Journal of Electronical & Cyber Defence
Vol. 9, No. 3, 2021, Serial No. 35

Detecting Fake Accounts in Social Networks Using Principal Components Analysis and Kernel Density Estimation Algorithm (A Case Study on the Twitter Social Network)

M. R. Mohammadrezaei*

*Islamic Azad University, Ramhormoz, Iran

(Received: 05/12/2020, Accepted: 17/02/2021)

ABSTRACT

The use of social networks is growing increasingly and people spend a lot of their time using these networks. Celebrities and companies have used these networks to connect with their fans and customers and news agencies use these networks to publish news. In line with the growing popularity of online social networks, security risks and threats are also increasing, and malicious activities and attacks such as phishing, creating fake accounts and spam on these networks have increased significantly. In a fake account attack, malicious users introduce themselves instead of other people by creating a fake account and in this way, they abuse the reputation of individuals or companies. This paper presents a new method for detecting fake accounts in social networks based on machine learning algorithms. The proposed method for machine training uses Various similarity features such as Cosine similarity, Jaccard similarity, friendship network similarity, and centrality measures. All these features are extracted from the graph adjacency matrix of the social network. Then, principal component analysis was used in order to reduce the data dimensions and solve the problem of overfitting. The data are then classified using the Kernel Density Estimation classification and the Self Organization map and the results of the proposed method are evaluated using the measure of accuracy, sensitivity, and false-positive rate. Examination of the results shows that the proposed method detects fake accounts with 99.6% accuracy which is about 5% better than Cao's method. The rate of misdiagnosis of fake accounts also improved by 3% compared to the same method.

Keywords: Fake Accounts, Social Networks, Graph Analysis, Kernel Density Estimation

* Corresponding Author Email: mohammadrezaei.m.reza@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۳، پاییز ۱۴۰۰، ص ۱۲۳- ۱۰۹

علمی- پژوهشی

تشخیص کاربران جعلی در شبکه‌های اجتماعی با استفاده از تحلیل مولفه‌های اصلی و الگوریتم تخمین چگالی هسته (مطالعه موردی: روی شبکه اجتماعی توئیتر)

محمدرضا محمدرضائی*
مربی گروه کامپیوتر، دانشگاه آزاد اسلامی واحد رامهرمز، رامهرمز

(دریافت: ۱۳۹۹/۰۹/۱۵، پذیرش: ۱۳۹۹/۱۱/۲۹)

چکیده

استفاده از شبکه‌های اجتماعی به شکل فزاینده‌ای در حال رشد است و افراد زمان زیادی از وقت خود را صرف استقاده از این شبکه‌ها می‌کنند. افراد مشهور و شرکت‌ها از این شبکه‌ها برای ارتباط با طرفداران و مشتریان خود استفاده کرده و آژانس‌های خبری برای توزیع خبر از این شبکه‌ها استفاده می‌کنند. در راستای ترقی محبوبیت و رواج شبکه‌های اجتماعی بر خط، خطرات و تهدیدات امنیتی نیز درحال افزایش است و انجام فعالیت‌های مخرب و حملاتی از قبیل فیشینگ، ایجاد کاربران جعلی و اسپم‌ها در این شبکه‌ها افزایش چشمگیری داشته است. در حمله ایجاد کاربر جعلی، کاربران مخرب با ایجاد کاربر جعلی خود را به جای افراد معرفی می‌کنند و از این طریق از شهرت افراد یا شرکت‌ها سوء استفاده می‌کنند. در این مقاله یک روش جدید برای کشف کاربران جعلی در شبکه‌های اجتماعی بر پایه الگوریتم‌های یادگیری ماشین ارائه می‌شود. در روش پیشنهادی برای آموزش ماشین از ویژگی‌های شباهت مختلفی مانند شباهت کسینوس، شباهت جاکارد، شباهت شبکه دوستی و معیارهای مرکزیت استفاده می‌شود که همه این ویژگی‌ها از ماتریس مجاورت گراف شبکه اجتماعی استخراج می‌شوند. در ادامه جهت کاهش ابعاد داده‌ها و حل مشکل بیش برازش از تحلیل مولفه‌های اصلی استفاده شد. سپس با استفاده از دسته‌بندهای تخمین چگالی هسته و الگوریتم شبکه عصبی خود سازمان‌ده داده‌ها دسته‌بندی شده و نتایج روش پیشنهادی با استفاده از معیارهای دقت، حساسیت و نرخ تشخیص اشتباه ارزیابی می‌شود. بررسی نتایج نشان می‌دهد، روش پیشنهادی با دقت ۹۹/۶٪ کاربران جعلی را تشخیص می‌دهد که نسبت به روش کاوو حدود ۵٪ بهبود یافته است، همچنین نرخ تشخیص اشتباه کاربران جعلی نیز نسبت به همین روش ۳٪ بهبود پیدا کرد.

کلمات کلیدی: کاربران جعلی، شبکه‌های اجتماعی، تحلیل گراف، تخمین چگالی هسته

۱- مقدمه

امروزه استفاده از شبکه‌های اجتماعی به دلیل امکان ارتباط میان افراد در سرتاسر دنیا و امکان اشتراک‌گذاری فیلم، عکس محبوبیت زیادی پیدا کرده است [۱]. رشد انتقال اطلاعات و تعاملات محرمانه میان کاربران ازمهمترین دلایلی هستند که افراد عواقب منفی به اشتراک گذاری اطلاعات شخصی دراینترنت را نادیده می‌گیرند به خصوص زمانی که اطلاعات به‌عنوان داده‌های عمومی برای مدت زمانی طولانی به اشتراک گذاشته می‌شود. در راستای ترقی محبوبیت و گسترش شبکه‌های اجتماعی بر خط، خطرات و تهدیدات امنیتی نیز درحال افزایش است که برحریم شخصی و قابلیت اعتماد کاربران تاثیر دارد [۲]. حفاظت از حریم شخصی کاربران نه تنها حفاظت از داده‌هایی است که کاربران در پروفایل‌های خود به اشتراک می‌گذارند، بلکه حفظ ارتباطات و فعالیت‌های آن‌ها در شبکه‌های اجتماعی بر خط نیز می‌باشد [۳]. به‌دلیل حجم زیاد داده‌ها در شبکه‌های اجتماعی فعالیت‌های مخرب و حملاتی از قبیل فیشینگ، ایجاد کاربران جعلی و اسپم‌ها نیز افزایش چشمگیری داشته است [۴] در حمله ایجاد کاربر جعلی، کاربران مخرب خود را به جای افراد معرفی می‌کنند [۵ و ۶]و از این طریق از شهرت افراد یا شرکت‌ها سوء استفاده می‌کنند یا از طریق ایجاد کاربر جعلی کنترل یک کاربر را در دست گرفته و اقدام به انتشار اخبار کذب می‌کنند [۷ و ۸]، هدف اصلی این حمله به‌دست آوردن اطلاعات شخصی دوستان قربانی به واسطه جعل کاربر و افزایش قابلیت اعتماد درمحیط‌های دوستانه برای فریب بیشتر کاربران درآینده است [۹]. شناسایی و کشف حملات جعل کاربر با روش‌های بهتر موجب بهبود امنیت کاربران فعال و ترغیب ارائه‌دهندگان سرویس‌های شبکه‌های اجتماعی به افزایش سطح ایمنی و حریم شخصی سرویس‌های

*رایانامه نویسنده مسئول: mohammadrezaei.m.reza@gmail.com

ناشر: دانشگاه جامع امام حسین (ع)

شبکه است [۱۰]. هدف این مقاله ارائه یک روش ترکیبی و استفاده از مزایای تحلیل گراف و یادگیری ماشین جهت تشخیص کاربران جعلی در شبکه‌های اجتماعی است. در تمام روش‌های قبلی برای حل مساله کشف کاربران جعلی از دسته‌بندهای دو کلاسه استفاده شد. چالش مطرح در دسته‌بندهای دوکلاسه این است که نمونه‌های ناشناخته و فاقد هرگونه تشابه به داده‌های دو کلاس، دریکی از دو کلاس دسته‌بندی می شوند. لذا عملکرد دسته‌بند دوکلاسه در مقابل این گونه نمونه‌ها مناسب نیست. در این مقاله برای حل این چالش از دسته‌بند تک کلاسه که عبارت است از توصیف داده‌ها در یک دامنه خاص استفاده می‌شود. ابتدا کاربران نرمال برای آموزش الگوریتم استفاده شده و هر کاربری که در این توصیف قرار نگیرد را به‌عنوان جعلی تشخیص می‌دهد.

در مجموعه تحقیقات و راه‌حل‌های ارائه شده پیشین برای کشف کاربران جعلی این مشکلات وجود دارند.

- استفاده از معیارهای شباهتی که قدرت ارتباط شبکه دوستان مشترک میان کاربران را در نظر نمی‌گیرند در صورتی که ما معتقدیم هر چه شبکه دوستی مشترک دو کاربر اتصالات بیشتری داشته باشد (تعداد یال بیشتر) شباهت کاربران بیشتر است.
- به‌دلیل حجم بالای اطلاعات استفاده از روش‌های یادگیری ماشین مشکل بیش برازش[1] را به‌دنبال دارد.

در این مقاله یک روش جدید مبتنی بر الگوریتم‌های یادگیری ماشین و تحلیل گراف شبکه اجتماعی جهت تشخیص کاربران جعلی پیشنهاد شده است که مهمترین ویژگی‌های آن در زیر آمده است:

۱- استفاده از معیارهای مرکزیت و معیارهای شباهت مختلف به منظور استفاده از قدرت ارتباط شبکه دوستان مشترک بین کاربران.

۲- استفاده از مدل استخراج ویژگی تحلیل مولفه‌های اصلی برای جلوگیری از مشکلات بیش برازش.

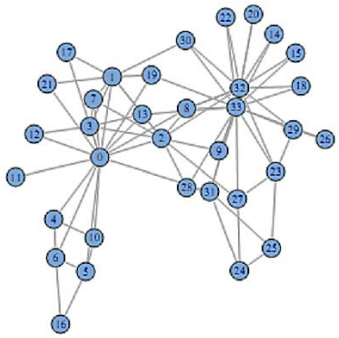
در ادامه در بخش ۲ مفاهیم پایه‌ای مربوط به تحلیل گراف و مفاهیم مرتبط با استفاده از آن بیان می‌شود، بخش ۳، مروری بر کارهای پیشین انجام می‌شود، روش پیشنهادی در بخش ۴ شرح داده می‌شود، بخش ۵، نتایج تجربی به‌دست آمده از ارزیابی سیستم پیشنهادی تشریح شده و نتیجه‌گیری و پیشنهادات کارهای آتی در بخش ۶ انجام می‌شود.

۲- مفاهیم

شبکه‌های اجتماعی و تحلیل گراف شبکه دارای مفاهیم پایه‌ای ریاضیاتی قوی هستند که در ادامه مفاهیم مورد نیاز معرفی می‌شوند. همچنین مفاهیم تحلیل مولفه‌های اصلی که برای تحلیل داده‌های چندبعدی استفاده می‌شود و روش‌های متوازن کردن داده‌ها تعریف می‌شوند.

۲-۱- شبکه‌های اجتماعی

شبکه اجتماعی ساختاری اجتماعی از گره‌هایی که عموماً افراد یا سازمان‌ها هستند تشکیل شده است که توسط یک یا چند نوع خاص از وابستگی به هم متصل شده اند. برای مثال قیمت‌ها، ایده‌ها و تبادلات مالی، دوست‌ها، خویشاوندی‌ها، تجارت، پیوندهای وب، سرایت بیماری‌ها (اپیدمولوژی) یا مسیرهای هواپیمایی. ساختارهای حاصل اغلب بسیار پیچیده هستند. تحلیل شبکه‌های اجتماعی روابط اجتماعی را با اصطلاحات گره و یال می‌نگرد. گره‌ها بازیگران فردی درون شبکه‌ها و یال‌ها روابط میان این افراد می‌باشند [۱۵- ۱۱]. شکل (۱) ساختار گراف یک شبکه اجتماعی را نشان می‌دهد [۱۶].



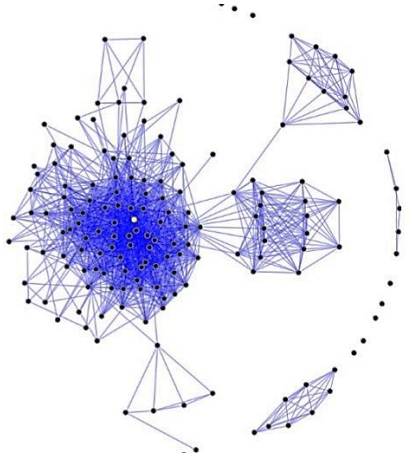
شکل (۱): ساختار گراف یک شبکه اجتماعی [۱۶].

با وجود اینکه سایت‌های شبکه‌های اجتماعی تفاوت‌های بسیاری دارند، مفهوم رایجی در میان آن‌ها وجود دارد به شکلی که هر کاربر یک کاربر و موجودیت یکتا را برای نشان دادن خود ارائه می‌کند و دارای یک کاربر قابل تغییر است که برای نشان دادن تصویر و فهرستی از مشخصات برای هر فرد در جهان واقعی استفاده می‌شود. وب‌سایت‌های شبکه‌های اجتماعی الگوی کلی را برای مشخصات کاربران فراهم می‌کنند و به آن‌ها امکان ورود فعالیت‌های اختیاری، علایق، موزیک، فیلم و اطلاعات کلی درباره آن‌ها را می‌دهد و همچنین کاربران می‌توانند زمینه‌های اختیاری را به کاربر خود اضافه کنند.

[1] Over fitting

تحلیل شبکه اجتماعی حوزه مطالعاتی است که خصیصه‌های شبکه‌های اجتماعی را مورد تحقیق و بررسی قرار می‌دهد. تحلیل شبکه اجتماعی به ما کمک می‌کند که روابط میان افرادی را بررسی کنیم که بواسطه شبکه‌های اجتماعی به هم مرتبط هستند، و درکی از الگوهای ذاتی فراهم کند که در این گراف‌های اجتماعی تعبیه شده است. برخی از مهمترین وظایف تحلیل شبکه اجتماعی تحلیل مرکزیت، تشخیص اجتماع، انتشار اطلاعات، حداکثرسازی تاثیر، پیش‌بینی لینک، سیستم‌های توصیه‌کننده و تشخیص ناهنجاری می‌باشند.

شبکه‌های اجتماعی عموما با استفاده از گراف‌ها الگوسازی می‌شوند [۱۷- ۱۹] یک گراف چارچوب نمایشی قدرتمندی برای یک شبکه پیچیده با گره‌های نشان دهنده شخصیت/ هویت‌ها و یال‌های نشان‌دهنده تعاملات میان آن‌ها است. به‌طور رسمی، یک شبکه اجتماعی به‌وسیله گراف G=(V,E,S,L) تعریف می‌شود، در این گراف افراد و سازمآن‌ها (کاربر ها) گره‌ها را تشکیل می‌دهند، E مجموعه‌ای از یالهایی است که ارتباط بین گره‌ها در شبکه اجتماعی را نشان می‌دهد، L مجموعه‌ای از برچسب‌های گره‌هاست. این برچسب قانونی یا جعلی بودن کاربرها را مشخص می‌کند. مساله مد نظر این است، ما یک گراف G=(V,E,S,L) با یک زیر مجموعه V1□V از گره های برچسب دار داریم، در اینجا V مجموعه‌ای از n گره در گراف است و V_2=V-V_1 مجموعه گره‌های بدون برچسب هستند. E نشان‌دهنده مجموعه یال‌ها، S مجموعه ای از شباهت‌های تعریف شده میان گره‌ها و L= {F, N} مجموعه برچسب ها را نشان می‌دهد که در واقع نشان‌دهنده نرمال یا جعلی بودن کاربر هستند، مساله مورد نظر این است که با توجه به شباهت‌های تعریف شده میان گره‌ها، همه گره‌های فاقد برچسب را برچسب‌گذاری کنیم.



شکل (۲): نگاشت شبکه اجتماعی به گراف [۱۳]

لبه‌ها: لبه (i,j) ∈E بین دو گره Vi, Vj نشان‌دهنده ارتباط و دوستی میان این دو گره است.

برچسب‌ها: مجموعه برچسب‌ها وضعیت قانونی یا جعلی بودن کاربر را نشان می‌دهند. البته برچسب‌ها مقادیر دیگری نیز می‌توانند بگیرند.

در این مقاله برای استفاده از تحلیل گراف شبکه اجتماعی دو دسته معیار کلی مورد بررسی قرار می‌گیرند که شامل معیارهای شباهت و معیارهای مرکزیت می‌باشند در ادامه این معیارها تعریف می‌شوند.

۲-۲- معیارهای شباهت کاربران

با توجه به نتایج خوبی که در استفاده از معیارهای شباهت در مقالات مختلف وجود دارد، در این مقاله از این معیارها که بر مبنای دوستان مشترک یا ارتباطات مشترک هستند برای ایجاد یک ماتریس‌گذار استفاده می‌شود معیارهای شباهت گراف از روش‌های مختلفی برای کاهش پیچیدگی مسائل تحلیل گراف استفاده می‌کنند [۲۰, ۲۱] که در ادامه این معیارها تعریف می‌شود البته به‌طور خاص برای در نظر گرفتن قدرت ارتباطات میان کاربران معیارهای دیگری نیز تعریف شده است.

۲-۲-۱- معیار شباهت گراف دوستی

گراف شبکه اجتماعی G را در نظر بگیرید گراف دوستی یک گره شامل همه گره‌هایی است که به‌صورت مستقیم به آن گره متصل هستند و مطابق رابطه (۱) تعریف می‌شود [۲۲].

$$FG(v).N = \{v\} \cup \{n \in G.N | n \neq v. \exists\, e \in Gtd;.E.e =< v.n >\} \quad (1)$$

$$FG(v).E = \{< v.n > \in G.E \mid n \in FG(v).N\} \cup \{< n.n' > \in G > E \mid n.n' \in FG(v).N\}$$

۲-۲-۲- دوستان مشترک

یکی از معیارهای شباهت در شبکه‌های اجتماعی تعداد دوستان مشترک میان آن‌هاست [۲۳]. در گراف شبکه اجتماعی تمام راس‌هایی که روی یک مسیر به طول ۲ بین دو گره قرار دارند دوستان مشترک دو گره هستند، دوستان مشترک با استفاده از رابطه (۲) محاسبه می‌شوند [۲۴, ۲۵].

$$CF(u.v) = |FG(v).N \cap FG(u).N| \quad (2)$$

۲-۲-۳- تعداد کل دوستان

تعداد کل دوستان، تعداد دوستان متفاوت بین دو گره V و U را نمایش می‌دهد که از رابطه (۳) محاسبه می‌شود [۲۲].

$$\text{Total friends}(v.u) = |FG(v).N \cup FG(u)N| \quad (۳)$$

۲-۲-۴- معیار شباهت جاکارد

ضریب جاکارد شباهت میان مجموعه نمونه‌ها را نمایش می‌دهد و در حقیقت نسبت دوستان مشترک دو گره به کل دوستان آن‌ها را محاسبه می‌کند که رابطه (۴) بیانگر این شباهت است [۲۶ و ۲۷].

$$\text{jaccard}(v.u) = \frac{|FG(u).N \cap FG(v).N|}{|FG(u).N \cup FG(v)N|} \quad (۴)$$

۲-۲-۵- اندیس ترفیع هاب

برای تعیین کیفیت همپوشانی توپولوژیک جفت لایه‌ها در یک شبکه دگرگون شونده بکار می‌رود و به‌صورت رابطه (۵) تعریف می‌شود [۲۸, ۲۹].

$$\text{HDI}(v.u) = \frac{|FG(v).N \cap FG(u).N|}{\max\{|FG(u).N| . |FG(v)N|\}} \quad (۵)$$

۲-۲-۶- اندیس فشرده هاب

همانند اندیس ترفیع هاب است با این تفاوت که مقدار حداکثر درجه‌ها را در نظر می‌گیرد. رابطه (۶) این معیار را محاسبه می‌کند [۲۹].

$$HPI(v.u) = \frac{|FG(v).N \cap FG(u).N|}{min\{|FG(u).N| . |FG(v)N|\}} \quad (۶)$$

۲-۲-۷- شباهت کسینوس

یکی دیگر از معیارهای شباهت میان گره‌های گراف شباهت کسینوس است. شباهت کسینوس در حقیقت شباهت میان دو بردار را محاسبه می‌کند که رابطه (۷) این شباهت را محاسبه می‌کند [۳۰, ۳۱].

$$\text{Cos}(v.u) = \frac{|FG(v).N \cap FG(u).N|}{\sqrt{|FG(v).N|.|FG(u).N|}} \quad (۷)$$

۲-۲-۸- شباهت نرم L1

معیار شباهت نرم L1 برای در نظر گرفتن لینک‌های دوستی در شبکه استفاده می‌شود. رابطه (۸) بیانگر این معیار است [۲۲ و ۳۲].

$$\text{L1 norm}(v.u) = \frac{|FG(v).N \cap FG(u).N|}{|FG(v).N|.|FG(u).N|} \quad (۸)$$

۲-۲-۹- معیار وزن یال

معیار وزن یال ابتدا به‌صورت دو ویژگی جداگانه برای هریک از دو بردار به‌صورت رابطه (۹) محاسبه می‌شود [۳۳].

$$w(v) = \frac{1}{\sqrt{1 + FG(v).N}}$$
$$w(u) = \frac{1}{\sqrt{1 + FG(u).N}} \quad (۹)$$

اکنون وزن یال میان دو راس, U و V می‌تواند به دو طریق زیر محاسبه شود.

جمع وزن‌ها: جمع وزنها برابر است با جمع دو وزن تعریف شده برای u و v که با استفاده از رابطه (۱۰) محاسبه می‌شود.

$$W(v.u) = w(v) + w(u) \quad (۱۰)$$

ضریب وزن‌ها: ضریب وزن‌ها برابر است با حاصل‌ضرب دو وزن تعریف شده برای u و v که به‌صورت رابطه (۱۱) محاسبه می‌شود.

$$W(v.u) = w(v) * w(u) \quad (۱۱)$$

۲-۳- معیارها مرکزیت و نحوه محاسبه آن‌ها

از دیگر معیارهای مهم در بحث شبکه‌های اجتماعی معیارهای مرکزیت است که در این مقاله به بررسی نقش این معیارها در تشخیص کاربران جعلی پرداخته می‌شود. برای این منظور این معیارها تعریف می شوند.

۲-۳-۱- مرکزیت

مرکزیت، یک معیار کمی باهدف آشکارسازی اهمیت‌گره‌ها می‌باشد، هرکدام از مولفه‌های مرکزیت درشبکه‌های اجتماعی نقش‌خاصی دارند در واقع، این معیارها مبتنی برجنبه‌های متفاوتی از خصوصیات گره‌ها هستند و اغلب با یکدیگر درتضاد هستند. هر معیار مرکزیت از خصوصیات خاصی برخوردار است. به‌دلیل این تفاوت‌ها در شبکه‌های اجتماعی، شاخص‌های ارائه‌شده و نتیجه‌گیری‌ها همواره برای همه انواع شبکه‌ها صادق نیستند. براساس تعریف و خصوصیت‌های مورد استفاده در تعیین اهمیت گره، مرکزیت‌های مختلفی تعریف می‌شوند که در ادامه به تعریف این مرکزیت‌ها پرداخته می‌شود.

۲-۳-۲- مرکزیت درجه[1]

مرکزیت درجه‌بندی در سال ۱۹۷۹ توسط فریمن معرفی شد. در تعریف این مرکزیت اهمیت هرگره بر اساس درجه هرگره تعریف می‌شود. درجه هرگره برابر با تعداد یال‌هایی است که به آن گره متصل باشند. اگر بردار مرکزیت درجه را DC بنامیم مرکزیت درجه با استفاده از رابطه (۱۲) محاسبه می‌شود [۴۷].

$$DC = [dc_i] \rightarrow dc_{i=\sum \min(\mathbf{1}.a_{ij})} \quad (۱۲)$$

۲-۳-۳- مرکزیت مابینیت[2]

مرکزیت مابینیت گره‌ای در گراف که در مسیرارتباطی دو گره دیگر قرار دارد. به‌عبارت دیگر فردی در شبکه که موجب ارتباط دو فرد دیگر در شبکه می‌شود به شرطی‌که این مسیر کوتاه‌ترین مسیر ارتباطی بین آن دو نفر باشد. هر چه این مقدار بیشتر باشد مرکزیت مابینیت بالاتر است. می‌توان گفت تعداد دفعاتی که یک گره به‌عنوان پل در طول کوتاه‌ترین مسیر بین دو گره دیگر واقع می‌شود را مابینیت آن گره می‌نامند [۴۷]. مرکزیت مابینیت با استفاده از رابطه (۱۳) قابل محاسبه است.

$$b_i = \sum_{j.k \neq i} \frac{g_{jk}(i)}{gjk} \quad (۱۳)$$

که در آن g_{jk} تعداد کوتاهترین مسیرهای دودویی بین گره j و k است و $g_{jk}(i)$ تعداد مسیرهایی است که از گره i عبور می‌کند.

۲-۳-۴- مرکزیت نزدیکی[3]

مرکزیت نزدیکی نیز توسط فریمن درسال ۱۹۷۹ تعریف شد. مرکزیت نزدیکی هر گره برابر با مجموع کوتاه‌ترین مسیرهای آن گره تا سایرگره‌های شبکه است.

اندازه‌گیری مرکزیت نزدیکی‌گره i در یک شبکه وزنی به‌صورت c_i^w است که به‌صورت رابطه (۱۴) قابل محاسبه است.

$$C_i^w = \left[\sum_j^N d^w(i.j)\right] \quad (۱۴)$$

که در آن d_{ij}^w کوتاه‌ترین فاصله یا قدرت اتصال بین گره i و j است.

۲-۳-۵- مرکزیت بردار ویژه[4]

در مرکزیت بردار ویژه برای ما مهم است که به گره‌های اصلی وصل باشیم. هرچند دوگره a و b دارای درجه یکسانی هستند، اما اهمیت این دوگره یکسان نیست. گره b مرکزیت بیشتری‌دارد، زیرا به گره‌های مهم‌تری وصل است. پس همسایگی در مرکزیت بردار ویژه بسیار مهم است. محاسبه بردارهای مرکزیت در [۴۷] بیان شده است.

۲-۴- تحلیل مولفه‌های اصلی[5]

تحلیل مولفه‌های اصلی یکی از روش‌های آماری چند متغیره است. وقتی که ابعاد داده‌ها بالا باشد، برای کاهش ابعاد داده‌ها و تبدیل داده‌ها به ابعاد قابل فهم و قابل تفسیر از این روش استفاده می‌شود. با اعمال این روش، متغیرهای اولیه به مولفه‌های جدید و مستقل از هم تبدیل می‌شوند. مولفه‌های جدید به‌دست آمده یک ترکیب خطی از متغیرهای اولیه هستند. با استفاده از این روش، یک ترکیب تشکیل شده از n متغیر اولیه $X_1, X_2, \ldots, X_n$ برای ایجاد n مولفه مستقل مانند $Y_1, Y_2, \ldots, Y_n$ به‌کار می‌رود. استقلال این مولفه‌ها جنبه‌های متفاوتی از متغیرهای اولیه را آشکار می‌کند. در این روش متغیرهای اولیه به طور مستقیم استفاده نمی‌شوند، بلکه به مولفه های جدیدی تبدیل شده که این مولفه‌ها به جای متغیرهای اولیه استفاده می‌شوند. هر مولفه می‌تواند به‌صورت رابطه (۱۴) در نظر گرفته شود.

$$Y_i = a_{i1}X_1 + a_{i2}X_2 + \ldots\ldots + a_{in}X_n \quad (۱۴)$$

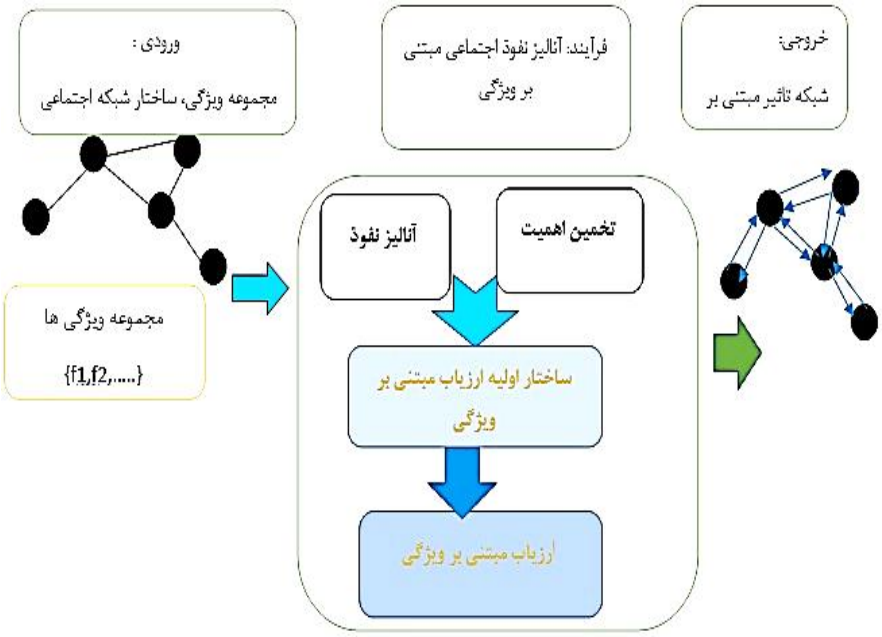
که در آن Y_i، i امین مولفه اصلی، a_{ij} ضرایب مربوط به متغیرهای اولیه، n تعداد تعداد متغیرهای اولیه و X_i نیز متغیرهای اولیه است [۳۴].

در ادامه برای استفاده از مولفه‌های اصلی از روش البو استفاده می‌شود. محاسبه نقطه البو به چند روش قابل محاسبه است که می‌توان ثابت کرد چه میزان از داده‌ها دارای بیشترین بار اطلاعاتی هستند. پویان و همکارانش [۳۵] در کار خود اثبات کرده که با روش البو ۰/۰۵ از داده ها حاوی بار اطلاعاتی هستند.

۲-۵- الگوریتم تخمین چگالی هسته[6]

تخمین چگالی، تخمین یک تابع چگالی از داده‌های مشاهده شده است که دو روش مولفه‌ای و غیر مولفه‌ای برای تخمین چگالی وجود دارد. روش تخمین چگالی هسته یک نوع توزیع غیر مولفه‌ای است که توسط پرزن [۳۶] ارائه شد. این روش پیچیدگی محاسباتی بالایی دارد. تخمین چگالی هسته در حل مسائل مختلف استفاده شده و همچنین از تخمین چگالی هسته برای تشخیص و آشکارسازی ناهنجاری، شناسایی آیتم ها، رویدادها یا مشاهداتی است که با یک الگوی مورد انتظار مطابقت ندارد استفاده می‌شود [۳۷].

[1] Degree Centrality
[2] Betweeness Centrality
[3] Closeness Centrality
[4] Eigenvector Centrality
[5] principle Component Analysis
[6] Kernel Dencity Estimator



شکل(۳): چارچوب روش پیشنهادی وانگ [۴۰].

۳- مروری بر کارهای پیشین

کشف و حذف کاربران جعلی در شبکه‌های اجتماعی باعث بهبود امنیت کاربران در این شبکه‌ها می‌شود و علاقه کاربران برای استفاده از این شبکه ها را افزایش می‌دهد. از این رو این مساله به یکی از چالش برانگیزترین مسایل تحقیقاتی در حوزه شبکه‌های اجتماعی شده است و محققان زیادی روش‌هایی برای حل این مساله ارایه کردند که روش‌های ارایه شده در سه دسته کلی بررسی می‌شوند.

۳-۱- روش‌های مبتنی بر رفتار

تحلیل و ارزیابی رفتار کاربران در شبکه‌های اجتماعی رایج شده است و این باعث افزایش ریسک‌های امنیتی در شبکه می‌شود. بیشتر مدل‌های مبتنی بر رفتار از الگوریتم های خوشه بندی و تئوری‌های آماری استنباط می‌کنند [۳۸]. جوراجالا[1] و همکاران [۳۹] یک روش مبتنی بر تحلیل ویژگی های پروفایل برای تشخیص کاربران جعلی در توئیتر ارایه دادند. آن‌ها ابتدا به جمع آوری سی و سه ویژگی متفاوت برای هر پروفایل پرداختند. سپس الگوهای ترکیبی از ویژگی‌ها را برای شناسایی مجموعه ای از هسته‌های قابل اعتماد از پروفایل‌های جعلی را ایجاد کردند که اساس شناسایی ویژگی‌های کلیدی تشخیص کاربران جعلی بر اساس اطلاعات در دسترس آن‌ها خواهد بود. آن‌ها برای محدود کردن فضای مولفه تحلیلشان، ابتدا پایگاه داده را به صورت نیمه دستی بررسی کرده تا ویژگی‌های اولیه را که در بین بیشتر کاربران تعریف شده است را تعیین کنند. برای تعیین ویژگی‌های محموعه حساب‌های جعلی، مجموعه‌ای از داده‌های حقیقی را تولید کرده و از یک جدول زمانی که شامل تحلیل زمان‌های بروزرسانی، زمان ایجاد و... بود، برای مقایسه حساب‌های جعلی و حقیقی استفاده کردند. وانگ[2] و همکاران [۴۰] یک مدل ارزیابی اجتماعی مبتنی بر ویژگی را ارایه کردند که در شکل (۲-۲) نشان داده شده است.

هر کاربر یک مقدار عددی را به عنوان معیار اجتماعی خود تعیین می‌کند و هر لبه با نسبت نفوذ مشارکت از یک کاربر به دیگری برچسب گذاری می‌شود.

شان[3] در [۴۱] یک رویکرد مبتنی بر ویژگی موثر و بسیار ساده آدرس IP بنام Clone spatter ارائه می‌کند. در این رویکرد ابتدا اطلاعات آی پی کاربران جمع آوری می‌شود. وقتی درخواست دوستی از A به سمت B ارسال می‌شود لیست دوستان b چک می‌شود برای اینکه ببینیم b دوستی با نام یکسان A دارد یا خیر؟ سپس برای هر فرد u در لیست دوستان b که نامی مشابه A دارد، پروفایل A ,U مقایسه می‌شود و شباهت آن‌ها محاسبه و در الگوریتم استفاده می‌شود. اگر شباهت بین پروفایل‌ها بیش از حد باشد به این معنی است که پروفایل ها متعلق به یک شخص هستند. البته هنوز دو احتمال وجود دارد: A یک کاربر دیگر از U است یا A یک کاربر جعلی است. برای قضاوت در مورد اینکه A جعل شده است یا خیر IP های آن‌ها با هم مقایسه می‌شوند.

[1] Gurajala
[2] Wang
[3] Shan

۳-۲- روش‌های مبتنی بر گراف

یکی از روش‌های تحلیل شبکه‌های اجتماعی استفاده از گراف است. در این روش شبکه اجتماعی به یک گراف نگاشت شده که در آن افراد و سازمآن‌ها، گره‌ها را تشکیل داده و ارتباطات میان آن‌ها یال‌ها را می‌سازند [۴۲، ۴۳].در شبکه های اجتماعی به این گراف، گراف اجتماعی گفته می‌شود که گراف شبکه اجتماعی می‌تواند استاتیک یا دینامیک و برچسب دار یا بدون برچسب باشد [۴۴].

کانتی[1] و همکاران [۴۵] یک چارچوب برای کشف کاربران جعلی بر پایه ی نرخ رشد گراف شبکه اجتماعی و تعامل کاربران با دوستانشان روی شبکه ارایه کردند. آن‌ها رشد کاربر و رشد گراف شبکه اجتماعی را مد نظر گرفته و در بازه‌های ۳۰، ۶۰ و ۹۰ روزه آن‌ها را بررسی کردند و متوجه شدند نرخ افزایش دوستان کاربران حقیقی در طول زمان یک نرخ ثابت بوده و نرخ رشد کاربران جعلی با آن‌ها متفاوت است که از این برای مشخص کردن کاربران جعلی استفاده کردند. آن‌ها همچنین روش پیشنهادی را بر روی مجموعه داده‌ها شبکه اجتماعی فیسبوک اجرا کردند.

ژانگ[2] و همکارانش [۴۶] یک روش جدید برای تشخیص کاربران جعلی ارایه دادند که در این روش حساب‌هایی که فالورهای مشترک زیاد داشتند را با هم مقایسه و جعلی بودن آن‌ها را بررسی می‌کرند. مرتضی یوسفی [۱۶]یک روش جدید برای شناسایی کلون‌شدگی پروفایل در شبکه‌های اجتماعی پیشنهاد داد. در این روش ابتدا شبکه اجتماعی به یک گراف نگاشت می‌شود و سپس طبق شباهت‌های میان کاربران این گراف به جوامع کوچکتری تقسیم می‌شود. پس از آن همه پروفایل‌های شبیه به پروفایل حقیقی از همان جامعه جمع‌آوری شده و قدرت رابطه میان پروفایل‌های منتخب و پروفایل حقیقی محاسبه می‌شود و آن‌هایی که قدرت ارتباط کمتری دارند تایید می‌شوند. در این مطالعه برای ارزیابی کارایی روش پیشنهادی تمام مراحل در مجموعه داده‌ای فیسبوک اجرا و نتایج با روش‌های پیشین مقایسه می‌شود.

ویسوانات[3] در [۴۷] نشان داده که علیرغم تفاوت‌های قابل توجه سیستم‌های موجود، سیستم تشخیص جعل آن‌ها با شناسایی جوامع محلی (یعنی خوشه های گره‌هایی که بیشتر از بقیه گره‌ها هستند) در اطراف یک گره قابل اعتماد کار می‌کند و یافته‌های آن‌ها پیامدهای مهمی برای طرح‌های موجود و آینده طرح‌های دفاع تشخیص جعل کننده‌ها دارد. آن‌ها نشان می‌دهند که شبکه‌های با ساختار مشخص شده جامعه، به طور ذاتی بیشتر به حملات جعل هویت آسیب‌پذیر هستند.

یانگ[4] و همکاران[۴۸] ، یک سیستم دفاعی مقیاس پذیر به نام VoteTrust را ارائه کردند که بیشتر فعالیت‌های سطح کاربر را ارزیابی می‌کند. VoteTrust تعاملات دعوت نامه دوستی را در میان کاربران به عنوان یک گراف به کار رفته، امضا کرده و از دو مکانیزم کلیدی برای تشخیص جعل بر روی نمودار استفاده می‌کند. آن‌ها از طریق ارزیابی شبکه اجتماعی رنرن[5] نشان دادند که VoteTrust قادر به جلوگیری از جعل بسیاری از درخواست‌های ناخواسته دوستان است. کائو[6] [۴۹] یک ابزار جدید برای اپراتورهای شبکه‌های اجتماعی معرفی کرد که آن را SybilRank نامید، این ابزار متکی به ویژگی‌های گراف اجتماعی است تا جعلی بودن کاربران را بر اساس یک احتمال تعیین کند. این ابزار از لحاظ محاسباتی کارآمد است و می‌تواند به صدها میلیون گره با نمودارها گسترش یابد.

بوشماف[7] و همکاران[۵۰] یک روش مبتنی بر پیاده‌روی تصادفی برای دسته بندی کاربران جعلی ارایه داده است. آن‌ها نشان دادند که قربانیان، کاربران نرمالی هستند که حساب‌های واقعی داشته ولی دارای دوستانی با کاربران تقلبی هستند.

جین و همکاران[۵۱] در چارچوب شناسایی فعالی جهت مشخص کردن کاربرهای جعل‌شده پیشنهاد کردند. این چارچوب شامل سه مرحله می‌باشد: مرحله اول، جستجو و جداسازی هویت‌ها به‌عنوان مجموعه‌ای از کاربرها است، زیرا ورودی جستجو، مشخصات کاربر می‌باشد. مرحله دوم، شناسایی کاربرهای مشکوک از طریق استفاده از طرح‌های شباهت کاربر بوده و مرحله سوم، حذف کاربرهای کلون شده از فهرست دوستان می‌باشد. در مرحله شناسایی، تنظیم مجموعه‌ای از مولفه‌ها می‌تواند به شناسایی درست در شبکه‌های اجتماعی مختلف، کمک کند.

۳-۳- روش‌های یادگیری ماشین

در اکثر روش‌های یادگیری ماشین به‌وسیله الگوریتم‌های یادگیری ماشین دسته‌بندها را آموزش می‌دهند و با استفاده از الگوهای کشف شده بدنبال ایجاد تمایز بین کاربران حقیقی و جعلی هستند.

[1] Conti
[2] Zhang
[3] Viswanath
[4] Yang
[5] Renren
[6] Cao
[7] Boshmaf

آرگا یک مدل جدید مبتنی بر یادگیری ماشین و روش‌های پردازش زبان طبیعی برای کشف کاربران جعلی در شبکه اجتماعی اینستاگرام پیشنهاد داد. برای افزایش میزان دقت شناسایی کاربران جعلی در شبکه های اجتماعی بر خط از ویژگی هایی مانند زمان، تاریخ انتشار پست، زبان و موقعیت جغرافیایی کاربران استفاده کرد [۵۲].

آکیون و همکاران یک روش جدید برای شناسایی حساب‌های جعلی جهت جلوگیری از تعاملات جعلی ارایه دادند. در روش پیشنهادی برای شناسایی حساب‌های دستی از الگوریتم‌های رگرسیون لاجستیک، ماشین بردار پشتیبان و شبکه عصبی و جهت تشخیص حساب هایی که به صورت خودکار[1] ایجاد می‌شوند از الگوریتم ژنتیک حساس به هزینه استفاده کردند. برای پیاده‌سازی روش پیشنهادی خود از دو مجموعه داده مختلف اینستاگرام برای حساب‌های جعلی ایجاد شده دستی و خودکار استفاده کردند. مجموعه داده استفاده شده شامل اطلاعاتی از قبیل تعداد دنبال کنندگان، تعداد دنبال شوندگان، تعداد عکس‌های نشانه گذاری[2] شده از یک کاربر و میانگین تعداد هشتگ‌های مربوط به یک کاربر است[۵۳].

ایگل و همکاران[۵۴] COMPA را ارائه دادند، COMPA یک سیستم برای شناسایی حساب‌های آسیب دیده در شبکه‌های اجتماعی است و از مدل‌های آماری برای توصیف رفتار کاربران شبکه‌های اجتماعی استفاده می‌کند همچنین از روش‌های تشخیص ناهنجاری برای شناسایی تغییرات ناگهانی در رفتار کاربران بهره می‌برد. نتایج نشان می‌دهد که رویکرد ارایه شده می تواند به طور قابل اعتماد تشخیص مصالحه‌ای که بر حساب‌های شبکه‌های اجتماعی بالا تاثیر می‌گذارد را شناسایی کرده و سازش‌های حساب‌های معمولی را که رفتار آن‌ها معمولاً بیشتر متغیر است را شناسایی کند

لی[3] و همکارا [۵۵] یک طرح جدیدی برای شناسایی کاربران بدخواه در توئیتر پیشنهاد کردند.

طرح پیشنهادی کاربرها را براساس ویژگی‌ها مشابه خوشه‌بندی کرده و سپس خوشه‌ها را براساس خصیصه‌های آن‌ها به خوب یا مشکوک دسته‌بندی می‌کند. نتایج ارزیابی نشان می‌دهد که طرح پیشنهادی به خوبی خوشه‌بندی و دسته‌بندی را انجام می‌دهد.

[1] Automate
[2] Tag
[3] Lee

یانگ[4] [۵۶] دو نوآوری را برای تشخیص کاربران جعلی در شبکه‌های اجتماعی ارایه داد. ابتدا از داده‌های حقیقی در مورد رفتار کاربران جعلی برای ایجاد یک تشخیص دهنده بلادرنگ مبتنی بر معیار استفاده کرد. دومین نوآوری این مقاله تشریح توپولوژیکی گراف کاربران جعلی روی یک شبکه اجتماعی است. آن‌ها نشان دادند که یک طبقه‌بندی مبتنی بر آستانه با کارایی محاسباتی مناسب تا ۹۹٪ کاربران جعلی را با کمترین میزان مثبت و منفی کاذب به‌دست می‌آورد.

مونیکا سین[5] و همکاران [۵۷] یک چارچوب برای شناسایی کاربران مخرب، غیر مخرب و مشهور ارائه دادند و با استفاده از ویژگی‌های تعیین شده برای طبقه بندی کاربران توسعه داده شد. آن‌ها به منظور تشخیص کاربران مخرب، کاربران غیر مخرب و افراد مشهور، یک Crawler برای توییتر را توسعه داده است و داده‌ها از حدود۲۲ هزار کاربر از اطلاعات در دسترس عموم جمع آوری شده است و از این داده‌ها برای استخراج الگو برای تمایز کاربران استفاده کردند.

گنی[6] و همکاران [۵۸] یک چارجوب مبتنی بر یادگیری ماشین و تحلیل عمیق از تعاملات اجتماعی ارایه کردند. چارچوب پیشنهادی برای تشخیص شناسه‌های چندگانه در شبکه‌های اجتماعی از متدهای ترکیب تحلیل نویسندگان با روش‌های خوشه‌بندی K میانه استفاده می‌کند. که آن شامل سه لایه است: فضای نمایش برای انتخاب و استخراج ویژگی ها برای محتوا و ارتباطات، لایه یادگیری برای بکار بردن روش های خوشه بندی جهت گروه بندی شناسه های مشابه و در گام نهایی اعتبارسنجی انجام می‌شود در اینجا تعاملات انسانی تصمیم گیری می‌کنند که کدام شناسه‌ها به‌وسیله نویسنده یکسان مدیریت می‌شوند.

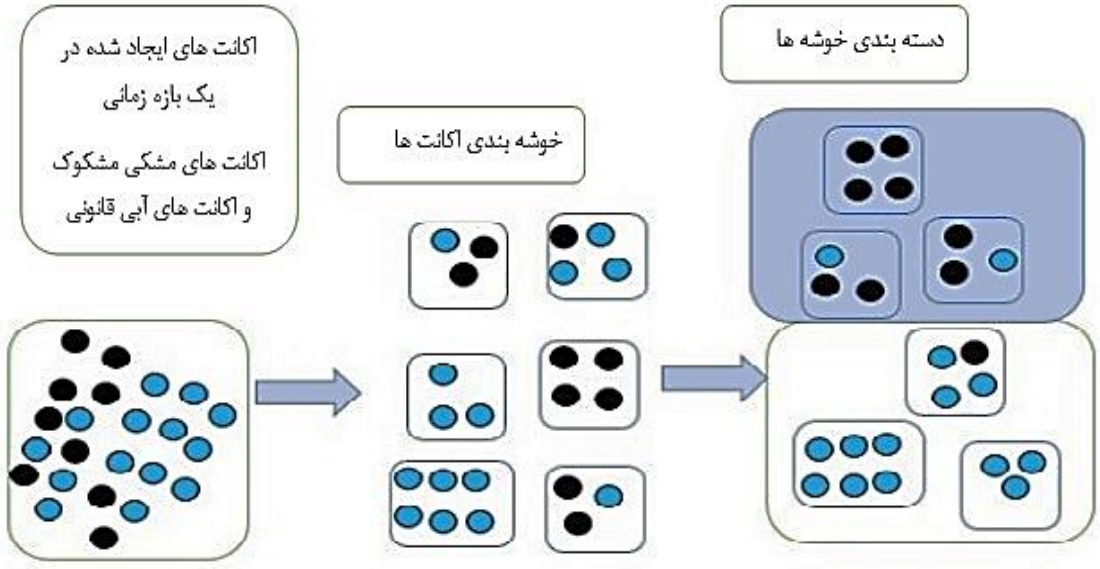
در مجموع کارهای ارایه شده قبلی دارای مشکلاتی هستند که عبارتند از:

۱- استفاده از معیارهای شباهتی که قدرت ارتباط شبکه دوستان مشترک میان کاربران را در نظر نمی گیرند.

[4] Yang
[5] Monika Singh
[6] Gani

۲- بـه‌دلیـل حجـم بـالای اطلاعـات اسـتفاده از روش‌هـای یادگیری ماشین مشکل بیش برازش را به‌دنبال دارد.

۳- در برخـی از کارهـای قبلـی جهـت پیـاده‌سـازی روش خـود بـدلایلی از جملـه عـدم دسترسـی بـه داده‌هـای شـبکه های اجتماعی واقعی یـا بـدلیل تعـداد انـدک کـاربران جعلـی نسـبت بـه کـاربران نرمـال در مجموعـه داده‌هـا بخشـی از کاربران نرمـال را جعلـی فـرض مـی‌کردنـد کـه بـه نظـر یـک فـرض کـاملا اشـتباه مـی باشـد. اکنـون روش پیشـنهادی برای برطرف کردن این مشکلات ارائه شده است.



شکل(۴): مراحل روش پیشنهادی لی [۵۵].

۴- روش پیشنهادی

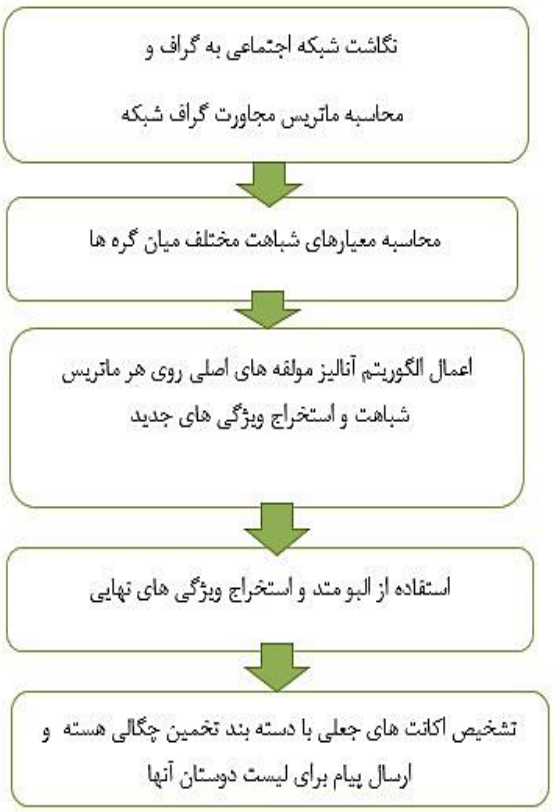
هدف این مقاله ارایه یک روش برای رفع مشـکلات بیـان شـده و بهبود کارایی حل ایـن مسـاله اسـت. در روش پیشـنهادی بـرای کشف کاربران جعلی در شبکه های اجتماعی موارد زیر مطرح می شوند:

۱- استفاده از معیارهای مرکزیت در کنار معیارهای شباهت مختلف به منظـور اسـتفاده از قـدرت ارتبـاط شـبکه دوسـتان مشترک بین کاربران

۲- استفاده از مدل استخراج ویژگی تحلیل مولفه‌های اصلی برای جلوگیری از مشکلات بیش برازش

۳- استفاده از روش‌های نمونه برداری برای تولیـد کـاربران جعلی مصنوعی به منظور ایجاد بالانس در مجموعه داده‌ها.

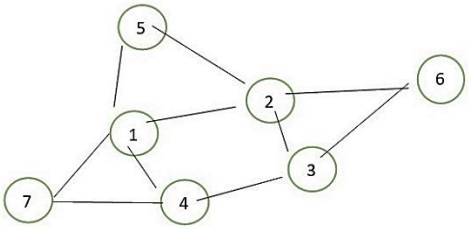
شکل (۵) روندنمای روش پیشـنهادی را نشـان مـی دهـد. ورودی آن گراف شبکه اجتماعی است که روابط میان کاربران را توصیف می‌کنـد. خروجـی روش پیشـنهادی فهرسـت کـاربران جعلی را نشان داده و پیامی حاوی جعلی بـودن ایـن کـاربر هـا برای لیست دوستان آن‌ها ارسال می‌کند.



شکل(۵): فلوچارت روش پیشنهادی

مرحله اول: نگاشت شبکه اجتماعی به گراف ومحاسبه ماتریس مجاورت گراف شبکه

برای تحلیل شبکه‌های اجتماعی با استفاده از گراف، ابتدا داده‌های شبکه اجتماعی را به یک گراف نگاشت می‌کنیم. در این مرحله به ازای هر کاربر یک گره در نظر گرفته و برای هر رابطه میان کاربران یک یال در نظر می‌گیریم. با توجه به تعریف رابطه در شبکه اجتماعی، گراف می‌تواند جهت دار یا بدون جهت باشد. برای یک گراف که دارای n کاربر است یک ماتریس مربعی $n \times n$ در نظر می‌گیریم. که اگر از راس i به راس j یک یال موجود باشد درایه سطر i ام ستون j ام و همچنین درایه سطر j و ستون i ام برابر یک در غیر اینصورت صفر می‌شود.



شکل (۶): نمونه‌ای از گراف شبکه اجتماعی

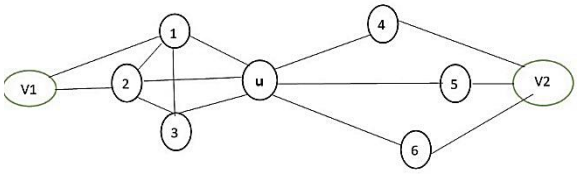
برای مثال ماتریس مجاورت مربوط به گراف شکل (۶) در شکل (۷) نمایش داده شده است.

	1	2	3	4	5	6	7
1	0	1	0	1	1	0	1
2	1	0	1	0	1	1	0
3	0	1	0	1	0	1	0
4	1	0	1	0	0	0	1
5	1	1	0	0	0	0	0
6	0	1	1	0	0	0	0
7	1	0	0	1	0	0	0

شکل (۷): ماتریس مجاورت گراف

مرحله دوم: محاسبه معیارهای شباهت مختلف میان گره‌ها

بررسی مقالات مختلف نشان می‌دهد که هیچ ویژگی به تنهائی قادر به تمایز میان کاربران یک شبکه نیست. لذا در روش پیشنهادی، برای افزایش دقت تشخیص کاربران جعلی از چندین ویژگی استفاده می شود. هدف از تعریف معیارهای مرکزیت و شباهت، بهینه‌سازی و ارتقاء کیفیت ویژگی‌های استخراج شده از کاربران شبکه است. هر چه ویژگی استخراج شده حاوی اطلاعات دقیق‌تر و با قابلیت تفکیک‌کنندگی بیشتر باشد آنگاه از ویژگی مورد نظر به نحو بهتری می‌توان در آشکارسازی کاربران جعلی استفاده کرد. در این مرحله به ازای هر کدام از معیارهای تعریف شده از قبیل شباهت دوستان مشترک، تعداد کل دوستان، شباهت جاکارد، شباهت کسینوس، شباهت نرم L_1 و جمع و ضریب وزن ها ماتریس شباهت محاسبه می‌شود. همانطور که در قسمت پیشینه پژوهش مطرح شد برخی پژوهشگران نیز از معیارهای شباهت کاربران در روش پیشنهادی خود استفاده کردند ولی هدف روش پیشنهادی علاوه بر استفاده از شباهت‌های تعریف شده پیشین استفاده از شباهت هایی است که بتواند قدرت ارتباطات کاربران را نیز در نظر بگیرد. برای مثال با توجه به شکل (۸) بدلیل بیشتر بودن تعداد ارتباطات دوستان در زیرگراف شبکه دوستی میزان شباهت گره v_1 به گره u از میزان شباهت گره v_2 به گره u بیشتر است در این مقاله از معیار شباهتی استفاده می‌شود که این میزان شباهت را در نظر بگیرد.



شکل (۸): گراف ارتباط بین گره u و گره‌های v_1 و v_2

در این بخش برای هر یک از معیارهای شباهت تعریف شده یک ماتریس مربعی با درایه‌های قطری صفر خواهیم داشت. که هر درایه میزان شباهت دو گره مشخص‌کننده سطر و ستون این درایه را بیان می‌کند.

مرحله سوم: اعمال الگوریتم تحلیل مولفه‌های اصلی

تحلیل مولفه‌های اصلی در حقیقت یک تبدیل خطی متعامد است که داده‌ها را به دستگاه مختصات جدیدی نگاشت می‌کند به‌طوری که بزرگترین واریانس داده بر روی اولین محور مختصات، دومین بزرگترین واریانس بر روی دومین محور مختصات قرار می‌گیرد و همینطور برای بقیه، تحلیل مولفه‌های اصلی انجام می‌شود. بدین ترتیب مولفه‌هایی از مجموعه داده را که بیشترین تاثیر در واریانس دارند را حفظ می‌کند. در روش پیشنهادی برای اینکه بتوانیم متغیر مستقل داشته باشیم و همچنین برای آنکه حجم داده‌ها کاهش پیدا کند، باید روش تحلیل مولفه‌های اصلی را روی هر کدام از ماتریس‌های شباهت اعمال کرده و سپس ویژگی‌های جدید استخراج کرد. وقتی که این الگوریتم روی یک ماتریس $n \times n$ اعمال شود خروجی آن یک ماتریس $n \times n$ جدید است.

مرحله چهارم: استفاده از البو متد و استخراج ماتریس ویژگی‌های نهایی

در ویژگی‌های استخراج شده جدید داده هایی انتخاب می‌شوند که حاوی بار اطلاعاتی بیشتری بوده که منجر به رفع مشکل بیش برازش می‌شوند، از طرفی کاهش بار سیستم سرعت

را افزایش می‌دهد به‌همین دلیل با پیدا کردن نقطه البو[1] و استفاده از روش البو[2] از هر کدام از ماتریس‌ها تعداد محدودی از ستون‌ها که دارای بیشترین واریانس هستند را انتخاب کرده و یک ماتریس ویژگی جدید تشکیل می شود.

مرحله پنجم: تشخیص کاربران جعلی

در روش پیشنهادی برای تشخیص کاربران جعلی از دسته بندهای تخمین چگالی هسته و شبکه عصبی خودسازمان‌ده استفاده شده است. دسته‌بندهای استفاده شده از نوع تک[3] کلاسه این دو الگوریتم می‌باشد دلیل انتخاب الگوریتم تک کلاسه این است که این نوع دسته بندها برای تشخیص ناهنجاری استفاده می‌شوند و به‌دلیل این‌که در اینجا کاربران جعلی داده‌های ناهنجار محسوب می‌شوند با دقت بهتری قابل تشخیص هستند. جهت استفاده از دسته‌بند باید ابتدا آن را به کمک داده آموزشی، آموزش داد. برای آموزش دسته‌بند تخمین چگالی هسته، باید ماتریس ویژگی نهائی به‌دست آمده از ماتریس‌های شباهت میان کاربران را به دو دسته کاربران نرمال و جعلی تقسیم کرد، به بیان دیگر به داده‌ها بر اساس نوع آن‌ها برچسب مناسب تعلق می‌گیرد. در مرحله بعد از مجموعه داده آماده شده برای آموزش و آزمایش کارایی روش پیشنهادی استفاده می‌شود. در مرحله نهایی با مشخص شدن کاربران جعلی یک هشدار برای مجموعه دوستان آن‌ها مبتنی بر جعلی بودن دوست شما ارسال می‌شود.

۵- نتایج شبیه‌سازی و ارزیابی

در این بخش برای ارزیابی کارایی روش پیشنهادی، روش مورد نظر شبیه‌سازی و نتایج بررسی می‌شوند. برای شبیه‌سازی به معرفی مجموعه داده ها، نحوه شبیه‌سازی، معیارهای ارزیابی و بررسی نتایج پرداخته می‌شوند.

۵-۱- مجموعه داده‌ها

در این مقاله از مجموعه داده‌های برچسب‌دار توئیتر استفاده شده است که دارای بیش از ۵ میلیون کاربر و ۱۶ میلیون ارتباط میان کاربران است [۵۹].

۵-۲- معیارهای ارزیابی نتایج

برای ارزیابی عملکرد یک روش دسته‌بندی معمولا از یک سازوکار اعتبارسنجی ده مرحله‌ای استفاده می شود [۶۰ و ۶۱]. در این روش، ده درصد نمونه‌های مجموعه داده را برای آزمون و نود درصد مابقی را به عنوان داده‌های آموزش به الگوریتم یادگیری اعمال می‌شود و دقت ۱۰ درصد آزمون اندازه گرفته می‌شود. سپس ۱۰ درصد دیگر از نمونه ها را انتخاب کرده و ۹۰ درصد مابقی را به‌عنوان داده‌های آموزش در نظر گرفته می‌شود. این عملیات ده مرحله تکرار می‌شود تا تمام نمونه‌ها هم به‌عنوان نمونه آموزش و هم به‌عنوان نمونه آزمون در نظر گرفته شوند. در نهایت از دقت‌های به‌دست آمده از هر مرحله میانگین گرفته و به‌عنوان دقت الگوریتم معرفی می‌شود.

به‌طورکلی در سامانه‌های یادگیری ماشین معیارهای متعددی برای ارزیابی و بررسی عملکرد الگوریتم‌ها و دسته‌بندها وجود دارد. در این بخش به معرفی تعدادی از این معیارها پرداخته می‌شود. یکی از روش‌هایی که برای ارزیابی عملکرد الگوریتم‌های یادگیری ماشین و دسته‌بندها مورد استفاده قرار می‌گیرد، استفاده از ماتریس درهم ریختگی[4] است. این ماتریس، یک ماتریس مربعی است که ابعاد آن برابر تعداد دسته‌های مسئله دسته‌بندی است که در جدول (۱) نمایش داده شده است. در ساده‌ترین حالت، زمانی که دو دسته برای داده‌ها وجود داشته باشد، یک ماتریس ۲ × ۲ خواهیم داشت. برای سادگی فرض کنید که هر نمونه به یکی از دو دسته‌ی مثبت و منفی تعلق داشته باشد، در این حالت، ماتریس درهم ریختگی به‌صورت زیر تعریف می‌شود:

جدول (۱): ماتریس درهم ریختگی برای مسئله ی دو کلاسه

برچسب‌های پیش‌بینی شده		
برچسب واقعی	مثبت	منفی
مثبت	True Positive (TP)	False Negative(FN)
منفی	False Positive (FP)	True Negative(TN)

توضیح هریک از درایه‌های این ماتریس به شرح زیر است:

- TP :تعداد نمونه‌های مثبتی که به‌درستی دسته‌بندی شده‌اند.
- FN :تعداد نمونه‌های مثبتی که اشتباه دسته‌بندی شده‌اند.
- FP :تعداد نمونه‌های منفی که اشتباه دسته‌بندی شده‌اند.
- TN : تعداد نمونه‌های منفی که به‌درستی دسته‌بندی شده‌اند.

در حالت کلی، زمانی که تعداد دسته‌های مسئله دسته‌بندی n باشد، ماتریس درهم ریختگی، یک ماتریس n × n به‌صورت $C=[c_{ij}]$ خواهد شد که درایه c_{ij} نشان‌دهنده تعداد نمونه‌های دسته i ام است که جزء دسته j ام دسته‌بندی (پیش‌بینی) شده

[1] Elbow point
[2] Elbow method
[3] One Class Classification
[4] Confusion Matrix

است. البته هر مسئله دسته‌بندی n تایی را می‌توان با استفاده از روش یکی در برابر همه به n مسئله دسته‌بندی دودویی تبدیل نمود. در این روش، در هر یک از دسته‌بندهای دودویی، یکی از دسته‌ها مثبت و سایر دسته‌ها منفی در نظر گرفته می‌شوند. زمانی که مسئله دسته‌بندی شامل دو دسته باشد، معیارهای دیگری از روی ماتریس درهم ریختگی قابل محاسبه است که در ادامه معرفی‌شده‌اند.

دقت[1]: به میزان تطابق پیش‌بینی‌های یک مدل اشاره دارد که با واقعیت مدل‌سازی شده هم‌خوانی دارد که با استفاده از رابطه (۱۵) قابل محاسبه است.

$$\frac{TP + TN}{TP + FN + FP + FN} \quad (۱۵)$$

حساسیت[2]: بیانگر درصد نمونه‌های مثبتی که به درستی دسته‌بندی شده‌اند که با استفاده از رابطه (۱۶) بیان می‌شود.

$$\frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} * 100 \quad (۱۶)$$

نرخ تشخیص اشتباه: درصد کاربران جعلی که واقعی تشخیص داده می شوند را نشان می‌دهد و به‌صورت رابطه (۱۷) تعریف می‌شود.

$$\frac{\mathrm{FP}}{\text{number of negative instances}} \quad (۱۷)$$

۵-۳- آزمایش‌ها

برای شبیه سازی روش پیشنهادی از نرم افزار متلب نسخه ۲۰۲۰ استفاده شده است. همچنین پلاگین ND.Tool که شامل الگوریتم‌های چگالی هسته، شبکه عصبی خودسازمان‌ده و چند الگوریتم دیگر است که بیشتر برای تشخیص ناهنجاری و پرتی‌ها در یک مجموعه داه‌ها استفاده می‌شوند و به صورت تک کلاسه قابل آموزش هستند به نرم افزار اضافه می‌شود.

۱- ابتدا ازروی گراف شبکه اجتماعی توییتر ۲۰۰۰ گره را جدا کرده و ماتریس مجاورت مربوط به آن استخراج می‌شود، در ماتریس مجاورت به ازای هر دو گره که با هم مرتبط هستند درایه مورد نظر عدد ۱ و در غیر این صورت ۰ است.

۲- از روی ماتریس مجاورت گراف معیارهای مرکزیت محاسبه شده و هر کدام در یک ماتریس نگهداری می‌شود، همچنین هر یک از ماتریس‌های شباهت از روی ماتریس مجاورت محاسبه می‌شود. اکنون برای هر یک از معیارها، یک ماتریس ۲۰۰۰×۲۰۰۰ وجود دارد. در ادامه روی هر کدام از ماتریس‌ها الگوریتم تحلیل مولفه‌های اصلی اعمال می‌شود. در این مرحله به تعداد معیارهای محاسبه شده ماتریس جدید وجود خواهد داشت.

۳- برای کاهش ابعاد و بالا بردن کارایی روش پیشنهادی از روش البو [۵۵ و ۵۶] استفاده شده است. روش البو بدین صورت عمل می‌کند که بعد از اعمال الگوریتم تحلیل مولفه‌های اصلی تنها ۰/۰۵ درصد ویژگی‌ها (ستون‌ها) که دارای بیشترین واریانس هستند را برای آموزش الگوریتم و استخراج نتایج استفاده می‌کند. در نتیجه از هر ماتریس تعداد ۱۰ ستون اول انتخاب شده و در یک ماتریس جدید قرار می‌گیرند سپس برچسب‌های کاربران را در ماتریس وارد کرده و مجموعه داده‌های جدید آماده می‌شود.

۴- با استفاده از الگوریتم تخمین چگالی هسته، سیستم آموزش داده شده و آزمایش می‌شود که در ادامه نتایج ارزیابی برای تشخیص کاربران جعلی نشان داده شده است.

آزمایش اول: در این آزمایش ابتدا ۲۰۰۰ گره اول از این شبکه جدا شده و سپس مراحل روش پیشنهادی روی آن‌ها اجرا می‌شود که ماتریس درهم ریختگی در جدول (۲) گزارش شده است که معیارهای دقت، حساسیت و نرخ تشخیص اشتباه با توجه به آن محاسبه و در جدول (۳) آمده است.

جدول (۲): ماتریس درهم ریختگی روش پیشنهادی

برچسب‌های پیش‌بینی شده		
جعلی	نرمال	برچسب واقعی
۲	۱۶۹۸	عادی
۲۹۱	۹	جعلی

جدول (۳): مقایسه روش پیشنهادی با کارهای پیشین

نام الگوریتم	دقت	حساسیت	نرخ تشخیص اشتباه
الگوریتم KDE	٪۹۹/۶	۱۰۰٪	٪۳
الگوریتم SOM	٪۹۹/۴	٪۱۰۰	٪۴/۷

نرخ تشخیص اشتباه معیار بسیار مهمی محسوب می‌شود زیرا بیانگر این است که یک کاربر جعلی به‌عنوان کاربر واقعی تشخیص داده شده است. هر چه این معیار به صفر نزدیک باشد کارایی مورد نظر سیستم مطلوب‌تر است. با توجه به جدول (۳) الگوریتم تخمین چگالی هسته با دقت ٪۹۹/۶ کاربران جعلی را تشخیص می‌دهد که نسبت به الگوریتم‌های دیگر استفاده شده عملکرد بهتری دارد.

[1] Accuracy
[2] Sensitivity

در جدول (۴) نتایج روش پیشنهادی با چند نمونه از روش‌های پیشین مقایسه شده است که نتایج نشان می‌دهد، مولفه‌ها از جمله نرخ تشخیص اشتباه در روش پیشنهادی بهبود یافته است.

جدول (۴): مقایسه روش پیشنهادی با کارهای پیشین

نام الگوریتم	دقت	حساسیت	نرخ تشخیص اشتباه
الگوریتم KDE	٪۹۹/۶	٪۱۰۰	٪۳
الگوریتم SOM	٪۹۹/۴	٪۱۰۰	۴٪
روش پیشنهادی کاوو[1]	٪۹۵/۵	٪۹۸	٪۶

در جدول (۵) دقت اجرای روش پیشنهادی با استفاده از معیارهای مرکزیت در کنار معیارهای شباهت و بدون استفاده از معیارهای مرکزیت را نشان می‌دهد. آزمایش انجام شده نشان می‌دهد که استفاده از معیارهای مرکزیت در تشخیص کاربران جعلی تاثیری در نتایج روش پیشنهادی ندارد. در این بخش از شبیه‌سازی مجموعه داده‌های ۱ تنها شامل معیارهای شباهت بوده و مجموعه داده‌های ۲ شامل معیارهای شباهت و معیارهای مرکزیت است.

جدول (۵): مقایسه دقت روش پیشنهادی

نام الگوریتم	مجموعه داده‌های ۱	مجموعه داده‌های ۲	دقت
الگوریتم KDE	-	✓	٪۹۹/۶۴
الگوریتم KDE	✓	-	٪۹۹/۶۴
الگوریتمSOM	-	✓	٪۹۹/۴۶
الگوریتمSOM	✓	-	٪۹۹/۴

۵-۴- بررسی تنومندی[2] داده‌ها

برای این‌که کارایی روش پیشنهادی در شرایط متفاوت بررسی شود. روش پیشنهادی با داده‌های متفاوتی آموزش و آزمایش شد که با توجه به جدول (۶) نتایج تقریبا یکسانی به‌دست می‌آید.

جدول(۶): نتایج با مجموعه داده‌های مختلف

نام الگوریتم	مجموعه داده ها	دقت	حساسیت	نرخ تشخیص اشتباه
الگوریتم KDE	۱	٪۹۹/۶	۱۰۰٪	٪۳
الگوریتم KDE	۲	٪۹۹/۶	٪۱۰۰	۳٪
الگوریتم SOM	۱	٪۹۹/۴۶	٪۱۰۰	٪۳/۲
الگوریتم SOM	۲	٪۹۹/۴۴	٪۹۹/۶	٪۳/۲

۵-۵- قابلیت گسترش

همان‌طور که در جدول (۷) مشاهده می‌شود با افزایش تعداد گره‌ها هنگام آزمایش، نتایج بهتر شده است. وقتی که تعداد گره های مورد آزمایش از ۲۰۰۰ به ۲۰۰۰۰ افزایش یافته نتایج پیش بینی بهبود یافته است.

جدول(۷): مقایسه نتایج روش پیشنهادی با مجموعه داده‌ها با تعداد کاربران مختلف

نام الگوریتم	مجموعه داده‌ها	دقت	حساسیت	نرخ تشخیص
الگوریتم KDE	۱	٪۹۹/۶	۱۰۰٪	٪۳
الگوریتم KDE	۲	٪۹۹/۷	٪۱۰۰	۲,۸٪
الگوریتم SOM	۱	٪۹۹/۴۶	٪۱۰۰	۴٪
الگوریتم SOM	۲	٪۹۹/۴	٪۱۰۰	٪۳/۸

۶- نتیجه‌گیری

در این مقاله یک روش جدید برای شناسایی کاربران جعلی در شبکه‌های اجتماعی ارایه شده است. در این روش ابتدا از روی گراف شبکه ماتریس مجاورت محاسبه شده و معیارهای شباهت از ماتریس مجاورت به‌دست می‌آیند. در ادامه با استفاده از روش تحلیل مولفه‌های اصلی ویژگی‌های جدید استخراج شده و داده‌ها انتخاب و ماتریس نهایی به‌دست می‌آید. با استفاده از الگوریتم‌های تخمین چگالی هسته و شبکه عصبی خودسازمان‌ده روش پیشنهادی آموزش داده شده و کاربران جعلی پیش‌بینی می‌شوند. روش پیشنهادی به‌دلیل محاسبات زیاد زمان اجرایی بالایی دارد و در کارهای آینده به‌دنبال ارائه روش‌هایی هستیم که بتوان به‌صورت بلادرنگ از آن‌ها استفاده کرد.

[1] Cao's method
[2] Robustness

۷- مراجع

[1] D. Kagan, Y. Elovichi, and M. Fire, "Generic anomalous vertices detection utilizing a link prediction algorithm, " Social Network Analysis and Mining, vol. 8, no. 1, p. 27, 2018.

[2] H. Gao, J. Hu, T. Huang, J. Wang, and Y. J. I. I. C. Chen, "Security issues in online social networks," vol. 15, no. 4, pp. 56-63, 2011.

[3] L. A. Cutillo, R. Molva, and T. J. I. C. M. Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," vol. 47, no. 12, pp. 94-101, 2009.

[4] K. Sakariyah, A. Nor, B. Anuara, A. Kamsina, K. D. Varathana, and S. A. Razakb, "Malicious accounts: Dark of the social networks," Journal of Network and Computer Applications, vol. 79, pp. 41-67, 1 February 2017.

[5] K. Krombholz, D. Merkl, and E. Weippl, "Fake identities in social media: A case study on the sustainability of the facebook business model," Journal of Service Science Research, vol. 4, no. 2, pp. 175-212, 2012.

[6] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in ACM SIGCOMM Computer Communication Review, ACM, vol. 36, no. 4, pp. 267-278, 2006.

[7] E. Van Der Walt and J. J. I. A. Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans," vol. 6, pp. 6540-6549, 2018.

[8] V. Subrahmanian et al., "The DARPA Twitter bot challenge," 2016.

[9] M. Fire, R. Goldschmidt, Y. J. I. C. S. Elovici, and Tutorials, "Online social networks: threats and solutions," vol. 16, no. 4, pp. 2019-2036, 2014.

[10] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," 2009.

[11] S. Jagadish and J. Parikh, "Discovery of friends using social network graph properties," ed: Google Patents, 2014.

[12] M. Cha, A. Mislove, and K. P. Gummadi, "A measurement-driven analysis of information propagation in the flickr social network," in Proceedings of the 18th international conference on World wide web, ACM, pp. 721-730, 2009.

[13] S. Wasserman and K. Faust, "Social network analysis: Methods and applications," Cambridge university press, 1994.

[14] J. Scott, "Social network analysis," Sage, 2017.

[15] E. Otte and R. J. J. o. i. S. Rousseau, "Social network analysis: a powerful strategy, also for the information sciences," vol. 28, no. 6, pp. 441-453, 2002.

[16] M. Y. Kharaji and F. S. J. a. p. a. Rizi, "An IAC Approach for Detecting Profile Cloning in Online Social Networks," 2014.

[17] R. Laxhammar, G. Falkman, and E. Sviestins, "Anomaly detection in sea traffic-a comparison of the gaussian mixture model and the kernel density estimator," in 2009 12th International Conference on Information Fusion, IEEE, pp. 756-763, 2009.

[18] J. A. J. S. Barnes, "Graph theory and social networks: A technical comment on connectedness and connectivity," vol. 3, no. 2, pp. 215-232, 1969.

[19] P. J. Carrington, J. Scott, and S. Wasserman, "Models and methods in social network analysis," Cambridge university press, 2005.

[20] S. Jouili, S. Tabbone, and E. Valveny, "Comparing graph similarity measures for graphical recognition," in International Workshop on Graphics Recognition, Springer, pp. 37-48, 2009.

[21] F. Golshahi, A. Toroghi Haghighat, "providing an improved method in social networks to predict links in multilayer networks," Electronic and Cyber Defense, vol. 8 (2), pp. 15-24, 2020. (In Persian)

[22] C. G. Akcora, B. Carminati, E. J. S. N. A. Ferrari, and Mining, "User similarities on social networks," vol. 3, no. 3, pp. 475-495, 2013.

[23] J. Bank and B. J. W. S. T. Cole, "Calculating the jaccard similarity coefficient with map reduce for entity pairs in wikipedia," pp. 1-18, 2008.

[24] L. Dong, Y. Li, H. Yin, H. Le, and M. J. M. P. i. E. Rui, "The algorithm of link prediction on social network," vol. 2013, 2013.

[25] J. Santisteban and J. Tejada-Cárcamo, "Unilateral Jaccard Similarity Coefficient," in GSB@ SIGIR, pp. 23-27, 2015.

[26] H. Seifoddini, M. J. C. Djassemi, and I. Engineering, "The production data-based similarity coefficient versus Jaccard's similarity coefficient," vol. 21, no. 1-4, pp. 263-266, 1991.

[27] S. Niwattanakul, J. Singthongchai, E. Naenudorn, and S. Wanapu, "Using of Jaccard coefficient for keywords similarity," in Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, no. 6, 2013.

[28] C. A. Bliss, M. R. Frank, C. M. Danforth, and P. S. J. J. o. C. S. Dodds, "An evolutionary algorithm approach to link prediction in dynamic social networks," vol. 5, no. 5, pp. 750-764, 2014.

[29] T. Zhou, L. Lü, and Y.-C. J. T. E. P. J. B. Zhang, "Predicting missing links via local information, " vol. 71, no. 4, pp. 623-630, 2009.

[30] Q. Li, Y. Zheng, X. Xie, Y. Chen, W. Liu, and W.-Y. Ma, "Mining user similarity based on location history, " in Proceedings of the 16th ACM SIGSPATIAL international conference on Advances in geographic information systems, ACM, p. 34, 2008.

[31] R. J. Bayardo, Y. Ma, and R. Srikant, "Scaling up all pairs similarity search, " in Proceedings of the 16th international conference on World Wide Web, ACM, pp. 131-140, 2007.

[32] A. Gionis, P. Indyk, and R. Motwani, "Similarity search in high dimensions via hashing, " in Vldb, vol. 99, no. 6, pp. 518-529, 1999.

[33] W. Cukierski, B. Hamner, and B. Yang, "Graph-based features for supervised link prediction, " in Neural Networks (IJCNN), The 2011 International Joint Conference on, IEEE, pp. 1237-1244, 2011.

[34] I. T. Jolliffe, "Principal component analysis and factor analysis, " Principal component analysis, pp. 150-166, 2002.

[35] M. B. Pouyan and D. Kostka, "Random forest based similarity learning for single cell RNA sequencing data, " Bioinformatics, vol. 34, no. 13, pp. i79-i88, 2018.

[36] E. Parzen, “On estimation of a probability density function and mode, ” The annals of mathematical statistics, vol. 33, no. 3, pp. 1065-1076, 1962.

[37] J. Kim and C. D. Scott, “Robust kernel density estimation, ” The Journal of Machine Learning Research, vol. 13, no. 1, pp. 2529-2565, 2012.

[38] J. Cao, Q. Fu, Q. Li, and D. J. I. S. Guo, “Discovering hidden suspicious accounts in online social networks, ” vol. 394, pp. 123-140, 2017.

[39] S. Gurajala, J. S. White, B. Hudson, B. R. Voter, J. N. J. B. D. Matthews, and Society, “Profile characteristics of fake Twitter accounts, ” vol. 3, no. 2, p. 2053951716674236, 2016.

[40] G. Wang, W. Jiang, J. Wu, Z. J. I. T. o. P. Xiong, and D. Systems, “Fine-grained feature-based social influence evaluation in online social networks, ” vol. 25, no. 9, pp. 2286-2296, 2014.

[41] Z. Shan, H. Cao, J. Lv, C. Yan, and A. Liu, “Enhancing and identifying cloning attacks in online social networks, ” in Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, ACM, p. 59, 2013.

[42] K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, S. A. J. J. o. N. Razak, and C. Applications, “Malicious accounts: dark of the social networks,” vol. 79, pp. 41-67, 2017.

[43] M. Al Hasan, V. Chaoji, S. Salem, and M. Zaki, “Link prediction using supervised learning,” in SDM06: workshop on link analysis, counter-terrorism and security, 2006.

[44] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. J. S. N. Wang, “Anomaly detection in online social networks,” vol. 39, pp. 62-70, 2014.

[45] M. Conti, R. Poovendran, and M. Secchiero, “Fakebook: Detecting fake profiles in on-line social networks,” in Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012), IEEE Computer Society, pp. 1071-1078, 2012.

[46] Y. Zhang, J. J. S. N. A. Lu, and Mining, “Discover millions of fake followers in Weibo,” vol. 6, no. 1, p. 16, 2016.

[47] B. Viswanath, A. Post, K. P. Gummadi, and A. J. A. S. C. C. R. Mislove, “An analysis of social network-based sybil defenses,” vol. 41, no. 4, pp. 363-374, 2011.

[48] J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai, “Votetrust: Leveraging friend invitation graph to defend against social network sybils,” in INFOCOM, 2013 Proceedings IEEE, pp. 2400-2408, 2013.

[49] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services,” in Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, USENIX Association, pp. 15-15, 2012.

[50] Y. Boshmaf et al., “Integro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs,” in NDSS, vol. 15, pp. 8-11, 2015.

[51] L. Jin, H. Takabi, and J. B. Joshi, “Towards active detection of identity clone attacks on online social networks,” in Proceedings of the first ACM conference on Data and application security and privacy, ACM, pp. 27-38, 2011.

[52] K. L. Arega, “Social Media Fake Account Detection for Afan Oromo Language using Machine Learning,” 2020.

[53] F. C. Akyon and M. E. Kalfaoglu, “Instagram Fake and Automated Account Detection,” in 2019 Innovations in Intelligent Systems and Applications Conference (ASYU), IEEE, pp. 1-7, 2019.

[54] M. Egele, G. Stringhini, C. Kruegel, G. J. I. T. o. D. Vigna, and S. Computing, “Towards detecting compromised accounts on social networks,” no. 1, pp. 1-1, 2017.

[55] S. Lee and J. J. C. C. Kim, “Early filtering of ephemeral malicious accounts on Twitter,” vol. 54, pp. 48-57, 2014.

[56] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. J. A. T. o. K. D. f. D. Dai, “Uncovering social network sybils in the wild,” vol. 8, no. 1, p. 2, 2014.

[57] M. Singh, D. Bansal, and S. Sofat, “Detecting malicious users in Twitter using classifiers,” in Proceedings of the 7th International Conference on Security of Information and Networks, ACM, p. 247, 2014.

[58] K. Gani, H. Hacid, and R. Skraba, “Towards multiple identity detection in social networks,” in Proceedings of the 21st International Conference on World Wide Web, ACM, pp. 503-504, 2012.

[59] Available: https://github.com/Kagandi/anomalous-vertices-detection/tree/master/data

[60] Y. Bengio and Y. J. J. o. m. l. r. Grandvalet, “No unbiased estimator of the variance of k-fold cross-validation,” vol. 5, no. Sep, pp. 1089-1105, 2004.

[61] R. Kohavi, “A study of cross-validation and bootstrap for accuracy estimation and model selection,” in Ijcai, 1995, Montreal, Canada, vol. 14, no. 2, pp. 1137-1145, 1995.