دوفصلنامه محاسبات و سامانه های توزیع شده
سال پنجم، شماره۲، شماره پیاپی۱۰، صفحه ۱۱۳ تا ۱۲۵ ، سال ۱۴۰۱

ارائه مدلی ترکیبی جهت ارزیابی اعتماد کاربران شبکه‌های اجتماعی آنلاین مبتنی بر تکنیک نرو-فازی و الگوریتم‌های تکاملی

ندا مجیدی*[1] ، بهارک شاکری اسکی[2]

[1]دانشجو کارشناسی ارشد مهندسی کامپیوتر-نرم افزار، واحد رامسر، دانشگاه آزاد اسلامی، مازندران، ایران

[2] گروه کامپیوتر، واحد رامسر، دانشگاه آزاد اسلامی، مازندران، ایران

چکیده

در این پژوهش، یک مدل یادگیری ماشین ترکیبی مبتنی بر نرو-فازی و یکی از الگوریتم‌های فرابتکاری به نام الگوریتم ژنتیک برای شناسایی اعتماد کاربران در شبکه‌های اجتماعی آنلاین پیشنهاد شده است. مدل پیشنهادی تشخیص خودکار اعتماد کاربران را انجام می‌دهد و بینشی در مورد تأثیرگذارترین ویژگی‌ها در طول فرآیند تشخیص می‌دهد. بخشی از کار، یک مدل آبشار رقابتی مبتنی بر اولویت برای انتشار شایعات رقیب و آبشارهای ضد شایعه پیشنهاد می‌شود. این مدلی برای محاسبه ارزش تقدم مبتنی بر باور ارائه شده که توسط آن کاربر تصمیم می‌گیرد شایعه یا ضد شایعه دریافتی در طول انتشار اطلاعات را باور کند. تأثیر شایعه و آبشارهای ضد شایعه در شبکه های اجتماعی آنلاین با در نظر گرفتن یک رویکرد انتشار مبتنی بر همسایگی تجزیه و تحلیل می‌شود. نتایج تجربی با در نظر گرفتن فیس‌بوک، ویکی و توییتر برای اعتبارسنجی مدل PCC برای انتشار شایعه و ضد شایعه در شبکه‌های اجتماعی و ارزیابی الگوریتم DMOG پیشنهادی به‌دست آمد. الگوریتم DMOG با صرفه جویی در حدود ۲۶٪ (برای مقدار تقدم ۱.۰) از کاربران از تحت تاثیر قرار گرفتن شایعات در فیس بوک در مقایسه با ۲۰٪ و ۱۳٪ توسط الگوریتم های موجود، بهبود قابل توجهی را ارائه داد. در توییتر، الگوریتم DMOG حدود ۲۵ درصد از کاربران را از تحت تأثیر قرار گرفتن شایعات نجات داد، در حالی که الگوریتم های دیگر ۱۹ درصد و ۲۱ درصد را تحت تاثیر قرار داده شد. علاوه بر این، در مجموعه داده‌های ویکی، الگوریتم DMOG در مقایسه با الگوریتم‌های موجود، از تعداد کمتری از کاربران اولیه برای انتشار ضد شایعه استفاده می‌کند تا حدود ۴ درصد از کاربران را از تحت تأثیر قرار گرفتن شایعه نجات داده شد. در نهایت، از نتایج تجربی، مشاهده شده است که الگوریتم پیشنهادی با استفاده از پارامترهایی مانند بودجه، تقدم شایعه و تاخیر زمانی در معرفی ضد شایعه عملکرد بهتری از الگوریتم‌های موجود دارد.

کلمات کلیدی: ارزیابی اعتماد کاربران، شبکه‌های اجتماعی آنلاین، تکنیک نرو-فازی و الگوریتم‌های تکاملی.

A hybrid model for Evaluation of the trust of online social network Based on neuro-fuzzy technique and evolutionary algorithms

Neda majidi[1] Baharak shakeri aski[2]

1. Master's student in computer-software engineering, Ramsar Branch, Islamic Azad University, Mazandaran, Iran.

2. Faculty member, Assistant Professor, Islamic Azad university, Mazandaran,Ramsar, Iran.

Abstract

In this research, a hybrid machine learning model based on neuro-fuzzy and one meta-heuristic algorithm called genetic algorithm is proposed to identify user trust in online social networks. The proposed model performs automatic recognition of users' trust and provides insight into the most influential features during the recognition process. As part of the work, a priority-based competitive cascade model is proposed for competing rumor propagation and anti-rumor cascades. This model is presented to calculate the belief-based precedence value by which the user decides to believe the received rumor or counter-rumor during information dissemination. The effect of rumor and anti-rumor cascades in online social networks is analyzed by considering a neighborhood-based diffusion approach. Experimental results were obtained by considering Facebook, Wiki, and Twitter to validate the PCC model for rumor and counter-rumor dissemination in social networks and to evaluate the proposed DMOG algorithm. The DMOG algorithm provided significant improvement by saving about 26% (for a precedence value of 1.0) of users from being influenced by rumors on Facebook compared to 20% and 13% by existing algorithms. On Twitter, the DMOG algorithm saved about 25 percent of users from being affected by rumors, while the other algorithms affected 19 percent and 21 percent. In addition, in the wiki dataset, the DMOG algorithm uses a smaller number of initial users for anti-rumor propagation compared to existing algorithms, saving about 4% of users from being affected by the rumor. Finally, from the experimental results, it has been observed that the proposed algorithm performs better than the existing algorithms by using parameters such as budget, rumor priority and time delay in introducing anti-rumor.

تاریخچه مقاله:

تاریخ ارسال:۱۴۰۱/۱۰/۱۰

تاریخ اصلاحات:۱۴۰۱/۱۱/۱۲

تاریخ پذیرش:۱۴۰۱/۱۲/۲۰

تاریخ انتشار:۱۴۰۱/۱۲/۲۵

Keywords:

evaluation of users' trust, online social networks, neuro-fuzzy technique and evolutionary algorithms

* ایمیل نویسنده مسئول:
nedamajidi6@gmail.com

۱ – مقدمه

شبکه‌های اجتماعی را می‌توان به عنوان مجموعه‌ای از گره‌ها و یال‌ها مشخص کرد که سیستماتیک هستند، به طوری که گره‌ها کاربران، گروه‌ها و جوامع را توصیف می‌کنند و یال‌ها ارتباطات را توصیف می‌کنند. شبکه‌های اجتماعی مبتنی بر وب راه دیگری برای برقراری ارتباط با دیگران فراهم می‌کند که بر روابط اجتماعی در دنیای واقعی تأثیر می‌گذارد. می‌توان گفت بسیاری از روابط ایجاد شده در این شبکه‌ها، علیرغم مجازی بودن، قوی‌تر از روابط واقعی هستند. رشد شبکه‌های اجتماعی مبتنی بر وب در جوامع آنلاین به یک منبع اصلی ارتباط تبدیل شده است و از محبوبیت سایت های شبکه های اجتماعی مانند فیس بوک، یوتیوب، اینستاگرام و غیره قابل مشاهده است. این محبوبیت انگیزه‌ای برای تولید و رشد بسیاری از شبکه‌های اجتماعی مبتنی بر وب در جوامع خاص بوده است. بسیاری از شبکه‌های اجتماعی در حال حاضر برای ارتباط و تعامل با کاربران مختلف در مکان های مختلف طراحی شده‌اند[1].

در همین راستا با پیشرفت زمان، شبکه‌های اجتماعی آنلاین[1] در حال تبدیل شدن به بخشی ضروری از زندگی روزمره مردم هستند، که برای افراد راحت است تا محتوا را منتشر کنند، با دیگران ارتباط برقرار کنند و علایق مشابهی را به اشتراک بگذارند. اخیراً تعداد کاربرانی که به تدریج در حال افزایش هستند برای تعاملات روزانه و سایر تراکنش‌ها با یکدیگر به شبکه‌های اجتماعی آنلاین ملحق شده‌اند که ممکن است قبلاً ملاقات نکرده باشند[2]. اعتماد رابطه‌ای دو طرفه، پیچیده و کمتر درک شده افراد در شبکه اجتماعی است، ابعاد بسیاری دارد و در شکل گیری اجتماعات پایدار، ارزیابی اعتبار و کیفیت اطلاعات و چگونگی جریان آنها در شبکه، تأثیر شایان توجهی می گذارد. با ظهور وب و به دنبال آن شبکه های اجتماعی برخط، ارتباط افراد به محیط های الکترونیکی نیز گسترش یافت. در کنار مزایای این شبکه ها همچون تقویت روابط اجتماعی، تعلق و هویت اجتماعی، مشارکت سیاسی و اجتماعی، توسعه استفاده از رایانه، بارگذاری اطلاعات و به طور کلی رشد سواد رسانه ای، معایب آن را نیز نباید دور از ذهن داشت؛ معایبی همچون اعمال کاربران غیرقابل اعتمادی که سبب نقض حریم خصوصی افراد و افزایش آسیب پذیری فرد و کاهش اعتماد وی به چنین شبکه هایی می شود و در نتیجه سبب محدود کردن اطلاعات به اشتراک گذاشته توسط فرد می گردد. همانگونه که اعتماد در دنیای واقعی پایه شکل گیری رابطه ها و گروه ها است، در اجتماع الکترونیکی نیز مطرح است و می توان گفت به دلیل نبود رابطه چهره به چهره و حضور فیزیکی در اجتماع برخط، اعتماد از اهمیت بیشتری نسبت به اجتماع برون خط برخوردار است. با توجه به نفوذ و گسترش شبکه های اجتماعی برخط بین کاربران و همچنین با توجه به اهمیت موضوع اعتماد در این زمینه، گردآوری و رتبه بندی عوامل اثر گذار بر اعتماد کاربران این شبکه ها به جا و مناسب است؛ چرا که شناسایی چنین عواملی کمکی خواهد بود به ارائه دهندگان شبکه های اجتماعی در زمینه های مختلف که با در نظر گرفتن آن به ارائه خدمات بهتری بپردازند و در نتیجه اعتماد کاربران شبکه ها را جلب کرده و افزایش دهند. ضمن آنکه تعداد کاربران ایرانی که به استفاده از شبکه های اجتماعی برخط می پردازند، رو به افزایش است و در پاسخ به نیاز این کاربران، شبکه های اجتماعی ایرانی نیز راه اندازی شدند[3]. عامل اعتماد به عنوان پایه اساسی روابط و تعاملات افراد در کانون توجه قرار گرفته است؛ به ویژه هنگامی که ضرر و منفعت مالی در میان باشد. از این رو اغلب مطالعات پیشین در زمینه اعتماد در بستر اینترنت و محیط الکترونیکی، اعتماد را با رویکرد تجاری بررسی کرده‌اند. اگر چه در شبکه‌های اجتماعی الکترونیکی موضوع پول و ریسک مالی مطرح نیست، با تأملی عمیق می‌توان دریافت اطلاعات به اشتراک گذاشته شده کاربران که در بعضی مواقع شخصی است، ارزش و ریسک کمتری از جنبه مالی ندارد؛ به ویژه سوء استفاده و استفاده هدفمند از این اطلاعات رو به افزایش است و بسیاری از شبکه‌ها بر مبنای کسب درآمد با استفاده از شناخت افراد از طریق اطلاعات به اشتراک گذاشته شده پایه‌ریزی شده‌اند. اغلب مطالعاتی که به موضوع اعتماد در شبکه‌های اجتماعی پرداخته اند، به دلیل ماهیت اینگونه وب‌گاه‌ها، بیشتر از نظر ساختاری با رتبه‌دهی هر یک از کاربران به محتوای کاربر دیگر، اعتماد کاربران این وبگاه‌ها را سنجیده‌اند[4]. در این تحقیق مدلی برای ارزیابی اعتماد کاربران ارائه می‌شود به این طریق که تعاملات کاربران در شبکه های اجتماعی مورد بررسی و آنالیز قرار می گیرد. این تحقیق به دنبال جواب این سوال است " آیا ارائه مدلی ترکیبی جهت ارزیابی اعتماد کاربران شبکه‌های اجتماعی آنلاین مبتنی بر تکنیک نروفازی و الگوریتم‌های تکاملی امکان‌پذیر است؟"

۲ – پیشینه تحقیق

ولوچ[2] و همکارانش در سال ۲۰۲۱ مدل ارائه حریم خصوصی مبتنی بر اعتماد برای شبکه های اجتماعی آنلاین را ارائه دادند. آنها معتقدند که شبکه‌های اجتماعی آنلاین به یک ابزار اصلی ارتباط و تعامل بین مردم در سراسر جهان تبدیل شده اند. ماهیت حریم خصوصی در طول دو دهه گذشته به چالش کشیده شده است زیرا پیشرفت های تکنولوژیکی مزایا و دیده شدن اجتماعی را برای اعضای فعالی که محتوا را در جوامع آنلاین به اشتراک می‌گذارند، امکان‌پذیر کرده است. در حالی که کاربران شبکه‌های اجتماعی آنلاین محتوای شخصی را با دوستان و همکاران خود به اشتراک می‌گذارند، اما همیشه از قرار گرفتن ناخواسته اطلاعات خود در معرض افراد مختلف از جمله دشمنان، ربات‌های اجتماعی، کاربران جعلی،

[1] Online Social Networks

[2] Voloch

ارسال‌کنندگان هرزنامه یا جمع‌آوری اطلاعات کاملاً آگاه نیستند. جلوگیری از این نشت اطلاعات یک هدف کلیدی بسیاری از مدل‌های امنیتی توسعه‌یافته برای شبکه‌های اجتماعی آنلاین از جمله کنترل دسترسی، مدل‌های مبتنی بر رابطه، مدل‌های مبتنی بر اعتماد و کنترل جریان اطلاعات است. به دنبال تحقیقات قبلی، ادعا می‌شود که برای غلبه بر کاستی هر مدل، یک رویکرد ترکیبی مورد نیاز است. در این مقاله یک مدل جدید برای محافظت از حریم خصوصی کاربران ارائه می‌شود که از سه مرحله اصلی تشکیل شده است که به سه جنبه اصلی اعتماد، کنترل دسترسی مبتنی بر نقش و جریان اطلاعات می-پردازد. این مدل زیر شبکه کاربر را در نظر می‌گیرد و ارتباطات مستقیم کاربر را با نقش‌ها طبقه‌بندی می‌کند. برای مشخص کردن کیفیت اتصالات شبکه به اطلاعات عمومی مانند تعداد کل دوستان، سن حساب کاربری و مدت زمان دوستی متکی است. همچنین اعتماد بین یک کاربر و اعضای شبکه کاربر را ارزیابی می‌کند تا بر اساس مسیرهای جریان اطلاعات بین آنها، این اعضا را آشنا یا دشمن ارزیابی کند. در نهایت، تصمیمات به اشتراک‌گذاری اطلاعات دقیق و قابل اجرا را ارائه می‌دهد و کنترل بهتر حریم خصوصی را در شبکه اجتماعی امکان پذیر می‌کند. در روش پیشنهادی مدل با آزمایش‌های گسترده با استفاده از شبکه‌های مصنوعی و واقعی کاربران ارزیابی شد تا توانایی آن در ارائه ابزاری خوب برای محافظت از حریم خصوصی به کاربر ساده لوح نشان داده شود. هر مرحله از مدل به طور جداگانه اعتبارسنجی و تصمیمات به‌دست‌آمده با دو رویکرد مختلف بررسی شد. نتایج نشان دهنده همبستگی قوی بین تصمیمات اتخاذ شده توسط الگوریتم و تصمیمات کاربران است[5].

شو[1] و همکارانش در سال ۲۰۲۱ یک مدل انتشار اعتماد و ارزیابی شبکه اعتماد در شبکه‌های اجتماعی بر اساس نظریه عدم قطعیت ارائه دادند. آنها معتقدند که توزیع عدم قطعیت می‌تواند به حل مشکل دشوار اندازه‌گیری عدم قطعیت ذهنی در یک رابطه اعتماد کمک کند. این مقاله با استفاده از نظریه عدم قطعیت به بررسی انتشار اعتماد و ارزیابی شبکه اعتماد در شبکه‌های اجتماعی می‌پردازد. ابتدا، انواع روابط بین تصمیم گیرندگان (DMs) [2] شناسایی شده و با تعریف تابع همبستگی بر اساس فواصل نامشخص، شبکه اعتماد زیربنایی ساخته. دوم، مدل‌های بهینه‌سازی عدم قطعیت اعتماد غیرمستقیم تک مسیری و جامع توسعه داده شده تا ارزش اعتماد غیرمستقیم جامع بین تصمیم گیرندگان به راحتی و سادگی محاسبه شود. یک مدل حداکثر درجه اعتقاد برای محاسبه حداکثر درجه اعتقاد و برای به دست آوردن مسیر انتشار اعتماد بهینه بین دو DM معرفی شده است. سوم، با تعریف چنین مفهومی به عنوان درجه سازگاری یک شبکه اعتماد، رابطه اعتماد بین تصمیم گیرندگان را می‌توان به طور موثر اندازه‌گیری کرد. این مدل همچنین یک شبکه اعتماد به ترتیب از منظر نفوذ فردی، سطح رضایت گروه تصمیم‌گیری و ثبات شبکه اعتماد محلی را ارزیابی می‌کند. در نهایت، یک مورد واقعی از انتخاب اعضای یک گروه اعتباری سازمانی برای تأیید اعتبار روش‌ها و مفاهیم پیشنهادی در این مقاله نشان داده شده است[6].

لین[3] و همکارانش در سال ۲۰۲۰ مدل گاردین: ارزیابی اعتماد در شبکه‌های اجتماعی آنلاین با شبکه‌های کانولوشن گراف را ارائه دادند. آنها معتقدند که در شبکه‌های اجتماعی آنلاین مدرن، هر کاربر معمولاً می‌تواند ارزشی برای نشان دادن میزان اعتماد دوستان مستقیم خود ارائه دهد. استنباط چنین ارزشی از اعتماد اجتماعی بین هر جفت گره در شبکه‌های اجتماعی آنلاین در طیف گسترده‌ای از برنامه‌ها مانند بازاریابی آنلاین و سیستم‌های توصیه مفید است. با این حال، ارزیابی دقیق و کارآمد اعتماد اجتماعی بین یک جفت کاربر در شبکه‌های اجتماعی آنلاین چالش برانگیز است. آثار موجود یا قوانین دست ساز را طراحی کرده‌اند که بر دانش حوزه تخصصی تکیه دارند، یا به مقدار قابل توجهی از منابع محاسباتی نیاز دارند، که بر مقیاس پذیری آنها تأثیر گذاشته است. در سال‌های اخیر، شبکه‌های عصبی کانولوشن گراف[4] نشان داده شده است که در یادگیری بر روی داده-های نمودار قدرتمند هستند. مزایای آنها پتانسیل زیادی برای ارزیابی اعتماد فراهم می کند زیرا اعتماد اجتماعی می تواند به عنوان داده های نموداری نمایش داده شود. در این مقاله، Guardian پیشنهاد می‌شود که یک چارچوب سرتاسر جدید که عوامل پنهان در اعتماد اجتماعی را باGCNها یاد می‌گیرد Guardian .برای ترکیب ساختارهای شبکه اجتماعی و روابط اعتماد برای تخمین اعتماد اجتماعی بین هر دو کاربر طراحی شده است. نتایج آزمایشی گسترده نشان داد که گاردین می‌تواند ارزیابی اعتماد را تا ۲۸۲۷ × با دقت قابل‌مقایسه، در مقایسه با پیشرفته‌ترین متون، افزایش دهد[7].

گویال[5] و همکارانش در سال ۲۰۲۰ برای تحلیل پیش‌بینی اعتماد در شبکه‌های اجتماعی پیچیده آنلاین مدلی ارائه دادند. آنها معتقدند که انسان ها در حال استفاده از یکی از بزرگترین شبکه‌های ارتباط اجتماعی توسط وب هستند، توسعه اینترنت راهی را به ظهور شبکه اجتماعی آنلاین می‌دهد که به کاربران کمک می‌کند تا بین کاربران ارتباط برقرار کنند و با آنها ارتباط برقرار کنند و به این ترتیب احساسات و اطلاعات خود را به اشتراک بگذارند و انتقال دهند. یک شبکه اجتماعی آنلاین از آنجایی که کاربران در شبکه اجتماعی آنلاین در حال رشد هستند و چندین فعالیت را انجام می دهند، کاربران یا منابع قابل اعتمادی را می-خواهند. کاربران قابل اعتماد یا منبع اطلاعات یکی از الزامات اولیه به دلیل امنیت و حفظ حریم خصوصی اطلاعات است. یافتن کاربر مورد اعتماد آینده را پیش‌بینی اعتماد می-نامند. چندین ابزار برای پیش‌بینی اعتماد بین کاربران در یک شبکه

[1] Xu
[2] decision-makers
[3] Lin
[4] graph convolutional neural networks
[5] Goyal

اجتماعی آنلاین موجود است. هدف اصلی پیش‌بینی اعتماد، یافتن ارتباط اعتماد بین کاربران در شبکه اجتماعی آنلاین است. در این مطالعه، محققان تکنیک‌های متنوع پیش‌بینی پیوند قابل اعتماد را بررسی کرده و آنها را بر اساس مجموعه داده استاندارد ارائه شده در اختیار ما ارزیابی کرده‌اند[8].

برای اندازه‌گیری اعتماد نیز گنگ[1] و همکارانش در سال ۲۰۲۰ مدلی در شبکه‌های اجتماعی بر اساس نظریه عدم قطعیت خطی ارائه دادند. آنها معتقدند که در شبکه‌های اجتماعی، روابط اعتماد مبنایی برای تعاملات بین گره های تصمیم‌گیری است. روابط اعتماد ذهنی و پویا هستند و تنها داده‌های نمونه کمی برای اندازه گیری قدرت این ارتباطات وجود دارد. تئوری عدم قطعیت یک سیستم ریاضی است که درجه اعتقادی کارشناسان را مطالعه می‌کند و روش جدیدی برای سنجش اعتماد به شبکه های اجتماعی ارائه می‌دهد. در این مقاله، نظریه عدم قطعیت برای مدل‌سازی شبکه‌های اجتماعی اعمال می‌شود. برای هر ویژگی که اطلاعات خاصی را نمی‌توان مستقیماً به دست آورد، اعتماد توصیه شده بر اساس مقادیر اعتماد مستقیم مشتق می‌شود و محدودیت‌های زنجیره‌های اعتماد تک مسیری ایجاد می‌شوند. برای جلوگیری از عدم قطعیت‌های ثانویه ناشی از وزن‌دهی ذهنی در حالی که زنجیره های چند گره‌ای و چند مسیری در نظر شد، دو عملگر تجمع اعتماد وزن دار برای انجام یک مدل تجمع متعدی چند اعتمادی توسعه داده شده‌اند. درجات باور گره‌ها، زنجیره‌های اعتماد و کل شبکه کمی‌سازی می‌شوند و یک مدل اندازه‌گیری اعتماد شبکه اجتماعی بر اساس نظریه عدم قطعیت ساخته می‌شود. در صورت کمبود داده در مورد زنجیره اعتماد، از یک محدودیت آستانه اعتماد برای محاسبه محدوده زنجیره ناقص استفاده می شود[9].

همچنین برای ارزیابی قابلیت اعتماد چندین مقاله ارائه شد که خان[2] و همکارانش در سال ۲۰۲۱ دیدن و باور، ارزیابی قابلیت اعتماد کاربران توییتر ارائه دادند. آنها معتقدند که شبکه‌های اجتماعی و سرویس‌های میکروبلاگینگ مانند توییتر نقش مهمی در به اشتراک گذاری اطلاعات دیجیتال دارند. با وجود محبوبیت و مفید بودن رسانه های اجتماعی، موارد زیادی به عنوان مثال، از طریق افزایش یا کاهش اعتبار کاربران وجود داشته است که کاربران فاسد راه‌هایی برای سوء استفاده از آن پیدا کرده اند. در نتیجه، در حالی که رسانه‌های اجتماعی دسترسی بی‌سابقه‌ای به اطلاعات را تسهیل می‌کنند، اما چالش جدیدی یعنی تعیین اعتبار اطلاعات مشترک را نیز به وجود می‌آورند. در حال حاضر، هیچ روش خودکاری برای تعیین اینکه کدام اخبار یا کاربران معتبر هستند و کدام غیر معتبر وجود ندارد. از این رو، ایجاد سیستمی که بتواند اعتبار کاربران شبکه های اجتماعی را بسنجد، به موضوعی بسیار مهم تبدیل شده است. تخصیص امتیاز اعتبار به یک کاربر، نه تنها جامعه تحقیقاتی، بلکه بیشتر بازیگران بزرگ هر دو طرف را برانگیخته است(مانند فیس بوک، در سمت صنعت، و احزاب سیاسی در بخش اجتماعی). در این مقاله مدلی ایجاد شده که امید است در نهایت افزایش اعتماد در جوامع شبکه های اجتماعی را تسهیل و حمایت کند. این مدل داده‌ها را جمع آوری کرد و رفتار ۵۰۰۰۰ سیاستمدار در توییتر را تجزیه و تحلیل کرد. امتیاز تأثیر، بر اساس چندین ویژگی انتخاب شده، به هر کاربر ارزیابی شده اختصاص داده شد. علاوه بر این، کاربران سیاسی توییتر با استفاده از جنگل تصادفی، پرسپترون چندلایه و ماشین بردار پشتیبان به عنوان قابل اعتماد یا غیرقابل اعتماد طبقه‌بندی شدند. یک مدل یادگیری فعال برای طبقه‌بندی هرگونه رکورد مبهم بدون برچسب از مجموعه داده استفاده شد. در نهایت، برای اندازه‌گیری عملکرد مدل پیشنهادی، از دقت، یادآوری، امتیاز F1 و دقت به عنوان معیارهای ارزیابی اصلی استفاده شد [10] و الخمیس[3] و همکارانش در سال ۲۰۲۱ قابلیت اعتماد کاربر در شبکه‌های اجتماعی آنلاین یک بررسی سیستماتیک را ارائه دادند. آنها معتقدند که محبوبیت روزافزون شبکه‌های اجتماعی و پذیرش آسان آنها از کاربران جدید، پیامد ناخواسته ایجاد محیطی است که در آن کاربران ناشناس می‌توانند به روش‌های مخرب عمل کنند. اگرچه این پلتفرم‌ها انگیزه های زیادی برای جلوگیری از چنین اتفاقاتی دارند، اما نتوانسته‌اند با حجم عظیم اطلاعاتی که باید پردازش شوند، کنار بیایند. علاوه بر این، تمایل مهاجمان به تغییر سریع استراتژی‌ها در پاسخ به اقدامات دفاعی نیز یک چالش است. از این رو، تحقیقات در مورد مسائل مربوط به قابلیت اعتماد کاربران در شبکه های اجتماعی، با مطالعات جالب بسیاری در سال های اخیر انجام شده است. در این کار، هدف بررسی وضعیت کنونی این حوزه و ارائه تحلیلی از مطالعات منتشر شده بین سال‌های ۲۰۱۲ و ۲۰۲۰ است که سعی در رفع این مشکل با استفاده از روش‌شناسی‌های مختلف دارد. برخی از راه حل‌های مورد بحث در ادبیات را می‌توان به عنوان پروتکل های شناسایی ربات توصیف کرد، در حالی که برخی دیگر بر محافظت از هرزنامه، تشخیص اخبار جعلی یا رتبه‌بندی صحت محتوای تولید شده توسط کاربر تمرکز دارند. بسیاری از این راه حل‌ها از جنبه های مختلف مزایای ملموسی را ارائه می‌دهند، با این حال هیچ یک از آنها قادر به ارائه حفاظت همه جانبه در برابر انواع حملات ممکن نیستند. بنابراین، نظارت بر این حوزه علمی یک وظیفه کلیدی است و این بررسی امیدوار است با برجسته کردن کارهای اخیری که به این موضوع می پردازد، به درک بهتر مفهوم اعتماد کاربران آنلاین منجر شود[11] و همچنین الشافعی[4] و همکارانش در سال ۲۰۲۲ نیز یک سیستم فازی برای ارزیابی قابلیت اعتماد کاربران در یک شبکه

[1] Gong
[2] Khan
[3] Alkhamees
[4] SHAFIEI

اجتماعی ارائه دادند. آنها معتقدند که در سال‌های اخیر، ظهور شبکه‌های اجتماعی مختلف مبتنی بر وب منجر به رشد کاربران شبکه‌های اجتماعی شده است. این شبکه‌ها به عنوان رسانه‌ای برای انتشار اطلاعات و ارتباطات محبوب شده‌اند. دولت‌ها و سازمان‌ها نیز از شبکه‌های اجتماعی به عنوان بستری برای خدمات بهتر استفاده می کنند. با این حال، فعالیت در چنین شبکه‌هایی به میزان اعتمادی که اعضا به یکدیگر دارند بستگی دارد. ترکیب ویژگی‌های شخصیتی یک فرد می‌تواند تصور ذهنی از میزان اعتمادی که یک فرد دارد ایجاد کند. این میزان اعتماد می‌تواند بر تعاملات آینده فرد تأثیر بگذارد. بنابراین، اعتماد یک امر ضروری و مهم در این شبکه‌ها است، به خصوص زمانی که شخصی با شخص دیگری در یک شبکه اجتماعی مبتنی بر وب تعامل دارد. در این مقاله به بررسی این موضوع پرداخته شده و روشی برای ارزیابی آن ارائه می‌شود. اندازه‌گیری دقت برای کاربرانی که با شبکه اجتماعی در تعامل هستند آسان نیست. در اینجا، تعاملات مجازی است. در این مقاله، از منطق فازی برای اعمال داده‌های مبهم و ارزیابی قابلیت اعتماد با در نظر گرفتن ویژگی‌های شخصیتی مختلف کاربران مانند قابلیت اطمینان، در دسترس بودن، علاقه، صبر و سازگاری استفاده شده است. با استفاده از این ویژگی‌ها به عنوان ورودی سیستم فازی و بر اساس قوانین فازی مربوطه، قابلیت اعتماد کاربران در شبکه‌های اجتماعی ارزیابی شد. سیستم فازی پیشنهادی قابل توسعه است، زیرا در این سیستم، اعتماد را می‌توان به عنوان مجموعه ای از یک یا چند ویژگی شخصیتی تعریف کرد. مجموعه داده شبکه اجتماعی Epinions نیز برای شبیه‌سازی و اعتبارسنجی رویکرد پیشنهادی استفاده شد. در روش پیشنهادی، مقدار MAE کمتر از ۰.۰۱۵ و مقدار F-Score بیشتر از ۰.۸۶ است. بر اساس نتایج، سیستم فازی ارائه شده دقت قابل قبولی را برای ارزیابی قابلیت اعتماد کاربران نشان می‌دهد[1].

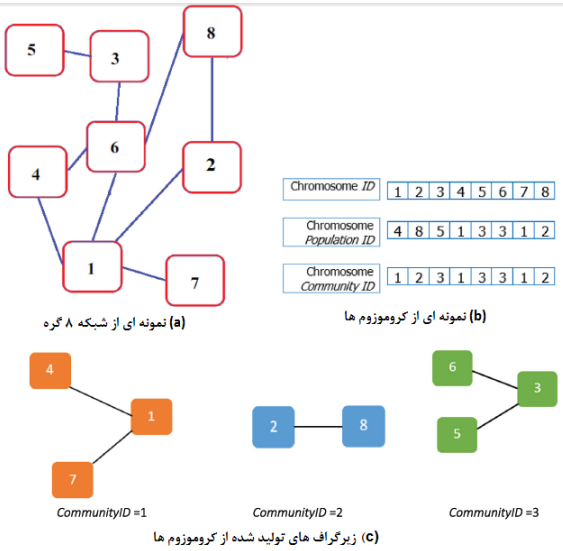
۳ – راهکار پیشنهادی

شبکه‌های اجتماعی رفتاری مشخص با ساختار اجتماعی دارند. جامعه شامل طیف گسترده ای از سازمان های گروهی مانند خانواده، حلقه های کاری و دوستی، روستاها، شهرها و ملت ها است. گسترش اینترنت همچنین منجر به ایجاد گروه های مجازی در وب مانند جوامع آنلاین شده است. جوامع اجتماعی در حال حاضر موضوع مهمی هستند که برای مدت طولانی مورد مطالعه قرار گرفته است. با توسعه فناوری اطلاعات، استفاده از شبکه های اجتماعی در جامعه ما به طور تصاعدی در حال افزایش است. این باعث تغییر شدید در نحوه واکنش افراد به رویدادها و تعامل با یکدیگر می شود. از آنجایی که ساختار جامعه یک ویژگی مهم شبکه های اجتماعی است، معمولاً گروه های سازمان یافته خاصی از کاربران را با شرایط، سرگرمی ها یا روابط نزدیک تر نشان می دهد. بنابراین، شناسایی ساختار جامعه در شبکه‌های اجتماعی فرآیند قابل توجهی برای تحلیل آنها است.

با توجه به اینکه تشخیص جامعه (CD) یک مشکل NP-hard است، روش‌های کلاسیک برای حل این نوع مشکلات کافی در نظر گرفته نمی‌شوند. در عوض، هدف آن تولید راه‌حل‌های نامزد مناسب برای مسائل CD با استفاده از رویکردها یا الگوریتم‌های فراابتکاری است.

در روش پیشنهادی ترکیب الگوریتم نرو-فازی و الگوریتم ژنتیک برای حل مسئله استفاده شده است و تا آنجا که مشخص است، این الگوریتم ها برای اولین بار در این مطالعه برای مسئله CD اعمال می‌شوند. از آنجایی که نسخه‌های اصلی الگوریتم‌ها برای حل مسائل پیوسته ارائه شده‌اند، الگوریتم‌ها ابتدا در معرض گسسته‌سازی قرار می‌گیرند و با حل مسئله سازگار می‌شوند. هدف ارایه روشی به جهت بهبود زمان و اعتماد ساخت CDها در نهایت است[12]. تشخیص جامعه یک ابزار مهم در تجزیه و تحلیل شبکه های پیچیده بزرگ است. جامعه به طور کلی به عنوان گروهی از رئوس با یال های با چگالی بالا در داخل گروه و یال های کم تراکم در خارج از گروه تعریف می شود. مشکلی که تشخیص جامعه در تلاش برای حل آن است، شناسایی جوامع رئوس است که نسبت به بقیه شبکه به هم پیوسته ترند. شناسایی و تجزیه و تحلیل ساختار اجتماعی شبکه ها یافته های مهمی را در زمینه های مختلف از زیست شناسی تا وب به دست آورده است. چنین مطالعاتی نشان می‌دهد که جوامع واحدهای سازمانی معناداری را تشکیل می‌دهند و مفاهیم جدیدی در مورد ساختار و عملکرد کل شبکه مورد مطالعه ارائه می‌دهند.

روش ها و الگوریتم های مختلفی برای یافتن ساختارهای جامعه در شبکه های پیچیده پیشنهاد شده است. هدف اصلی الگوریتم ها آشکار ساختن ساختاری است که در آن یک جامعه را تعریف می کنند. تعاریف رسمی مختلفی برای یک جامعه وجود دارد. روش پیشنهادی از معادله (معادل (۱)) پیشنهاد شده توسط گیروان و نیومن استفاده می کند که از معیاری به نام مدولار بودن شبکه استفاده می کند[12].



شکل ۱: نمایش یک شبکه نمونه و زیرگراف های به دست آمده[12].

الگوریتم‌های روش پیشنهادی از ساختار نمایش مجاورت مبتنی بر مکان (LAR) برای نمایش مبتنی بر نمودار استفاده می‌کنند. هر ژن در کروموزوم حاوی دو بخش مختلف اطلاعات به نام‌های PopulationID و CommunityID است. قسمت اول یک گره مجاور به طور تصادفی انتخاب شده از همسایگان گره i را نشان می دهد. دومی اطلاعات جامعه به نام CommunityID گره iامین جوامع تولید شده توسط قسمت اول را نشان می دهد. در روش پیشنهادی، نمونه ای از یک شبکه ۸ گره در شکل ۱(a) ارائه شده است. شکل ۱(b) نیز نمونه ای از کروموزوم های ساخته شده بر اساس شبکه داده شده را نشان می دهد. در این شکل، کروموزوم با سه توالی مختلف نشان داده شده است که اطلاعات مربوط به ID، PopulationID و CommunityID را ارائه می دهد. لیست اول نمایانگر توالی گره، لیست دوم نشان دهنده گره همسایه انتخاب شده و لیست سوم نمایانگر جامعه گره است. علاوه بر این، شکل ۱(c) زیرگراف های تولید شده توسط کروموزوم داده شده را نشان می دهد. در این مثال، سه زیرگراف با رنگ‌های مختلف نشان داده شده‌اند[12].

ماکزیمم سازی مدولاریته یکی از پرکاربردترین روش ها برای تشخیص جوامع در شبکه‌ها است. این رویکرد با ارزیابی کیفیت تقسیم یک شبکه به چندین اجتماع عمل می کند. با کمک این تابع هدف، جوامع بالقوه و گره های آنها از شبکه مربوطه بهینه می شوند تا ساختار جامعه ای را پیدا کنند که بالاترین هزینه را ایجاد کند. روش‌های مبتنی بر مدولار سعی در به حداکثر رساندن مقدار مدولاریته دارند که تعریف آن در معادله (۱) قابل مشاهده است[12].

$$Q_{Basic} = \sum_{i=1}^{n}(e_{ij} - a_i^2) \quad (1)$$

که در آن e_{ij} تعداد اتصالات با یک سر در گروه i و سر دیگر در گروه j و $\sum_{i=1}^{n}(e_{ij})$ تعداد اتصالات با یک سر در گروه است. این الگوریتم سعی می‌کنند بهترین مقدار Q_{Basic} را در مسائل تشخیص جامعه سخت NP، بیشتر با استفاده از الگوریتم فراابتکاری مانند الگوریتم ژنتیک بیابند.

برای ایجاد یک تابع مدولاریته کلی تر، زمانی که یک شبکه نمونه معین با هر ساختار نموداری نشان داده می شود، ساختارهای جامعه حاصل را می توان به عنوان زیرگراف هایی با ویژگی ها و کمیت هایی مانند حداکثر ویژگی های مشترک و تعداد تعامل در نظر گرفت. در حالی که گره ها که اعضای اصلی این جوامع هستند، باید حداکثر روابط یا حداکثر ویژگی های مشترک را با گره های دیگر جامعه خود داشته باشند، در حالی که باید حداقل روابط یا حداقل ویژگی های مشترک را با گره های جامعه دیگر داشته باشند. با توجه به تراکم روابط یا ویژگی های مشترک، ساختارهای جامعه نیز نمونه های متفاوتی در زندگی واقعی دارند. در حوزه‌های اجتماعی، افرادی که روابط شدید دارند در یک اجتماع هستند، در مناطق بیولوژیکی، موجودات زنده که از یکدیگر تغذیه می‌کنند در مستعمرات مشابه هستند و در حوزه انفورماتیک، رایانه با حداکثر تبادل داده در یک توپولوژی قرار دارند. و همه اینها را می توان به عنوان مثالی از مشکل CD بیان کرد[12].

فرض کنید یک ساختار گراف داده شده G(V, E) یک شبکه را نشان می دهد و G، V و E به ترتیب نمودار، مجموعه ای از رئوس و مجموعه ای از یال ها را نشان می دهند[12].

$$V = [v_i | i = 1,2,3,\dots,n] and\ e = [e_j | j = 1,2,3,\dots,m] \quad (2)$$

که در آن i و j نشان دهنده شاخص رأس و شاخص یال هستند در حالی که n و m نشان دهنده تعداد کل رئوس و تعداد کل یال ها هستند. علاوه بر این، فرض کنید یک ماتریس مجاورت به نام AdjM تعریف شده است که روابط بین اعضای مجموعه E و V را با ابعاد nxn نشان می دهد. AdjM بر اساس معادله (۳) محاسبه می شود[12].

$$AdjM_{(i,j)} = \begin{cases} 1 & if\ node\ i\ and\ j\ are\ connected\ to\ each\ other \\ 0 & otherwise \end{cases} \quad (3)$$

معادله ۳-۳ تابع تناسب مدولار بودن نمودار G را نشان می دهد.

$$Q = \frac{1}{2\times m}\sum_{ij}\left(AdjM_{(i,j)} - \frac{k_i \times k_j}{2\times m}\right) \times \delta(C_i, C_j) \quad (4)$$

جایی که Q نشان دهنده تابع تناسب است که باید حداکثر شود. $AdjM_{(i,j)}$ نشان دهنده ماتریس مجاورت گراف G است، در حالی که تعداد کل یال ها در کل شبکه با استفاده از معادله (۵) ارزیابی می‌شود. ki و j به ترتیب درجات راس های iام و jام را مشخص می کنند. درجه راس ki با کمک معادله (۶) پیدا می شود. Ci و j به ترتیب نشان دهنده جامعه ای هستند که رئوس iام و jام به آن تعلق دارند. $\delta(C_i, C_j)$ همچنین وضعیتی را نشان می دهد که نشان می دهد آیا رئوس i و j در یک جامعه هستند یا خیر. خروجی $\delta(C_i, C_j)$ مطابق معادله (۷) محاسبه می‌شود[12].

$$m = \frac{1}{2}\sum_{ij} Ad_jM_{(i,j)} \quad (5)$$

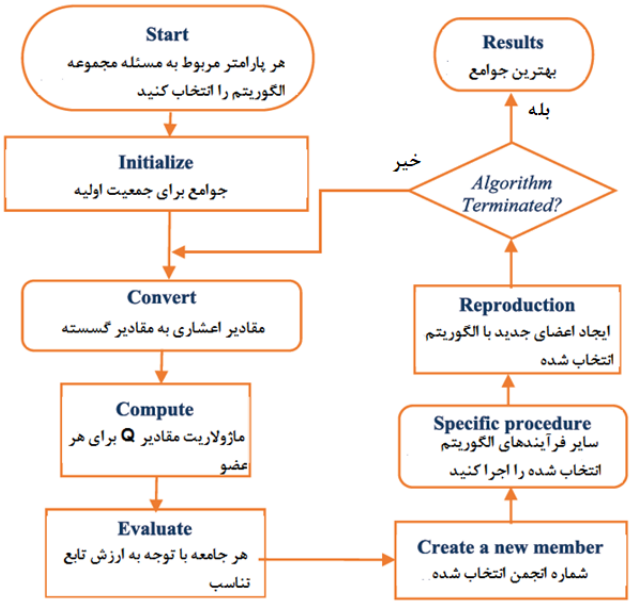
$$k_i = \sum_j Ad_jM_{(i,j)} \quad (6)$$

$$\delta = \begin{cases} 1 & if\ C_i = C_j \\ 0 & if\ C_i \neq C_j \end{cases} \quad (7)$$

در روش پیشنهادی، الگوریتم فراابتکاری که در سال‌های اخیر پیشنهاد شده‌اند، با مشکل تشخیص جامعه (*CD*) سازگار شده‌اند. از آنجایی که الگوریتم‌های پیشنهادی در حل مسائل پیوسته استفاده می‌شوند، راه‌حل‌های نامزد تولید شده توسط الگوریتم‌ها باید به مقادیر گسسته تبدیل شوند تا آنها را با مشکل *CD* تطبیق دهند. همراه با این مکانیسم تبدیل، شکل ۲ نمودار جریانی را که برای حل مشکل *CD* دنبال می‌شود، ارائه می‌دهد[12].

طبقه بندی *Neuro-Fuzzy* بررسی های فعلی را بر اساس بررسی های گذشته ارائه شده توسط کاربران طبقه بندی می کند. مجموعه ای از قوانین فازی برای استخراج زمینه از بررسی فرموله شده است، و بررسی ها با عبور از قوانین فازی طبقه بندی می شوند. در این

پیشنهاد، زمینه در جمله مروری به کلمه مقصد (اسم/فعل) و رابطه بین کلمه مقصد و کلمه نظر اشاره دارد. قوانین فازی ساختارهای زبانی هستند که به صورت پویا برای حل موقعیت‌های دشواری که ممکن است تکراری نباشند، قاب‌بندی شده‌اند. یک رابطه فازی نشان دهنده ارتباط بین یک یا چند عنصر در طول اتفاقات نادر است. به طور متوالی، برای هر بازبینی، مقدار قطبیت محاسبه می شود و در نتیجه قطبیت سند محاسبه می شود. قطبیت سند به قطبیت محصول اشاره دارد، زیرا هر سند حاوی بررسی های مربوط به محصول جداگانه است. روش پایه به کار رفته در روش پیشنهادی با ساخت یک مدل پیش بینی با کمک نرم افزار *MATLAB* ایجاد می‌شود. در روش پیشنهادی از جعبه ابزار *ANFIS* استفاده می‌شود که در آن داده‌های ورودی در مدل‌های مختلف ایجاد شد. نمودار جریان فهرست شده در شکل ۲ کل فرآیند چارچوب کنترل پیش بینی را نشان می دهد. دسته یا تخصص مورد استفاده در طول عملیات در نقاط مختلفی اندازه گیری شد که دقت، حساسیت و ویژگی برای آن ها تخمین زده شد و در مدل *ANFIS* وارد شد. متغیرهای جمع‌آوری‌شده به عنوان پارامترهای ورودی در نظر گرفته می‌شوند که قوانین مختلفی برای آنها در ترکیب‌های ورودی مختلف ایجاد شده‌اند.



شکل ۲: فلوچارت روش پیشنهادی[12].

الگوریتم ژنتیک چند هدفه مبتنی بر تجزیه :در روش پیشنهادی یک الگوریتم ژنتیک چند هدفه مبتنی بر تجزیه (DMOG) را برای به حداکثر رساندن اعتماد کاربران در یک شبکه اجتماعی با حداقل مجموعه ای از کاربران seed (با بودجه k) برای اعتماد کاربران پیشنهاد می شود. هنگامی که یک اعتماد کاربر در OSN در حال محاسبه است، اعتماد کاربر ممکن است تصمیم بگیرند که یک ضد اعتماد را برای کاهش تأثیر اعتماد آغاز کنند. در چنین حالتی، الگوریتم DMOG را می توان اجرا کرد و نتایج به دست آمده از تجزیه و تحلیل را می توان با کاربران قربانی به اشتراک گذاشت. در یک OSN، مجموعه ای از کاربران شناسایی شده ممکن است توسط قربانیان ترغیب شوند که ضد اعتماد را آغاز کنند که تأثیر اعتماد را کاهش می دهد[13]. به طور کلی در روش پیشنهادی یک مدل یادگیری ماشین ترکیبی مبتنی بر نرو-فازی و یکی از الگوریتم‌های فراابتکاری به نام الگوریتم ژنتیک برای شناسایی اعتماد کاربران در شبکه‌های اجتماعی آنلاین پیشنهاد شده است. مدل پیشنهادی تشخیص خودکار اعتماد کاربران را انجام می‌دهد و بینشی در مورد تأثیرگذارترین ویژگی‌ها در طول فرآیند تشخیص می‌دهد.

۴– نتایج و تحلیل شبیه‌سازی

برای ارزیابی روش پیشنهادی از مجموعه داده‌های wiki4HE که در آدرس M[1] قرار دارد استفاده شده است. این مجموعه دارای ۹۱۳ نمونه بوده است و در هر نمونه ویژگی‌های مختلف فردی و اجتماعی از یک شبکه اجتماعی بیان کننده میزان استفاده از ویکیپدیا است. به طور عمده به همراه ویژگی‌های فردی، ویژگی‌های میزان علاقه، اشتراک‌گذاری، میزان سودمندی، موثر بودن، تصویر، میزان تعامل و میزان مرتبط بودن در آن قرار دارد. در این مجموعه داده تعداد ۵۳ ویژگی از دسته‌های نامبرده قرار دارد.

شبیه‌سازی و ارزیابی: عملکرد روش پیشنهادی با استفاده از مجموعه داده معرفی شده، بررسی می‌شوند. شبکه ها دارای گره ها و لبه های متفاوتی هستند. جداول ۴-۱ ترتیب شبکه های اجتماعی کوچک و بزرگ را با تعداد گره و لبه نشان می دهند. در مطالعات تجربی، هر الگوریتم در شرایط مساوی در ۳۰ اجرای مستقل اجرا می‌شود. بهترین مقادیر برای هر مقایسه به صورت پررنگ گزارش شده است. برای هر اجرا، اندازه جمعیت، تعداد تکرار و سپس maxFEs (تکرار popSize X) به صورت ۲۰، ۵۰۰ و ۱۰۰۰۰ تعیین می شود. تمامی مطالعات تجربی بر روی دستگاهی با پردازنده Intel Core i7 2.80 گیگاهرتز، ۱۶ گیگابایت رم و سیستم عامل ۶۴ بیتی ویندوز ۱۰ انجام شده و تمامی کدها بر روی Matlab R2021a انجام شده است.

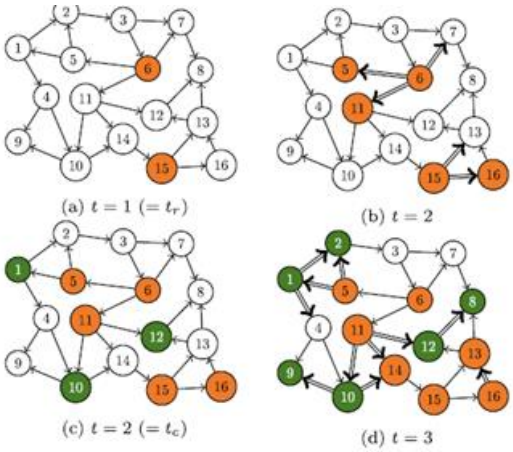
عملکرد روش پیشنهادی با استفاده از مجموعه داده معرفی شده، بررسی می‌شوند. شبکه ها دارای گره ها و لبه های متفاوتی هستند. جداول ۱ ترتیب شبکه های اجتماعی کوچک و بزرگ را با تعداد گره و لبه نشان می دهند. در مطالعات تجربی، هر الگوریتم در شرایط مساوی در ۳۰ اجرای مستقل اجرا می‌شود. بهترین مقادیر برای هر مقایسه به صورت پررنگ گزارش شده است. برای هر اجرا، اندازه جمعیت، تعداد تکرار و سپس maxFEs (تکرار popSize X) به صورت ۲۰، ۵۰۰ و ۱۰۰۰۰ تعیین می شود. تمامی مطالعات تجربی بر روی دستگاهی با پردازنده Intel Core i7 2.80 گیگاهرتز، ۱۶ گیگابایت رم و سیستم عامل ۶۴ بیتی ویندوز ۱۰ انجام شده و تمامی کدها بر روی Matlab R2021a انجام شده است.

[1] https://archive.ics.uci.edu/ml/datasets/wiki4he

جدول ۱: شبکه های اجتماعی بزرگی که در این آزمایش ها مورد استفاده قرار گرفتند

Networks	#Node	#Edge
Physicians (Physicians)	241	**98**
Jazz musicians (Jazz)	198	**2742**
FilmTrust trust (FilmTrust)	874	**1853**
Little Rock Lake (Rock)	183	**2494**
Similarities (Similarities)	430	**565**

اجازه دهید $G = (V, E)$ یک نمودار جهت دار از یک OSN باشد که در آن V مجموعه گره هایی است که کاربران را نشان می دهد. E مجموعه ای از لبه های جهت دار است که نشان دهنده جریان اطلاعات بین کاربران با یک رابطه اجتماعی است. در ابتدا، در گام زمانی $t = 0$، کاربران تحت تأثیر شایعه یا ضد شایعه قرار نمی گیرند. شایعه ای را در نظر بگیرید که توسط مجموعه ای از کاربران seed در زمان tr آغاز شده است. این شایعه از طریق شبکه اجتماعی در مدل IC پخش می شود. پس از یک تاخیر Δt، به منظور محدود کردن انتشار و نفوذ شایعه، یک ضد شایعه توسط مجموعه ای از کاربران seed در زمان tc $= tr + \Delta t$ آغاز می شود. سپس، آبشار شایعه و ضد شایعه با یکدیگر رقابت می‌کنند و تحت مدل PCC با تقدم شایعه بر ضد شایعه منتشر می‌شوند. این فرآیند تا تعداد محدودی از مراحل زمانی ادامه می‌یابد که هیچ کاربر دیگری نمی‌تواند تحت تأثیر قرار گیرد. روند انتشار شایعه و ضد شایعه در شکل ۳ نشان داده شده است. همه کاربران در شبکه در $t0 = 0$ تحت تأثیر قرار نمی گیرند. شایعه در شبکه در $tr = 1$ با $Sr = \{6, 15\}$ آغاز می شود، به عنوان در شکل a۳ نشان داده شده است. این شایعه در شبکه در مدل IC برای $\Delta t = 1$ مرحله زمانی پخش می شود، همانطور که در شکل b۳ نشان داده شده است. بنابراین، تأثیر شایعه در مرحله زمانی tc مجموعه کاربری {۶، ۱۵، ۵، ۱۱، ۱۶} است. همچنین مجموعه‌ای از کاربران seed برای ضد شایعه $Sc = \{1$، 10، 12} شناسایی می‌شود. همانطور که در شکلd۳ نشان داده شده است، شایعه و ضد شایعه در مدل PCC منتشر شد. در $t = 3$، مجموعه کاربران تحت تأثیر شایعه {۵، ۱۵، ۵، ۱۱، ۱۳، ۱۴، ۱۶} و افرادی که تحت تأثیر شایعه متقابل هستند {۱، ۳، ۹، ۸، ۱۰، ۱۲ است. }.



شکل ۳: کاربران تحت تأثیر یک شایعه (نارنجی رنگ) و یک ضد شایعه (به رنگ سبز) که در یک شبکه منتشر می شود.

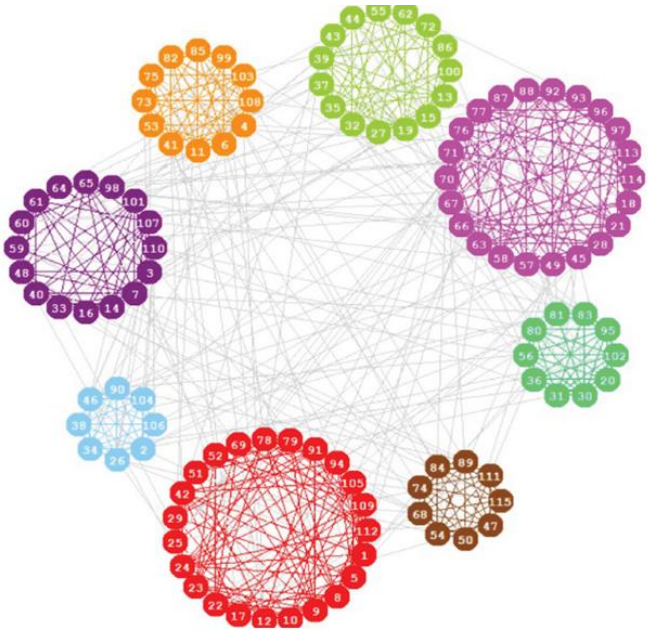
(الف) کاربران Seed برای شایعه (ب) شایعه منتشر شده در مدل IC (ج) کاربران Seed برای شایعه متقابل (د) شایعه و شایعه ضد شایعه در مدل PCC منتشر می شود. در ادامه، اعتبار و کارایی مدل پیشنهادی آبشار رقابتی مبتنی بر اولویت (PCC) برای انتشار نفوذ رقابتی و الگوریتم ژنتیک چند هدفه مبتنی بر تجزیه (DMOG) در شبکه‌های اجتماعی دنیای واقعی ارزیابی می‌شود.

الگوریتم DMOG برای انتخاب کاربر ضد شایعه در شبکه‌های اجتماعی آنلاین برای کاهش تأثیر شایعه با الگوریتم‌های پایه زیر مقایسه می‌شود:

Unmitigated (Unmtg): شایعه بدون هیچ مانعی در شبکه های اجتماعی پخش می شود، یعنی هیچ شایعه متقابلی وجود ندارد. در اینجا شایعه در مدل Independent Cascade پخش می شود.

تصادفی (رند): تعداد کاربران seed برای شایعه متقابل به طور تصادفی انتخاب می شود به طوری که $|Sc| \leq k| \geq ۱$. سپس کاربران seed به طور تصادفی از مجموعه کاربران بدون تأثیر انتخاب می شوند.

نزدیکی (Prox): تعداد کاربران seed برای شایعه متقابل به طور تصادفی انتخاب می شود به طوری که $|Sc| \leq k| \geq ۱$. نزدیکترین همسایگان بدون تأثیر کاربران تحت تأثیر شایعه به عنوان گره های اولیه برای ضد شایعه انتخاب می شوند.

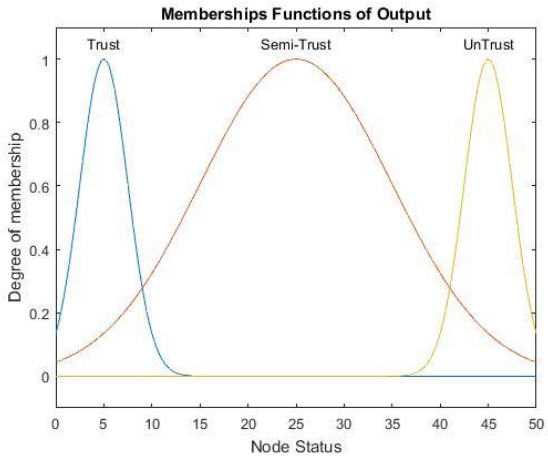


شکل ۴: نمونه ایی از شبکه استخراج شده

تعداد کاربران تحت تاثیر شایعه و تعداد کاربران seed برای ضد شایعه معیارهای مهمی در ارزیابی عملکرد الگوریتم DMOG هستند. علاوه بر این، سایر معیارهای مورد استفاده برای مقایسه عملکرد الگوریتم های مختلف در آزمایش های انجام شده عبارتند از:

تاثیر: درصد کاربران شبکه اجتماعی تحت تاثیر شایعه را تاثیر شایعه می نامند. به همین ترتیب، درصد کاربران شبکه اجتماعی تحت تأثیر ضد شایعه را تأثیر ضد شایعه می نامند. تاثیر شایعه (Er) و ضد شایعه (Ec) را می توان به صورت $Er=|R|/N*100$ و $Ec=|C|/N*100$ که در آن N تعداد گره های شبکه اجتماعی است. همچنین تاثیر شایعه در زمان t کسری از کاربران تحت تاثیر شایعه تا مرحله زمانی است.

Impact Gain: سود تاثیر به عنوان بخشی از کاربران در شبکه اجتماعی تعریف می‌شود که تحت تأثیر شایعه ممانعت یا نجات داده شده‌اند. سود تاثیر $E'r$ تعداد کاربرانی است که تحت تاثیر قرار گرفته اند و تاثیر شایعه زمانی که هیچ شایعه متقابلی وجود ندارد (یعنی شایعه منتشر شده Unmitigated در مدل IC).



شکل ۵: تابع عضویت در نروفازی

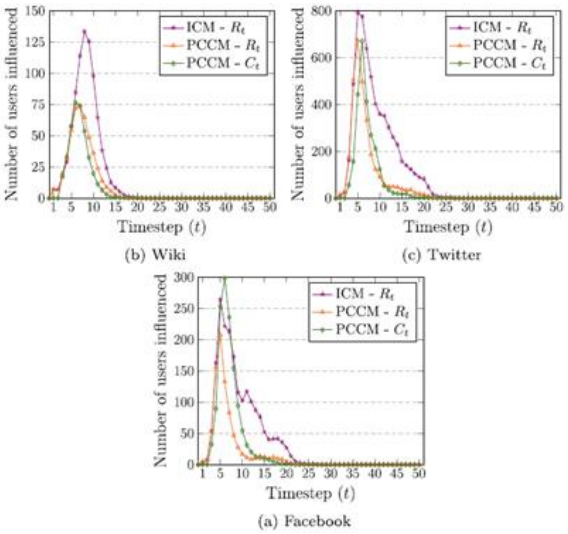
تقدم شایعه بر ضد شایعه در مدل آبشار رقابتی مبتنی بر اولویت برای الگوریتم‌های مختلف انتخاب کاربر ضد شایعه بر اساس مقادیر باور شایعه و ضد شایعه محاسبه شده و در جدول ۲ فهرست شده است.

جدول ۲: تقدم شایعه بر ضد شایعه.

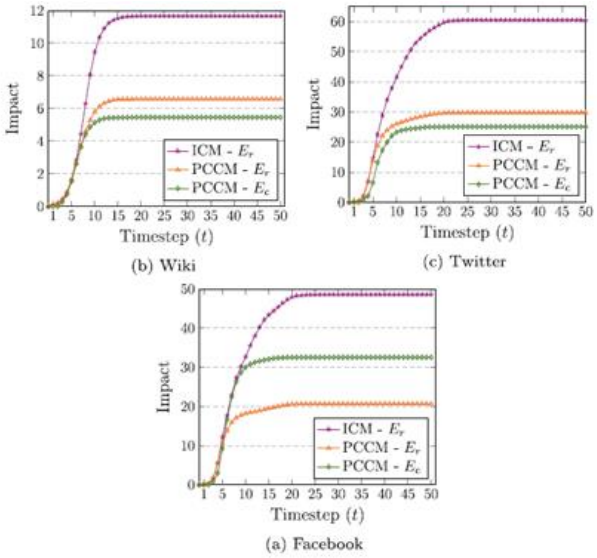
Dataset	B_r	Random		Proximity		DMOG	
		B_c	q	B_r	q	B_r	q
Facebook	0.59	0.19	0.75	0.42	0.60	0.45	0.55
Wiki	0.57	0.13	0.80	0.20	0.75	0.30	0.65
Twitter	0.60	0.17	0.80	0.39	0.60	0.55	0.50

ارزش باور برای شایعه در سراسر الگوریتم ها یکسان است در حالی که ارزش باور برای ضد شایعه با الگوریتم انتخاب بذر ضد شایعه متفاوت است. این به این دلیل است که ارزش باور بر اساس ویژگی های نموداری کاربران هسته انتخاب شده تعیین می شود. بنابراین، تقدم شایعه بر ضد برای الگوریتم‌های انتخاب کاربر بذر متفاوت است. الگوریتم DMOG کمترین اولویت را برای مجموعه داده ها برمی گرداند، یعنی ۰.۵۵ در مجموعه داده فیس بوک، ۰.۶۵ در مجموعه داده Wiki و ۰.۵۰ در مجموعه داده Twitter.

انتشار شایعات و آبشارهای ضد شایعه در مدل پیشنهادی آبشار رقابتی مبتنی بر اولویت با انتشار شایعه در مدل آبشار مستقل برای اعتبار بخشیدن به مدل PCC مقایسه شده است. علاوه بر این، الگوریتم DMOG پیشنهادی برای انتخاب کاربران seed برای ضد شایعه با اولویت جدول ۲ استفاده می شود. تعداد کاربران تحت تاثیر شایعه و ضد شایعه در هر مرحله زمانی در مدل IC و مدل PCC در شکل ۶ مقایسه شده اند و یک منحنی شکل 'تپه' در شکل مشاهده شده است. تاثیر شایعه و ضد شایعه در هر مرحله زمانی در شکل ۷ مقایسه شده و یک منحنی S شکل در شکل مشاهده شده است.

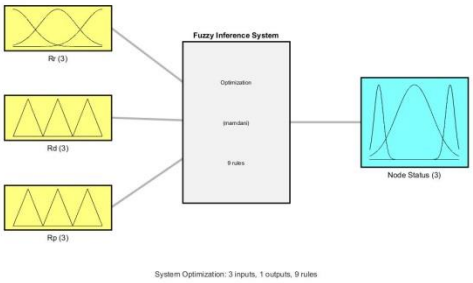


شکل ۶: تعداد کاربران تحت تأثیر شایعه و ضد شایعه در هر مرحله زمانی که در شبکه در مدل IC و مدل PCC با اولویت ۰.۵۵ برای Facebook، 0.65 برای Wiki و ۵۰.۰ برای Twitter منتشر می شوند.

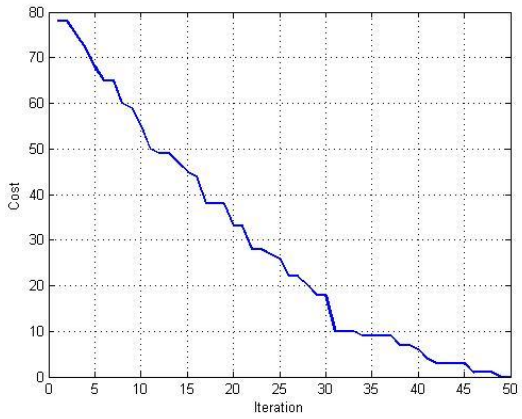


شکل ۷: تأثیر شایعه و ضد شایعه در هر مرحله زمانی که در شبکه در مدل IC و مدل PCC با اولویت ۰.۵۵ برای فیس بوک، ۰.۶۵ برای Wiki و ۰.۵۰ برای Twitter منتشر می شود.

برای مجموعه داده فیس بوک در شکل a۶، شایعه هنگام انتشار بدون کاهش در مدل IC در مرحله زمانی t = 7 با تأثیرگذاری بر حداکثر Rt = 264 کاربر به اوج خود می رسد. گسترش شایعه بعد از t = 21 ناچیز می شود. این در شکل a۷ منعکس شده است که در آن منحنی تا ۲۱ = t افزایش می یابد و پس از آن با Er = 48.5٪ صاف می شود. هنگامی که ضد شایعه وارد سیستم می شود، شایعه و ضد شایعه سپس در مدل PCC منتشر می شود. در نتیجه، برخی از کاربران بدون تأثیر قبل از اینکه با شایعه روبرو شوند تحت تأثیر ضد شایعه قرار می گیرند. همچنین، برخی از کاربرانی که هم با شایعه و هم با شایعه روبرو می شوند، بر اساس تقدم، ضد شایعه را باور می کنند. بنابراین، ضد شایعه مانع نفوذ شایعه می شود. این منجر به یک پیک کوچکتر برای شایعه در شکل a۶ در t = 5 با Rt = 207 کاربر می شود. همچنین تعداد کاربران تحت تاثیر ضد شایعه به t = 6 با Ct = 298 کاربر به اوج می رسد. گسترش هر دو شایعه و شایعه متقابل پس از t = 20 ناچیز می شود. بر این اساس، در شکل a۷، منحنی تاثیر شایعه و ضد شایعه در مدل PCC تا ۲۱ = t بالا می رود و سپس با Er = 20.7٪ مسطح می شود. و Ec = 32.5٪. روندهای مشابهی برای مجموعه داده های ویکی و توییتر در شکل مشاهده شده است. b۷، b۶ و c۷، c۶ به ترتیب. در ویکی، تعداد کاربران تحت تأثیر شایعه در مدل IC در مرحله زمانی t = 8 با Rt = 133 حداکثر است و پس از t = 20 در شکل b۶، ناچیز می شود. پیک برای شایعه در مدل PCC با Rt = 74 در t = 7 بسیار کوچکتر است و گسترش آن پس از t = 15 ناچیز است. در شکل b۷، برای مدل IC، تأثیر شایعه تا ۲۰ = t افزایش می یابد و تبدیل می شود. ثابت در Er = 11.6٪. برای مدل PCC، منحنی های ضربه تا ۱۵ = t افزایش می یابد و سپس با Er = 6.6٪ و Ec = 5.5٪ صاف می شوند. در توییتر، در مدل IC، حداکثر تعداد کاربران تحت تأثیر شایعه در مرحله زمانی t = 5 با Rt = 792 قرار می گیرند و تعداد کاربران تحت تأثیر پس از t = 26 همانطور که در شکل c۶ مشاهده شده است، ناچیز می شود. اوج شایعه در t = 5 با Rt = 671 کمتر است و بعد از t = 22 ناچیز می شود. در شکل c۷، تأثیر شایعه در مدل IC تا ۲۶ = t افزایش می یابد و در Er = 60.44٪ ثابت می شود. با این حال برای مدل PCC، منحنی ضربه تا ۲۵ = t افزایش می یابد و در Er = 29.73٪ صاف می شود.



شکل ۸: نمایی از سیستم فازی طراحی شده



شکل ۹: تابع هزینه خروجی الگوریتم ژنتیک چند هدفه

در حالی که موضوع پیام های هرزنامه بیشتر در زمینه سیستم پست الکترونیکی شناخته می شود، در OSN های مختلف که در آن کاربران به شدت از هرزنامه رنج می برند قابل توجه است. هرزنامه اجتماعی بردار حمله ترجیحی است که توسط مجرمان سایبری برای شروع فعالیت های مخرب خود استفاده می شود. این پیام‌های ناخواسته محتویات فریبنده را با URLهای مبهم به سایر سایت‌های خارجی که ممکن است حاوی بدافزارها، صفحات وب فیشینگ، اسکریپت‌های کلاهبرداری کلیک و/یا سایر محتوای نامناسب باشند، منتقل می‌کنند. علاوه بر این، یک گزارش اولیه هشدار داد که هرزنامه رسانه‌های اجتماعی سریع‌تر از نظرات در اکثر سایت‌های OSN در حال رشد است. این گزارش همچنین نشان می دهد که ۱۵ درصد از هرزنامه های اجتماعی حاوی پیوندهایی به محتوای مخرب، پورنوگرافی یا بدافزار است.

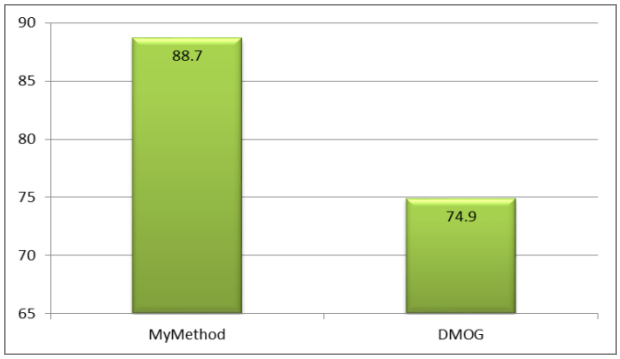
به منظور مقایسه نتایج الگوریتم های موجود، تعداد مشابهی از کاربران seed برای ضد شایعه به عنوان الگوریتم DMOG انتخاب

شده است. تعداد کاربران اولیه برای شایعه متقابل ۳۱.۲۷ (۷۸.۲٪ از بودجه) در فیس بوک، ۲۲.۸ (۵۸٪ از بودجه) برای مجموعه داده ویکی و ۴۶.۸۱ (۹۳.۵٪ از بودجه) در مجموعه داده فیس بوک است. تأثیر این شایعه از ۴۸.۵ درصد در فیس بوک، ۱۱.۶ درصد در ویکی و ۶۰.۴ درصد در توییتر برای مورد غیرقابل کاهش (یعنی زمانی که شایعه متقابل وجود ندارد) به ۲۱.۷-۳۵.۷ درصد در فیس بوک، ۶.۳-۹.۴ درصد در ویکی کاهش می یابد. و ۲۹.۵٪ - ۳۵.۵٪ در توییتر، با ضد شایعه توسط کاربران seed که توسط الگوریتم های مختلف انتخاب شده اند، آغاز شده است. الگوریتم DMOG از الگوریتم های پایه موجود در همه مجموعه داده ها بهتر عمل می کند و تأثیر شایعه ۲۱.۷٪ در فیس بوک، ۶.۳۱٪ در Wiki و ۲۰.۷٪ در توییتر است. مشاهده می‌کنیم که با افزایش تأثیر شایعه، تأثیر شایعه کاهش می‌یابد. الگوریتم DMOG 30.75 درصد تأثیر ضد شایعه در فیس بوک، ۶.۲۷ درصد در ویکی و ۲۵.۱ درصد در توییتر را برمی گرداند که از الگوریتم های دیگر بیشتر است.

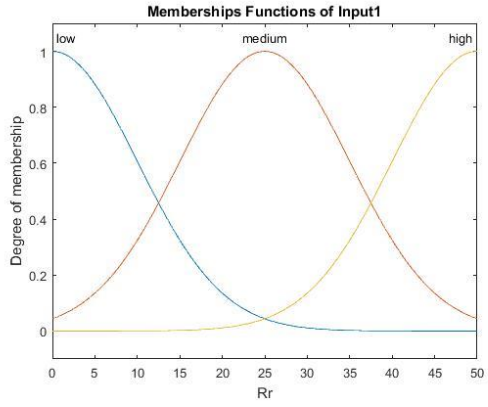
جدول ۳: مقایسه الگوریتم DMOG با سایر الگوریتم ها

Dataset	Algorithm	E_r	E_c	ΔE_r	|Sc|
Facebook	Unmitigated	48.54	-	-	-
	Random	24.12	25.06	24.42	31.3
	Proximity	24.18	26.48	24.36	31.59
	DMOG	21.71	30.75	26.85	31.27
Wiki	Unmitigated	11.66	-	-	-
	Random	9.36	3.51	2.3	22.65
	Proximity	7.3	4.28	4.36	22.8
	DMOG	6.31	6.27	5.34	22.77
Twitter	Unmitigated	60.443	-	-	-
	Random	35.47	22.06	24.97	46.7
	Proximity	32.45	23.48	27.0	46.25
	DMOG	29.729	25.089	30.714	46.81

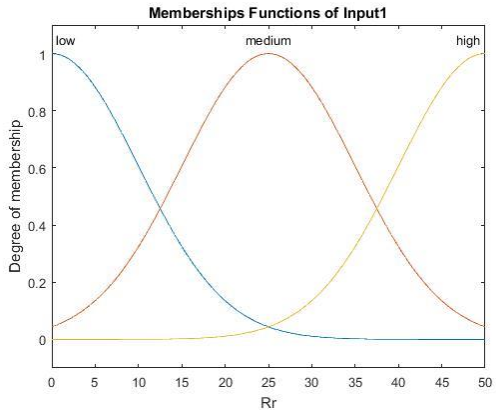
با کاهش تاثیر شایعه و افزایش تاثیر ضد شایعه، سود ناشی از شایعه افزایش می‌یابد. الگوریتم DMOG در مقایسه با الگوریتم‌های استاندارد، بیشترین تأثیر را در همه مجموعه‌های داده نشان می‌دهد. برای فیس بوک، الگوریتم DMOG 26.85% افزایش تاثیر را در مقابل ۲۰٪ و ۱۲.۸۵٪ در الگوریتم های تصادفی و مجاورت نشان می دهد. به طور مشابه، برای مجموعه داده ویکی، الگوریتم DMOG 5.34% افزایش تاثیر را در مقابل ۲.۲۹٪ و ۴٪ در الگوریتم‌های تصادفی و مجاورت نشان می‌دهد. علاوه بر این، برای مجموعه داده توییتر، الگوریتم DMOG 30.71٪ افزایش تاثیر را در مقایسه با ۲۴.۹۷٪ و ۲۷٪ در الگوریتم های تصادفی و مجاورت نشان می دهد.



شکل ۱۰: مقایسه روش پیشنهادی با روش DMOG پایه



(الف)



(ب)

شکل ۱۱: انواع توابع عضویت استفاده شده

الگوریتم DMOG حداقل تعداد کاربران مورد نیاز برای انتشار ضد شایعه را برای کاهش شایعه انتخاب می کند. در صورت الگوریتم تصادفی، برخی از کاربران seed ممکن است از بخشی از شبکه که به شایعه بی ربط است، یعنی در بخشی از شبکه که تحت تأثیر شایعه نیست، انتخاب شوند. این کاربرانی که ضد شایعه را منتشر می کنند هیچ تاثیری در شایعه ندارند. در الگوریتم مجاورت، کاربران از بین همسایه‌های بدون تأثیر کاربران تحت تأثیر شایعه انتخاب می‌شوند. در حالی که انتخاب چنین کاربرانی مانع از انتشار شایعه می شود، ممکن است کاربران seed منتخب رابطه قوی با بقیه کاربران بدون تأثیر نداشته باشند. بنابراین ارزش اعتقادی ضد شایعه پایین است و در نتیجه تقدم شایعه بیشتر می شود. با این حال، الگوریتم DMOG، کاربران اولیه را از میان کاربران بدون تأثیر با بالاترین ارزش اعتقادی ضد شایعه، از بخشی از شبکه که تحت تأثیر شایعه است، انتخاب می کند. بنابراین، الگوریتم DMOG در مقایسه با الگوریتم های دیگر بهتر عمل می کند. براساس این ارزیابی روش پیشنهادی با بهبود ۱۴ درصدی نسبت به روش پایه نتایج بهتری را به ثبت رسانده است.

۶– نتیجه‌گیری و پژوهش‌های آتی

در این مقاله یک مدل آبشار رقابتی مبتنی بر اولویت (PCC) برای انتشار شایعات رقیب و آبشارهای ضد شایعه پیشنهاد می‌کنیم. ما مدلی

را برای محاسبه ارزش تقدم مبتنی بر باور ارائه کرده‌ایم که توسط آن کاربر تصمیم می‌گیرد شایعه یا ضد شایعه دریافتی در طول انتشار اطلاعات را باور کند. تأثیر شایعه و آبشارهای ضد شایعه در OSN ها با در نظر گرفتن یک رویکرد انتشار مبتنی بر همسایگی تجزیه و تحلیل می شود. یکی دیگر از مسائل چالش برانگیز که در این کار به آن پرداخته شده است، انتخاب حداقل مجموعه اولیه کاربران برای شروع ضد شایعه است تا سربار پیام در برنامه کاهش یابد. این به عنوان یک مسئله بهینه‌سازی چند هدفه برای انتخاب حداقل مجموعه‌ای از کاربران seed برای ضد شایعه برای به حداقل رساندن تأثیر شایعه فرمول‌بندی شده است.

ما یک مسئله بهینه‌سازی چند هدفه را برای یافتن حداقل مجموعه‌ای از کاربران اولیه برای ضد شایعه، با توجه به بودجه k، به منظور به حداقل رساندن تأثیر شایعه فرموله می‌کنیم. ما چارچوب تجزیه را برای حل مسئله بهینه‌سازی چند هدفه اتخاذ می‌کنیم، زیرا به عنوان یکی از رویکردهای همگرا سریع‌تر ثابت شده است. برای حل مسئله بهینه سازی ترکیبی گسسته، از الگوریتم ژنتیک کلاسیک (GA) (گلدبرگ، ۱۹۸۹) استفاده می کنیم که به طور گسترده و با موفقیت برای شناسایی کاربران تأثیرگذار در OSN ها استفاده شده است. علاوه بر این، GA همچنین به طور طبیعی اندازه پویا مجموعه کاربر بذر را با رمزگذاری مقدار طول متغیر برای راه حل های کاندید ترکیب می‌کند. بنابراین، یک الگوریتم ژنتیک را بر اساس رویکرد تجزیه طراحی می‌کنیم تا کاربران بذر را برای انتشار ضد شایعه در OSN انتخاب کنیم. علاوه بر این، تابع تناسب الگوریتم ژنتیک تعداد کاربران در OSN را تحت تأثیر شایعه و تعداد کاربران seed برای ضد شایعه ارزیابی می کند، زمانی که ضد شایعه توسط مجموعه خاصی از کاربران آغاز می شود. آزمایش بر روی مجموعه داده های دنیای واقعی انجام شده است و تأثیر پارامترهای مختلف (مانند تقدم، تاخیر زمانی و بودجه) بر انتشار شایعه و ضد شایعه در شبکه در این کار بررسی می شود. نتایج به‌دست‌آمده از رویکرد GA پیشنهادی ما با رویکردهای موجود مقایسه می‌شود. طراحی و تجزیه و تحلیل یک مدل آبشار رقابتی مبتنی بر اولویت (PCC) برای انتشار نفوذ در یک شبکه اجتماعی آنلاین برای شایعات رقابتی و آبشارهای ضد شایعه با یک مدل باور یکپارچه در نظر گرفته شد. فرمول‌بندی یک مسئله بهینه‌سازی چند هدفه برای انتخاب حداقل مجموعه‌ای از کاربران seed برای ضد شایعه، با توجه به محدودیتی برای تعداد کاربران seed، برای به حداقل رساندن تأثیر شایعه در یک OSN و طراحی یک الگوریتم ژنتیک چند هدفه مبتنی بر تجزیه (DMOG) برای به حداقل رساندن تأثیر شایعه در یک OSN با حداقل مجموعه‌ای از کاربران اولیه برای ضد شایعه زمانی که هم شایعه و هم ضد شایعه در مدل PCC منتشر می‌شوند. ارزیابی کارایی مدل PCC پیشنهادی و الگوریتم DMOG بر روی سه مجموعه داده دنیای واقعی (فیس بوک، ویکی، توییتر) از نظر تأثیر شایعه و ضد شایعه، سود تأثیر شایعه و تعداد کاربران seed برای ضد شایعه است.

این کار را می توان با گنجاندن تکنیک های یادگیری افزایشی به منظور استخراج پویایی ترجیحات کاربران در مورد موارد مختلف بهبود بخشید. شامل سایر روابط هستی شناسی برای محاسبات شباهت معنایی اقلام می تواند مدل پیشنهادی را بیشتر بهینه کند. علاوه بر این، تجزیه و تحلیل دقیق‌تری از الگوی دو وجهی ارائه شده در هیستوگرام خطاهای پیش‌بینی مورد نیاز است. حتی اگر فقط از هستی شناسی خاصی استفاده شود، این مدل را می توان به راحتی به سایر حوزه های هستی شناسی در زمینه های معنایی مختلف و برای کاربردهای مختلف گسترش داد. این پیشنهاد را می توان با در نظر گرفتن نمایه های کاربر به روشی مشابه گسترش داد.

۷– مراجع

.1 SHAFIEI, M.M., et al., *A Fuzzy System for Evaluating Trustworthiness of Users in a Social Network.* IIUM Engineering Journal, 2022. **23**(2): p. 154-170.

.2 Cheng, X. and X. Li. *Trust evaluation in online social networks based on knowledge graph*. in *Proceedings of the 2018 International Conference on Algorithms, Computing and Artificial Intelligence*. 2018.

.3 Liu, G., et al., *Trust assessment in online social networks.* IEEE Transactions on Dependable and Secure Computing, 2019. **18**(2): p. 994-1007.

.4 Khan ,J. and S. Lee, *Implicit user trust modeling based on user attributes and behavior in online social networks.* IEEE Access, 2019. **7**: p. 142826-142842.

.5 Voloch, N., N. Gal-Oz, and E. Gudes, *A trust based privacy providing model for online social networks* . Online Social Networks and Media, 2021. **24**: p. 100138.

.6 Xu, Y., et al., *Trust propagation and trust network evaluation in social networks based on uncertainty theory.* Knowledge-Based Systems, 2021. **234**: p. 107610.

.7 Lin, W., Z. Gao, and B. Li. *Guardian: Evaluating trust in online social networks with graph convolutional networks*. in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. 2020. IEEE.

.8 Goyal, R., et al., *Analysis of Predicting Trust in Complex Online Social Networks.* Materials Today: Proceedings, 2020. **29**: p. 573-580.

روش ارجاع به مقاله: ن. مجیدی، ب. شاکری اسکی ارائه مدلی ترکیبی جهت ارزیابی اعتماد کاربران شبکه‌های اجتماعی آنلاین مبتنی بر تکنیک نرو-فازی و الگوریتم‌های تکاملی، فصلنامه محاسبات و سامانه‌های توزیع شده، سال پنجم، شماره۲، شماره پیاپی۱۰، صفحه ۱۱۳ تا ۱۲۵، سال۱۴۰۱

How to cite: Neda majidi, Baharak shakeri aski, A hybrid model for Evaluation of the trust of online social network Based on neuro-fuzzy technique and evolutionary algorithms, Journal of Distributed Computing and Systems (JDCS), Vol 5, Issue 2, Page 113-125, 2023.

.9 Gong, Z., et al., *Measuring trust in social networks based on linear uncertainty theory.* Information Sciences, 2020. **508**: p. 154-172.

.10 Khan, T. and A. Michalas, *Seeing and Believing: Evaluating the Trustworthiness of Twitter Users.* IEEE Access, 2021. **9**: p. 110505-110516.

.11 Alkhamees, M., et al., *User trustworthiness in online social networks: A systematic review.* Applied Soft Computing, 2021. **103**: p. 107159.

.12 Koc, I., *A fast community detection algorithm based on coot bird metaheuristic optimizer in social networks.* Engineering Applications of Artificial Intelligence, 2022. **114**: p. 105202.

.13 Parimi, P. and R.R. Rout, *Genetic algorithm based rumor mitigation in online social networks through counter-rumors: A multi-objective optimization.* Information Processing & Management, 2021. **58**(5): p. 102669.

ندا مجیدی معلم رشته کامپیوتر در استان گیلان، مدرک کارشناسی خود را در رشته کامپیوتر گرایش نرم افزار در سال ۱۳۹۱از دانشگاه آزاد اسلامی اخذ نمودم و در سال ۱۴۰۲مدرک کارشناسی ارشد خود را در رشته مهندسی کامپیوتر گرایش نرم افزار از دانشگاه آزاد اسلامی واحد رامسر اخذ نموده ام.

نشانه رایا نامه ایشان عبارتند از :

nedamajidi6@gmail.com

بهارک شاکری اسکی دکترای کامپیوتر از دانشگاه آزاد اسلتمی واحد علوم تحقیقات تهران و از سال ۱۳۸۵ تا کنون عضو هئیت علمی دانشگاه آزاد واحد رامسر فعالیت میکنم.

نشانه رایانامه ایشان عبارتند از :

Shakeriaski.b@gmail.com