نشریه علمی «پدافند الکترونیکی و سایبری»
سال هفتم، شماره ۱، بهار ۱۳۹۸؛ ص ۱۰۳-۹۵

طبقه‌بندی تقلب‌های همکارانه در شبکه حراجی الکترونیکی با استفاده از معیار شباهت در طبقه‌بندی جمعی

مهیلا دادفرنیا[۱]، فضل‌الله ادیب‌نیا[۲*]

۱- دانشجوی دکتری، ۲- استادیار، گروه مهندسی کامپیوتر، دانشگاه یزد

(دریافت: ۹۶/۱۱/۲۲، پذیرش: ۹۷/۷/۲۱)

چکیده

در دنیای امروز بحث طبقه‌بندی اطلاعات اهمیت زیادی یافته است. در مسائل طبقه‌بندی هدف شناسایی ویژگی‌هایی است که گروهی را که هر موجودیت به آن تعلق دارد را نشان دهند. یکی از مواردی که می‌توان برای طبقه‌بندی استفاده نمود، طبقه‌بندی کاربران حراجی می‌باشد. با توجه به این‌که در طی سال‌های گذشته حراجی الکترونیکی اهمیت فراوانی پیدا کرده است، مسئله شناسایی افراد متقلب در این نوع شبکه‌ها توجه کاربران زیادی را به خود جذب کرده است. یکی از انواع تقلب، تقلب با روش همکاری و تبانی کاربران متقلب دیگر در حراجی می‌باشد که این نوع تقلب در صورت وقوع بسیار خطرناک می‌باشد و ممکن است ضررهای مالی جبران‌ناپذیری را در پی داشته باشد. در این مقاله روشی را پیشنهاد می‌دهیم که ابتدا ویژگی‌های موثر در یافتن افراد عادی را برای هر کاربر حراجی استخراج نموده و سپس طبقه‌بندی کاربران را با روش طبقه‌بندی جمعی انجام می‌دهد. در روش پیشنهادی، برای بهبود نتایج، تابع پتانسیل لبه در روش طبقه‌بندی جمعی تعریف می‌گردد که از فاصله L1-norm به‌عنوان معیار شباهت بین دو گره مجاور استفاده می‌نماید. نتایج نشان می‌دهند که تابع پتانسیل لبه تعریف شده، در بهبود نرخ طبقه‌بندی شناسایی کاربران متقلب همکار کارآیی خوبی را دارد.

کلید واژگان: معیار شباهت، طبقه‌بندی جمعی، فاصله L1-norm، مدل تصادفی مارکف، روش انتشار باور حلقه‌ای

۱- مقدمه

پیشرفت‌های به‌وجود آمده در دنیای کامپیوتر و افزایش تعداد کاربران اینترنتی، در طی دهه‌های اخیر باعث شده در بسیاری از علوم با حجم زیادی از اطلاعات روبرو شویم که نیاز به طبقه‌بندی آنها باشد. در دنیای سایبری امروزی یکی از مسائل کلیدی، امنیت ارتباطات در شبکه‌های اجتماعی بین کاربران اینترنتی می‌باشد که به همین دلیل، پژوهش های مختلفی با رویکرد تمیز دادن افراد متقلب با روش طبقه‌بندی داده‌ها انجام پذیرفته است [۱]. یکی از شبکه‌های اجتماعی که در طی سال‌های اخیر گسترش سریعی داشته است، شبکه اجتماعی حراجی می‌باشد که با توجه به بعد مالی از اهمیت فراوانی برخوردار است و در صورت وقوع تقلب می‌تواند ضررهای مالی تاسف باری را به همراه داشته باشد [۲]. از این رو، طبقه‌بندی افراد متقلب و شناسایی کاربران عادی و غیرعادی با توجه به رفتارهای هر کاربر در حراجی الکترونیکی از اهمیت زیادی برخوردار است.

اطلاعات حجیم و بسترهای داده‌ای امروزی باعث ایجاد چالش‌های زیادی در زمینه تحلیل و طبقه‌بندی داده‌ها شده است که روش‌های آماری قدیمی به دلیل افزایش تعداد مشاهدات و همچنین افزایش تعداد متغیرهای مربوط به یک مشاهده کارایی لازم را ندارند. تعداد متغیرهایی که برای هر مشاهده باید اندازه‌گیری شود ابعاد داده نامیده می‌شود که با توجه به چالش‌های موجود، رویکرد کاهش ابعاد داده مورد توجه محققان بسیاری قرار گرفته است [۳]. یکی از روش‌های کاهش ابعاد داده، روش‌های مبتنی بر استخراج ویژگی می‌باشد؛ این روش‌ها یک فضای چند بعدی را به یک فضای با ابعاد کمتر نگاشت می‌کنند. در واقع با ترکیب مقادیر ویژگی‌های موجود، تعداد کمتری ویژگی بوجود می‌آورند؛ به‌طوری‌که این ویژگی‌ها دارای تمام یا بخش زیادی از اطلاعات موجود در ویژگی‌های اولیه باشند. به همین دلیل استخراج صحیح ویژگی‌ها از اهمیت بالایی برخوردار می‌باشد.

در طبقه‌بندی اطلاعات که با توجه به ویژگی‌های استخراج شده موجودیت‌ها انجام می‌پذیرد، هدف به‌دست آوردن مدلی برای الگوی رفتاری و ویژگی‌های مجموعه‌ای از داده‌ها است تا با

رایانامه نویسنده مسئول: fadib@yazd.ac.ir

کمک آن بتوان بدون دانستن رفتار یک موجودیت، با توجه به ویژگی‌های آن و با استفاده از مدل به‌دست آورده شده، رفتار آن را تشخیص داد و آن موجودیت را در گروه خاصی طبقه‌بندی کرد. فرایند طبقه‌بندی در واقع نوعی یادگیری با ناظر می‌باشد که در طی دو مرحله انجام می‌گردد. در مرحله اول، مجموعه‌ای از داده‌ها برای ایجاد مدل داده بکار می‌روند که در آن هر داده شامل تعدادی ویژگی می‌باشد که متعلق به یک کلاس خاص است و این مدل تولید شده، در واقع توصیف کننده مفهوم و خصوصیات مجموعه داده‌های متعلق به آن کلاس خاص می‌باشد. مرحله دوم، فرآیند طبقه‌بندی یا به‌کارگیری مدل داده ایجاد شده بر روی سایر داده‌ها می‌باشد که هدف از این فرآیند نیز تخمین تعلق آن داده به کلاس خاص می‌باشد. یکی از روش‌های طبقه‌بندی، روش طبقه‌بندی جمعی[1] می‌باشد که در این روش یک مدل پیش‌بینی با توجه به ساختار داده‌های شبکه ساخته می‌شود. در این روش فرض می‌شود که داده‌های همسایه از نظر رفتاری به هم شبیه‌تر هستند [۴]. امروزه با استفاده از این علم به تحلیل، بررسی و پیش بینی رفتارهای مشتریان شرکت های زیادی در سراسر نقاط جهان پرداخته می‌شود. به عنوان مثال، تحلیل های مختلفی بر روی اطلاعات شرکت eBay شده است. این شرکت، یک شرکت پیشرو در حراج‌های اینترنتی است و در حال حاضر دارای یک جامعه ۲۲۱ میلیون نفری از کاربران فعال در سراسر جهان است [۶-۵] و نشان داده که تقلب در حراجی‌ها می‌تواند تاثیر قابل توجهی در بازار میلیارد دلاری در سراسر جهان بگذارد [۷]. متاسفانه، تشخیص رفتارهای متقلبانه در شبکه های اجتماعی و به خصوص در حراجی‌ها به دلیل پیچیده بودن حراجی‌ها بسیار مشکل می‌باشد [۲ و ۹-۸]. یکی از انواع تقلب در حراجی الکترونیکی، به‌صورت همکاری با کاربران متقلب دیگر می‌باشد که با وجودی که این نوع تقلب چندان معمول نیست، اما به‌دلیل تشخیص سخت این نوع تقلب، بسیار خطرناک می‌باشد.

الگوریتم‌ها و روش‌های مختلفی برای طبقه‌بندی تاکنون پیشنهاد شده‌اند که یکی از این روش‌ها روش طبقه‌بندی جمعی می‌باشد که با هدف انتشار برچسب های گره‌ها در یک کلاس انجام می‌پذیرد. درواقع در این روش، گره‌های مرتبط با یکدیگر نه تنها بر اساس ویژگی‌های خود آن گره، بلکه بر اساس ویژگی‌ها و برچسب‌های سایر کلاس‌ها در یک طبقه‌بندی قرار می‌گیرند. روش‌های مختلفی برای طبقه‌بندی وجود دارد که به‌عنوان مثال در [۱۰] از روش طبقه‌بندی تک کلاسی استفاده شده است. در این مقاله نیز از روش تک کلاسی استفاده می‌شود که با توجه به اطلاعات یک کلاس عمل طبقه‌بندی انجام می‌پذیرد. در هر شبکه با توجه به ماهیت آن، ویژگی‌های مختلفی به کار می‌آیند. در شبکه حراجی الکترونیکی نیز برای طبقه‌بندی لازم است یکسری ویژگی‌ها تعریف گردند. همان‌طور که اشاره گردید، با توجه به افزایش تقلب همواره تشخیص افراد متقلب در حراجی‌ها یکی از مسائل مورد علاقه محققان بوده است که لازم است یکسری ویژگی برای طبقه‌بندی تعریف شود. تحقیق‌های زیادی از ویژگی‌های پروفایل کاربران استفاده نمودند تا کاربران متقلب را طبقه‌بندی کنند [۱۳-۱۱]. این روش‌ها از روش طبقه‌بندی جمعی استفاده نمی‌نمایند و روابط بین کاربران را درنظر نمی‌گیرند و به همین دلیل برای طبقه‌بندی کاربران متقلب همکار مفید نیستند. علاوه براین روش‌های دیگری مانند [۱۴] و [۱۵] از طبقه‌بندی جمعی استفاده نموده‌اند، اما این روش‌ها عمدتا ضعف در سرعت همگرایی پایین دارند و سرعت اجرای این روش‌ها بسیار کند می‌باشد.

در این مقاله روشی پیشنهاد می‌شود که با تغییر پارامترهای طبقه‌بندی جمعی بتوان نتایج بهتری را برای طبقه‌بندی رفتارهای همکارانه متقلب در زمان منطقی به‌دست آورد. در این روش، ابتدا ویژگی‌هایی را برای تمیز دادن کاربران عادی و غیرعادی، بر مبنای رفتار آنها در حراجی تعریف نموده و سپس با روش طبقه‌بندی جمعی، کاربران عادی و غیر عادی از همدیگر تشخیص داده می‌شوند. با توجه به این‌که اغلب کاربران متقلب با مشارکت یکدیگر در خرید و فروش شرکت می‌نمایند، این روش درواقع با در نظر گرفتن همسایه‌ها در گراف به یافتن افراد همکار متقلب کمک می‌نماید. در واقع در روش پیشنهادی، ابتدا با روش SVDD[2] کاربران را بدون در نظر گرفتن همسایه‌ها و تنها بر اساس بردار ویژگی طبقه‌بندی نموده و سپس ارتباطات بین کاربران مختلف با یک گراف در روش تصادفی مارکف (MRF) مدل‌سازی خواهد شد. درنهایت، روش انتشار باور بر روی این گراف انجام داده تا طبقه‌بندی با دقت بیشتر انجام گردد. به همین منظور تغییراتی در مدل مارکف انجام می‌شود که با تعریف تابع لبه و تابع گره نتایج بهتری کسب خواهد شد. در بخش های بعد این روش به صورت جزئی‌تر بررسی می‌گردد. این مقاله در ادامه به‌صورت زیر سازماندهی شده است:

با توجه به این‌که روش طبقه‌بندی جمعی در این مقاله استفاده شده است، در بخش ۲ به این مباحث پرداخته می‌شود.

1- Collective classification

2- Support Vector Data Descriptor

در بخش ۳، مدل پیشنهادی را برای شبکه حراجی الکترونیکی تعریف کرده و سپس در بخش ۴، به الگوریتم پیشنهادی برای تشخیص افراد متقلب در حراجی پرداخته می‌شود. در بخش ۵ نیز به آزمایشات پرداخته می‌شود و در بخش ۶ به نتیجه‌گیری پرداخته می‌شود.

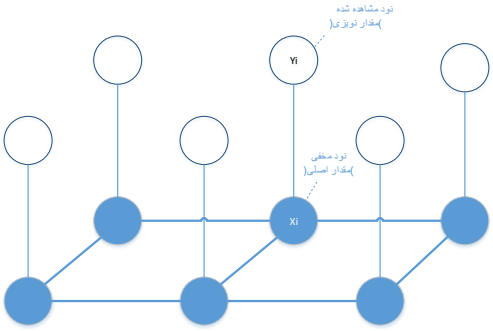
۲- طبقه‌بندی جمعی

طبقه‌بندی افراد متقلب می‌تواند توسط روش طبقه‌بندی جمعی انجام شود. در واقع، در این روش یک مدل پیش بینی از داده‌های شبکه ساخته می‌شود. این روش، روش ترکیبی از طبقه‌بندی یک مجموعه از موجودیت های به هم مرتبط می‌باشد که در این طبقه‌بندی سه نوع ارتباط ۱) ارتباط بین برچسب گره و مقدار مشاهده شده گره ۲) ارتباط بین برچسب گره و مقدار مشاهده شده گره همسایه و ۳) ارتباط بین برچسب گره و برچسب های مشاهده نشده گره وجود دارد [۱۶،۴]. یکی از انواع طبقه‌بندی جمعی، روش انتشار باور[1] تکراری می‌باشد که در ادامه توضیح می‌دهیم. این روش بر مبنای تئوری هموفیلی می‌باشد که گره‌هایی که به هم متصل می‌شوند، تمایل دارند به یک کلاس تعلق داشته باشند. روش انتشار باور حلقه‌ای[2] که بر روی مدل تصادفی مارکف (MRF)[3] اعمال می‌شود، یکی از روش‌های تقریبی استنتاج می‌باشد که برای طبقه‌بندی جمعی به‌کار می‌رود [۴].

مدل تصادفی مارکف نیز، نوعی از مدل گرافیکی برای حل مسائل استنتاج با توجه به داده مشاهده شده می‌باشد. شکل (۱) یک مثال از مدل تصادفی مارکف را نشان می‌دهد. این مدل از یک گراف بدون جهت تشکیل شده است که دارای گره‌های مخفی[4] و گره‌های مشاهده شده[5] می‌باشد که حالات مختلف دارند. گره‌های مخفی (w) گره‌هایی هستند که داده نویزی دارند و می‌خواهیم مقدار واقعی داده را از آن استنتاج نماییم. به‌ازای هر گره مخفی، یکسری اطلاعات مشاهده شده درباره گره (y) وجود دارد. گره‌های مشاهده شده در شکل با دایره توخالی و گره‌های مخفی با دایره توپر نشان داده شده‌اند. در این مدل فرض بر این است که اگر w و y را دو گره همسایه در گراف در نظر بگیریم، ارتباط آماری بین دوگره w و y وجود دارد که با نام تابع پتانسیل لبه ψ_{wy} شناخته می‌شود. همچنین به هر گره w مقداری به نام پتانسیل گره[6] φ_w نسبت داده می‌شود که باور آن گره را نمایش می‌دهد. مهم ترین موضوع در میدان های تصادفی مارکف نحوه تعریف همسایگی گره می‌باشد.

روش انتشار باور، یک الگوریتم انتشار پیغام در مدل های گرافیکی می‌باشد که باور هر گره بر مبنای همسایه‌ها تعیین می‌شود. اگر $m_{yw}(x_w)$ را پیغامی درنظر بگیریم که از گره y به گره w ارسال می‌شود، با رابطه (۱) می‌توان آن را محاسبه نمود [۱۷]. همانطور که این رابطه نشان می‌دهد، پیغام m_{yw} از ضرب همه پیغام‌های همسایگان y به غیر از w به‌دست می‌آید.

$$m_{yw}(x_w) = \sum_{x_i} \psi_y(x_w)\psi_{yw}(x_y, x_w) \prod_{k\in\Gamma_y\setminus\{w\}} m_{ky}(x_y), \qquad (۱)$$



شکل (۱): مثال از مدل تصادفی مارکف

در این رابطه Γ_w مجموعه همسایگان گره w است. سپس هر گره باورش را با توجه به پیغام‌هایی که از طرف همسایگانش به او فرستاده می‌شود، به‌روزرسانی می‌نماید. با توجه به رابطه (۲) باور هر گره w از ضرب همه مشاهدات و همه پیغام‌هایی که از همسایگان w فرستاده می‌شود، به‌دست می‌آید.

$$b_w(x_w) = C\psi_w(x_w) \prod_{y\in\Gamma(w)} m_{yw}(x_w) \qquad (۲)$$

در این رابطه، C ثابت عادی‌سازی است.

۳- مدل پیشنهادی برای شبکه حراجی الکترونیکی

هر شبکه حراجی از مجموعه کاربران تشکیل‌شده که این کاربران فروشنده یا خریدار هستند. فروشنده حراجی، یک حراجی را ایجاد می‌نماید و کالایی را برای فروش پیشنهاد می‌دهد؛ خریدار یا پیشنهاد دهنده نیز قیمت پیشنهادی کالای مورد نظر خود را به فروشنده پیشنهاد می‌نماید. در واقع روابط بین کاربران با توجه به پیشنهادهای پیشنهاد دهندگان در حراجی‌ها تعریف می‌گردد.

1- Belief Propagation
2- Loopy Belief Propagation
3- Markov Random Field
4- Hidden Node
5- Observed Node
6- Node potential

هرکاربر می‌تواند به‌صورت همزمان در یک حراجی یا در حراجی‌های مختلف، هم فروشنده و هم خریدار باشد.

شبکه حراجی به‌صورت $N = (U, A, B)$ تعریف می‌گردد که U مجموعه کاربران، A مجموعه حراجی، B مجموعه پیشنهادها می‌باشد.

اگر در شبکه حراجی، حراجی $a \in A$ و کاربر $u \in U$ داشته باشیم، برای ادامه مجموعه‌های زیر با کمک ۳ مجموعه اصلی بالا تعریف می‌گردد:

- B_a، مجموعه پیشنهادهایی که در حراجی a داده شده است.
- U_a، مجموعه کاربرانی که در حراجی a پیشنهاد داده‌اند.
- $T_a^{\rightarrow}$، زمانی که حراجی a ایجاد شده است.
- $\Delta T_a^{\rightarrow}$، مدت زمانی که حراجی a اعتبار دارد.
- $T_u^{\leftarrow}$، مجموعه زمان‌هایی که کاربر u در آنها پیشنهاد داده است.
- $A_u^{\rightarrow}$، مجموعه حراجی‌هایی که توسط فروشنده u ایجاد شده است.
- $A_u^{\leftarrow}$، مجموعه حراجی هایی که کاربر u در آنها پیشنهاد داده است.
- $A_u^{\leftarrow +}$، مجموعه حراجی‌هایی که کاربر u در آن‌ها برنده شده است.
- $B_{u,a}$، مجموعه پیشنهادهایی که توسط کاربر u در حراجی a داده شده است.

۴- الگوریتم پیشنهادی

در این بخش، الگوریتم پیشنهادی توضیح داده می‌شود که روشی برای تشخیص افراد متقلب همکار در شبکه حراجی می‌باشد. این الگوریتم در دو گام انجام می‌شود: گام اول استخراج ویژگی‌ها در شبکه حراجی می‌باشد و گام دوم محاسبه طبقه‌بندی کاربران با استفاده از ویژگی‌های استخراج‌شده می‌باشد.

۴-۱- استخراج ویژگی‌ها

یکی از مهمترین الزامات برای تشخیص رفتارهای ناهنجار، شناخت رفتار عادی کاربران حراجی می‌باشد تا بتوان ناهنجاری‌ها و حمله‌ها را که به‌عنوان انحراف از حالت عادی تعریف می‌شود، تشخیص داد. گام نخست در شناخت رفتار عادی کاربران، توصیف دقیق و جامع ویژگی‌ها و رفتار کاربران می‌باشد. این توصیف، اغلب با تعریف ویژگی صورت می‌پذیرد و به تبع آن رفتار عادی به‌عنوان قیدی روی مقدار ویژگی‌های تعریف شده یا رابطه‌ای مابین ویژگی‌ها تعریف می‌شود. در این مرحله، ابتدا اطلاعات مجموعه‌ای از کاربران عادی به‌عنوان ورودی دریافت گردیده و سپس برای هر کاربر یک بردار ویژگی محاسبه می‌گردد. ضمنا ۱۰ ویژگی موثر برای تشخیص ناهنجاری شناسایی گردیده است. این ویژگی‌ها بر اساس ویژگی اغلب فروشنده‌های متقلب و پیشنهاد دهنده‌های متقلب انتخاب شده است، مانند اینکه معمولا فروشنده‌های متقلب تعداد زیادی حراجی ایجاد مینمایند تا کاربران بیشتری را اغفال نمایند؛ همچنین معمولا پیشنهاد دهنده‌های متقلب تعداد زیادی پیشنهاد را می‌فرستند تا قیمت را افزایش دهند و تعداد زیادی از حراجی‌ها را می‌بازند. همچنین کاربران متقلب در ابتدا و انتهای بازه زمانی تعداد پیشنهادهای بیشتری را می‌فرستند تا بتوانند بر روی قیمت حراجی تاثیر گذار باشند. در ادامه به این ویژگی‌ها پرداخته می‌شود:

۱) متوسط تعداد پیشنهادهای کاربر در یک چهارم زمان ابتدایی حراجی

$$v1 = |T_u^{\leftarrow} < T_a + 1/4\Delta T_a^{\rightarrow}| \quad (۳)$$

۲) متوسط تعداد پیشنهادهای کاربر در یک چهارم زمان انتهایی حراجی

$$v2 = |T_u^{\leftarrow} > T_a + 3/4\Delta T_a^{\rightarrow}| \quad (۴)$$

۳) تعداد پیشنهاددهندگان در حراجی‌هایی که کاربر u راه‌اندازی نموده است.

$$v3 = \sum_{a \in \vec{A}_u} |U_a| \quad (۵)$$

۴) تعداد حراجی‌هایی که کاربر u در آنها مشارکت کرده است.

$$v4 = |\vec{A}_u| \quad (۶)$$

۵) تعداد کل حراجی‌هایی که کاربر u برنده شده است:

$$v5 = |A_u^{\leftarrow +}| \quad (۷)$$

۶) تعداد پیشنهاددهندگان متمایزی که با کاربر u در حراجی‌های یکسان مشارکت داشته‌اند.

$$v6 = \left| \bigcup_{a \in \vec{A}_u} U_a \setminus \{u\} \right| \quad (۸)$$

۷) متوسط تعداد پیشنهادها در حراجی‌هایی که کاربر u راه‌اندازی کرده است.

$$v7 = \frac{\sum_{a \in \vec{A}_u} |B_a|}{|\vec{A}_u|} \quad (۹)$$

۸) تعداد کل حراجی‌هایی که کاربر u راه‌اندازی نموده است.

$$v8 = |\vec{A}_u| \quad (۱۰)$$

۹) متوسط تعداد پیشنهادها در حراجی‌هایی که کاربر u راه‌اندازی نموده است.

$$v9 = \frac{\left|\bigcup_{a\in\vec{A}_u} B_a\right|}{|B|} \quad (۱۱)$$

۱۰) تعداد پیشنهادهای کاربر u در حراجی‌هایی که در آن‌ها بازنده شده است.

$$v10 = \sum_{a\in\vec{A}_u} |B_{u,a}| \quad (۱۲)$$

۴-۲- طبقه‌بندی

در فرآیند آموزش در روش های طبقه‌بندی دو یا چند کلاسی، داده‌های مربوط به همه کلاس‌ها موجود می‌باشد؛ در صورتی که در مساله تشخیص ناهنجاری پیشنهادی از روش تک دسته‌بند استفاده شده که در هنگام توصیف رفتار عادی مجموعه، داده حمله وجود ندارد و در فرآیند آموزش فقط داده‌های مربوط به یک کلاس (کلاس رفتار عادی) موجود می‌باشد. به‌منظور طبقه‌بندی، فقط داده‌های مربوط به یک کلاس درنظر گرفته می‌شود و با توجه به این داده‌ها، رفتار کلاس عادی با استفاده از دسته بندهای تک کلاسی یادگیری می‌شود و سپس هر انحرافی از این رفتار عادی به عنوان ناهنجاری درنظر گرفته می‌شود.

در روش‌های طبقه‌بندی تک کلاسی، پارامتر شباهت یک کاربر به کلاس عادی و همچنین پارامتر حد آستانه فاصله یا شباهت مهم می‌باشد. اگر یک کاربر از کلاس عادی فاصله کمتر از پارامتر حد آستانه داشته باشد، عادی می‌باشد و در غیر این صورت، غیرعادی طبقه‌بندی می‌شود. یکی از روش‌های تک دسته‌بند، روش SVDD می‌باشد که در طراحی آن از مفهوم ماشین بردار پشتیبان[1] استفاده شده است [۱۸].

این روش یک ابر کره با حداقل شعاع را بر روی کلاس عادی محاط می‌کند و محدوده این کره توسط کاربران کلاس عادی تعیین می‌شود. این کاربران، بردار پشتیبان هستند و فاصله آن‌ها از کلاس عادی مطابق رابطه (۱۳) به‌دست می‌آید:

$$D_{SVDD}(w) = k(w,w) - 2\sum_i a_i * k(w,w_i) + \sum_{i,j} \alpha_i\alpha_j * k(w_i,w_j) \quad (۱۳)$$

در این رابطه، k نشان دهنده تابع هسته و w_iها نشان دهنده بردارهای پشتیبان و α_i ضریب لاگرانژ منتسب به بردار پشتیبان w_i می‌باشد.

به همین منظور بعد از محاسبه بردار ویژگی برای کاربران عادی، یک مدل از رفتارهای کاربران عادی ساخته شده و از بردار ویژگی تعدادی از کاربران عادی استفاده می‌گردد تا بتوان مشخصات کلاس موجود را یادگیری نمود. در واقع با توجه به مدل رفتاری که از کاربران عادی یاد گرفته شد، بقیه کاربران نیز برچسب گذاری خواهد شد. در این روش از الگوریتم طبقه‌بندی SVDD استفاده خواهد شد و کاربران عادی نیز در مجموعه+L طبقه‌بندی می‌گردد. در واقع $D_{SVDD}(w)$ عددی است که فاصله کاربر w را از کلاس عادی نشان می‌دهد.

سپس مطابق بخش ۲ از مدل تصادفی مارکف استفاده خواهد شد. همان‌طور که قبلا اشاره شد، مدل تصادفی مارکف از اطلاعات قبلی برای تابع پتانسیل گره برای هر کاربر استفاده می‌نماید و از تابع پتانسیل لبه برای ارتباط همبستگی بین دوکاربر همسایه استفاده می‌نماید. این دوتابع به صورت زیر تعریف می‌گردد:

تعریف تابع پتانسیل گره برای هر کاربر: چنانچه $\beta > 0$ پارامتر ثابت عادی سازی درنظر گرفته شود، θ_w را با توجه به رابطه (۱۴) می‌توان محاسبه نمود:

$$\theta_w = \begin{cases} 0 & \text{if } w \in L^+, \\ \dfrac{1}{1+\exp(-D_{SVDD}(w)/\beta)} & \text{if } w \notin L^+, \end{cases} \quad (۱۴)$$

که با توجه به آن، تابع پتانسیل گره از رابطه (۱۵) محاسبه گردید:

$$\psi_w(x_w) = \begin{cases} 1-\theta_w & \text{if } X_w = +1, \\ \theta_w & \text{if } X_w = -1, \end{cases} \quad (۱۵)$$

تعریف تابع پتانسیل لبه برای هر ارتباط بین دو کاربر: برای محاسبه تابع پتانسیل لبه $w = (w_1, w_2, w_3, \dots, w_{10})$ و $y = (y_1, y_2, y_3, \dots, y_{10})$ که $(w, y) \in E$ از معیار شباهت[2] استفاده خواهد شد. در واقع از معیار شباهت جهت بهبود کارآیی مدل تصادفی مارکف استفاده خواهد شد. بر این اساس هر چه اختلاف بین مقادیر یک ویژگی در دو گره انتخاب شده کمتر باشد، شباهت بیشتری بین دوگره وجود دارد و در واقع اختلاف بیشتر، فاصله معناداری بین مقادیر نمونه‌های یک کلاس وسایر کلاس(ها) نشان می‌دهد. با توجه به بخش ۴-۱ بردار ویژگی برای هر کاربر تعریف می‌شود که شامل ۱۰ تعداد ویژگی می‌باشد و به‌عنوان یک نقطه در فضای n بعدی قابل نمایش می‌باشد. بنابراین، در اینجا از فاصله L1-norm به‌عنوان معیار شباهت در فضای n بعدی استفاده شده است. در واقع این معیار، معیار فاصله می‌باشد که برای محاسبه میزان تفاوت بین دو نمونه به‌کار می‌رود. فاصله L1-norm بین دو کاربر یا دو نقطه w, y در این فضای n بعدی از رابطه (۱۶) محاسبه می‌شود [۱۹]:

1- Support vector machine (SVM)

2- Similarity Measures

$$D_{L1} = \sum_i |(w_i - y_i)| \qquad (۱۶)$$

تابع پتانسیل لبه را با استفاده از معیار شباهت یا فاصله تعریف نموده ($\vartheta_{wy} = D_{L1}$) و آن از رابطه (۱۷) محاسبه خواهد شد:

$$\psi_{wy}(x_w, x_y) = \begin{cases} \vartheta_{wy} & \text{if } x_w x_y = +1\,, \\ 1 - \vartheta_{wy} & \text{if } x_w x_y = -1\,, \end{cases} \qquad (۱۷)$$

در اینجا ϑ_{wy} با توجه به فاصله L1-norm محاسبه خواهد شد تا نشان داده شود که دو کاربر w, y ارتباط مثبت با یکدیگر دارند و احتمالا دارای برچسب‌های یکسان می‌باشند. یعنی چنانچه یکی عادی باشد، به احتمال زیاد همسایه عادی دارد و در غیراین‌صورت چنانچه یکی متقلب باشد، با همسایه‌های متقلب خود تبانی خواهد نمود.

سپس از روش انتشار باور استفاده گردید تا توزیع پسین[1] برای هر متغیر تصادفی از کاربران برچسب نخورده را محاسبه نماید. همان‌طور که قبلا در بخش ۲-۳ اشاره شد، این روش با توجه به ارتباط پیغام‌ها بین همسایه‌ها، باور هر گره را از همسایه خود به‌دست می‌آورد. پیغامی‌که از کاربر $w \in U$ به کاربر $y \in U$ در زمان t فرستاده می‌شود، با رابطه (۱۸) به‌دست می‌آید:

$$m_{wy}^{(t)}(x_w) = \sum_{x_w} \varphi_y^{L^+}(x_y)\psi_{wy}(x_w, x_y) \prod_{k \in \Gamma_Y \setminus \{w\}} m_{ky}(x_y)\,. \qquad (۱۸)$$

سپس باور هر کاربر برچسب نخورده $w \in U \setminus L^+$ را با رابطه ۱۹

$$b_w(x_w) = K\psi_w^{L^+}(x_w) \prod_{y \in \Gamma_w} m_{yw}(x_w)\,. \qquad (۱۹)$$

محاسبه نموده و با توجه به خروجی این رابطه، کاربران برچسب نخورده با عادی و متقلب برچسب گذاری خواهد شد.

چنانچه σ را پارامتر حد آستانه تعریف‌شده توسط کاربر درنظر گرفته شود، اگر در آخرین تکرار، مقدار $b_w(+1) > \sigma$ باشد، کاربر را عادی در نظر گرفته و در غیر این صورت متقلب خواهد بود.

۵- نتایج و آزمایشات

در این بخش نتیجه با توجه به معیار اندازه گیری، نتایج ارزیابی آمده است.

۵-۱- معیار اندازه‌گیری کارآیی

برای اندازه‌گیری کارآیی مدل، برچسب‌هایی که برای کاربران مجموعه تست، توسط مدل تخمین زده می‌شود با برچسب واقعی کاربر مقایسه می‌گردد. به‌منظور مقایسه کارآیی روش پیشنهادی از معیار TPR[2] (نشان‌دهنده دقت تشخیص کلاس عادی) و معیار FPR[3] (نشان‌دهنده نرخ هشدار غلط با توجه به دسته غیرعادی) استفاده می‌شود. این معیارها از روابط (۲۰-۲۱) محاسبه می‌گردند:

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}\,, \qquad (۲۰)$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}\,, \qquad (۲۱)$$

در این معامله‌ها، TN تعداد رکوردهایی را نشان می‌دهد که کلاس واقعی آنها غیرعادی بوده و الگوریتم طبقه‌بندی نیز دسته آنها را به‌درستی غیرعادی تشخیص داده است. متغیر TP تعداد رکوردهایی را نشان می‌دهد که دسته واقعی آنها عادی بوده و الگوریتم طبقه‌بندی نیز دسته آنها را به‌درستی عادی تشخیص داده است. متغیر FP تعداد رکوردهایی را نشان می‌دهد که دسته واقعی آنها غیرعادی بوده و الگوریتم طبقه‌بندی دسته آنها را به اشتباه عادی تشخیص داده است. متغیر FN تعداد رکوردهایی را نشان می‌دهد که دسته واقعی آنها عادی بوده و الگوریتم طبقه‌بندی دسته آنها را به اشتباه غیرعادی تشخیص داده است.

۵-۲- پایگاه‌داده

در این مقاله، پایگاه‌داده مقاله [۱۴] استفاده شده است. این پایگاه داده شامل ۶۰ مجموعه داده می‌باشد که شامل درخواست‌های عادی و غیرعادی کاربران در حراجی می‌باشد و سه نوع حمله زیر را شامل می‌شود:

تقلب در اعتبار[4]: این تقلب زمانی رخ می‌دهد که تعدادی از پیشنهاد دهندگان با یک فروشنده خاص تبانی می‌نمایند تا اعتبار خود را بالا ببرند.

تقلب ستاره‌ای[5]: این رفتار متقلبانه نیز در زمانی می‌باشد که چندین پیشنهاد دهنده متقلب، پیشنهادهای خود را در حراجی‌ای می‌دهند که یک کاربر خاص راه‌اندازی نموده است.

تقلب حلقه‌ای[6]: این رفتار متقلبانه زمانی می‌باشد که یک گروه از کاربران متقلب هم به‌عنوان پیشنهاددهنده و هم به‌عنوان فروشنده با هم تبانی می‌نمایند.

1- Posterior distribution

2- True positive rate
3- False positive rate
4- Reputation Fraud
5- Collusive Star
6- Collusive Clique

جدول (۱): مشخصات کلی پایگاه‌داده

Datasets	Records Number	Number of Sellers in train data	Number of Bidders in train data	Percentage of Sellers in train data	Percentage of Bidders in train data
Reputation Fraud	۲۱۲۰۳/۶	۱۹۹۰/۵	۳۶۵/۵	%۹/۷	%۱۰
Collusive Star	۲۱۲۰۴/۱	۱۹۹۱/۸	۳۶۴/۲	%۹/۸	%۹/۹
Collusive Clique	۲۱۲۰۴	۱۹۹۵/۸	۳۶۰/۳	%۹/۸	%۹

از هرکدام از این حملات به تعداد ۲۰ مجموعه داده متفاوت در کل پایگاه داده موجود می‌باشد. برای آزمایش از کل رکوردهای موجود استفاده نموده و در هرمجموعه داده نتایج را میانگین گرفتیم. برای آزمایش ده درصد از رکوردها را به عنوان داده تست به صورت تصادفی انتخاب نمودیم. این مجموعه داده به صورت جدول (۱) می‌باشد. ستون اول تعداد کل رکوردهای موجود در مجموعه داده را نشان می‌دهد. ستون های دوم و چهارم به ترتیب تعداد کل فروشندگان و درصد فروشندگان را در مجموعه رکوردهای تستی نشان می‌دهند. ستون سوم و پنجم به ترتیب تعداد کل پیشنهاددهندگان و درصد پیشنهاد دهندگان را در مجموعه رکوردهای تستی انتخاب شده نشان می‌دهند.

۵-۳- نتایج ارزیابی

برای به‌دست آوردن کارآیی روش خود از کامپیوتر ۵ هسته‌ای با مشخصات ۱۶ گیگابایت حافظه داخلی و ویندوز ۷ استفاده شده است. جدول (۲) کارآیی روش پیشنهادی را در مقایسه با روش‌های دیگر با توجه به معیارهای TPR و FPR نشان می‌دهد. همان‌طور که مشخص می‌باشد، روش پیشنهادی به‌صورت قابل توجه بهتر از روش‌های SPAN و 2LFS عمل می‌نماید و عمل تشخیص افراد صادق و متقلب را با دقت بیشتری انجام می‌دهد.

برای تحلیل بیشتر، در ادامه به‌منظور تاثیر روش انتشار باور و همچنین تابع پتانسیل گره و تابع پتانسیل لبه بر روی عملکرد الگوریتم، در حالت‌های مختلف عملکرد الگوریتم را مورد بررسی قرار داده شد که نتایج آن بر حسب درصد در جدول (۳) آمده است. همان‌طور که ردیف اول این جدول نشان می‌دهد، کارآیی روش SPAN در [۱۵] بدون در نظر گرفتن مرحله انتشار باور بسیار پایین می‌باشد. در ردیف دوم کارآیی روش پیشنهادی بدون مرحله انتشار باور آورده شده است که با توجه به نتایج FPR بالایی دارد. در ردیف سوم کارآیی روش پیشنهادی بدون در نظر گرفتن تابع پتانسیل گره آورده شده است که در واقع تابع پتانسیل گره ثابت بوده و در رابطه (۱۵)، $\theta_w = 0.02$ قرار داده شده است. ردیف چهارم نتایج را با در نظر گرفتن تابع پتانسیل گره تعریف شده مطابق رابطه (۱۴) (بدون در نظر گرفتن تابع پتانسیل لبه) نشان می‌دهد و ردیف پنجم روش پیشنهادی را با در نظر گرفتن تابع پتانسیل گره و همچنین تابع پتانسیل لبه تعریف شده نشان می‌دهد. مقایسه جدول‌های (۲-۳) نشان می‌دهد که مرحله انتشار باور با محاسبه باور هر گره با توجه به باورهای گره‌های همسایه، در بهبود کارآیی روش SPAN تاثیر به سزایی دارد. همچنین جدول (۳) نشان می‌دهد که مرحله انتشار باور در بهبود کارآیی روش پیشنهادی نیز تاثیر زیادی دارد و باعث افزایش TPR و کاهش FPR شده است. این جدول اثر تابع پتانسیل گره و همچنین ترکیب اثر پتانسیل گره و لبه را نشان می‌دهد. با توجه به نتایج، انتخاب مقدار مناسب $\boldsymbol{\theta_w}$ برای تابع پتانسیل گره در کارآیی روش پیشنهادی تاثیر خوبی دارد. چنانچه $\boldsymbol{\theta_w}$ مقدار ثابتی در نظر گرفته شود، در واقع تنها برچسب هر کاربر در نظر گرفته‌شده و فاصله کاربران از کلاس نرمال درنظر گرفته نمی‌شود و به همین دلیل اثر کمتری در بهبود دارد. همان‌طور که مشخص می‌باشد چنانچه مرحله انتشار باور با تابع پتانسیل گره و لبه انجام شود، کارآیی روش پیشنهادی به‌طور چشم‌گیری افزایش می‌یابد

جدول (۲): مقایسه کارآیی روش پیشنهادی با روش‌های دیگر

Technique	Reputation Fraud		Collusive Star		Collusive Clique	
	TPR	*FPR*	*TPR*	*FPR*	*TPR*	*FPR*
2LFS	۱۳/۳	۱/۰	۱۴/۴	۱/۰	۳۱/۲	۱/۰
SPAN	۹۸/۹	۱/۰	۴۷/۶	۱/۰	۹۴/۴	۱/۰
روش پیشنهادی	۹۹/۹	۰/۶	۷۶/۹	۰/۶	۹۷/۵	۰/۶

جدول (۳): مقایسه کارآیی روش پیشنهادی با در نظرگرفتن توابع تعریف‌شده

Technique	Reputation Fraud		Collusive Star		Collusive Clique	
	TPR	*FPR*	*TPR*	*FPR*	*TPR*	*FPR*
بدون مرحله انتشار باور SPAN	۹/۱	۱/۰	۲۰/۴	۱/۰	۷۵/۸	۱/۰
روش پیشنهادی بدون مرحله انتشار باور	۷۶/۹	۵/۹	۸۶/۸	۵/۷	۹۲/۰	۵/۷
روش پیشنهادی با تابع پتانسیل گره ثابت $\boldsymbol{\theta_w = 0.02}$	۹۶/۵	۷/۴	۸۴/۵	۶/۳	۹۷/۲	۶/۲
روش پیشنهادی با تابع پتانسیل گره مطابق رابطه ۱۴	۹۵/۶	۳/۸	۸۲/۸	۴/۱	۹۷/۳	۴/۷
روش پیشنهادی با تابع پتانسیل گره و لبه	۹۹/۹	۰/۶	۷۶/۹	۰/۶	۹۷/۵	۰/۶

علاوه براین روش پیشنهادی نسبت به روش SPAN سریعتر همگرا می‌شود. همان‌طور که نتایج در جدول (۴) نشان می‌دهند، روش پیشنهادی برای هر سه نوع تقلب، در کمتر از ۱۰ تکرار همگرا می‌شود، درصورتی که در روش SPAN لازم است بیشتر از ۳۰ بار تکرار گردد تا همگرا شود. به همین دلیل، هزینه زمانی صرف شده برای این روش بسیار کمتر از روش SPAN می‌باشد و این یک مزیت مهم نسبت به روش SPAN می‌باشد.

جدول (۴): مقایسه تعداد حلقه تکرار LBP روش پیشنهادی با روش‌های دیگر

Technique	Reputation Fraud	Collusive Star	Collusive Clique
SPAN	۳۰-۴۰	۳۰-۴۰	۸۰-۹۰
روش پیشنهادی	۷/۹	۸/۵	۸/۴

۶- نتیجه‌گیری

در طی سال‌های گذشته، طبقه‌بندی کاربران مورد توجه بسیاری از پژوهشگران قرار گرفته است. در مسائل طبقه‌بندی، هدف این است که گروهی را که هر موجودیت به آن تعلق دارد را نشان دهد. به همین دلیل در دنیای امروز بحث طبقه‌بندی اطلاعات اهمیت بسیاری دارد. یکی از موارد کاربرد طبقه‌بندی، در بحث امنیت و طبقه‌بندی کاربران عادی و غیرعادی می‌باشد. با توجه به این‌که در دنیای امروز شبکه‌های اجتماعی زیادی وجود دارند که کاربران با یکدیگر در آن شبکه‌ها تعامل می‌کنند، تقلب پیچیده‌تر شده و حفظ امنیت شبکه نیاز به بررسی و تحقیق بیشتری دارد. یکی از انواع تقلب تبانی در تقلب می‌باشد که با همکاری کاربران انجام می‌شود. در دنیا به امنیت حراجی‌ها اهمیت زیادی داده شده است، زیرا مسائل مالی و ضررهای مالی زیادی می‌تواند به همراه داشته باشد. در این مقاله یک مدل ریاضی برای حراجی مطرح می‌گردد و سپس روشی پیشنهاد می‌گردد که بتوان به نحو دقیقی اطلاعات را طبقه‌بندی نمود. در ابتدا، مرحله استخراج ویژگی انجام می‌شود که با توجه به رفتار کاربران متقلب با سایر افراد، ویژگی‌های هر کاربر استخراج می‌گردد. سپس با روش SVDD طبقه‌بندی کاربران را انجام داده و با توجه به تابع پتانسیل لبه و گره که تعریف نمودیم، مدل مارکف را به مساله حراجی بهینه‌سازی نمودیم. سپس کارآیی روش پیشنهادی را با توجه به رفتارهای مختلف همکاری متقلبانه بررسی نمودیم. نتایج نشان می‌دهند که نرخ FP و TP بهبود یافته‌اند.

۷- منابع

[1] Y. Li, A. Tripathi, and A. Srinivasan, "Challenges in Short Text Classification: The Case of Online Auction Disclosure," p. 18, 2016.

[2] S. Ganguly and S Sadaoui, "Classification of Imbalanced Auction Fraud Data," Canadian Conference on Artificial Intelligence, pp. 84-89, 2017.

[3] I. Lee, "Big data: Dimensions, evolution, impacts, and challenges," Business Horizons, pp. 293-303, 2017.

[4] P. Sen, G. Namata, M. Bilgic, L. Getoor, B. Galligher, and T. Eliassi-Rad, "Collective classification in network data," AI magazine, 2008.

[5] MI. Melnik, "Confronting the Challenges of Asymmetry of Information and Competition: The Rise of eBay," InTrends and Innovations in Marketing Information Systems, pp. 293-307, 2015.

[6] DataStax, eBay Engages Customers with Personalized Recommendations, Aug. 2017.

[7] M. M. Flax, "Economic Crimes," San Clemente, CA, USA: LawTech Publishing Group, 2005.

[8] CH. Yu, "A Fuzzy Genetic Approach for Optimization of Online Auction Fraud Detection," Frontier Computing, pp. 965-974, 2016.

[9] DH. Chau and C. Faloutsos, "Fraud Detection Using Social Network Analysis, a Case Study, Encyclopedia of Social Network Analysis and Mining," pp. 547-552, 2014.

[10] A. Jamalyfard and H. Shirazi, "Web-based Military Management Systems Security Using Combination of One-class Classifiers," Journal of Electronical & Cyber Defence, vol. 3, no. 3, pp. 19-30, 2013. (in Persian)

[11] J. Li, KF. Tso, and F. Liu, "Profit earning and monetary loss bidding in online entertainment shopping: the impacts of bidding patterns and characteristics," Electronic Markets, pp. 77-90, 2017.

[12] D. H. Chau and C. Faloutsos, "Fraud detection in electronic auction," European Web Mining Forum Proceeding, pp. 87–97, 2005.

[13] TD. Kavu, T. Rugube, F. Kawondera, and N. Chifamba, "A fraud detection tool in E-auctions," African Journal of Mathematics and Computer Science Research, pp. 1–11, 2016.

[14] S. Pandit, D. Chau, S. Wang, and C. Faloutsos, "Netprobe: a Fast and Scalable System for Fraud Detection in Online Auction Networks," Conference on World Wide Web, vol. 42, pp. 201–210, 2007.

[15] S. Tsang, Y. S. Koh, G. Dobbie, and S. Alam, "SPAN: Finding Collaborative Frauds in Online Auctions," Knowledge-Based Syst., vol. 71, pp. 389–408, 2014.

[16] Q Wu, Y. Ye, S. S. Ho, and S. Zhou, "Semi-supervised multi-label collective classification ensemble for functional genomics," BMC genomics, vol. 15, no. 9, 2014.

[17] K. P. Murphy, Y. Weiss, and M. I. Jordan, "Loopy belief propagation for approximate inference: An empirical study," 15th Conference Uncertainty in Artificial Intelligence, pp. 467–475, 1999.

[18] D. Tax and R. Duin, "Support vector domain description," Pattern Recognition Letters, vol. 20, no. 11-13, pp. 1191– 1199, 1999.

[19] AA. Goshtasby, "Similarity and dissimilarity measures," In Image registration, pp. 7-66, 2012.

Journal of Electronical & Cyber Defence
Vol. 7, No. 1, 2019, Serial No. 25

Collusive Fraud Classification in Network of Online Auction Using Similarity Measure in Collective Classification

M. Dadfarnia, F. Adibnia*

*Department of Computer Engineering, Yazd University
(Received: 11/02/2018, Accepted: 13/10/2018)

ABSTRACT

Nowadays, data classification is extremely important used with the purpose of identifying the features that indicate the group of the classification of each item. Classification of the user auctions is one of the usages of classification. In previous years, electronic auctions have become more important, so detecting fraudulent activities has attracted attention of many researchers. One type of fraud is the collusion of fraudulent users at the auction, which is a very dangerous type of fraud and if occurred, may lead to irreparable financial losses. In this paper, we propose a method that first extracts the effective features for finding normal people in the auction and then classifies the users by collective classification method. We define an edge potential function to use in collective classification, in which it uses the distance L1-norm as the similarity measure between the two adjacent nodes. The results show that the defined edge potential function is suitable for improving the classification rate of collaborative fraudulent users.

Keywords: Similarity Measure, Collective Classification, L1-norm, Markov Random Field, Loopy Belief Propagation

* Corresponding Author Email: fadib@yazd.ac.ir