و منبع هدف[۱۴] باشد). همچنین یک کاربر کنترل‌کننده[۱۵] وجود دارد که دسترسی به یک منبع را کنترل می‌کند و مانند مالک منبع

[۳] User-to-User Relationship-based Access Control (UURAC)
[۴] User-to-User
[۵] Online Social Networks (OSNs)
[۶] Authorization
[۷] Policy
[۸] Expression-based
[۹] Action
[10] Poke
[۱۱] Accessing user (u_a)
[۱۲] Accessing User Policies (AUP)
[۱۳] Target User (TU)
[۱۴] Target Resource (TR)
[۱۵] Controlling User (CU)

دارای رابطه کاربر-به-منبع[۱۶] با خودش است. دسترسی به یک کاربر هدف بر اساس خط‌مشی‌های کاربر هدف[۱۷] کنترل می‌شود که با استفاده از روابط بین کاربران هدف و کاربران درخواست‌کننده دسترسی پیکربندی می‌شود. این درحالی است که دسترسی به یک منبع هدف بر اساس خط‌مشی‌های منبع هدف[۱۸] کنترل می‌شود که با استفاده از روابط بین کاربر کنترل‌کننده و درخواست‌کننده دسترسی پیکربندی‌شده است.

یک درخواست دسترسی $<u_a, act, target>$ نشان‌دهنده شروع یک دسترسی است که $act \in Act$ نوع دسترسی درخواست شده [توسط کاربر در حال دسترسی به هدف] را تعیین می‌کند. اگر u_a درخواست برقراری ارتباط متقابل با یک کاربر دیگر داشته باشد، هدف $u_t \in U$ خواهد بود. اگر u_a تلاش کند به منبعی که متعلق به یک کاربر دیگر است یعنی u_c دسترسی پیدا کند، هدف همان منبع $r_t \in R$ خواهد بود که در آن R یک مجموعه محدود از منابع در شبکه اجتماعی آنلاین است. یک خط‌مشی، شامل قوانینی است که تنظیمات لازم جهت صدور مجوز را تعیین می‌کنند. خط‌مشی‌ها می‌توانند به‌صورت مشخص‌شده توسط سیستم[۱۹] یا مشخص‌شده توسط کاربر[۲۰] باشند. خط‌مشی‌های مشخص‌شده توسط سیستم[۲۱]، قوانین دستگاهی گسترده‌ای هستند که توسط سیستم شبکه اجتماعی آنلاین اجرا می‌شوند درحالی‌که سیاست‌های مشخص‌شده توسط کاربر برای کاربران یا منابع خاص اعمال می‌شود. سیاست‌های مشخص‌شده توسط کاربر شامل TUP،AUP و TRP است که به ترتیب همان خط‌مشی‌های کاربر در حال دسترسی، کاربر هدف و منبع هدف هستند.

۳-۱-۳- نمودار اجتماعی[۲۲]

همان‌طور که در شکل۲ نشان داده‌شده است، شبکه اجتماعی آنلاین به‌عنوان یک گراف ساده علامت‌دار جهت‌دار خلاصه‌شده است که در آن هر گره یک کاربر و هر یال[۲۳] مربوط به یک رابطه کاربر با کاربر است. نمودار اجتماعی یک شبکه اجتماعی آنلاین به‌صورت سه‌گانه $G = <U, E, \Sigma>$ مدل‌سازی می‌شود؛ که در آن، U یک مجموعه محدود از کاربران ثبت‌شده در سیستم است و به‌صورت گره‌هایی در نمودار نشان داده‌شده است.

در این تعریف $\Sigma = \{\sigma_1.\sigma_2.\ldots.\sigma_n.\sigma_1^{-1}.\sigma_2^{-1}.\ldots.\sigma_n^{-1}\}$ یک مجموعه محدود از انواع روابط را نشان می‌دهد، که هر شاخص[۲۴] از نوع σ نشان‌دهنده یک نوع ارتباط است که در سیستم پشتیبانی می‌شود و $E \subseteq U \times U \times \Sigma$ نشان‌دهنده یال‌های گراف اجتماعی و مجموعه‌ای از روابط موجود کاربر است. برای هر $\sigma_i \in \Sigma$ یک $\sigma_i^{-1} \in \Sigma$ وجود دارد که نشان‌دهنده معکوس رابطه نوع σ_i است. برای جلوگیری از بروز خطا و بالا بردن دقت، می‌بایست روابط اصلی و معکوس آن‌ها همواره بر روی نمودار اجتماعی به‌طور هم‌زمان وجود داشته باشند. با در نظر گرفتن یک کاربر $u \in U$، یک کاربر $v \in U$ و یک رابطه نوع $\sigma \in \Sigma$، رابطه (u،v،σ) بیان می‌کند که رابطه نوع σ از کاربر u شروع و در v پایان می‌پذیرد. این رابطه همیشه دارای فرم معادل $(v، u،\sigma^{-1})$ است.

۳-۲ مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر

در این بخش، مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر را توسعه می‌دهیم تا معیارها و اجرای خط‌مشی ReBAC مشخصه آگاه[۲۵] ساده‌تر شود.[۲۶]

۳-۲-۱ مشخصه‌ها[۲۷] در شبکه‌های اجتماعی آنلاین

شبکه‌های اجتماعی آنلاین اطلاعات زیادی مربوط به مشخصه‌های کاربران و منابع را نگهداری می‌کنند. کاربران اطلاعات پروفایل موردنیازدر شبکه‌های اجتماعی مانند نام، سن، جنسیت و غیره را نگه می‌دارند. هنگامی‌که یک بخش از منبع در شبکه اجتماعی آنلاین آپلود می‌شود، ارائه‌دهنده منبع[۲۸] نیز می‌تواند بعضی از

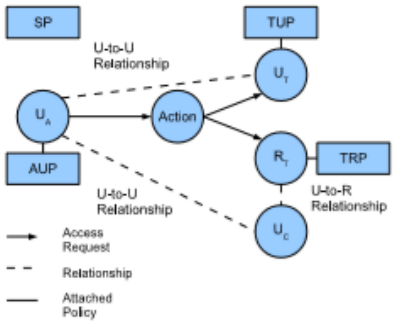
[۱۶] User-to-Resource (U۲R)
[۱۷] Target User Policies (TUP)
[۱۸] Target Resource Policies (TRP)
[۱۹] System-Specified (SS)
[۲۰] User-Specified (US)
[۲۱] System-Specified Policies (SSP)
[۲۲] Social Graph
[۲۳] Edge
[۲۴] Specifier

[۲۵] Attribute-Aware
[۲۶] تأکید می‌کنیم که در مدل کنترل دسترسی مبتنی بر روابط کاربر به کاربر فقط روابط کاربربه‌کاربر در نظر گرفته می‌شود بنابراین منابع تنها می‌توانند به‌عنوان هدف مسیر ارتباط واقع شوند و مسیر ارتباط فقط می‌تواند شامل کاربران باشد.
[۲۷] Attributes
[۲۸] Resource Provider

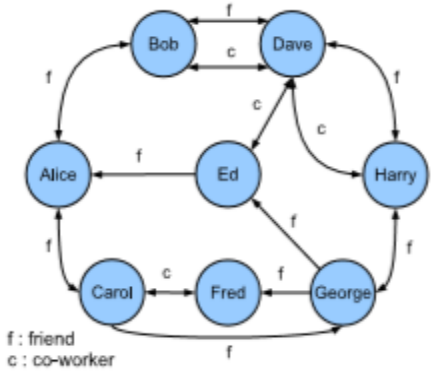
اطلاعـات جـانبی[۲۹] را در مورد منبع پیوســـت کنـد. می توانیم خطم شی‌های مبتنی بر این اطلاعات م شخ صه مرتبط با کاربران و منابع را تعریف کنیم. بااین‌حال، اکثر سیستم‌های ReBAC بر روی برخی از جنبه های خاص روابط مانند نوع، عمق و قدرت تمرکز کرده‌اند. این امر باعث می شود که ReBAC ن سبتاً ساده و کارآمد باشد اما استفاده از ReBAC را ازنظر قابلیت کنترل محدود می‌کند. در ســال‌های اخیر، مطالعات بر روی کنترل دســترســی مبتنی بر مشــخصــه ABAC[۳۰] نشـان داده اسـت که اطلاعات متنی مختلف کاربر، منبع و محاســبات محیط می‌تواند برای کنترل‌های بســیار انعطاف‌پذیر و دقیق‌تر استفاده شود [۷]. بااین‌حال، راه‌حل‌های فعلی ABAC به‌راحتی قابل ا ستفاده در ReBAC در شبکه‌های اجتماعی آنلاین نیســتنـد. درحـالی کـه مـدل هـای معمول ABAC فقط م شخ صه‌های کاربر در حال د ستر سی، منبع هدف و گاهی اوقات محیط محا سبات را در نظر می‌گیرند، ReBAC م شخ صه آگاه باید مشــخص کند که کدام صــفات و صــفات چه کســانی (یعنی مشــخصــه‌های کاربر، مشــخصــه‌های ارتباط) در مسـیر ارتباط بین کاربران در حال د سترسی و کاربران هدف/کنترل‌کننده باید بررسی شود. برای ReBAC مشخصه آگاه، سه نوع مشخصه را به‌صورت زیر تعیین می‌کنیم: مشخصه گره (کاربر، منبع)، مشخصه یال (رابطه) و مشخصه تعداد.[۳۱]

م شخ صه‌گره: کاربران و منابع به‌صــورت گره‌هایی بر روی نمودار اجتماعی نمایش داده می‌شــوند. کاربران مشــخصــه‌هایی دارند که هویت و ویژگی‌های خود مانند نام، سن، جن سیت و غیره را تعریف می‌کنند. ویژگی‌های منبع ممکن است شامل عنوان، مالک، تاریخ و غیره باشد.

مشخصه یال: هر یال با مشخصه‌هایی مرتبط است که ویژگی‌های یال را تو صیف می‌کنند. چنین م شخ صه‌هایی ممکن ا ست شامل رابطه وزن‌ها، نوع‌ها و غیره باشد.



شکل۱. اجزای مدل [۷]



شکل۲ .یک گراف اجتماعی ساده [۷]

همچنین گره‌ها می‌توانند برای یک یا چند شــیء در نظر گرفته شوند. یک نمونه برای مشخصه‌های چند یال، اعتماد انتقال‌پذیری[۳۲] بین دو گره اســت که به‌طور مســتقیم متصــل نیســتند[۳۳]. به‌عنوان‌مثال، ارزش اعتماد دو یا چند یال باید در نظر گرفته شــود تا اعتماد کلی بین کاربر در حال دســترســی و کاربر هدف/ کنترل‌کننده محا سبه شود. م شخ صه‌هایی که گره‌های چندگانه را توصــیف می‌کنند بیشــتر در شــبکه‌های اجتماعی آنلاین دیده می‌شوند، مانند سن متوسط، موقعیت متداول یا عادت مشترک بین افراد. مشــخصــه‌های گره و یال مربوطه نیز می‌توانند برای ایجاد ترکیبات خطمشــی‌ای مونتاژ شــوند. به‌عنوان‌مثال، "آلیس" ممکن است یک خطمشی‌ای را مشخص کند که "فقط کاربرانی که دارای بیش از ۰/۵ اعتماد با "باب" هستند بتوانند به اطلاعات او دسترسی داشته باشند."

مشخصه تعداد: مشخصه‌ی تعداد مواردی را توصیف می‌کند که با هیچ گره و یالی مرتبط نباشند. این مشخصه، الزام رخداد برای

[۲۹] Metadata
[۳۰] Attribute-Based Access Control (ABAC)
[۳۱] Count Attribute

[۳۲] Transitive Trust
[33] منظور از trust ایجاد اعتماد برای اشتراک‌گذاری اطلاعات می‌باشد.

ویژگی‌های مسیر مبتنی بر مشخصه را نشان می‌دهد و پایین‌ترین حد وقوع چنین مسیری را مشخص می‌کند.

۳-۲-۲ فرمول‌بندی خط‌مشی مبتنی بر مشخصه

خط‌مشی مبتنی بر مشخصه، نیازهای کنترل دسترسی را مشخص می‌کند که مربوط به مشخصه‌های کاربران و روابط آن‌هاست. در اینجا، به‌طور قراردادی زبان اساسی مبتنی بر خط‌مشی مشخصه‌ها را تعریف می‌کنیم.

- N و E به ترتیب گره‌ها و یال‌ها هستند.
- ($N\ A_k\ (1 \le k \le K)$ و $E\ A_l\ (1 \le l \le L)$) به ترتیب مشخصه‌های از پیش تعریف‌شده برای گره‌ها و یال‌ها هستند که K تعداد مشخصه‌های گره و L تعداد مشخصه‌های یال است.
- $ATTR(n)$ و $ATTR(e)$ به ترتیب تخصیص مشخصه برای گره n و یال e است، به‌طوری‌که $ATTR(n) \in N\ A_1 \times N\ A_2 \times \cdots \times N\ A_K$ و $ATTR(e) \in EA_1 \times EA_2 \times \dots EA_L$. هر مشخصه تنها دارای یک مقدار در دامنه تعریف شده برای آن است.

در مسیر ارتباط بین دو کاربر در شبکه‌های اجتماعی آنلاین، ممکن است کاربران بسیار دیگری وجود داشته باشند که با روابط متفاوت متصل شده‌اند. هر کاربر یا رابطه دارای مشخصه‌هایی است که می‌تواند برای تعیین قوانین کنترل دسترسی استفاده شود. در برخی موارد، مشخصه‌های تمام کاربران یا روابط در مسیر باید موردتوجه قرار گیرد اما گاهی اوقات تنها مشخصه‌های برخی از کاربران یا روابط استفاده می‌شود. همان‌طور که در جدول (۱) نشان داده‌شده است، از کمیت سنج[۳۴] جامع $\forall$ و کمیت سنج همگانی $\exists$ به ترتیب برای نشان دادن "همه" و "حداقل یک" کاربر(ها) یارابطه (ها) استفاده می‌کنیم. علامت [] برای نشان دادن محدوده‌ها در مسیر رابطه استفاد می‌شود، در حالی که {}مجموعه‌ای از کاربران/روابط واقع شده در یک‌فاصله خاص در مسیر بین کاربر در حال دسترسی و کاربر هدف/کنترل‌کننده را نشان می‌دهد.

جدول۱.کمیت سنج‌های مشخصه

$\forall$ [+m, -n]	تمام اشخاص از m^{th} به n^{th} ام آخر به طوری که، $m + n \le h$ که m و n عدد صحیح غیر منفی هستند و h یک حد حلقه شمارنده است.
$\forall$ [+m, +n]	تمام اشخاص از m^{th} به n^{th} ام آخر به طوری که $m \le n \le h$ باشد.
$\forall$ [-m, -n]	تمام اشخاص از m^{th} ام آخر به n^{th} ام آخر به طوری که $h \ge m \ge n$ باشد.
$\exists$ [+m, -n]	یک نهاد از m^{th} به n^{th} ام آخر به طوری که $m + n \le h$ باشد.
$\exists$ [+m, +n]	یک نهاد از m^{th} به n^{th} ام به طوری که $m \le n \le h$ باشد.
$\exists$ [-m, -n]	یک نهاد از m^{th} ام آخر به n^{th} ام آخر به طوری که $h \ge m \ge n$ باشد.
$\forall$ { $2^{\{\pm N\}}$}	تمام نهادهایی که در این مجموعه وجود دارند.
$\exists$ { $2^{\{\pm N\}}$}	یک نهادی که در این مجموعه وجود دارد.

برای بیان یک محدوده یا موقعیت دقیق در مسیر، از علائم + و - برای نشان دادن جهت‌های مستقیم (از ابتدا) و عقب (از انتها) استفاده می‌کنیم، بعدازاین علامت یک عدد که موقعیت را از جلو یا عقب نشان می‌دهد قرار می‌گیرد. توجه داشته باشید که شاخص برای کاربران از ۰ شروع می‌شود، درحالی‌که شاخص برای روابط از ۱آغاز می‌شود. به‌عنوان‌مثال، برای کاربران، +۰ به معنای کاربر شروع‌کننده و ۱- نشان‌دهنده آخرین کاربر با رابطه از نوع دوم[۳۵] موجود در مسیر است؛ درحالی‌که برای روابط، ۱+ نشان‌دهنده اولین رابطه در مسیر و ۲- آخرین رابطه از نوع دوم است. علامت‌های مثبت و منفی در دو سطر گذشته، به‌جای معنا و مفهوم طبیعی ریاضی، جهت مستقیم یا عقب را نشان می‌دهند.

یک قانون خط‌مشی مبتنی بر مشخصه متشکل از یک کمیت سنجِ تعیین‌کننده مقدار گره /یال خاص، یک عملکرد بولی از مشخصه‌های (گره/یال) و یک پیش‌بین[۳۶] مشخصه تعداد $count \ge i$ به شرح زیر است:

<<quantifier, f(ATTR(N), ATTR(E)), count $\ge$ i>

[۳۴] Quantifier
[۳۵] Second Last User
[۳۶] Predicate

توجه داشته باشید که یک کمیت سنج به یک تابع گره/یال اعمال می‌شود، اما به پیش‌بین مشخصه تعداد اعمال نمی‌شود. به‌عنوان‌مثال، R۳ قانونی را بیان می‌کند که "حداقل باید پنج ارتباط مشترک بین درخواست‌کنندگان و مالک باشد، که شغل آنان دانش‌آموز است". در R۲ و R۳، از پیش‌بین مشخصه تعداد استفاده نمی‌شود و این به‌عنوان "-" نشان داده‌شده است که به‌طور پیش‌فرض count≤۱ را نشان می‌دهد. در اینجا، این خط‌مشی حاوی یک قانون است که نشان می‌دهد "یک کاربر که از طریق بزرگ‌سالانی که آدرسشان" تگزاس" است می‌تواند دسترسی داشته باشد". R۳ نیازمند آن است که در مسیر بین کاربر در حال دسترسی و کاربر هدف/در حال کنترل، کاربران باید در سه فاصله خاص با بزرگ‌سالان باشند.

- $R۱ : (\exists[+۱,-۱], occupation(u) = \text{“student”}, count \geq ۵)$
- $R۲ : (\forall[+۱,-۱], (age(u) \geq ۱۸) \wedge (address(u) = \text{“Texas”}), -)$
- $R۳ : (\forall\{+۱, +۲,-۱\}, (age(u) \geq ۱۸),-)$

۳-۲-۳ مشخصه‌های خط‌مشی

خط‌مشی‌های مبتنی بر مشخصه در مسیرهای ارتباطی خاص بین کاربر در حال دسترسی و کاربر هدف/در حال کنترل اعمال می‌شود. برای این منظور، زبان توصیف خط‌مشی مبتنی بر عبارات منظم پیشنهادشده در [۷] را گسترش می‌دهیم. جدول۲، فهرستی از نمادهای مورداستفاده در زبان توصیف خط‌مشی را تعریف می‌کند. خط‌مشی‌های مدل کنترل دسترسی رابطه محور کاربربه‌کاربر مشخصه آگاه شامل دو بخش است: یک عملیات درخواست شده و یک قانون گراف که دسترسی را بر اساس نمودار اجتماعی تعیین می‌کند. همان‌طور که در جدول۳ نشان داده‌شده است، انواع مختلفی از خط‌مشی‌ها را شناسایی کرده‌ایم. عملیات به شکل غیرفعال اقدام[۱-] در خط‌مشی کاربر هدف و خط‌مشی منبع هدف نشان داده‌شده‌اند، چراکه منبع/کاربر هدف همیشه گیرنده عمل است. خط‌مشی منبع هدف دارای پارامتر اضافی u_c است که نشان‌دهنده کاربر در حال کنترل منابع است. تمایز فرم فعال و غیرفعال یک عمل به خط‌مشی‌های مشخص شده سیستم اعمال نمی‌شود، زیرا این خط‌مشی‌ها با هیچ موجودیت خاص در عمل مرتبط نیست. بااین‌حال، هنگام تعیین خط‌مشی یک سیستم برای یک منبع، می‌توانیم به‌صورت اختیاری منبع را ازلحاظ نوع منبع (r.typename, r.typevalue) اصلاح کنیم. جدول۴ قالب[۳۷] قواعد گراف را با استفاده از فرم Backus-Naur[۳۸] تعریف می‌کند. هر قانون گراف یک گره شروع شونده[۳۹] و یک قانون مسیر[۴۰] را مشخص می‌کند. گره شروع شونده، کاربری را نشان می‌دهد که در آن ارزیابی خط‌مشی در آن شروع‌شده است. یک قانون مسیر نشان‌دهنده یک مجموعه از خصوصیات مسیر است. هر مشخصه مسیر شامل یک جفت (مسیر[۴۱]، حلقه شمارنده) است که الگوی مسیر ارتباط بین دو کاربر و حداکثر تعداد یال‌های مسیر را تعیین می‌کند که برای دسترسی پیدا کردن باید برآورده شود. مشخصه‌های مسیر چندگانه را می‌توان با ربط دهنده "∧" و مجزا ساز "∨" متصل کرد. "¬" بر روی مشخصه‌های مسیر نشان‌دهنده عدم وجود جفت مشخص‌شده الگوی ارتباطی و حد حلقه شمارنده است. الگوی مسیر ارتباط مسیر نشان‌دهنده یک دنباله از تصریح کننده‌های[۴۲] نوع از گره شروع شونده به گره ارزیابی است. برخلاف مدل کنترل دسترسی رابطه محور کاربربه‌کاربر، به‌منظور تسهیل خط‌مشی‌های مبتنی بر مشخصه عبارت جدید AttPolicy را به دستورالعمل اضافه می‌کنیم. AttPolicy می‌تواند پس از مشخصه تمام‌مسیر (مسیر، حلقه شمارنده) یا یک بخش از الگوی مسیر یافت شود. چیزی که به (مسیر، حلقه شمارنده) اعمال می‌شود خط‌مشی مبتنی بر مشخصه فراگیر گفته می‌شود. هنگامی‌که آن از یک بخش مسیر پیروی می‌کند، یک خط‌مشی مبتنی بر مشخصه‌های محلی است که تنها برای این بخش قابل‌استفاده است. برای سادگی، مثال‌ها ازاین‌پس تنها از مشخصه‌های مبتنی بر ویژگی‌های فراگیر استفاده می‌کنند. اکنون نشان می‌دهیم که چگونه قوانین مبتنی بر مشخصه‌ها می‌توانند به برخی از نمونه‌های $UURAC_A$ اعمال شوند.

مثال۱: خط‌مشی مشخصه گره و مشخصه تعداد. "آلیس" می‌خواهد مشخصات خود را برای کاربرانی که حداقل پنج دوست از

[۳۷] Syntax
[۳۸] Backus-Naur Form (BNF)
[۳۹] Startingnode
[۴۰] Pathrule

[41] Path
[42] Specifiers

دانش‌آموزان مشترک دارند به اشتراک بگذارد. او می‌تواند خط‌مشی زیر را برای دوستان- دوستان خود مشخص کند:

- P۱: <profile access, (ua, ((ff, ۲): ∃[+۱, −۱], occupation(u) = “student”, count ≥ ۵))>

اگر او بخواهد به کسی که یک دوست مشترک "باب" را با او به اشتراک گذاشته است، اجازه بدهد پروفایلش را ببیند، این خط‌مشی را می‌توان به شرح زیر بیان کرد:

- P۲: <profile access, (ua, ((ff, ۲): ∃[+۱, −۱], name(u) = “Bob”,))>

برای P۱، سیستم نیاز به پیدا کردن مسیرهایی دارد که با (f f, ۲) مطابقت داشته و مشخصه شغلی کاربران در مسیرها را بررسی کند. اگر حداقل پنج مسیر با این مشخصات وجود داشته باشد، به u_a اجازه داده می‌شود تا اطلاعات پروفایل هدف را ببینند. برای P۲، یک‌بار مسیر (f f, ۲) پیداشده است و نام کاربر در مسیر برابر با "باب" است، و لذا سیستم اجازه دسترسی به آن را خواهد داد.

جدول ۲. علامت‌های مشخصات خط‌مشی

اتصال بده دو کارکتر را با $\sigma \in \Sigma$ یا بال مجموعه خودش پایان – به – پایان که نشانه ی یکسری وقایع از انواع رابطه‌هاست.	الحاق (·)
علامت اتحاد وهمبستگی σ که بزرگتر/مساوی صفر است	ستاره (*)
متصل کردن σ را یک یا چند بار نشان می دهد.	جمع (+)
وقایع σ را صفر یا یک بار را نشان می دهد.	علامت سؤال(?)
تقسیم مشخصات چندین مسیر را نشان می دهد.	اتصال ناپیوسته(∨)
نشانگر پیوند مشخصات چندین مسیر است.	رابط متصل (∧)
عدم وجود جفت مشخص رابطه را نشان می دهد.	علامت منفی(-)
الگوی رابطه و سیاست های مبتنی بر ویژگی را از هم جدا می کند.	دونقطه (:)

جدول ۳. نمایش خط‌مشی کنترل دسترسی

<اقدام، نمودار>	دسترسی به خط‌مشی کاربر
< نمودار ,act^{-1}>	سیاست کاربر هدف
< نمودار ,u_c,act^{-1}>	سیاست منبع هدف

<اقدام، نمودار>	سیاست سیستم برای کاربر
<اقدام, <r.typename, r.typevalue>, نمودار>	سیاست سیستم برای منابع

جدول ۴.دستور زبان برای قوانین گراف

قوانین گرافیکی → “(”StartingNode“, ”PathRule“)”
قوانین مسیر → AttP athSpecExp |AttP athSpecExp Connective PathRule
AttP athSpecExp→ PathSpecExp |PathSpecExp“ : ”AttP olicy
ارتباطات→ ∨|∧
مسیرهای ویژه→ PathSpec |“¬”PathSpec
مسیرهای اختصاصی → “(”AttP ath“, ”HopCount“) ”|“(”EmptySet“, ”HopCount“)”
اعداد → شمارنده حلقه
پیوست خط و مشی‌ها\” : “مسیر| مسیر →پیوست مسیر
انواع توالی مسیر | انواع توالی → مسیر
فضای خالی→ ∅
انواع توالی” ·“انواع پیوست توالی | پیوست توالی → انواع توالی
پیوست انواع توالی→ TypeExp |TypeExp“ : ”AttP olicy
کلمات انواع مشخص کننده |انواع مشخص کننده →انواع خروجی ها
برای پردازی از تحلیل کننده اختصاصی استفاده کنید → خط و مشی
گره شروع → ua|ut|uc
انواع ویژه کلمات → $\sigma_1|\sigma_2|\ldots|\sigma_n|\sigma^{-1}{}_1|\sigma^{-1}{}_2|\ldots|\sigma^{-1}{}_n|\Sigma$
کلمات → “ * ”|“?”|“ + ”
اعداد → [۰ − ۹]+

مثال۲:خط‌مشی مشخصه یال. آلیس به کاربران اجازه دسترسی به تصویر۱ را می‌دهد درصورتی‌که کاربر در فاصله ۳ حلقه (جهش) قرار داشته باشد و بتواند در مسیری با حداقل اعتماد (۰/۵) روابط دوستانه در هر حلقه به او دست یابند. چنین خط‌مشی‌ای به شرح زیر است:

- P۳: <read, P hoto۱, (ua, ((f∗, ۳) : ∀[+۱, −۱], trust(r) ≥ ۰,۵,))>

سیستم قبل از اعطای دسترسی، هر یال موجود در مسیر را بررسی می‌کند تا اطمینان حاصل شود که ارزش اعتماد آن مطابق نیاز است.

مثال ۳: اتخاذ یک خط‌مشی مدل کنترل دسترسی رابطه محور کاربربه‌کاربر، خط‌مشی زیر فقط شامل الزامات مبتنی بر رابطه *(f*,۳)* می‌باشد، درحالی‌که مشخصه‌های گره/یال و مشخصه تعداد هر دو خالی هستند:

- P۴: <poke, (ua, (f∗, ۳) : ∃[+۰, −۰], ,))>

مدل $UURAC_A$ به‌طور یکپارچه با مدل مدل کنترل دسترسی رابطه محور کاربربه‌کاربر، سازگار است. مثال۳ نشان می‌دهد که چگونه خط‌مشی مدل کنترل دسترسی رابطه محور کاربربه‌کاربر، سیاست را می‌توان در $UURAC_A$ اتخاذ کرد.

۴- الگوریتم

این بخش به بررسی دسترسی $UURAC_A$ می‌پردازد. مدل کنترل دسترسی رابطه محور کاربربه‌کاربر، یک الگوریتم بررسی مسیر را فراهم می‌کند تا مسیر صحیح بین درخواست دهنده دسترسی و هدف (و یا مالک منبع) را که مطابق با نیازهای ReBAC است، پیدا کند. برای اجرای خط‌مشی‌های مبتنی بر مشخصه، ارزیابی دسترسی باید در زمان بررسی مسیر، سیاست‌های مبتنی بر مشخصه را در نظر بگیرد. ممکن است فردی بررسی کردن مشخصه را بر روی مسیرهای حاصل که توسط الگوریتم پژوهش حاضرپیدا می‌شود، اجرا کند. بااین‌حال، این احتمال وجود دارد که این کار ناکارآمد باشد. در این تحقیق، یک الگوریتم مسیریابی اصلاح‌شده را برای ترکیب کردن ارزیابی یک خط‌مشی مبتنی بر مشخصه در طی روند یافتن مسیر، ارائه می‌کنیم.

روش ارزیابی دسترسی: درخواست‌های دسترسی می‌توانند به روش توضیح داده‌شده در الگوریتم۱ ارزیابی شوند. برای یک درخواست دسترسی اقدام (u_a)، سیستم خط‌مشی u_a را در مورد اقدام بررسی کرده و بر اساس آن خط‌مشی اقدام$^{-1}$ برای هدف و همچنین سیاست مشخص‌شده در سیستم برای اقدام را به دست می‌آورد. ماژول تصمیم‌گیری، مشخصات مسیر، حلقه شمارنده و قوانین مبتنی بر مشخصه attpolicy را از این خط‌مشی‌ها استخراج می‌کند. این روش، الگوریتم بررسی مسیر را برای تعیین نتیجه هر خط‌مشی اجرا می‌کند. در طی بررسی مسیر، ماژول تصمیم‌گیری نیز باید تمام مشخصه‌های مربوطه را پیگیری کند و مطمئن شود که آن‌ها بر اساس خط‌مشی‌های مبتنی بر مشخصه‌ها برآورده می‌شوند. درنهایت، نتایج تمام خط‌مشی‌های انتخاب‌شده در ارزیابی، یک نتیجه واحد را تشکیل می‌دهند. وجود خط‌مشی‌های چند کاربره ممکن است منازعات خط‌مشی‌ها را افزایش دهد. برای حل این مسئله، می‌توانیم سیاست حل مناقشات مرجع [۷] را اتخاذ کنیم که بر اساس یک استراتژی منسجم، هماهنگ و یا اولویت‌بندی شده عمل می‌کند.

الگوریتم بررسی مسیر مشخصه-آگاه: همان‌طور که در شکل۲ نشان داده‌شده است الگوریتم بررسی مسیر برای عبور از نمودار گرافیکی G از یک استراتژی جستجوی اول عمق(DFS)[۴۳] از گره شروع s استفاده می‌کند. هدف پیدا کردن مسیرهای ارتباط بین گره شروع s و گره ارزیابی t است که این مسیرها الزامات خط‌مشی را برآورده سازند. الگوی مسیر ***path*** و محدودیت حلقه شمارنده الزامات مبتنی بر رابطه را مشخص می‌کنند درحالی‌که ***globalattpol*** نشان‌دهنده قوانین مبتنی بر مشخصه است.

الگوریتم ۱: ارزیابی دسترسی
۱. (Policy Collecting Phase) ۲. if target = u_t then ۳. AUP ← u_a's policy for act, TUP ← u_t's policy for act $^{-1}$, SP ← system's policy for act ٤. else ٥. u_c ← owner(r_t), AUP ← u_a's policy for act, TRP ← u_c's policy for act $^{-1}$ on r_t, SP ← system's policy for act, r.type ٦. (Policy Evaluation Phase) ۷. for all policy in AUP, TUP/TRP and SP do ۸. Extract graph rules (start, path rule) from policy ۹. for all graph rule extracted do ۱۰. Determine the starting node, specified by start, where the path evaluation starts ۱۱. Determine the evaluating node which is the other user involved in access ۱۲. Extract path rules path rule from graph rule ۱۳. Extract each path spec path, hopcount and/or attribute rule attpolicy from path rules ۱٤. Simultaneously path-check each path spec and evaluate the corresponding attribute rule using Algorithm ۳-۲ ۱٥. Evaluate a combined result based on conjunctive or disjunctive connectives between path specs ۱٦. Compose the final result from the result of each policy

الگوریتم ۲: DFSPathChecker(G, path, hopcount, s, t, globalattpol)
۱. DFA ← REtoDFA(path); currentPath ← NIL; d ← ۰ ۲. stateHistory ← DFA starts at the initial state

[۴۳] Depth-First Search (DFS)

```
۳. Extract the quantifier symbol and interval/set information from globalattpol
٤. Get the required rules for attributes of edges and nodes f(ATTR(E),ATTR(N))
٥. Fetch the requirements of count attribute "count ≥ i". If it is omitted, "count ≥ ١".
٦. Assign temporary space for attributes according to the size of the interval/set and the hopcount limit
٧. Initialize counter count ← ٠
٨. if hopcount ≠ ٠ then
٩. return DFST(s)
```

الگوریتم۳. (DFST(u))

```
١. if d + ١ > hopcount then
٢.     return FALSE
٣. else
٤.     for all (v, σ) where (u, v, σ) in G do
٥.     switch
٦.     case ١ v ∈ currentPath
٧.     break
٨.     case ٢ v /∈ currentPath and v = t and DFA with transition σ is at accepting state
٩.      if v and (u, v, σ) is within the range specified by quantifier then
١٠.         attrList ← attrList.(ATTR(v),ATTR(u, v, σ))
١١.       if f(ATTR(v),ATTR(u, v, σ)) = TRUE then
١٢.          count ← count + ١
١٣.          if count ≥ i then
١٤.                    d ← d + ١; currentPath ← currentPath.(u, v, σ)
١٥.              currentState ← DFA takes transition σ
١٦.                                  stateHistory ← stateHistory.(currentState)
١٧.              return TRUE
١٨.         else
١٩.            attrList ← attrList\(ATTR(v),ATTR(u, v, σ))
٢٠.     else
٢١.          d ← d + ١; currentPath ← currentPath.(u, v, σ)
٢٢.            currentState ← DFA takes transition σ
٢٣.                                  stateHistory ← stateHistory.(currentState)
٢٤.              return TRUE
٢٥.              break
٢٦.              case ٣ v /∈ currentPath and v = t and transition σ is valid for DFA but DFA with
```

```
                transition σ is not at accepting state
٢٧.             break
٢٨.              case ٤ v /∈ currentPath and v = t and transition σ is invalid for DFA
٢٩.             break
٣٠.              case ٥ v /∈ currentPath and v ≠ t and transition σ is invalid for DFA
٣١.             break
٣٢.              case ٦ v /∈ currentPath and v ≠t and transition σ is valid for DFA
٣٣.          d ← d + ١; currentPath ← currentPath.(u, v, σ)
٣٤.           currentState ← DFA takes transition σ
٣٥.                                  stateHistory ← stateHistory.(currentState)
٣٦.           if (DFST(v)) then
٣٧.                return TRUE
٣٨.           else
٣٩.                          d ← d − ١; currentPath ← currentPath\(u, v, σ)
٤٠.            attrList ← attrList\(ATTR(v),ATTR(u, v, σ)
٤١. previousState ← last element in stateHistory
٤٢. DFA backs off the last taken transition σ to previousState
٤٣. stateHistory ← stateHistory\(previousState)
٤٤. return FALSE
```

مثال خط‌مشی P۱ را در بخش قبلی در نظر بگیریم:

<profile access, (ua, ((ff, ٢): ∃[+١,−١], occupation(u) = "student", count ≥ ٥))>

گرامر قواعد زبانی[44] ، ابتدا گره شروع شونده u_a را استخراج می‌کند و قوانین مبتنی بر رابطه (f f. ٢) و قوانین مبتنی بر مشخصه "∃[+١,−١], occupation(u) = "student", count ≤ ٥" را تجزیه می‌کند.

سپس الگوریتم۲ یک DFA (ماشین‌های خودکار محدود قطعی[45]) را از عبارات منظم f f ایجاد می‌کند. این کار با استفاده از تابع (REtoDFA) انجام می‌شود. متغیرهای *currentPath* و *stateHistory* به ترتیب به *NIL* و حالت اولیه *DFA* مقداردهی می‌شوند. قواعد مبتنی بر مشخصه به سه بخش تقسیم می‌شود:

"∃[+١,−١], "occupation(u) = 'student' " and "count ≥ ٥". "∃[+١,−١]" ، کل مسیر رابین درخواست‌کننده دسترسی و

[44] Grammar

[45] Deterministic Finite Automata (DFA)

هدف (یا صاحب منبع) که عملکرد تابع گره زیر را اعمال می‌کند، تعیین می‌کند.

"occupation(u) = 'student'" یک تابع مشخصه‌های گره است که شغل کاربران را در مسیر بررسی می‌کند. پیش‌بین مشخصه تعداد "count attribute ≤ ۵" تعداد مشخصی از مسیرهای ارتباط واجد شرایط را مشخص می‌کند. در این مثال برای ذخیره مقادیر مشخصه گره‌ها و یال‌ها در طول گذران، برای مشخصه‌های ۱گره و ۲ یال نیاز به فضا داریم. به‌طورکلی، اگر فاصله [a,–b+] باشد و محدودیت حلقه شمارنده برابر c باشد، باید فضایی را برای مشخصه‌های (c-a-b + ۱) گره و (c-a-b) یال اختصاص دهیم.

پس از مقداردهی d (شاخص حلقه شمارنده) به ۰، الگوریتم۲ تابع تراوایی[۴۶] (تابع گذار، تابع عبور) (DFS DFST) را که در الگوریتم۳ نشان داده‌شده است از گره شروع شونده اجرا می‌کند. با توجه به گره u، الگوریتم ابتدا مطمئن می‌شود که یک گام روبه‌جلو، محدودیت حلقه شمارنده را نقض نمی‌کند. در غیر این صورت، باید خارج و به گره قبلی برگردد. اگر گذار بیشتری مجاز باشد، الگوریتم شروع به انتخاب یک یال (σ، v،u) از مجموعه‌ای از تمام یال‌های پیشامد می‌کند که از u یک‌به‌یک خارج می‌شوند. با توجه به الگوی مسیر ff در مثال، در مرحله اول، الگوریتم به‌طور خاص به دنبال یک یال مشاهده نشده نوع f می‌گردد که در گره دیگری به‌جز گره ارزیابی متوقف می‌شود (مورد۶). اگر چنین لبه‌ای پیدا شود، بیایید بگوییم (u_a, u_1, f) ، الگوریتم مقدار d را یک واحد افزایش داده است، یال را به currentPath اضافه می‌کند، DFA را از حالت اولیه با حرکت گذار f حرکت می‌دهد و تاریخچه وضعیت DFA را بروز رسانی می‌کند. همچنین مشخصه‌های متناظر یال f)، u_1، u_a) و گره u_1 را به لیست مشخصه attrList برای ارزیابی بعدی اضافه می‌کند، زیرا u_1 یک hop از u_a دور است و بنابراین در محدوده [+۱، -۱] قرار دارد. الگوریتم سپس به اجرای (DFST) در گره جدید u_1 ادامه می‌دهد. از گره u_1، فرآیند قبلی را با چک کردن حد حلقه شمارنده و انتخاب یال‌های پیشامد جدید مجدداً تکرار می‌کند. ازآنجاکه حد حلقه شمارنده برابر ۲ است، الگوریتم باید یک یال مشاهده نشده نوع f را پیدا کند که در t (case ۲) پایان می‌یابد. هنگامی‌که یال (u_1، t،f) کشف می‌شود، الگوریتم برای پیدا کردن مشخصه متناظر برای ارزیابی ادامه می‌یابد. [-۱, ۱] نشان می‌دهد که ما همچنین نیاز به بررسی مشخصه آخرین گره دوم در مسیر که u_1 است، داریم. ازآنجایی‌که ما قبلاً ویژگی‌های u_1 را به لیست اضافه کردیم، الگوریتم به‌سادگی تابع ویژگی f (ATTR (u_1) را اجرا می‌کند تا ببیند آیا آن الزامات را برآورده می‌کند یا خیر. اگر الزامات برآورده شوند، بعدازآن مقدار مشخصه تعداد را که در این مورد count است، بررسی می‌کنیم. این خط‌مشی بیان می‌کند که به پنج مسیر مجاز نیاز دارد، بنابراین الگوریتم باید شمارنده را افزایش داده و به گره قبلی بازگردد تا ۴ مسیر دیگر جستجو کند. اگر (u_a, u_1, f)(u, t, f) مسیر پنجم پیداشده توسط ما باشد، DFST (u) الگوریتم ۱، باید مقدار درست و همچنین تمام فراخوانی‌های (DFST) قبلی خود را نیز بازگرداند. درنهایت، این کار سبب می‌شود الگوریتم ۲ مقدار درست را برگرداند (خروجی الگوریتم یک مقدار صحیح و درست باشد)، که نشان می‌دهد تعداد مسیرهای ضروری مناسب برای خط‌مشی را پیداکرده‌ایم. اگر مشخصه گره/یال با الزامات مطابقت نداشته باشد، الگوریتم مشخصه‌ها را از لیست حذف می‌کند (خط۱۸-۱۹) و یال بعدی را امتحان می‌کند.

پس از اتمام جستجوی یال در این سطح و بازگشت به فراخوانی قبلی (DFST) (خط۳۸-۴۳)، باید لبه را رها کرده و تمام متغیرها را به مقادیر قبلی بازنشانی کند. الگوریتم۲پس‌ازاینکه تمام یال‌های پیشامد سبب شوند ua جستجوی ناموفقی داشته باشد مقدار نادرست[۴۷] را برمی‌گرداند.

اثبات صحت این الگوریتم اساساً همانند الگوریتم حلقه شمارنده [۷] است. الگوریتم جدید نه لبه‌های بیشتری را به‌حساب می‌آورد و نه عمق مسیر عبور مجدد را افزایش می‌دهد. ازاین‌رو، پیچیدگی آن هنوز بین O ($dmin^{Hopcount}$) و O ($dmax^{Hopcount}$) محدود می‌شود، جایی که dmin و dmax نشان‌دهنده حداقل و حداکثر درجه خروجی[۴۸] گره و حلقه شمارنده نشان‌دهنده محدودیت حلقه شمارنده است. بررسی ویژگی مشخصه هنگامی‌که الگوریتم یک مسیر واجد شرایط ممکن را پیدا می‌کند سربار[۴۹] اضافی را نشان می‌دهد. هزینه‌های سربار متناسب با مقدار مشخصه‌ها و نوع توابع مشخصه در نظر گرفته‌شده است که به ساختار نمودار اجتماعی مرتبط نیست.

[۴۶] traversal
[۴۷] False
[۴۸] Out-Degree
[۴۹] Overhead

۵- ارزیابی نتایج

در این بخش، نتایجی را نشان می‌دهیم که از مطالعات عملکردی ما روی الگوریتم پیشنهادی بررسی مسیر در مقایسه با الگوریتم مقاله [۷] به‌دست‌آمده است. الگوریتم‌ها را در متلب۲۰۱۴ پیاده‌سازی کردیم و دو مجموعه از آزمایش‌ها را طراحی کردیم تا اجرای ارزیابی درخواست دسترسی را با استفاده از دو الگوریتم آزمایش کنیم. یک تصمیم‌گیرنده‌ی کنترل دسترسی را با چک‌کننده‌های مسیر الگوریتم پیشنهادی و الگوریتم مقاله [۷] روی یک ماشین مجازی با ۴ گیگابایت حافظه و پردازنده‌ی مرکزی ۴هسته‌ای ۲,۵۳ GHz تعبیه کردیم. گراف‌های اجتماعی که باید آزمایش شوند، در پایگاه داده‌ی MySQL روی ماشین آزمایش به همراه قواعد کنترلی نمونه ذخیره شدند تا برای آزمایش آماده شوند. قواعد نمونه و درخواست‌های کنترلی را طراحی کردیم تا اطلاعات لازم گراف را برای تصمیم‌گیری‌های دسترسی گردآوری کنیم. سپس زمانی را ارزیابی کردم که طول می‌کشد تا الگوریتم یک بررسی مسیر را روی گراف کامل کند و نتیجه‌ای را به تصمیم‌گیرنده بازگرداند.

۵-۱ مجموعه داده‌های تحقیق

به هنگام طراحی آزمایش‌ها، دو پارامتر گراف را در نظر می‌گیریم: تعداد حلقه شـــمارنده (عمق) و درجه (عرض). اگرچه تعداد کل گره‌ها در ســیســتم می‌تواند بر عملکرد و مقیاس‌پذیری بســیاری از سیستم‌های گراف تأثیر بگذارد، در سیستم ما، الگوریتم‌ها کل گراف را بررســی نمی‌کنند بلکه تنها مســیرهایی با حلقه شــمارنده های محدود ناشــی از یک گره را بررســی می‌کنند. بنابراین، تعداد کل گره‌ها با توجه به عملکرد چندان قابل‌توجه نیســت. درواقع، حد تعداد حلقه شــمارنده و تعداد لبه‌ها اســت که باید در هر حلقه شمارنده بررسی شود که به‌اندازه‌ی مسأله کمک می‌کند و ازاین‌رو عملکرد سیستم ما را تحت تأثیر قرار می‌دهد.

یک مســئله‌ی مهم در این ارزیابی شــامل انتخاب مجموعه‌های داده‌های نمایشــی اســت. چندین مجموعه‌ی داده‌ی عمومی وجود دارد که از سیستم‌های شبکه‌های اجتماعی آنلاین دنیای واقعی با داده‌های واقعی زیاد گردآوری‌شــده‌اند. بااین‌حال، اغلب آن‌ها تنها یک نوع رابطه را در نظر می‌گیرند یا از اصــلاً از هیچ رابطه‌ای پشــتیبانی نمی‌کنند. قبلا در یک آنالیز مرتبط[۱۳]، نویســندگان مجموعه‌های داده‌های اصلی را اصلاح کرده بودند تا اطلاعات نوع را به آن اضافه کنند، که در آن انواع رابطه به‌طور یکنواخت توزیع‌شده بود. بااین‌حال، افزودن دستی اطلاعات نوع به مجموعه‌های داده‌های واقعی، ممکن است رفتارهای واقعی کاربر را نشان ندهد و درنتیجه تمامیت مجموعه های داده ها را خراب می‌کند و مقدار داده های واقعی را کاهش می‌دهد. علاوه بر این، مجموعه های داده های مختلف، خواص متفاوتی دارند که آن‌ها را غیرقابل مقایسه می‌سازد. ازاین‌رو، داده‌های ترکیبی به جایگزینی برای ما تبدیل می‌شــود، که در آن می‌توانیم گراف های اجتماعی متفاوت را تحت کنترل خود بیاوریم و چند خاصــیت ویژه‌ی این گراف‌ها را آنالیز می‌کنیم. برای تولید گراف‌های اجتماعی ترکیبی، چون آزمایش ما روی مقایســه‌ی شدت متمرکز است، درجه‌ی پیشروی هر گره را به تعدادی ثابت در هر گراف تنظیم می‌کنیم. انتخاب مقصد هر لبه به صورت تصادفی انجام می‌شود.

در مجموعه‌ی اول آزمایش‌ها، عملکرد الگوریتم‌های پیشنهادی و الگوریتم مقاله[۷] را با توجه به قواعد حد تعداد حلقه شمارنده متفاوت بررسی می‌کنیم. به‌طور خاص، پارامترها را به ۱۰۰۰ کاربر و یک نوع رابطه برای مجموعه‌ی آزمایش‌ها تنظیم می‌کنیم. هر کاربر دارای تعداد همسایه‌های یکسانی است، که به‌طور تصادفی در میان۹۹۹ کاربر دیگر انتخاب می‌شوند. انواع مختلف الگوهای مسیر، شامل سرشماری (شمارش یک‌به‌یک) و *-الگو، در قواعد به کار گرفته‌شده‌اند تا تأثیر حد تعداد حلقه شمارنده را روی عملکرد الگوریتم‌ها تحقیق کنند.

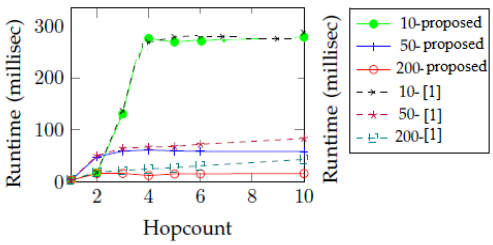
در مجموعه‌ی دوم آزمایش‌ها، قصد داریم تا عملکرد الگوریتم‌ها را در تعداد لبه‌های متفاوتی مطالعه کنیم که باید پیموده شود (یعنی درجه‌ی متوسط گره‌ها در گراف)، تا مقیاس‌پذیری رویکرد خود را نسبت به گراف تراکم نشان دهیم. مانند حالت قبل، ۱۰۰۰ کاربر را انتخاب می‌کنیم، ولی دو نوع از روابط را ایجاد می‌کنیم، به نام‌های «f(riend)» و «c(oworker)»، و به‌طور تصادفی هر رابطه را بین کاربران با یکی از این دو نوع اختصاص می‌دهیم. تعداد همسایه‌ها برای هر کاربر در مقادیر ۱۰۰، ۲۰۰، ۵۰۰ و ۱۰۰۰ در نظر گرفته‌شده است. تنها دو نوع از رابطه وجود دارد و گرف اجتماعی در واقعیت یک گراف پراکنده است، ۱۰۰۰ همسایه برای هر ۱۰۰۰ کاربر، ارزیابی گراف اجتماعی را متراکم می‌کند. سپس قواعد مختلف را روی این۴ گراف اجرا می‌کنیم تا تفاوت‌های آن‌ها را با هم مقایسه کنیم.

در یک قاعده‌ی کنترل دسترسی معین، به طور تصادفی ۱۰۰۰ جفت متفاوت از گره‌های هدف و درخواست دهنده را از گراف انتخاب می‌کنیم و هر الگوریتم را ۵ بار روی این ۱۰۰۰ جفت گره اجرا می‌کنیم. هر اندازه‌گیری، نتیجه‌ی متوسط این ۵۰۰۰ اجرا است. برای انجام مقایسه‌ی عادلانه بین موارد درست و غلط، قواعد مختلفی را طراحی کردیم تا به ۵۰۰۰ مورد درست و ۵۰۰۰ مورد غلط برسیم. برای مقایسه‌ی مساوی بین موارد درست تنظیمات مختلف، تعداد کاربران انتخاب‌شده را طوری مقیاس زدیم که بتوانیم از تعداد مشابه موارد درست به نتایج موردنظر دست‌یابیم.

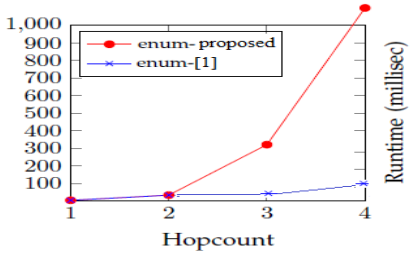
۵-۲ نتایج تجربی

شکل۳ نتایج مجموعه‌ی اول آزمایش‌ها را نشان می‌دهد. الگوریتم‌های پیشنهادی و الگوریتم مقاله [۷] را با استفاده از قواعد با حدود حلقه شمارنده مختلف در هر دو حالت مورد غلط و مورد درست، با هم مقایسه کردیم. برای موارد درست مسیرهای *-الگو، شکل۳ (الف) نشان می‌دهد که زمان اجرای متوسط چگونه با توجه به افزایش در حد حلقه شمارنده تغییر می‌کند. برای انجام یک قیاس گسترده‌تر، در این تست خاص، مقادیر ۱۰، ۵۰ و ۲۰۰ را که نزدیک به ۱۹۰ برابر تعداد دوست‌های متوسط بنا به ادعای فیسبوک است [۱۴] برای تعداد همسایه‌های هر کاربر تنظیم کردیم. مسیرهای *-الگو انعطاف‌پذیری بیشتری نسبت به مسیرهای شماشی در بررسی مسیر دارند. درواقع، نتایج *-الگو، گذشت زمانی کوتاه‌ترین مسیر واجد شرایط را ثبت می‌کند. همان‌طور که انتظار داریم، با افزایش حلقه شمارنده، زمان اجرای موردنیاز برای هر دو الگوریتم افزایش می‌یابد، ولی وقتی تعداد آن به ۴ برسد، روند آن هموار می‌شود. این نشان می‌دهد که یک مسیر واجد شرایط را می‌توان همواره بین دو کاربر در ۴ حلقه شمارنده در این تنظیمات یافت. یک محاسبه‌ی احتمال هم این یافته‌ها را تائید می‌کند. در مورد ۱۰ همسایه برای هر کاربر، تجمع احتمال یافته‌های یک مسیر واجد شرایط، به ترتیب برای سه حلقه شمارنده اول برابر ۱، ۱۰/۵ و ۶۷/۳ درصد است، و نهایتاً برای حلقه شمارنده چهارم به ۱۰۰ درصد می‌رسد. احتمال در دو گراف متراکم دیگر، در سه حلقه شمارنده اول به ۱۰۰ درصد می‌رسد. همچنین یافتیم که الگوریتم پیشنهادی کمی بهتر از الگوریتم BFS برای حد بالای حلقه شمارنده در گراف‌های پراکنده عمل می‌کند، زیرا الگوریتم مقاله [۷] کاوش‌های طولی را پیش از یافتن یک مسیر واجد شرایط انتخاب می‌کند، درحالی‌که الگوریتم پیشنهادی از سرریز در گراف‌های متراکم آسیب نمی‌بینند.

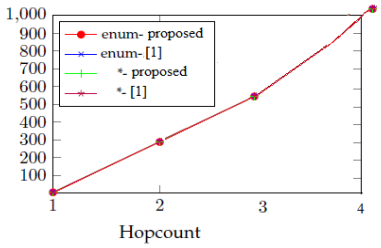
با توجه به ایده‌ی کلاسیک «۶ درجه جدایی» و یافته های «آزمایش‌های جهان کوچک» [۳]، هیچ جفت از افراد در فاصله‌ی بیشتر از ۶ اتصال متوسط قرار نگرفته‌اند. بکستروم و همکاران در [۱۵] نشان دادند که فاصله‌ی متوسط روی گراف اجتماعی کنونی فیسبوک، کمتر از ۶ درجه است و با رشد فیسبوک به ۴,۷۴ کاهش یافته است. بر اساس این یافته‌ها، برای موارد درست مسیرهای شمارشی، حد حلقه شمارنده را برابر ۴ در نظر گرفتیم، زیرا مجموعه‌ی داده‌های ما نسبت به فیسبوک کمتر است. همان‌طور که در شکل۳ (ب) نشان داده‌شده است، وقتی حد حلقه شمارنده افزایش یابد، هزینه‌ی زمانی با الگوریتم مقاله[۷] به طور قابل‌توجهی افزایش می‌یابد، زیرا بدون اینکه جستجو روی تمامی لبه‌ها را در سطح فعلی انجام ندهد، به حلقه شمارنده بعدی نمی‌رود؛ درحالی‌که انتخاب حلقه شمارنده بالاتر، عملکرد الگوریتم پیشنهادی را بدتر نمی‌کند. شکل۳ (ج) مقایسه‌ی بین دو الگوریتم را در حالت‌های مورد غلط نشان می‌دهد. حالت‌های مورد غلط، درواقع بدترین حالت را برای بررسی مسیر نشان می‌دهد که در آن، هر دو الگوریتم باید به طور جامع، تمامی مسیرهای محتمل را در حد حلقه شمارنده از گره آغازین جستجو کرد. بنابراین، دو الگوریتم به طور هم‌زمان در دو تنظیم شمارشی و *-الگوی اجرا می شوند. با افزایش حلقه شمارنده، هزینه‌های زمانی الگوریتم افزایش می‌یابد.



الف

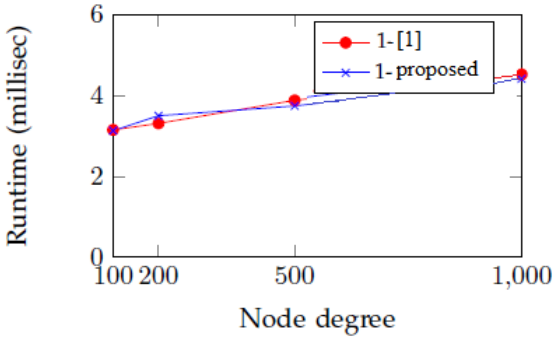


ب

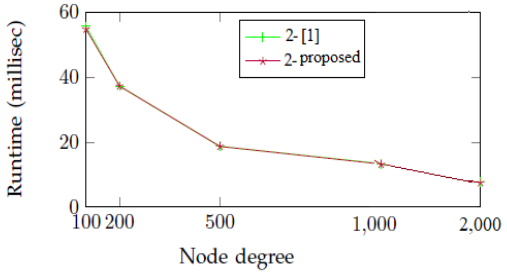


ج

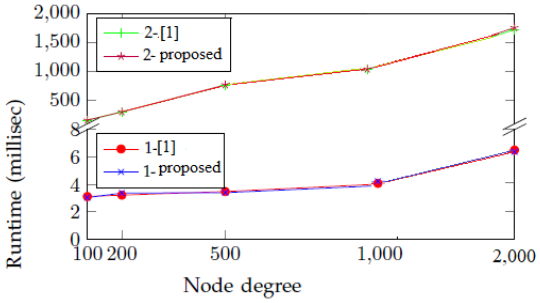
شکل۳. مقایسه حلقه شمارنده در الگوریتم پیشنهادی و الگوریتم مقاله[۷]



الف) حلقه شمارنده۱ –سناریوی درست



ب) ۲ حلقه شمارنده– سناریوی درست



ج) سناریوی غلط

شکل۴. مقایسه الگوریتم پیشنهادی و الگوریتم مقاله[۷] روی درجه گره

شکل۴ مقایسه‌ی عملکردی دو الگوریتم را روی گراف‌ها با درجات متفاوت گره نشان می‌دهد. در حالت‌های مورد درست، همان‌طور که در شکل۴(الف و ب) نشان داده‌شده است، مشخص است که افزایش حد حلقه شمارنده، زمان یافتن یک مسیر واجد شرایط را برای هر دو الگوریتم افزایش می‌دهد، زیرا فضای جستجو افزایش می‌یابد. همچنین مشاهده می‌کنیم که وقتی با قواعد ۲ حلقه شمارنده سروکار داشته باشیم، هزینه‌های زمانی با افزایش در درجات گره کاهش می‌یابد. این اساساً به این دلیل است که احتمال بیشتری وجود دارد تا سریع‌تر یک مسیر واجد شرایط را بین دو گره در گراف متراکم نسبت به گراف پراکنده پیدا کرد، هرچند که بدترین زمان محتمل برای گراف متراکم بیشتر است. برای قواعد ۳ حلقه شمارنده، الگوریتم مقاله [۷] باید تمامی مسیرهای احتمالی را در ۲ حلقه شمارنده اول جستجو کند و بعد به جستجوی حلقه شمارنده سوم بپردازد، در نتیجه با افزایش درجه‌ی گره، زمان بیشتری طول می‌کشد تا یک انطباق را بیابد. در مقابل، الگوریتم پیشنهادی نسبت به همتای الگوریتم مقاله[۷] خود در مواجه با قواعد ۳ حلقه شمارنده و بیشتر، بهتر عمل می‌کند. مانند مجموعه آزمایش‌های اول، به نتایج مشابهی برای دو الگوریتم در حالت‌های مورد غلط دست یافتیم. در انطباق با آنالیز قبلی ما روی پیچیدگی، نتایج مشاهده‌شده از ۴ گراف اجتماعی متفاوت، افزایش زمان نسبت به درجه‌ی گره را نشان می‌دهد.

۶- نتیجه‌گیری و پیشنهادها

در این مقاله، یک مدل کنترل دسترسی رابطه محور کاربر به کاربر توسعه‌یافته برای شبکه‌های اجتماعی آنلاین ارائه داد که از خط‌مشی‌های مبتنی بر رابطه و مبتنی بر مشخصه برای تعیین دسترسی استفاده کرد. اطلاعات مشخصه کاربران و روابط آن‌ها به‌عنوان نمودار اجتماعی در شبکه‌های اجتماعی آنلاین با توجه به کنترل دسترسی مهم است. در این تحقیق، خط‌مشی‌های مبتنی بر مشخصه را فرمول‌بندی شد و دستور زبان را برای مشخصه‌های خط‌مشی توسعه دادیم. زبان خط‌مشی از بیان الزامات در خصوص برخی یا همه کاربران و روابط در مسیر پشتیبانی می‌کند. نتایج ما نشان می‌دهد که هر دو پارامتر درجه‌ی گره و حد حلقه شمارنده، به طور قابل‌توجهی بر عملکرد دو الگوریتم تأثیر می‌گذارد. در چند مورد، جستجوی یک مسیر واجد شرایط با طول ۳ حلقه شمارنده، مدت‌زمان زیادی طول می‌کشد که سیستم و کاربر نمی‌توانند آن را تحمل کنند. بااین‌حال، گراف‌های اجتماعی در واقعیت بزرگ و پراکنده هستند. علاوه بر این، افراد اغلب تمایل دارند تا با سایر

کاربران در یک‌فاصله‌ی نزدیک رابطه داشته باشند، بنابراین حلقه شمارنده بزرگ در عمل چندان مرسوم نیست. اگر کاربران قواعد را با محدودیت‌های کم و حد حلقه شمارنده کوچک تعیین کنند، الگوریتم‌ها قادر هستند تا یک نتیجه را در یک‌زمان کوتاه و منطقی بازگردانند. همچنین به سیستم پیشنهاد می‌دهیم تا یک تایم اضافی را برای هر جستار دسترسی اضافه کند تا از منتظر ماندن برای این حالت‌های شدید اجتناب شود. راه محتمل دیگر برای کاهش طول‌ها این است که به کاربران اجازه داده شود تا یک دید سفارشی و شخصی از گراف اجتماعی داشته باشند و مسیرهای کوتاه را ایجاد کنند تا به طور مکرر برای الگوهای رابطه به کار روند. مشاهده‌ی مهم دیگر از آزمایش‌های ما این است که اگرچه آن‌ها تقریباً دارای عملکرد یکسان برای قواعد ۱ و ۲ حلقه شمارنده هستند، الگوریتم پیشنهادی برای قواعد با مقادیر حلقه شمارنده متوسط (مانند ۳، ۴، ۵ و ...) نسبت به الگوریتم مقاله[۷] بهتر است.بنابراین،الگوریتم‌های بررسی مسیر را بر اساس روش پیشنهادی و روش مقاله[۷] ارائه کردیم و پیچیدگی الگوریتم‌ها را آنالیز نمودیم. امکان‌پذیری رویکرد خود را با بررسی اثبات اصل پیاده‌سازی دو الگوریتم نشان دادیم. درحالی‌که می‌توان مدل پیشنهادی را برای کنترل‌های مبتنی بر مشخصه‌های حتی دقیق‌تر توسعه داد، مدل پیشنهادی یک مکانیسم پایه‌ای جامع برای ReBAC فراهم می‌کند که اجازه کنترل دسترسی به مشخصه‌های متمایز را می‌دهد.

مراجع

[۱] D.M. Boyd, and N.B. Ellison, “Social network sites: Definition,history, and scholarship,” *J.Computer-Mediated Communication*, Vol. ۱۳, no. ۱, pp. ۲۱۰–۲۳۰, ۲۰۰۷.

[۲] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, “Security issues in online social networks,” *Internet Computing*, IEEE, Vol.۱۵, no. ٤, pp. ٥٦–٦٣, ۲۰۱۱.

[۳] G. Bruns, P.W. Fong, I. Siahaan, and M. Huth, “Relationshipbased access control: its expression and enforcement through hybrid logic,” *In Proceedings of the second CODASPY*, pp.۱۱۷–۱۲٤, ۲۰۱۲.

[٤] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. “A semantic web based framework for social network access control,” In Proceedings of the ۱٤th ACM SACMAT, pp. ۱۷۷–۱۸٦, ۲۰۰۹.

[٥] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Semantic web-based social network access control,” *Computers and Security*, p. ۳۰, ۲۰۱۱.

[٦] فاطمه رنجبر کاهریزی، حسین مومن زاده و حسن ارفعی- نیا، "مدل کنترل دسترسی در شبکه‌های اجتماعی"، نخستین کنفرانس تدبیر علوم کامپیوتر، مهندسی برق، ارتباطات و فناوری اطلاعات ایران در جهان اسلام، اردیبهشت ۱۳۹۸.

[۷] Y. Cheng, J. Park, and R. Sandhu, “An Access Control Model for Online Social Networks Using User-to-User Relationships,” *IEEE Transactions on Dependable and Secure Computing* , Vol. ۱۳, no. ٤, ۲۰۱٦.

[۸] Mohammad Soryani, Behrooz Minaei, “Social Networks Research Aspects: A Vast and Fast Survey Focused on the Issue of Privacy in Social Network Sites,” arXiv, ۲۰۱۲.

[۹] X. Yang, H. Steck,Y.Liu, “Circle-based recommendation in online social networks,” *KDD '۱۲ Proceedings of the ۱۸th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. ۱۲٦۷-۱۲۷٥, ۲۰۱۲.

[۱۰] A.J. Sarode, A. Mishra, “Audit and Analysis of Impostors: An experimental approach to detect fake profile in online

[۱۸] P. W. Fong. “Relationship-based access control: protection model and policy language,” *In Proceedings of the first CODASPY*, pp. ۱۹۱–۲۰۲, ۲۰۱۱.

[۱۹] P. W. Fong, M. Anwar, and Z. Zhao. “A privacy preservation model for facebook-style social network systems,” In Computer Security–ESORICS ۲۰۰۹, pp. ۳۰۳–۳۲۰, ۲۰۰۹.

[۲۰] P. W. Fong and I. Siahaan. “Relationship-based access control policies and their policy languages,” *In Proceedings of the ۱۴th SACMAT*, pp. ۵۱–۶۰, ۲۰۱۱.

[۲۱] S. R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H.-C. Choi, “D-FOAF: Distributed identity management with access rights delegation,” *In The Semantic Web–ASWC*, pp. ۱۴۰–۱۵۴, ۲۰۰۶.

[۲۲] M.K. Christy. Cheung, K.O. Matthew Lee, “A theoretical model of intentional social action in online social networks,ELSEVIER,” *Decision Support Systems*, Vol. ۴۹, no.۲, pp. ۲۴–۳۰, ۲۰۱۰.

[۲۳] B. Carminati, E. Ferrari, and J. Girardi. “Performance analysis of relationship-based access control in osns,” *In IEEE IRI*, pp. ۴۴۹–۴۵۶, ۲۰۱۲.

[۲۴] S. Milgram, “The small world problem,” Psychology today, Vol. ۲, no. ۱, pp. ۶۰–۶۷, ۱۹۶۷.

social network,” *ICCCT ۱۵*, pp. ۲۵-۲۷, ۲۰۱۵.

[۱۱] Yong Li, Mengjiong Qian, Depeng Jin, Pan Hui, Athanasios V. Vasilakos , “Revealing the efficiency of information diffusion in online social networks of microblog,” *Information Sciences*, no. ۲۹۳ (۲۰۱۵) ۳۸۳–۳۸۹.

[۱۲] Ben Light and Elija Cassidy, “Strategies for the suspension and prevention of connection: Rendering disconnection as socioeconomic lubricant with Facebook,” *New Media & Society*, Vol. ۱۶, no. ۷, pp. ۱۱۶۹–۱۱۸۴, ۲۰۱۴.

[۱۳] Y. Cheng, J. Park, and R. Sandhu, Relationship-Based Access Control for Online Social Networks: Beyond User-to-User Relationships, Paper presented at the SocialCom/PASSAT, ۲۰۱۲.

[۱۴] J. Ugander, B. Karrer, L. Backstrom, and C. Marlow. “The anatomy of the facebook social graph,” CoRR, ۲۰۱۱.

[۱۵] L. Backstrom, P. Boldi, M. Rosa, J. Ugander, and S. Vigna, “Four degrees of separation,” *CoRR* , ۲۰۰۷.

[۱۶] B. Carminati, E. Ferrari, and A. Perego. “A decentralized security framework for web-based social networks,” *Int.J.o Info. Security and Privacy*, Vol. ۲, no. ۴, ۲۰۰۸.

[۱۷] B. Carminati, E. Ferrari, and A. Perego. “Enforcing access control in web-based social networks,” *ACM Trans. Inf. Syst. Secur*, Vol. ۱۳, no. ۱, ۲۰۰۹.