

فناوری‌ها و الگوریتم‌های پیاده‌سازی شبکه‌های اجتماعی

صدیقه غلامرضایی^۱، سیده آرزو حاجی میرمالک^۲، علیرضا خلیلیان^۳

^۱ کارشناس نرم‌افزار، دانشگاه فنی حرفه‌ای، دانشکده فنی دکتر شریعتی، تهران، sgholamrezaei@yahoo.com

^۲ کارشناس نرم‌افزار، دانشگاه فنی حرفه‌ای، دانشکده فنی دکتر شریعتی، تهران، a.mirmalek@yahoo.com

^۳ دانشجوی دکتری نرم‌افزار، دانشگاه اصفهان، اصفهان، khalilian@eng.ui.ac.ir

چکیده: رشد روزافزون شبکه‌های اجتماعی برخط به شدت بر زندگی روزمره‌ی افراد تأثیر گذاشته و نوع ارتباطات افراد را دست‌خوش تغییرات فراوان کرده است. در این مقاله به تحلیل و بررسی شبکه‌های اجتماعی برخط پرداخته شده است. برای این منظور روش‌های تحلیل شبکه‌ها و کاربرد آن‌ها مورد بررسی قرار گرفت و سپس به مجسم‌سازی شبکه‌های اجتماعی در مقیاس کوچک و بزرگ پرداخته شده است. پس از آن نحوه‌ی کاوش داده از این شبکه‌ها و زیربنا و معماری آنها مورد مطالعه قرار گرفت است. در نهایت امنیت در شبکه‌های اجتماعی برخط به‌عنوان اصلی مهم و حیاتی در روابط کاربران هم در محیط مجازی و هم در دنیای واقعی بررسی شد. در نتیجه در این بررسی سعی شده است تا دیدی کلی در مورد این نوع خاص از شبکه‌های اجتماعی که در زندگی روزانه‌ی مردم نقش به‌سزایی دارند، ارائه شود.

کلید واژه: تحلیل شبکه‌های اجتماعی، مرکزیت، سیستم نقطه به نقطه، مجسم‌سازی، استخراج انجمن، کاوش داده، حریم خصوصی

۱- مقدمه

شبکه‌ی اجتماعی مفهومی با قدمتی طولانی است. شبکه‌ی اجتماعی، یک ساختار اجتماعی تشکیل شده از گره‌هایی (عموماً فردی یا سازمانی) است که توسط یک یا چند نوع خاص از وابستگی‌ها به هم متصل هستند. یک شبکه‌ی اجتماعی برخط، تارنما یا مجموعه تارنماهایی است که به کاربران امکان اشتراک‌گذاری علاقه‌مندی‌ها، افکار و فعالیت‌ها را می‌دهد [1]. با انفجار اینترنت شبکه‌های اجتماعی برخط به ابزاری برای اتصال مردم به روشی که در گذشته غیر ممکن بوده، تبدیل شده‌اند.

یک شبکه‌ی اجتماعی برخط، معمولاً خدمات‌های دستیابی برخط را پیشنهاد می‌کند که شامل نمایش‌های دیجیتال یک زیر مجموعه از روابط کاربران آن، افراد ثبت نام کرده و نهادهای سرگرم در دنیای فیزیکی می‌شود [2]. با گسترش تمام شرکت‌کنندگان در روابط، آنها شبکه‌ی اجتماعی را به‌عنوان یک گراف مدل می‌کنند. هر کاربر شبکه‌ی اجتماعی برخط می‌تواند خود را با یک پروفایل معرفی کند. کاربران از نرم‌افزارهای کاربردی در دسترس شبکه‌ی اجتماعی برخط برای به اشتراک گذاشتن راحت اطلاعات با دیگران و اهداف شخصی یا

حرفه‌ای استفاده می‌کنند. شبکه‌ی اجتماعی برخط با پس زمینه‌ی حرفه‌ای و تجارت‌گرا، معمولاً به‌عنوان یک وسیله‌ی تنظیم‌کننده برای مخاطبان تجارت یا مدیریت مشاغل استفاده می‌شود؛ چنین شبکه‌هایی معمولاً خدمات‌های شبکه‌ی اجتماعی را با تصویر جدی‌تری فراهم می‌کنند [3]. اما شبکه‌ی اجتماعی برخط با پس زمینه‌ی شخصی و فراغت‌گرا، معمولاً برای به اشتراک‌گذاری و تبادل اطلاعات شخصی‌تر مانند داده‌ی مخاطب، عکس‌ها و ویدئو استفاده می‌شود. هسته‌ی نرم‌افزار کاربردی شبکه‌ی اجتماعی برخط، اجرا و نگهداری لیست مخاطبان را برعهده دارد. خدمات‌های شبکه‌ی اجتماعی با آگاه‌سازی خودکار کاربران از تغییرات پروفایلشان، به آنها کمک می‌کنند تا اخبار مخاطبان خود را دریافت کنند و در اغلب اوقات محبوبیت کاربران، با اندازه‌ی لیست دوستان آنها اندازه‌گیری می‌شود.

شبکه‌های اجتماعی برخط، به‌خصوص آنهایی که کاربردهای معمولی و غیرتجاری دارند، مکان‌هایی در دنیای مجازی هستند که مردم در آنها خود را به‌طور خلاصه معرفی می‌کنند و امکان برقراری ارتباط بین خود و هم‌فکران خود را در زمینه‌های مختلف مورد علاقه فراهم می‌سازند [1].

علاقه و پیوندها برای یک شبکه‌ی اجتماعی قالب‌دهی می‌شود و تعاملات نقش‌های وابسته‌ی خارجی که در حالت عادی در شبکه‌های معین در دسترس نیستند را کشف می‌کند [4].

۱-۲- کاربردهای تحلیل شبکه‌ی اجتماعی

- **مسائل سازمانی:** تحلیل شبکه‌ی اجتماعی می‌تواند برای شناسایی افراد کلیدی یا مرکزی در یک سازمان به کار برده شود. بر مبنای دانش به دست آمده از تحلیل شبکه‌ی اجتماعی راهبرد مدیریت اصلاحی می‌تواند برای بهبود بازده یک سازمان به کار رود.

- **سیستم‌های پیشنهاد دهنده و تجارت الکترونیک:** یکی از نیازهای مهم سیستم‌های پیشنهاددهنده کشف الگوهای تعاملی کاربران به دست جست‌وجوی کاربران شبکه‌ی اجتماعی و علاقه‌مندی‌ها و نفرت‌های مشترک آنها است. تحلیل شبکه‌ی اجتماعی در این سیستم‌ها نیز سودمند است تا به روابط بین افراد مختلف در سیستم رسیدگی کند و ترجیحات کاربران را پیش‌بینی کند. بنابراین تحلیل شبکه‌ی اجتماعی می‌تواند برای تعیین روابط بین کاربران به کار برده شود، و برآیند این که در ساخت پیشنهادها کمک کند. کارایی سیستم‌های پیشنهادی با شگردهای تحلیل شبکه‌ی اجتماعی ارزیابی می‌شود. برای تسهیل این کار، درصد پیش‌بینی داده شده به دست سیستم می‌تواند با استنتاج تحلیل شبکه‌ی اجتماعی از مشتری‌های شبکه پیش‌بینی شود.

- **شبکه‌های سری:** به طور عمومی اطلاعات مربوط به نقش‌ها، روابط آنها و درگیری‌ها در یک شبکه‌ی تروریستی به راحتی در دسترس قرار نمی‌گیرد. تحلیل شبکه‌ی اجتماعی با موفقیت قادر به فهم عملیات سری و سازماندهی‌های آنها است. تحلیل شبکه‌ی اجتماعی به منظور فهم اجتماع‌ها و ساختار سلول‌های تروریستی به کار برده می‌شود و روی شناسایی نقاط ضعف شبکه تمرکز می‌کند، عوامل مرکزی را شناسایی می‌کند، نقش افراد را می‌فهمد و روابط اصلی را نشان می‌دهد.

به عنوان مثال در شبکه‌های تروریستی ابتدا شاخص قطعه قطعه بودن در صورت عدم حضور یک گره در گراف محاسبه می‌شود. هر گره‌ای که با حذف باعث قطعه قطعه شدن بیشتر گراف شبکه شود، دارای اهمیت بیشتری است. برای نمونه در یک ماتریس A که در آن $A_{ij} = I$ است i می‌تواند به j برسد و در غیر این صورت $A_{ij} = 0$ است، اندازه‌ی قطعه قطعه بودن که با F نمایش داده شده است از طریق فرمول زیر محاسبه می‌شود [5]:

$$F = 1 - \frac{2 \sum_i \sum_{j < i} A_{ij}}{n(n-1)} \quad (1)$$

- **نرم‌افزارهای کاربردی تارنما:** با تحلیل الگوهای مصرفی تارنما، بهبودهای بهتری می‌توانند در الگوریتم‌های تارنما برای گردآوری،

با توجه به ابعاد مختلف شبکه‌های اجتماعی و تحقیقات گسترده‌ی انجام شده در این زمینه، بررسی جامع همه‌ی این ابعاد به زمانی طولانی و مطالعات بسیار زیاد نیاز دارد. از این رو در این مقاله برآن شدیم تا بخشی از این تحقیقات را مورد مطالعه قرار داده و بتوانیم دیدی کلی و جامع در مورد این نوع خاص از شبکه‌های اجتماعی که در زندگی روزانه‌ی مردم نقش به‌سزایی دارند، ارائه کنیم. ساختار مقاله در ادامه به شرح زیر است: در بخش دوم، تحلیل شبکه‌های اجتماعی و کاربرد این تحلیل‌ها در زندگی مردم بررسی می‌شود. بخش سوم در زمینه‌ی مجسم‌سازی شبکه‌های اجتماعی است. بخش چهارم، به کاوش هویت‌های برخط می‌پردازد. در بخش پنجم، زیربنا و در بخش ششم امنیت در شبکه‌های اجتماعی مورد بررسی قرار گرفته است. بخش هفتم هم به نتیجه‌گیری اختصاص دارد.

۲- تحلیل شبکه‌های اجتماعی

تحلیل شبکه‌های اجتماعی افزون بر این که یک علم اجتماعی است، بیشتر به روشی برای بررسی و تحلیل ساختارهای اجتماعی اطلاق می‌شود که می‌تواند در سطوح مختلفی از گروه‌های کوچک تا سازمان‌های بزرگ، احاطه شده باشد. برای تحلیل شبکه‌های اجتماعی، بسیاری از مطالعات شبکه‌های اجتماعی فعلی را با گراف نشان می‌دهند. زمانی که یک شبکه‌ی اجتماعی ساخته می‌شود، گره‌ها و یال‌ها می‌توانند به خوبی نشان‌دهنده‌ی افراد و روابط آنها در اجتماع باشند. این گراف‌ها به دست کارآزمودگان از جنبه‌های مختلف تحلیل و بررسی می‌شوند.

- گونه‌های مختلفی از شبکه‌ها وجود دارند و عموماً تحلیل‌گران شبکه، شبکه‌های زیر را تفکیک می‌کنند [3]:

- شبکه‌های تک حالت در روبه‌روی شبکه‌های دو حالت: در شبکه‌های تک حالت روابط، میان یک سری نقش و در شبکه‌های دو حالت میان دو سری متفاوت از نقش‌ها است.

- شبکه‌های تمام/سراسر در روبه‌روی شبکه‌های اگو: شبکه‌های تمام/سراسر، شبکه‌هایی هستند که شامل ارتباطات میان اعضای یک اجتماع تنها یا کران‌دار می‌شوند. اما شبکه‌های اگو حول یک واحد مشخص به نام اگو ساخته می‌شوند. شبکه‌ی اگو یک نقشه از دنیای اجتماعی اگو است [2].

مفاهیم پایه‌ای تحلیل شبکه‌های اجتماعی شامل یال، چگالی، مسیر، طول، فاصله، گروه و مرکزیت می‌شود. اندازه‌گیری مرکزیت برجسته‌ترین نقش‌ها را که به طور وسیعی در روابط با سایر اعضای شبکه همکاری دارند مشخص می‌کند. مهم‌ترین اندازه‌های مرکزیت عبارتند از: مرکزیت درجه، مرکزیت میانگی و مرکزیت نزدیکی [3].

شبکه‌های اجتماعی با سه روش تحلیل می‌شوند. (۱) تحلیل همه‌ی اشیا از جمعیت و اتصالات بین آنها؛ (۲) تحلیل اگو - میانی^۲ شبکه‌ها که با استخراج اشیا مورد علاقه و تعاملات بین آنها به وجود آمده است؛ (۳) تحلیل هایپرید شبکه‌ها که با استخراج اشیا مورد

مزایای ماتریس‌ها:

- ماتریس‌ها مجسم‌سازی قوی را تهیه می‌کنند، چون زمان تولید آنها خیلی کم است و معمولاً خوانایی بالایی دارند. آنها ارائه‌ای خوب برای آغاز کاوش‌ها نمایش می‌دهند.
- ماتریس‌ها از هم‌پوشانی گره‌ها زیان نمی‌بینند، و اگر لازم باشد پی‌درپی برچسب نقش‌ها را بخوانند این کار را به بهترین نحو انجام می‌دهند.
- ماتریس‌ها از تقاطع یال‌ها با هم زیان نمی‌بینند، به همین دلیل در شبکه‌های چگال کاربرد دارند.
- ماتریس‌ها همه‌ی زوج رئوس شدنی را نمایش می‌دهند، آنها می‌توانند کمبود اتصالات و اتصالات غیر مستقیم را برجسته کنند. آنها برای شبکه‌های چگال و مستقیم مناسب هستند.

مزایای نمودارهای گره - یال

- این نمودار برای شنوندگان آشنا است؛ دارای ابزار ارتباطی قدرتمندی است. در تقابل با ماتریس‌ها نیاز به آموزش چندانی برای کاربران جدید ندارد.
- برای شبکه‌های کوچک یا پراکنده، نمودارهای گره - یال کارایی بیشتری از ماتریس‌ها دارند.
- برای مراحل با جزئیات مشابه، فضای مصرفی ماتریس از فضای مصرفی نمودار گره - یال بیشتر است. بنابراین در ارائه‌های خلاصه نمودار گره - یال گزینش بهتری است.
- وقتی تحلیل به یافتن شماری مسیر وابسته است (مثلاً یافتن کوتاهترین مسیر بین دو گره‌ی مشخص)، نمودار گره - یال مناسب است.

- **نمودارهای ماتریس + گره - یال:** ادغام مزایای دو ارائه و پشتیبانی از کاوش چشمی شبکه‌های اجتماعی، باعث کشف ماتریس جستجوگر ماتریکس اکسپلورر^۶ شد.

۳-۱ - سنجش شبکه‌های بزرگ

سیستم‌های زیادی برای تحلیل شبکه‌هایی با اندازه‌های کوچک و میانه وجود دارد اما سنجش شبکه‌هایی با هزاران یا میلیون‌ها گره چالش برانگیز است. برای این کار تحلیل گر یک یا بیشتر راه‌کارهای زیر را به کار می‌برد:

- **کاهش مقدار اطلاعات:** برای الگ کردن شبکه‌ها دو روش موجود عبارتند از: ۱- الگ کردن عنصرهای خارجی که نگهدارنده‌ی یک نماینده‌ی نمونه هستند. ۲- الگ کردن داده‌ای که به طور مستقیم در تحلیل حضور ندارد. یک روش متفاوت برای کاهش مقدار اطلاعات نمایش داده شده بدون الگ کردن، چگال ساختن مجموعه گره‌ها و یال‌ها با

جستجو و کشف اطلاعات به دست آیند. تحلیل شبکه‌ی اجتماعی برای کشف جوامع تارنما و در مهندسی جستجو مثل گوگل برای کمک به کیفیت جستجوی کلیدواژه و همچنین رتبه‌بندی صفحات تارنما برای مشخص کردن محبوبیت به کار می‌رود.

یکی از مؤلفه‌های بحرانی در تارنماهای گسترده‌ی اجتماعی، رتبه‌بندی کاربران و صفحات تارنما است. به عنوان مثال توییت‌رنک برای رتبه‌بندی کاربران سه مرحله‌ی الف) گردآوری داده و انتقال آن به مدل تانسور، ب) پردازش داده و ج) تحلیل را دنبال می‌کند [6].

- **کمک‌های اجتماعی عمومی:** تحلیل شبکه‌ی اجتماعی ممکن است الگوهایی از تماس بشر را آشکار کند که می‌تواند انتشار بیماری مثل ایدز در بین افراد باشد. تحلیل شبکه‌ی اجتماعی در علم امراض مسری به کار رفته است و نتایج چشم‌گیری برای بهبود روابط داشته است. شبکه‌های اجتماعی که برای تقویت ارتباطات در برابر فجایع (طبیعی یا بشری) شکل گرفته‌اند می‌توانند با یک شبکه آشکار شوند. تحلیل این شبکه‌ها با ابزار تحلیل شبکه‌ی اجتماعی مطالعه‌ی دگرگونی‌هایی است، که در طول فاجعه رخ می‌دهند و در آینده به عنوان راهبرد حل بحران به کار برده می‌شوند [7].

۲-۲ - ارتباطات در شبکه‌های اجتماعی

ارتباطات رکن اصلی سیستم‌های اجتماعی بوده و ارتباطات برخط دارای ویژگی‌هایی نظیر حصول (به‌دست آوردن شنوندگان جهانی)، دسترسی، قابلیت کاربرد مجدد، پاسخ‌دهی سریع و پایداری است. همچنین این ارتباطات در شبکه‌های اجتماعی برخط با سبک‌هایی همچون پیام‌ها، نظرها، گفت‌وگو در رسانه‌های اشتراک مصنوعی، فعالیت‌های اجتماعی مثل دیگ^۴ و میکروبلگینگ^۵ ظاهر می‌شوند [4].

۳ - مجسم‌سازی شبکه‌های اجتماعی

مجسم‌سازی در تعیین و شناسایی الگوها و استخراج بینش از حجم زیادی از اطلاعات کمک زیادی می‌کند. برای مجسم‌سازی شبکه‌های اجتماعی، ابزارهایی مثل نمودارهای گره - یال و ماتریس‌ها وجود دارند که هرکدام ویژگی‌ها، مزایا و معایب خاصی دارند [8].

- **ماتریس یا نمودار گره - یال:** ماتریس و نمودار گره - یال ویژگی‌های متفاوتی دارند که آنها را برای ارائه‌ی کارها یا پایگاه داده‌ها مناسب می‌کند. مطالعات نشان داده که نمودارهای گره - یال برای شبکه‌های بسیار کوچک (کمتر از ۲۰ رأس) و پراکنده بسیار سودمند هستند، درحالی که اجزای خارجی ماتریس‌ها زمانی که کارها دنبال هم می‌آیند آنها را چیزی به غیر از این کرده است. این نتایج و تجربیات باعث برپایی لیستی از مزایای هر دو ارائه می‌شود که در زیر آمده است.

هدلولی هدایت می‌شود برای کاربران غیر متجانس است، و هدایت وسیعی را نیاز دارد و ساخت و ارائه یک نقشه‌ی ذهنی از کل شبکه بسیار دشوار است.

- **نمایش‌های متناوب:** راه‌کار پایانی برای مجسم‌سازی نمودارهای بزرگ، طبقه‌بندی کردن ارائه‌های مختلف از نمودارهای گره - یال است. یک گزینش مشخص به کارگیری ماتریس مجاورت است. پیشنهاد دیگر تری‌مپ‌ها^۸ هستند. پژوهندگان تلاش دارند تا تری‌مپ‌ها به‌علاوه‌ی پیوندها را برای ارائه‌ی شبکه‌ها به کار ببرند. به طور مشابه توصیف‌های جدید، کاهش این ارائه‌ها در خوانایی شبکه‌های چگال را کشف کرد [9].

۴- هویت‌های برخط و شبکه‌ی اجتماعی

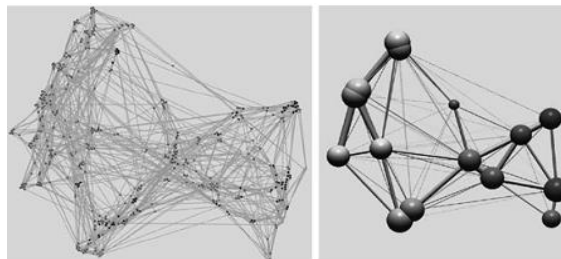
تعیین هویت افراد در اینترنت یکی از دشواری‌های مطرح است. سه موضوع مهم متحد برای تعیین هویت برخط در تارنمای اجتماعی وجود دارد: شکل، ظرفیت و صحت. نام کاربری و واژه‌ی عبور معمولاً شکل تصدیق کاربر در تارنما هستند. یک روش جدید، پیشنهاد تصادفی نام کاربری است که در URLها برای تعیین هویت کاربران به کار برده می‌شود. هدف اصلی در تعیین هویت افراد الحاق یک داده به یک فرد است. برای نمونه یک دانشگاه برای شناسایی افراد در هنگام ثبت‌نام به دانشجویان خود شماره دانشجویی منحصر به فرد می‌دهد [10].

۴-۱- روش‌های استخراج اجتماع‌ها

روش‌ها برای کشف اجتماع‌ها به طور کامل به دست موارد زیر رتبه‌بندی شده‌اند.

- **الگوریتم‌های بخش‌کننده:** یک روش ساده برای شناسایی اجتماع‌ها در یک شبکه این است که یال‌هایی که رئوس از اجتماع‌های مختلف را بهم متصل کرده پیدا شده و پاک شوند؛ بنابراین اجتماع‌های جدا از هم به وجود می‌آیند. مراحل این الگوریتم عبارتند از: (۱) محاسبه‌ی مرکزیت در همه‌ی گره‌ها؛ (۲) حذف یال‌هایی با مرکزیت بزرگتر؛ (۳) تجدید محاسبه‌ی مرکزیت روی شبکه در حال اجرا؛ (۴) تکرار این روند از مرحله‌ی ۲.
- **بهینه‌سازی پیمانه‌ای:** بهینه‌سازی یک تابع کیفیت برای ارزیابی بخش‌بندی‌ها است. بنابراین بخش‌بندی نظیر به نظیر متعلق به مقادیر بزرگ شبکه باید بهترین باشد. این، ایده‌ی اصلی بهینه‌سازی پیمانه‌ای است.
- **الگوریتم‌های طیفی:** این الگوریتم‌ها شبکه‌ی ثابت را به تکه‌هایی می‌برند، بنابراین تعداد یال‌هایی که بریده شده کمینه خواهد شد.
- **الگوریتم‌های دیگر:** الگوریتم‌های بسیار دیگری برای تعریف اجتماع‌ها وجود دارد، مثل روش‌هایی که روی پیاده‌روی تصادفی تمرکز می‌کنند، یا جستجوکننده‌ای برای هم‌پوشانی کلیک‌ها [11].

هم است. به طوری که ابتدا گراف خوشه‌بندی شود، سپس برای بهبود فضا کل رئوس ظاهر شده در یک خوشه در یک ابرگره مانند شکل (۱) دانه‌بندی شوند. اشکال‌های این روش شامل موارد زیر می‌شود: ۱- کاهش مقدار اطلاعات نمایش داده شده با توزیع‌های چندگانه انجام می‌شود؛ ۲- وقتی گره‌ها و پیوندها الک می‌شوند، ممکن است ساختار پیکربندی^۷ خراب شود یا برخی ویژگی‌ها گم شوند؛ ۳- وقتی گره‌ها با هم چگال می‌شوند، جزئیات اطلاعاتی که روی اتصال داخلی ابرگره است گم می‌شود.



شکل (۱): شبکه‌ی اصلی و شبکه‌ی کاهش یافته [9]

- **جستجوی افزایشی:** با روش جستجوی افزایشی، پژوهندگان امکان رسم شبکه‌ها با درخت‌ها و ثابت کردن آنها با اضافه کردن پیوندهای اضافی را کشف کردند. متأسفانه در شبکه‌ای که پی در پی از ساختار درختی دور می‌شود، قابلیت خوانایی ارائه‌های تصویری کم می‌شود. در این مورد، راه‌کار باقیمانده، به کار برده شده تا فقط زیرمجموعه‌ای از شبکه را نشان دهد و تعاملی را برای کشف بخش‌های باقیمانده تهیه کند. اشکال این روش کمبود دید فراهم شده روی کاربر است که باعث سخت شدن تحلیل می‌شود و بنابراین نیاز به جستجوی کل شبکه دارد.
- **کاربرد بیشتر از فضا:** برای اضافه کردن فضای تصویری در دسترس، شماری از پژوهندگان روی بعد سوم تجسس کار کردند. که فضای بیشتری را پیشنهاد می‌دهد و هم‌چنین استقلال بیشتری را در بهینه‌سازی موضوع فراهم می‌کند. اشکال اصلی ارائه‌ی سه بعدی دشوار بودن برای کاربران در برپایی یک نقشه‌ی ذهنی از کل شبکه است. برای حل این دشواری، برخی سیستم‌ها تلاش می‌کنند تا چند دید را برای کاربران فراهم کنند؛ پیشنهاد دیگر آنها تعامل و هدایت شگردها برای مجسم‌سازی شبکه‌ی پایین‌تر از زوایای چندگانه است.
- روش دیگری برای افزایش فضای دید، به کارگیری علوم هندسی مثل هدلولی هندسی به جای هندسه‌ی اقلیدسی است. در فضای هدلولی، اصل مبهم موازی بودن پذیرفته نمی‌شود (یعنی دو خط موازی فضای اقلیدسی، در فضای هدلولی از هم دور می‌شوند). بنابراین با نظر به یک دیسک در فضای هدلولی، فضا به طور نمایی رشد می‌کند. یک شبکه‌ی ممتد روی چنین دیسکی مزایایی برای یک فضای نامحدود روی حریم آن است. متأسفانه صفحه نمایش فضای هدلولی ناچار است در یک فضای اقلیدسی ارائه شود و به طور مشابه نمایش سه‌بعدی که به فضای

یا یک شبکه‌ی تک‌کاره باشد. مدیریت پوشش^۱ نقطه به نقطه یا توزیع شده، عاملیت‌های هسته‌ای را برای مدیریت منابع در زیربنای حامی سیستم، فراهم می‌آورد که می‌تواند یک شبکه‌ی توزیع شده از سرورهای قابل اعتماد و یا یک پوشش نقطه به نقطه باشد.



شکل (۲): معماری عمومی یک شبکه‌ی اجتماعی توزیع شده [14]

در روی این پوشش، لایه‌ی مدیریت داده‌ی نامتمرکز قرار دارد که عاملیت‌های یک سیستم اطلاعات نقطه به نقطه یا توزیع شده را برای پرس‌وجو، اضافه و به‌روزرسانی اشیای مانای مختلف در سیستم، به کار می‌گیرد.

لایه‌ی شبکه‌ی اجتماعی تمامی عاملیت‌ها و ویژگی‌های پایه‌ای را که به دست خدمات شبکه‌ی اجتماعی متمرکز معاصر فراهم می‌شوند، ارائه می‌کند. بالاترین لایه‌ی معماری، شامل واسط کاربر برای سیستم و نرم‌افزارهای کاربردی مختلف ساخته شده روی پایگاه گسترش فراهم شده به دست شبکه‌ی اجتماعی برخط نامتمرکز، است. کاربر شبکه‌ی اجتماعی برخط نامتمرکز، انتظار دارد که شفافیت لازم همانند سایر شبکه‌های اجتماعی برخط متمرکز، برایش فراهم باشد.

۲-۵- روش‌های موجود برای اجرای شبکه‌ی اجتماعی برخط نامتمرکز

روش‌های موجود شامل سیف‌بوک^{۱۱} (یک شبکه‌ی اجتماعی برخط محافظ حریم خصوصی است [12])، فوفا^{۱۱} (یک روش کاربردی دیگر برای مدیریت نامتمرکز شبکه‌های اجتماعی جاری ارائه می‌دهد)، لایف‌سوشال^{۱۲} (سعی در قابل مقیاس‌پذیر نگه داشتن خدمات شبکه‌ی اجتماعی به دست توزیع بار بین منابع کاربران دارد)، پیرسان^{۱۳} (می‌خواهد ویژگی‌های شبکه‌های اجتماعی برخط را با غلبه بر دو محدودیت حریم خصوصی و نیاز برای اتصال به اینترنت برای تمام ترانکنش‌ها حفظ کند) و لیکیر^{۱۴} (یک جدول درهم سازی توزیع شده برای شبکه‌های رایانه‌ی توزیع شده است [13])، می‌شود.

۵- شبکه‌های اجتماعی برخط نامتمرکز

خدمات متمرکز شبکه‌ی اجتماعی باعث برپایی برخی دشواری‌ها شده‌اند. این دشواری‌ها هم شامل مسائل فنی و هم مسائل اجتماعی می‌شود که نتیجه‌ی مدیریت متمرکز خدمات است. از جنبه‌ی فنی، مدیریت متمرکز شبکه‌ی اجتماعی با رشد سریع در تعداد کاربران، آن را به مسائل مقیاس‌پذیری عمل‌کردی مختلفی هدایت می‌کند. از جنبه‌ی اجتماعی، قابلیت به اشتراک‌گذاری نامحدود اطلاعات به برخوردهای اجتماعی منجر شده است؛ به این معنی که رشد سریع تارنماهای شبکه، بدون برنامه‌های مناسب محافظت از حریم خصوصی، منجر به فروپاشی در درون مایه‌ی اجتماعی شده است. قطع اعتماد میان کاربران و فراهم کنندگان تارنما نیز از مسائل کلیدی است که منجر به فروپاشی برخی خدمات اجتماعی اخیر شده است.

شبکه‌ی اجتماعی برخط نامتمرکز، یک شبکه‌ی اجتماعی برخط است که در یک پایگاه مدیریت اطلاعات توزیع شده، قرار گرفته است؛ مانند شبکه‌ای از سرورهای مطمئن یا یک سیستم نقطه به نقطه. در مقایسه با شبکه‌های اجتماعی برخط متمرکز که دارند، تمام هزینه را در فراهم کردن خدمات، تحمل می‌کند، شبکه‌ی اجتماعی برخط نقطه به نقطه یا توزیع شده، یک جایگزین هزینه -کارا را پیشنهاد می‌کند. شبکه‌ی اجتماعی برخط نامتمرکز، ترکیبی از اجزای اجتماعی و نامتمرکز است.

نامتمرکز ساختن عملیات موجود شبکه‌های اجتماعی برخط، نیاز به پیدا کردن روش‌هایی برای ذخیره‌سازی، به‌روزرسانی‌ها، پیکربندی، جست‌وجو و آدرس‌دهی، آزادی برای نرم‌افزارهای کاربردی جدید، امنیت، قدرت در رویارویی با بدرفتاری، نقاط محدود شده و محلی بودن دارد.

هنگامی که عاملیت توزیع شده باشد، شبکه‌های اجتماعی به اتصال اینترنت برای هر تراکنش وابسته نیستند. در این روش، نرم‌افزارهای کاربردی شبکه‌های اجتماعی می‌توانند از ذخیره‌سازی محلی، اتصال و انتقال داده‌ی مقاوم به تأخیر در تداخلات اجتماعی سود ببرند. انجمن‌های محلی نیز می‌توانند از نرم‌افزارهای کاربردی شبکه‌ی اجتماعی که به دست چنین سیستمی توانا شده‌اند، سود ببرند. همین که فناوری در دسترس قرار گیرد، کاربران با نرم‌افزارهای کاربردی جدید و اصلی مانند همراهی با تارنمای گسترده‌ی جهانی و شبکه‌های اجتماعی برخط، همراه می‌شوند.

۱-۵- معماری مرجع برای شبکه‌های اجتماعی

برای داشتن یک دید بهتر از روش‌های موجود در خدمات شبکه‌ی اجتماعی برخط نامتمرکز، یک معماری مرجع پایگاه شبکه‌ی اجتماعی نامتمرکز همه منظوره در شکل (۲) آورده شده است. معماری مرجع شامل شش لایه است و یک معماری خلاصه از روش‌های شبکه‌ی اجتماعی نامتمرکز موجود، به زبان تحقیق، فراهم می‌کند. پایین‌ترین لایه‌ی این معماری، شبکه‌ی ارتباطی فیزیکی است که می‌تواند اینترنت

۳-۵- نرم افزار کاربردی اختصاصی واقع در مرکز

شبکه‌های اجتماعی برخط نامتمرکز

علاوه بر همتهای نرم‌افزارهای شبکه‌های اجتماعی برخط همه منظوره، پیش‌گام‌هایی مانند موارد زیر برای واقعی کردن همتهای نامتمرکز نرم‌افزارهای کاربردی وجود دارند.

- **اشتراک فایل نقطه به نقطه بر مبنای اجتماع:** در میان کارهای انجام شده در این زمینه بهترین پیش‌گام گسترش یافته تریبلسر^{۱۵} است که به طور بنیادی یک سیستم اشتراک درون‌مایه‌ی نقطه به نقطه است که روابط اجتماعی موجود و تشابهات میان کاربران خود را برای کشف و پیشنهاددهی سریع درون‌مایه‌ی دیجیتالی به کار می‌برد.
- **بوک‌مارک‌های به اشتراک گذاشته شده و جست‌وجوی همکاری:** خدمت بوک‌مارک کردن اجتماعی، دیکی است که به کاربران اجازه می‌دهد، بوک‌مارک‌های خود را رمزگذاری کنند و با دوستان مطمئن به اشتراک بگذارند. حریم خصوصی کاربر در سه قاعده‌ی طراحی محافظت می‌شود: تبادل داده تنها میان دوستان مطمئن شدنی است، هیچ داده‌ای به طور مرکزی ذخیره نمی‌شود، و هر داده‌ی ذخیره شده‌ای رمزگذاری شده است.
- **میکرو بلاگینگ:** پروتکل فتر^{۱۶} یک پروتکل سبک وزن است که کاربران را قادر می‌سازد تا هر خدمت میکرو بلاگینگ موجود را برای ارتباط با سایر کاربران به طور بلادرنگ به کار ببرند. کاربرانی که از پروتکل فتر پیروی می‌کنند می‌توانند به روزرسانی‌های دیگران را ثبت کنند و آنها را بلادرنگ دریافت کنند [1].
- **حریم خصوصی:** هدف حریم خصوصی، پنهان کردن هر گونه اطلاعاتی در مورد کاربر در هر زمان، حتی هنگام گسترش پنهان‌سازی عضویت و فعالیت‌های آنها در ابتدا در شبکه‌ی اجتماعی برخط است. حریم خصوصی باید پیش فرض باشد، یعنی تمام اطلاعات تمام کاربران و فعالیت‌های آنها را باید از هر شخص سوم داخلی یا خارجی در سیستم پنهان کند، مگر این‌که آنها به دست خود کاربران صریحاً فاش شوند.
- **یک پارچگی:** هدف یک‌پارچگی در شبکه‌های اجتماعی برخط، جلوگیری از دخالت یا دگرگونی‌های غیر مجاز درون‌مایه‌ی کاربر یا اطلاعات پروفایل است. حفاظت از شناسه‌های واقعی در پایگاه‌های امروزی، ناکافی است. مخصوصاً این‌که هیچ کدام از فراهم‌کنندگان شبکه‌های اجتماعی برخط بزرگ جاری، نمی‌توانند اطمینان بدهند که یک پروفایل در رابطه با فرد مربوط از دنیای واقعی است. از آنجایی که کاربران ذاتاً به فراهم‌کنندگان شبکه‌ی اجتماعی برخط، اعتماد دارند، آسیب‌پذیری‌های گفته شده می‌توانند با یک رویه‌ی مجازشناسی مناسب برای اطمینان از وجود افراد واقعی پشت پروفایل‌های ثبت‌نام کرده‌ی شبکه‌ی اجتماعی برخط، خنثی شوند.
- **دسترسی پذیری:** هدف دسترسی‌پذیری برای شبکه‌های اجتماعی برخط، ایمن‌سازی قابلیت عملیات خدمات شبکه‌ی اجتماعی در رویایی با حمله‌ها و نقص‌ها است. تضمین ناکافی برای دسترسی پذیری ممکن است کاربران را از دستیابی به خدمت باز دارد و پایگاه شبکه‌ی اجتماعی برخط را غیر جذاب کند. مخصوصاً برای شبکه‌های اجتماعی برخط با کانون حرفه‌ای که لازم است داده‌ی کاربر به طور مداوم در دسترس باشد. دسترسی‌پذیری داده‌ی تولید شده به دست کاربر و پروفایل‌ها یک نیاز بنیادی است که باید به دست پایگاه‌ها فراهم شود.

۶- امنیت و حریم خصوصی در شبکه‌های

اجتماعی

به طور کلی، عاملیت شبکه‌ی اجتماعی می‌تواند به سه نوع اصلی دسته بندی شود: ۱- توابع شبکه: برای تغذیه‌ی روابط اجتماعی میان کاربران در پایگاه مجازی ۲- توابع داده: برای مدیریت درون‌مایه‌ی فراهم شده به دست کاربر و ارتباطات میان کاربران ۳- توابع کنترل دستیابی: برای گرفتن اندازه‌های حریم خصوصی تعیین شده به دست کاربر و برای محدود کردن دسترسی غیر مجاز به داده و اطلاعات فراهم شده به دست کاربر.

۶-۱- اهداف امنیت: حریم خصوصی، یکپارچگی و

دسترسی پذیری

اهداف امنیت، نیازمندی‌هایی هستند که باید برای محافظت از سیستم در برابر حملات و تهدیدهای بالقوه برطرف شوند. نفوذ غیرقانونی به حریم خصوصی و یک‌پارچگی درون‌مایه‌ی فراهم شده به دست کاربر، ممکن است به زیان اقتصادی برای کاربران منجر شود یا وضعیت‌های

۲-۶- طیف حمله و اقدام‌های متقابل

فهم فنی پشت یک حمله، به عاملیت و کارکرد سازوکارهای حفاظتی در پایگاه شبکه‌ی اجتماعی برخط وابسته است. بنابراین، همه‌ی فنون حمله، هنگامی که در روبه‌روی پایگاه‌های شبکه‌های اجتماعی برخط متفاوت به کار برده می‌شوند، کارایی یکسانی ندارند. علاوه بر آن، از آنجایی که فراهم‌کنندگان شبکه‌ی اجتماعی برخط، معمولاً کنترل کاملی روی منابع شبکه دارند، اگر حمله‌ها به دست خود فراهم‌کننده سوار شوند، هیچ محافظت معنی‌داری ظاهر نمی‌شود. برخی گونه‌های حمله در زیر آورده شده‌اند.

محافظت معنی داری در برابر حمله‌های گردآوری داده‌ی فرعی وجود ندارد چرا که داده معمولاً از مکان‌های مختلف گردآوری می‌شود. بنابراین، این مسئولیت کاربر است که اطلاعات نگه داشته شده در پروفایل را برای اجتناب از اتصال به منابع فرعی محدود کند.

بازیابی عکس و تحلیل: بازیابی عکس و تحلیل، یک حمله‌ی خودکار است که سعی در گردآوری داده‌ی چندرسانه در پایگاه شبکه‌ی اجتماعی برخط دارد. این حمله معمولاً با یک تحلیل با ابزارهای شناسایی الگوی خودکار برای پیدا کردن پیوندهای نمایش داده شده به پروفایل‌های شبکه‌ی اجتماعی برخط کاربران، دنبال می‌شود.

پروفایل‌های جعلی و حمله‌های سای بیبل: در بسیاری از پایگاه‌های شبکه‌های اجتماعی، کاربران می‌توانند پروفایل‌های بسیاری تحت شناسه‌ها و درون‌مایه‌های متفاوت بسازند. یک راه کار برای فراهم کنندگان شبکه‌ی اجتماعی برخط برای شناسایی پروفایل‌های جعلی، به کارگیری ردیابی IP است. در حقیقت اگر ورود به پروفایل‌های بسیاری از طریق یک آدرس IP صورت گیرد در این صورت شاید برخی از این پروفایل‌ها جعلی هستند. هر چند با به کارگیری پروکسی‌های مختلف از ردیابی IP جلوگیری می‌شود.

تغییر شکل گروه: تغییر شکل گروه، حمله‌ای است که در آن اداره کنندگان گروه، موضوع گروه را برای دنبال کردن علاقه‌مندی‌های خود مثل سیاست عوض می‌کنند. یک راه کار ممکن برای فراهم کنندگان شبکه‌ی اجتماعی برخط، محدود کردن کنترل اداره کنندگان در گروه‌های علاقه‌مند است.

مسائل رأی مخفی و افترا زدن: مسائل رأی مخفی^۸، حمله‌ای است که در آن حمله کننده می‌خواهد علاقه‌ی عمومی به کاربر شبکه‌ی اجتماعی برخط را افزایش دهد. در روبه‌رو حمله‌های افترا، سعی در کاهش علاقه‌ی عمومی به کاربر هدف دارند، مخصوصاً با لکه‌دار کردن اعتبار کاربر. افترا ممکن است منجر به لیست سیاه شدن کاربر در لیست مخاطبان کاربران دیگر شود.

سانسور: این قابلیت برای جلوگیری از پخش درون‌مایه‌ی غیر مجاز ضروری است. از طرف دیگر، هنگامی که سانسور بدون دلایل محکم انجام گیرد، تأثیر منفی روی کاربران شبکه‌ی اجتماعی برخط می‌گذارد.

حمله‌های تبانی: در این حمله، بسیاری از کاربران برای آسیب رساندن به سایر کاربران شبکه‌ی اجتماعی برخط به فعالیت‌های بدکاری ملحق می‌شوند یا در برابر پایگاه شبکه‌ی اجتماعی برخط حمله‌هایی انجام می‌دهند. شناسایی این حمله‌ها نسبت به حمله‌های مشابه از طریق پروفایل‌های جعلی دشوارتر است. دلیل آن این است که ردیابی IP حتی اگر کاربران تبانی کرده هیچ پروکسی اضافی گسترش نداده باشند، کمکی نمی‌کند [14].

جعل هویت ساده: با حمله‌ی جعل هویت ساده، حمله کننده پروفایلی ساختگی برای کاربران دنیای واقعی، می‌سازد. موفقیت این حمله به شدت به سازوکارهای مجازشناسی در فرآیند ثبت نام ربط دارد. نتیجه‌ی جعل هویت ساده این است که دشمن می‌تواند در نرم‌افزارهای کاربردی شبکه‌ی اجتماعی برخط، با تمام نتایج زبان آور برای کاربر، به جای کاربر جعل هویت شده شرکت کند. این حمله، تنها با گسترش فنون مجاز شناسی قوی‌تر، خنثی می‌شود.

تولید مثل پروفایل: حمله کننده با این حمله، یک پروفایل برای کاربری که اکنون در همان شبکه پروفایلی معتبر دارد، می‌سازد. از نقطه نظر فنی، این حمله می‌تواند در ثبت نام پروفایل جدید با به کارگیری درون‌مایه‌ی پروفایل موجود، شناسایی شود. یک راه کار ممکن برای فراهم کنندگان شبکه‌ی اجتماعی برخط برای جلوگیری از تولید مثل پروفایل، گسترش سازوکارهایی است که قادر به شناسایی همانندی میان پروفایل‌های مختلف هستند. از آنجایی که پروفایل‌های تولید مثل شده معمولاً تاریخ ثبت نام دیرتری نسبت به پروفایل‌های اصلی دارند، تشخیص و حذف آنها از شبکه برای فراهم کنندگان شبکه‌ی اجتماعی برخط امکان پذیر است.

پروفایل ربائی: در این حمله، حمله کننده کنترل برخی پروفایل‌های موجود را در پایگاه شبکه‌ی اجتماعی برخط به دست می‌آورد. بسیاری از پایگاه‌های شبکه‌ی اجتماعی برخط، دستیابی کاربر به پروفایل‌های خود را با به کارگیری رمز عبور محافظت می‌کنند. از این رو، از نقطه نظر فنی، پروفایل ربائی زمانی موفقیت آمیز است که دشمن بتواند رمز عبور سایر کاربران را به دست آورد. فراهم کنندگان شبکه‌ی اجتماعی برخط، محافظتی را در برابر چنین حمله‌هایی، با محدود کردن تعداد تلاش‌ها برای ورود یا به کارگیری فزونی که به تعامل انسانی نیاز دارند مانند کپتچا^۹ها، گسترش می‌دهند.

انتقال پروفایل: حمله کننده در این حمله برخی پروفایل‌هایی که در یک پایگاه شبکه‌ی اجتماعی برخط وجود دارند، در پایگاه شبکه‌ی اجتماعی برخط دیگری تولید می‌کند. خنثی کردن انتقال پروفایل به این سادگی‌ها نیست. از آنجایی که هر پایگاه شبکه‌ی اجتماعی برخطی به دست فراهم کننده‌ی متفاوتی اداره می‌شود، گسترش ابزارهای تشخیص همانندی پروفایل نیازمند همکاری میان فراهم کنندگان است. رسیدن به این موضوع دشوار است، چرا که فراهم کنندگان شبکه‌ی اجتماعی برخط در دادن هر شکل دستیابی به پایگاه داده‌ی پروفایل خود به رقبا، محتاط هستند.

گردآوری داده‌ی فرعی: گردآوری داده‌ی فرعی حمله‌ای است که تلاش دارد تا اطلاعاتی در مورد صاحب پروفایل را از منابع فرعی جدا از پایگاه شبکه‌ی اجتماعی برخط، گردآوری کند. هیچ

کوتاه‌ترین مسیرها میان s و t با گذر از دست کم یک عضو گروه C باشد. مرکزیت میانگی گروه C از فرمول زیر محاسبه می‌شود:

$$GBC(C) = \sum_{s,t \in V | s \neq t} \left(\frac{\sigma_{s,t}(C)}{\sigma_{s,t}} \right) \quad (4)$$

• **مرکزیت میانگی گردش تصادفی:** در مرکزیت میانگی گردش تصادفی^{۲۵} مسیرهای کوتاه‌تر بیشتر از مسیرهای بلندتر در نظر گرفته می‌شوند. این مرکزیت فکر می‌کند که مسیرها ممکن است شامل چرخه‌ها باشند که البته این در بیشتر شبکه‌های ارتباطی وجود ندارد. هرچند مرکزیت میانگی گردش تصادفی یک سری مدل‌های انتشار شایعه را تطبیق می‌دهد. این برای تخمین کنترل بالقوه‌ای که یک گره در جریان اطلاعات در شبکه‌های غیبت که پیام‌ها به طور تصادفی در شبکه سرگردانند تا زمانی که به هدف مورد نظرشان برسند دارد، بسیار مناسب است [15].

۷- نتیجه‌گیری

با توجه به رشد روزافزون شبکه‌های اجتماعی برخط می‌توان پیش‌بینی کرد که در آینده‌ای نه چندان دور آنها به عضوی جدا نشدنی در زندگی تمام مردم جهان تبدیل خواهند شد، در نتیجه در این مقاله سعی شد تا اطلاعاتی مختصر در مورد این شبکه‌ها ارائه شود.

در این مقاله ابتدا به تحلیل و مجسم‌سازی شبکه‌های اجتماعی پرداخته شد و کاربرد این تحلیل‌ها در زندگی مردم بیان شد، سپس به تعیین هویت افراد و شناسایی جوامع در شبکه‌های اجتماعی برخط و همچنین زیربنای این شبکه‌ها پرداخته شد، و در نهایت امنیت و تهدیدهای مختلف موجود در این نوع جدید ارتباطات معرفی شد.

مراجع

- [1] L. A. Cutillo, M. Manulis, and T. Strufe, "Security and Privacy in Online Social Networks," in Handbook of Social Network Technologies, 2010, pp. 497-522.
- [2] C. Freeman, "Center graphs and the structure of sgo networks", Linton, 1982.
- [3] M. Zhang, "Social Network Analysis: History, Concepts, and Research," in Handbook of Social Network Technologies, 2010, pp. 3-21.
- [4] M. D. Choudhury, H. Sundaram, A. John, and D. D. Seligmann, "Analyzing the Dynamics of Communication in Online Social Networks," in Handbook of Social Network Technologies, 2010, pp. 59-94.
- [5] D.M. Akbar Hussain, "Investigation of Key-Player Problem in Terrorist Networks Using Bayes Conditional Probability," in Handbook of Social Network Technologies, 2010, pp. 523-547.
- [6] S. Sizov, S. Staab, and T. Franz, "Analysis of Social Networks by Tensor Decomposition," in Handbook of Social Network Technologies, 2010, pp. 45-58.
- [7] P. S. Thilagam, "Applications of Social Network Analysis," in Handbook of Social Network Technologies, 2010, pp. 637-649.
- [8] I. Chen and C. Yang, "Visualization of Social Networks," in Handbook of Social Network Technologies, 2010, pp. 585-610.

۳-۶- حفظ امنیت شبکه‌های اجتماعی در برابر

تهدیدات

ابزارهای اصلی مبارزه با تهدیدات (ویروس‌ها و کرم‌ها)، سیستم‌های شناسایی نفوذ هستند که ترافیک اینترنت را برای اثرهای حمله‌ای از پیش تعیین شده یا لیست سیاه‌های آدرس منبع تصفیه می‌کنند. از آنجایی که این سیستم‌ها قادر به بررسی تمام ترافیک موجود در شبکه نیستند، به جای انتخاب تصادفی گره‌ها از شاخص‌های مرکزیت برای انتخاب درست و بهینه استفاده می‌کنند. برای تحلیل و فهم نقش‌های بازی شده در شبکه‌های پیچیده، بسیاری از مطالعات تحلیل گران شبکه در سال‌های اخیر به ارزشیابی مرکزیت وابسته است. برخی اندازه‌های مرکزیت در زیر آورده شده‌اند:

- **مرکزیت درجه:** مرکزیت درجه^{۱۹}، تعداد اتصالات جهت‌دار گره است.
- **مرکزیت درجه‌ی گروه:** مرکزیت درجه‌ی گروه^{۲۰} به عنوان تعداد گره‌های غیر گروه مجاور اعضای گروه یا همسایگی محلی است. همسایه‌ی محلی شامل تمام رأس‌هایی است که در بیشتر از یک گام از اعضای گروه قرار نگرفته‌اند.
- **مرکزیت نزدیکی:** مرکزیت نزدیکی^{۲۱} یک رأس، جمع فاصله‌های کوتاه‌ترین مسیرها به تمام رأس‌های دیگر در گراف است. زمان میانگین تا زمانی که یک رأس در شبکه، رازی را بشنود با نزدیکی رأس کاهش می‌یابد.
- **مرکزیت نزدیکی گروه:** مرکزیت نزدیکی گروه^{۲۲} یک گروه C ، جمع دو طرفه‌ی فاصله‌های کوتاه‌ترین مسیرها از تمام گره‌های مرتبط در شبکه به نزدیک‌ترین عضو گروه تعریف می‌شود:

$$closenes(C) = \frac{1}{\sum_{v \in V} \min_{m \in C} [dist(v, m)]} \quad (2)$$

- مرکزیت‌ترین گروه‌ها، گروه‌هایی با بیشترین نزدیکی گروه هستند.
- **مرکزیت میانگی:** مرکزیت میانگی^{۲۳}، میزانی که یک رأس بر جریان اطلاعات میان سایر رأس‌ها کنترل دارد را اندازه می‌گیرد. مرکزیت میانگی یک رأس به عنوان تمام کسرهای از کوتاه‌ترین مسیرها میان تمام جفت رأس‌ها در یک شبکه که آن رأس در آن مسیر وجود دارد، تعریف می‌شود. برای یک گراف $G=(V, E)$ ، فرض می‌شود $\sigma_{s,t}$ تعداد کوتاه‌ترین مسیرها میان s و t ، $\sigma_{s,t}(v)$ تعداد کوتاه‌ترین مسیرها میان s و t با عبور از v باشد. مرکزیت میانگی رأس v از فرمول زیر محاسبه می‌شود:

$$BC(v) = \sum_{s,t \in V | s \neq v \neq t} \left(\frac{\sigma_{s,t}(v)}{\sigma_{s,t}} \right) \quad (3)$$

- **مرکزیت میانگی گروه:** مرکزیت میانگی گروه^{۲۴} C ، تمام کسرهای از کوتاه‌ترین مسیرها میان تمام جفت رأس‌ها است که دست کم از یک عضو گروه C عبور کرده باشد. اگر $\sigma_{s,t}(C)$ تعداد

- [9] N. H. Riche and J. D. Fekete, "Novel Visualizations and Interactions for Social Networks Exploration," in Handbook of Social Network Technologies, 2010, pp. 611-636.
- [10] M. Maheswaran, B. Ali, H. Ozguven, and J. Lord, "Online Identities and Social Networking," in Handbook of Social Network Technologies, 2010, pp. 241-267.
- [11] T. Murata, "Detecting Communities in Social Networks," in Handbook of Social Network Technologies, 2010, pp. 269-280.
- [12] prototype. safebook. [Online]. Available: <http://www.safebook.eu/prototype.html>.
- [13] wiki/Kademlia. wikipedia. [Online]. Available: <http://en.wikipedia.org/wiki/Kademlia>.
- [14] A. Datta, S. Buchegger, L. Vu, T. Strufe, and K. Rzadca, "Decentralized Online Social Networks," in Handbook of Social Network Technologies, 2010, pp. 349-378.
- [15] R. Puzis, M. Tubi, and Y. Elovici, "Optimizing Targeting of Intrusion Detection Systems in Social Networks," in Handbook of Social Network Technologies, 2010, pp. 549-568.
- [16] Y. Lin, H. Sundaram, and A. Kelliher, "Multi-Relational Characterization of Dynamic Social Network Communities" in Handbook of Social Network Technologies, 2010, pp. 379-408.

زیر نویس ها

-
- 1 One Mode Versus Two Mode Networks
 - 2 Complete/Whole Versus Ego Networks
 - 3 Ego-centric
 - 4 www.digg.com
 - 5 Micro-blogging
 - 6 MatrixExplorer
 - 7 topology
 - 8 Treemap
 - 9 overlay
 - 10 Safebook
 - 11 FOAF
 - 12 LifeSocial
 - 13 PeerSoN
 - 14 Likir
 - 15 Tribler
 - 16 FETHR
 - 17 CAPTCHA
 - 18 Ballot Stuffing
 - 19 Degree Centrality(DC)
 - 20 Group Degree Centrality(GDC)
 - 21 Closeness Centrality(CC)
 - 22 Group Closeness Centrality(GCC)
 - 23 Betweenness Centrality(BC)
 - 24 Group Betweenness Centrality(GBC)
 - 25 Random Walk Betweenness-Centrality (RWBC)