بسمه تعالی

موضوع

تشخیص تقلب در کارت اعتباری:
یک مدل سازی واقع بینانه و یک استراتژی یادگیری جدید

درس

یادگیری ماشین

اساتید

دکتر یغمایی - شکری

گردآورنده

حوا عسکری

400I1920006 : ش.د

خلاصه

شناسایی تقلب در تراکنش‌های کارت اعتباری شاید یکی از بهترین بسترهای آزمایشی برای الگوریتم‌های هوش محاسباتی باشد. در واقع، این مشکل شامل تعدادی چالش مرتبط است، از جمله: تغییر مفهوم (عادات مشتریان تکامل می‌یابد و کلاهبرداران استراتژی‌های خود را در طول زمان تغییر می‌دهند)، عدم تعادل طبقه (تعداد معاملات واقعی بسیار بیشتر از تقلب‌ها) و تأخیر تأیید (فقط مجموعه کوچکی از تراکنش‌ها به موقع توسط بازرسان بررسی می شوند). با این حال، اکثریت قریب به اتفاق الگوریتم‌های یادگیری که برای کشف تقلب پیشنهاد شده‌اند، بر مفروضاتی تکیه می‌کنند که به سختی در یک سیستم تشخیص تقلب در دنیای واقعی (FDS) وجود دارند. این فقدان واقع‌گرایی به دو جنبه اصلی مربوط می‌شود:

1) روش و زمان‌بندی ارائه اطلاعات تحت نظارت

2) اقدامات مورد استفاده برای ارزیابی عملکرد کشف تقلب.

این مقاله سه سهم عمده دارد. اول، ما با کمک شریک صنعتی خود، رسمی کردن مشکل کشف تقلب را پیشنهاد می کنیم که به طور واقع بینانه شرایط عملیاتی FDS هایی را که هر روز جریان های عظیم تراکنش های کارت اعتباری را تجزیه و تحلیل می کنند، توصیف می کند. ما همچنین مناسب‌ترین معیارهای عملکردی را که برای اهداف کشف تقلب استفاده می‌شود، نشان می‌دهیم. دوم، ما یک استراتژی یادگیری جدید را طراحی و ارزیابی می‌کنیم که به طور موثر عدم تعادل کلاس، جابجایی مفهوم و تأخیر تأیید را بررسی می‌کند. سوم، در آزمایش‌های خود، تأثیر عدم تعادل طبقاتی و رانش مفهومی را در جریان داده‌های دنیای واقعی حاوی بیش از ۷۵ میلیون تراکنش، که در یک بازه زمانی سه ساله مجاز است، نشان می‌دهیم.

1-مقدمه

تشخیص تقلب کارت اعتباری یک مشکل مرتبط است که توجه جوامع یادگیری ماشینی و هوش محاسباتی را به خود جلب می کند، جایی که تعداد زیادی راه حل خودکار پیشنهاد شده است. در واقع، به نظر می رسد که این مشکل از منظر یادگیری چالش برانگیز باشد، زیرا در عین حال با عدم تعادل طبقاتی مشخص می شود، یعنی، تعداد تراکنش‌های واقعی بسیار بیشتر از تقلب‌ها است، و مفهوم منحرف می‌شود، یعنی تراکنش‌ها ممکن است ویژگی‌های آماری خود را در طول زمان تغییر دهند. با این حال، اینها تنها چالش هایی نیستند که مشکلات یادگیری را در یک سیستم کشف تقلب در دنیای واقعی (FDS) مشخص می کنند.

در یک FDS دنیای واقعی، جریان عظیم درخواست‌های پرداخت به سرعت توسط ابزارهای خودکار اسکن می‌شوند که تعیین می‌کنند کدام تراکنش‌ها باید مجاز باشند. طبقه بندی کننده ها معمولاً برای تجزیه و تحلیل

تمام تراکنش های مجاز و هشدار دادن به مشکوک ترین تراکنش ها استفاده می شوند. سپس هشدارها توسط بازرسان حرفه‌ای بازرسی می‌شوند که با دارندگان کارت تماس می‌گیرند تا ماهیت واقعی (اعم از واقعی یا تقلبی) هر تراکنش هشدار داده شده را تعیین کنند. با انجام این کار، محققین بازخوردی به سیستم در قالب تراکنش‌های برچسب‌گذاری شده ارائه می‌کنند که می‌تواند برای آموزش یا به‌روزرسانی طبقه‌بندی‌کننده استفاده شود تا عملکرد کشف تقلب در طول زمان حفظ شود (یا در نهایت بهبود یابد). اکثریت قریب به اتفاق تراکنش ها نمی توانند توسط محققین برای محدودیت های زمانی و هزینه ای آشکار تأیید شوند. این تراکنش‌ها بدون برچسب باقی می‌مانند تا زمانی که مشتریان تقلب‌ها را کشف و گزارش ندهند، یا تا زمانی که زمان کافی سپری شود به طوری که تراکنش‌های بدون مناقشه واقعی تلقی شوند.

بنابراین، در عمل، اکثر نمونه های نظارت شده با تاخیر قابل توجهی ارائه می شوند، مشکلی که به عنوان تأخیر تأیید شناخته می شود. تنها اطلاعات نظارت شده اخیری که برای به‌روزرسانی طبقه‌بندی‌کننده در دسترس است، از طریق تعامل هشدار-بازخورد ارائه می‌شود. اکثر مقالات در ادبیات، تأخیر تأیید و همچنین تعامل هشدار-بازخورد را نادیده می‌گیرند و به طور غیرواقعی فرض می‌کنند که برچسب هر تراکنش به طور منظم در دسترس FDS قرار می‌گیرد، به عنوان مثال، به صورت روزانه. با این حال، این جنبه‌ها باید هنگام طراحی یک FDS دنیای واقعی در نظر گرفته شوند، زیرا تأخیر تأیید در هنگام رخ دادن مفهوم مضر است، و تعامل هشدار-بازخورد مسئول نوعی سوگیری انتخاب نمونه (SSB) که تفاوت‌های بیشتری را بین توزیع داده های آموزش و آزمون است.

تفاوت مهم دیگر بین آنچه معمولاً در ادبیات انجام می شود و شرایط عملیاتی دنیای واقعی سیستم تشخیص تقلب (FDS) مربوط به اقدامات مورد استفاده برای ارزیابی عملکرد کشف تقلب است. اغلب، معیارهای رتبه‌بندی جهانی، مانند ناحیه زیر منحنی ROC (AUC)، یا معیارهای مبتنی بر هزینه استفاده می‌شوند، اما اینها این واقعیت را نادیده می‌گیرند که فقط تعداد کمی از هشدارها را می‌توان روزانه کنترل کرد، و شرکت‌ها به شدت نگران دقت هشدارهای تولید شده اند.

سهم اصلی این مقاله به شرح زیر است:

1) ما مکانیسم‌های تنظیم کننده یک FDS واقعی را توصیف می‌کنیم و یک مدل رسمی از مشکل طبقه‌بندی مفصل ارائه می‌کنیم تا در تشخیص تقلب مورد توجه قرار گیرد.
2) ما معیارهای عملکردی را معرفی می‌کنیم که در یک FDS واقعی در نظر گرفته می‌شوند.
3) در این مدل صحیح و واقع بینانه، ما یک استراتژی یادگیری موثر برای پرداختن به چالش‌های فوق، از جمله تأخیر تأیید و تعامل هشدار-بازخورد پیشنهاد می‌کنیم. این استراتژی یادگیری بر روی تعداد زیادی از تراکنش های کارت اعتباری آزمایش شده است.

این مقاله به شرح زیر تنظیم شده است. ما ابتدا شرایط عملیاتی یک FDS دنیای واقعی را در بخش 2 به تفصیل شرح می‌دهیم، و سپس در بخش 3 مشکل آشکارسازی تقلب را مدل می‌کنیم و مناسب‌ترین معیارهای عملکرد را ارائه می‌کنیم. به‌ویژه، ما فکر می‌کنیم که مناسب‌ترین ارزیابی تعداد تراکنش‌های (یا کارت‌های) جعلی کشف‌شده بر روی حداکثر تعداد تراکنش‌ها (یا کارت‌هایی) است که بازرسان می‌توانند بررسی کنند. چالش‌های اصلی که هنگام آموزش یک طبقه‌بندی کننده برای اهداف کشف تقلب مطرح می‌شوند، سپس در بخش 4 مورد بحث قرار می‌گیرند. بخش 5 استراتژی یادگیری پیشنهادی را معرفی می‌کند، که شامل آموزش جداگانه طبقه‌بندی کننده‌های مختلف از بازخوردها و نمونه‌های نظارت شده با تأخیر، و سپس جمع‌آوری پیش‌بینی‌های آن‌ها است. این استراتژی، با الهام از ماهیت متفاوت بازخوردها و نمونه‌های نظارت شده با تأخیر، به ویژه در FDS با استفاده از پنجره کشویی یا مجموعه طبقه‌بندی‌کننده‌ها مؤثر است. ما ادعاهای خود را در آزمایش‌ها (بخش 6) روی بیش از 75 میلیون تراکنش کارت اعتباری تجارت الکترونیکی که طی سه سال به دست آمده‌اند، تأیید می‌کنیم، که همچنین برای مشاهده تأثیر عدم تعادل طبقاتی و تغییر مفهوم در جریان‌های تراکنش در دنیای واقعی تجزیه و تحلیل می‌شوند.

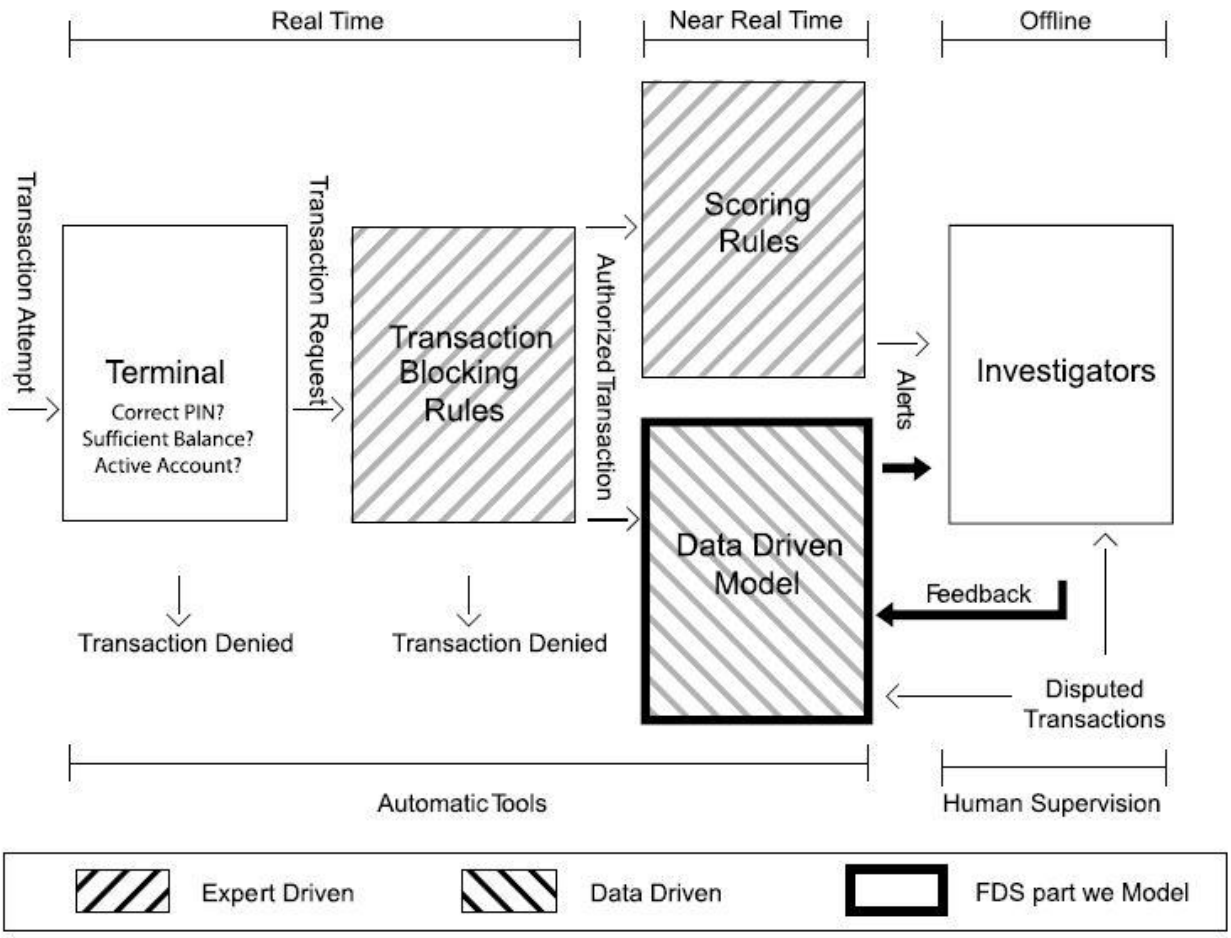
کار ما بر اساس [1] است، که به طور قابل توجهی با توصیف جزئیات شرایط عملیاتی در دنیای واقعی یک FDS و با تجزیه و تحلیل SSB معرفی شده توسط تعامل هشدار-بازخورد گسترش می‌یابد. علاوه بر این، بخش تجربی با ارائه تجزیه و تحلیل اضافی در دو مجموعه داده بزرگ تا حد زیادی به روز و تکمیل شده است.

2- FDS دنیای واقعی

در اینجا ما ویژگی های اصلی و شرایط عملیاتی یک FDS در دنیای واقعی را شرح می دهیم، که با الهام از موردی که به طور معمول توسط شریک صنعتی ما استفاده می شود، الهام گرفته شده است. شکل 1 پنج لایه کنترل را نشان می دهد که معمولاً در یک FDS استفاده می شود:

1) ترمینال 2) قوانین مسدود کردن معاملات 3) قوانین امتیازدهی 4) مدل داده محور (DDM) 5) محققین

لایه های (1-4) به طور کامل کنترل های خودکار را اجرا می کنند، در حالی که لایه 5 تنها لایه ای است که نیاز به دخالت انسان دارد.



شکل 1: طرحی که لایه های کنترل را در یک FDS نشان می دهد. تمرکز ما عمدتا بر روی DDM و تعامل هشدار-بازخورد است، که نحوه ارائه نمونه‌های نظارت شده اخیر را تنظیم می‌کند.

A. لایه های کنترل در یک FDS

1) **ترمینال:** ترمینال اولین لایه کنترلی را در یک FDS نشان می دهد و بررسی های امنیتی معمولی را روی تمام درخواست های پرداخت انجام می دهد. بررسی‌های امنیتی شامل کنترل کد پین (فقط در مورد کارت‌هایی که دارای تراشه هستند امکان پذیر است)، تعداد تلاش‌ها، وضعیت کارت (فعال یا مسدود شده)، موجودی موجود و محدودیت هزینه‌ها. در صورت تراکنش های آنلاین، این عملیات باید به صورت بلادرنگ انجام شود (پاسخ باید در چند میلی ثانیه ارائه شود)، که طی آن ترمینال از سرور شرکت صادرکننده کارت استعلام می گیرد. درخواست هایی که از هیچ یک از این کنترل ها عبور نمی کنند رد می شوند، در حالی که بقیه به درخواست های تراکنش تبدیل می شوند که توسط لایه دوم کنترل پردازش می شوند.

2) **قوانین مسدود کردن تراکنش:** قوانین مسدودکننده تراکنش عبارت‌اند از اگر-آنگاه (-else) برای مسدود کردن درخواست‌های تراکنش که به وضوح به عنوان کلاهبرداری درک می‌شوند. این قوانین از اندک اطلاعات موجود در هنگام درخواست پرداخت، بدون تجزیه و تحلیل سوابق تاریخی یا مشخصات دارنده کارت استفاده می کنند. یک مثال از قانون مسدود کردن می‌تواند این باشد: «اگر تراکنش‌های اینترنتی و وب‌سایت ناامن، آنگاه تراکنش را رد کنید». در عمل، چندین قانون مسدود کردن تراکنش به طور همزمان اجرا می‌شوند و تراکنش‌هایی که هر یک از این قوانین را اجرا می‌کنند مسدود می‌شوند (اگرچه کارت‌ها غیرفعال نمی‌شوند). قوانین مسدودسازی تراکنش ها به صورت دستی توسط محقق طراحی می شوند و به این ترتیب، اجزای متخصص محور FDS هستند. برای تضمین عملیات بلادرنگ و جلوگیری از مسدود کردن بسیاری از تراکنش‌های واقعی، قوانین مسدود کردن باید: 1) سریع محاسبه شوند و 2) بسیار دقیق باشند، یعنی هشدارهای نادرست بسیار کمی ایجاد کنند.

تمام تراکنش هایی که قوانین مسدودسازی را پشت سر می گذارند در نهایت مجاز هستند. با این حال، فعالیت کشف تقلب پس از غنی‌سازی داده‌های تراکنش با ویژگی‌های انبوهی که برای مقایسه خرید فعلی با خریدهای قبلی و نمایه دارنده کارت استفاده می‌شود، ادامه می‌یابد. این ویژگی‌های جمع‌آوری شده شامل، برای مثال، میانگین هزینه، میانگین تعداد تراکنش‌ها در همان روز، یا مکان خریدهای قبلی است. فرآیند محاسبه ویژگی‌های انباشته به عنوان افزایش ویژگی نامیده می‌شود و در بخش B توضیح داده شده است. ویژگی‌های افزوده شده و داده‌های تراکنش فعلی در یک بردار ویژگی انباشته می‌شوند که قرار است برای تعیین تقلبی یا واقعی بودن تراکنش مجاز آموزنده باشد. لایه های زیر از FDS بر روی این بردار ویژگی عمل می کنند.

3) **قوانین امتیازدهی:** قوانین امتیازدهی نیز مدل های متخصص محور هستند که به صورت عبارات if-then – else بیان می شوند. با این حال، اینها بر روی بردارهای ویژگی عمل می کنند و به هر تراکنش مجاز امتیازی اختصاص می دهند: هر چه امتیاز بزرگتر باشد، احتمال تقلب تراکنش بیشتر است. قوانین امتیازدهی به صورت دستی توسط محققین طراحی می شوند که به طور دلخواه نمرات مرتبط خود را مشخص می کنند. یک مثال از قانون امتیازدهی می تواند این باشد که "اگر تراکنش قبلی در قاره ای متفاوت و کمتر از 1 ساعت از تراکنش قبلی باشد، امتیاز تقلب = 0.95." متأسفانه، قوانین امتیازدهی فقط می‌توانند استراتژی‌های متقلبانه‌ای را شناسایی کنند که قبلاً توسط محققین کشف شده‌اند و الگوهایی را نشان می‌دهند که اجزای کمی از بردارهای ویژگی را شامل می‌شوند.

علاوه بر این، قوانین امتیازدهی نسبتاً ذهنی هستند، زیرا کارشناسان مختلف قوانین متفاوتی را طراحی می کنند.

4) **مدل داده محور (DDM)**: این لایه صرفاً مبتنی بر داده است و از یک طبقه بندی کننده یا مدل آماری دیگری برای تخمین احتمال تقلب بودن هر بردار ویژگی استفاده می کند. این احتمال به عنوان امتیاز تقلب مرتبط با تراکنش های مجاز استفاده می شود. بنابراین، DDM از مجموعه‌ای از تراکنش‌های برچسب‌گذاری شده آموزش داده می‌شود و نمی‌تواند توسط محققین تفسیر یا به صورت دستی اصلاح شود. انتظار می رود که یک DDM موثر الگوهای تقلبی را با تجزیه و تحلیل همزمان چندین مؤلفه بردار ویژگی، احتمالاً از طریق عبارات غیرخطی، شناسایی کند. بنابراین، از DDM انتظار می‌رود که تقلب‌ها را طبق قوانینی که فراتر از تجربه محقق است، پیدا کند و لزوماً با قوانین قابل تفسیر مطابقت ندارد.

این مقاله بر این مؤلفه از FDS متمرکز است و یک استراتژی برای طراحی، آموزش و به روز رسانی DDM برای بهبود عملکرد تشخیص تقلب پیشنهاد می کند. تراکنش‌های مرتبط با بردارهای ویژگی که امتیاز تقلب زیادی را دریافت کرده‌اند یا احتمال کلاهبرداری بالایی دارند، هشدارهایی را ایجاد می‌کنند. تنها تعداد محدودی از تراکنش‌های هشدار داده شده به بازرسان گزارش می‌شوند که لایه نهایی کنترل را نشان می‌دهند.

5) **محققین:** محققین حرفه ای با تجربه در تجزیه و تحلیل تراکنش های کارت اعتباری هستند و مسئولیت لایه های متخصص محور FDS را بر عهده دارند. به طور خاص، بازرسان قوانین مسدود کردن تراکنش و امتیازدهی را طراحی می کنند.

بازرسان همچنین مسئول کنترل هشدارهای اعلام شده توسط قوانین امتیازدهی و DDM هستند تا تعیین کنند که آیا این هشدارها با تقلب یا هشدارهای نادرست مطابقت دارند. به طور خاص، آنها تمام تراکنش های هشدار داده شده را در یک ابزار مدیریت پرونده، که در آن تمام اطلاعات مربوط به تراکنش، از جمله امتیازات/احتمالات اختصاص داده شده، گزارش می شود، تجسم می کنند، که در عمل نشان می دهد که هر تراکنش چقدر مخاطره آمیز است. بازرسان با دارندگان کارت تماس می گیرند و پس از تأیید، برچسب "اصیل" یا "تقلب" را به تراکنش هشدار داده شده اختصاص می دهند و این اطلاعات را به FDS برمی گردانند. در ادامه، ما به این تراکنش‌های برچسب‌گذاری شده به عنوان بازخورد اشاره می‌کنیم و از عبارت تعامل هشدار-بازخورد برای توصیف این مکانیسم استفاده می‌کنیم که اطلاعات نظارت شده را در یک FDS دنیای واقعی به دست می‌دهد.

هر کارتی که قربانی کلاهبرداری شود بلافاصله مسدود می شود تا از فعالیت های متقلبانه بیشتر جلوگیری شود. به طور معمول، بازرسان تمام تراکنش‌های اخیر را از یک کارت در معرض خطر بررسی می‌کنند، به این معنی که هر کلاهبرداری شناسایی شده به طور بالقوه می‌تواند بیش از یک بازخورد ایجاد کند، که لزوماً با هشدارها یا کلاهبرداری‌ها مطابقت ندارد. در یک FDS دنیای واقعی، محققین فقط می توانند چند هشدار را در روز بررسی کنند زیرا این فرآیند می تواند طولانی و خسته کننده باشد. بنابراین، هدف اولیه یک DDM، بازگرداندن هشدارهای دقیق است، زیرا زمانی که هشدارهای نادرست بیش از حد گزارش می شود، محققان ممکن است هشدارهای بیشتر را نادیده بگیرند.

B. تقویت ویژگی ها

هر درخواست تراکنش با چند متغیر مانند شناسه تاجر، شناسه دارنده کارت، مبلغ خرید، تاریخ و زمان توصیف می‌شود. تمام درخواست‌های تراکنش‌هایی که قوانین مسدود کردن را تصویب می‌کنند در یک پایگاه داده حاوی تمام تراکنش‌های مجاز اخیر، جایی که فرآیند افزایش ویژگی‌ها شروع می‌شود، وارد می‌شوند. در طول افزایش ویژگی، مجموعه خاصی از ویژگی‌های انبوه مرتبط با هر تراکنش مجاز محاسبه می‌شود تا اطلاعات بیشتری در مورد خرید ارائه کند و کلاهبرداری‌ها را از تراکنش‌های واقعی تشخیص دهد. نمونه‌هایی از ویژگی‌های جمع‌آوری شده عبارتند از میانگین هزینه‌های مشتری در هر هفته/ماه، میانگین تعداد تراکنش‌ها در روز یا در همان فروشگاه، میانگین مبلغ تراکنش، و مکان آخرین خریدها. Van Vlasselaer و همکاران نشان می دهد که ویژگی های اطلاعاتی اضافی را می توان از شبکه های اجتماعی که دارندگان کارت را با بازرگانان/فروشگاه ها متصل می کند استخراج کرد.

ویژگی‌های جمع‌آوری شده بسیار آموزنده هستند، زیرا فعالیت‌های اخیر دارنده کارت را خلاصه می‌کنند. بنابراین، آنها به تراکنش هایی هشدار می دهند که به خودی خود مشکوک نیستند اما ممکن است در مقایسه با عادات خرید دارنده کارت خاص غیرعادی باشند. افزایش ویژگی‌ها می‌تواند از نظر محاسباتی گران باشد، و ویژگی‌های انبوه اغلب برای هر دارنده کارت بر اساس تراکنش‌های تاریخی، به‌صورت آفلاین محاسبه می‌شوند. ویژگی های تجمیع شده با داده های تراکنش در بردار ویژگی انباشته می شوند.

C. اطلاعات نظارت شده

بازخوردهای محققین جدیدترین اطلاعات نظارت شده ای است که در اختیار FDS قرار گرفته است، اما تنها بخش کوچکی از تراکنش های پردازش شده هر روز را نشان می دهد. تراکنش‌های برچسب‌دار اضافی توسط دارندگان کارت ارائه می‌شوند که مستقیماً با تراکنش‌های غیرمجاز مخالفت می‌کنند. زمان تراکنش های مورد مناقشه می تواند به طور قابل توجهی متفاوت باشد، زیرا دارندگان کارت هنگام بررسی رونوشت

کارت اعتباری ارسال شده توسط بانک، عادت های متفاوتی دارند. علاوه بر این، بررسی تراکنش‌های مورد مناقشه مستلزم برخی رویه‌های اداری لازم است که ممکن است تاخیرهای قابل توجهی ایجاد کند. تمام تراکنش‌های دیگر بدون برچسب باقی می‌مانند: این تراکنش‌ها می‌توانند تراکنش‌های واقعی یا کلاهبرداری‌هایی باشند که توسط FDS نادیده گرفته شده و توسط دارندگان کارت نادیده گرفته شده‌اند. با این حال، پس از گذشت تعداد معینی از روزهای بدون اختلاف دارنده کارت، تمام تراکنش های گزارش نشده به طور پیش فرض واقعی در نظر گرفته می شوند و در مجموعه آموزشی DDM درج می شوند.

به طور کلی، دو نوع اطلاعات نظارت شده وجود دارد: 1) بازخوردهای ارائه شده توسط محققین که تعداد آنها محدود است اما به تراکنش های اخیر اشاره دارد و 2) تراکنش های نظارت شده با تأخیر که اکثریت قریب به اتفاق آن برچسب ها پس از چند روز در دسترس قرار می گیرند (به عنوان مثال، یک ماه). این مورد اخیر شامل معاملات مورد مناقشه و غیرمنازعه می شود.

D. به روزرسانی سیستم

رفتار خرج کردن مشتریان تکامل می یابد و کلاهبرداران به طور مداوم حملات جدیدی را طراحی می کنند و بنابراین استراتژی های آنها نیز در طول زمان تغییر می کند. سپس لازم است به طور مداوم FDS را به روز کنید تا عملکرد رضایت بخش را تضمین کنید. سیستم‌های متخصص محور مرتباً توسط محققینی به‌روزرسانی می‌شوند که قوانین موقت (مسدود کردن تراکنش یا امتیازدهی) را برای مقابله با شروع فعالیت‌های جعلی جدید اضافه می‌کنند و آن قوانینی را که در معرض هشدارهای نادرست زیاد هستند حذف می‌کنند. با این حال، محققین نمی توانند DDM را تغییر دهند، زیرا قابل تفسیر نیست و فقط می تواند بر اساس اطلاعات نظارت شده اخیر، همانطور که در شکل 1 نشان داده شده است، به روز شود (به عنوان مثال، دوباره آموزش داده شود). بنابراین، اگرچه محققین به طور پیوسته در طول روز بازخورد ارائه می کنند، طبقه بندی کننده معمولاً فقط یک بار به روز می شود/بازآموز می شود، به ویژه در پایان روز، زمانی که تعداد کافی بازخورد در دسترس باشد.

3-فرمول مسأله

در اینجا، ما مشکل طبقه‌بندی را مدل‌سازی می‌کنیم تا در یک FDS دنیای واقعی به آن پرداخته شود، و یک توصیف رسمی از تعامل هشدار-بازخورد و ارائه معیارهای عملکرد مناسب ارائه می‌کنیم. استراتژی یادگیری پیشنهادی (بخش پنجم) و آزمایش‌های ما (بخش ششم) بر اساس این مدل ساخته شده‌اند.

اجازه دهید x_i بردار ویژگی مرتبط با iامین تراکنش مجاز را نشان دهد و$y_i \in \{+,-\}$ کلاس مربوطه باشد، جایی که + نشان دهنده یک تقلب و - یک تراکنش واقعی است. برای مقابله با ماهیت متغیر زمانی جریان تراکنش، یک طبقه بندی کننده K هر روز به روز می شود (یا تازه آموزش می بیند). به طور خاص، طبقه‌بندی‌کننده‌ای را که تا روز $t-1$ در دسترس است، با $\mathcal{K}_{t-1}$ نشان می‌دهیم. طبقه بندی کننده $\mathcal{K}_{t-1}$ سپس برای پردازش مجموعه ای از تراکنش های T_t که در روز t مجاز شده اند استفاده می شود. ما با $\mathcal{P}_{\mathcal{K}_{t-1}}(+|x_i)$ قسمت عقبی $\mathcal{K}_{t-1}$ را نشان می دهیم، یعنی احتمال تقلب بودن x_i مطابق $\mathcal{K}_{t-1}$. محققین فقط چند تراکنش پرخطر را بررسی می کنند. بنابراین، ما هشدارها را به عنوان K-ریسک ترین معاملات، یعنی

$$\mathrm{A}_t = \{x_i \in \mathrm{T}_t \text{ s.t. } r(x_i) \leq k\} \qquad (1)$$

جایی که$r\,(xi\,) \in \{1,\ldots,|\mathrm{T}t\,|\}$ رتبه x_i با توجه به $\mathcal{P}_{\mathcal{K}_t}(+|x_i)$ است و k > 0 حداکثر تعداد هشدارهایی است که می تواند توسط محققین بررسی شود. همانطور که در بخش 2-A.5 بحث شد، محققین با دارندگان کارت تماس می گیرند و نمونه های نظارت شده را در قالب *بازخورد* در اختیار FDS قرار می دهند. به طور خاص، بازخوردها شامل تمام تراکنش‌های اخیر از کارت‌های کنترل‌شده است که ما آن‌ها را به‌عنوان مدل‌سازی می‌کنیم

$$\mathrm{F}_t = \{(x_i, y_i) \text{ s.t. } x_i \text{ is from cards}(\mathrm{A}_t)\} \qquad (2)$$

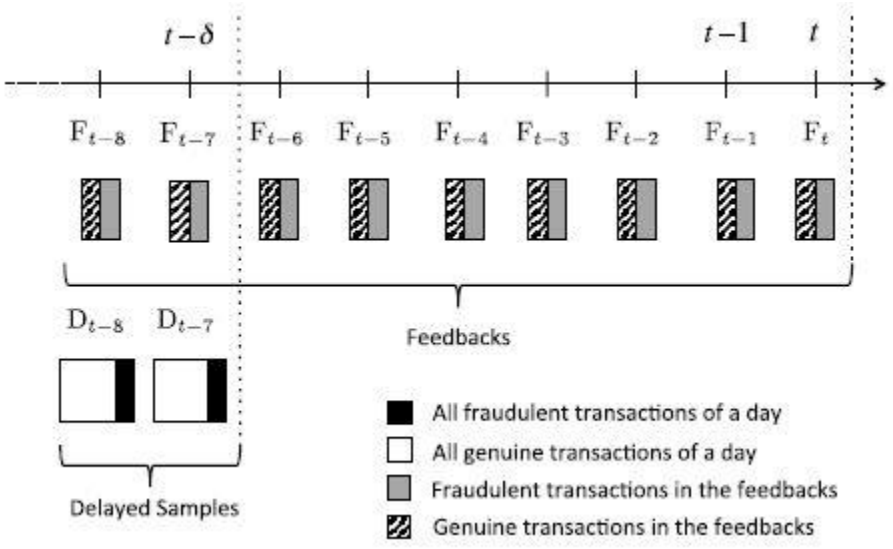
که در آن cards $(\mathcal{A}_t)$ مجموعه کارتهایی را نشان می دهد که حداقل تراکنش در $\mathcal{A}_t$ دارند. تعداد بازخوردها، یعنی $|\mathcal{F}_t|$، به تعداد تراکنش های مرتبط با k کارت های کنترل شده بستگی دارد.

پس از تأخیر مشخصی در تأیید، برچسب‌های همه تراکنش‌ها در اختیار FDS قرار می‌گیرد، زیرا همانطور که در بخش 2-C بحث شد، تراکنش‌های بدون مناقشه واقعی در نظر گرفته می‌شوند. برای سادگی، ما تأخیر تأیید ثابت δ روز را فرض می کنیم، به طوری که در روز t، برچسب های تمام تراکنش های مجاز در روز t - δ ارائه می شود. ما به این نمونه‌های تحت نظارت تأخیری اشاره می‌کنیم

$$\mathrm{D}_{t-\delta} = \{(x_i, y_i), \quad x_i \in \mathrm{T}_{t-\delta}\}. \qquad (3)$$

توجه داشته باشید که $F_{t-\delta} \subset D_{t-\delta}$ از آنجایی که تراکنش‌ها در روز $t-\delta$ آشکارا شامل مواردی هستند که هشدار داده شده‌اند. شکل 2 انواع مختلف اطلاعات تحت نظارت موجود در یک FDS را نشان می دهد.

شایان ذکر است که علیرغم اینکه توضیحات رسمی ما شامل چندین جنبه و جزئیات است که تاکنون در ادبیات کشف تقلب نادیده گرفته شده است، این مدل همچنان یک مدل ساده شده است. در واقع، هشدارها در یک FDS دنیای واقعی معمولاً به صورت آنلاین هنگام پردازش تراکنش‌ها، بدون نیاز به رتبه‌بندی همه تراکنش‌ها در T_t، مطرح می‌شوند. به طور مشابه، زوج‌های تحت نظارت تأخیر یک‌باره نمی‌آیند، زیرا هر تراکنش مورد اختلاف ممکن است کمتر (یا احتمالاً بیشتر) از δ روز طول بکشد. با وجود این، ما فکر می‌کنیم که فرمول‌بندی ما جنبه‌های یک FDS دنیای واقعی را در نظر می‌گیرد که از منظر یادگیری مهم‌ترین آنها هستند، که شامل هشدارها، تعامل تغییر بازخورد و تأخیر تأیید می‌شود. ما همچنین اظهار می‌کنیم که در اصل، از آنجایی که طبقه‌بندی‌کننده هر بردار ویژگی x_iرا به طور مستقل تجزیه و تحلیل می‌کند، به کارت‌هایی که چندین تراکنش مخاطره‌آمیز دریافت می‌کنند هشدار نمی‌دهد تا زمانی که هر یک از اینها در مخزن هشدارها وارد شود (1). با این حال، این موقعیت‌ها به‌ویژه برای محققین مرتبط هستند و می‌توانند با قوانین امتیازدهی مناسب یا افزایش ویژگی‌ها کنترل شوند، به عنوان مثال، مؤلفه‌ای اضافه شود که امتیازات تراکنش‌های اخیر را پیگیری می‌کند.



شکل 2: نمونه های نظارت شده موجود در پایان روز t شامل: 1) بازخورد $F_{(\cdot)}$ و 2) زوج های تاخیری $D_{(\cdot)}$ قبل از $t-\delta$ روز رخ داده اند. در این نمودار، ما $\delta = 7$ را فرض کرده‌ایم. الگوها برچسب‌های مختلف را نشان می‌دهند، و اندازه این مناطق نشان‌دهنده نسبت‌های کلاس متعادل/نامتعادل است.

عملکرد تشخیص تقلب را می توان به راحتی از نظر دقت هشدار $P_k(t)$ ارزیابی کرد که به صورت تعریف می شود

$$\mathrm{P}_k(t) = \frac{|\mathrm{TP}_k(t)|}{k} \qquad (4)$$

جایی که $P_k(t)$ نسبت تقلب ها در هشدارها است. اگرچه طبقه‌بندی‌کننده به‌طور مستقل هر بردار ویژگی را پردازش می‌کند، اما دقت هشدار به‌جای تراکنش‌های مجاز، به‌طور واقعی‌تر از نظر کارت‌ها اندازه‌گیری می‌شود. در واقع، چندین تراکنش در $\mathcal{A}_t$ از یک کارت باید به عنوان یک هشدار واحد در نظر گرفته شود، زیرا محققان هنگام تماس با دارندگان کارت، تمام تراکنش‌های اخیر را بررسی می‌کنند. این بدان معناست که k به حداکثر تعداد کارتهایی که محققین می توانند کنترل کنند بستگی دارد. در این زمینه، اندازه گیری عملکرد شناسایی در سطح کارت آموزنده تر است، به طوری که چندین تراکنش متقلبانه از یک کارت به عنوان یک تشخیص صحیح منفرد محسوب می شود. بنابراین، ما CP_k، دقت کارت، را به عنوان نسبت کارت های تقلبی شناسایی شده در کارت های k که توسط محققین کنترل می شود، معرفی می کنیم.

$$\mathrm{CP}_k(t) = \frac{|\mathrm{C}_t^+|}{k} \qquad (5)$$

که در آن C_t^+مجموعه ای از کارت های تقلبی را نشان می دهد که به درستی در روز t شناسایی شده اند، یعنی کارت های تقلبی که حداقل یک هشدار را گزارش کرده اند. برای محاسبه صحیح روزهایی که کمتر از k کارت تقلبی هستند، $CP_k(t)$ نرمال شده را به عنوان

$$\mathrm{NCP}_k(t) = \frac{\mathrm{CP}_k(t)}{\Gamma(t)} \quad \text{with} \quad \Gamma(t) = \begin{cases} 1 & \text{if } \gamma_t \geq k \\ \frac{\gamma_t}{k} & \text{if } \gamma_t < k \end{cases} \qquad (6)$$

که در آن $\Gamma_{(t)}$ حداکثر مقدار $CP_k(t)$ و γ_t تعداد کارت های تقلبی در روز t است. از (6)، داریم که $NCP_k(t)$ مقادیری را در محدوده [0، 1] می گیرد، در حالی که $CP_k(t)$ وقتی$\gamma_t > k$ در [0، 1] و در غیر این صورت در $\{(\gamma_t/k),0\}$ است. به عنوان مثال، اگر در روز t، 40 کارت تقلبی$(|C_t^+| = 40)$ از 100 کارت بررسی شده توسط محققین را به درستی شناسایی کرده باشیم، و تعداد کلی کارت های تقلبی 50 باشد $(\gamma_t = 50)$ ، پس $CP_k(t) = 0.4$در حالی که $NCP_k(t) = \frac{0.4}{0.5} = 0.8$.

توجه داشته باشید که از آنجایی که $\Gamma_{(t)}$ به طبقه‌بندی‌کننده خاص $\mathcal{K}_{t-1}$ اتخاذ شده بستگی ندارد، وقتی الگوریتم "A" از الگوریتم "B" از نظر CP_k بهتر است، "A" نیز از نظر "B" بهتر است. NCP_k علاوه بر این، به دلیل تأخیر تأیید، تعداد کارت های تقلبی در روز t (یعنی γ_t) فقط پس از چند روز قابل محاسبه است و بنابراین NCP_k نمی تواند در زمان واقعی محاسبه شود. بنابراین، توصیه می‌کنیم از CP_k برای ارزیابی عملکرد

در حال اجرا استفاده کنید، در حالی که از NCP_k برای آزمایش برگشتی استفاده کنید، به عنوان مثال، هنگام آزمایش پیکربندی‌های مختلف FDS، مانند بخش 6-F.

4-کار مرتبط

A. رویکردهای داده محور در تشخیص تقلب در کارت اعتباری

هر دو روش نظارت شده و بدون نظارت برای اهداف کشف کلاهبرداری کارت اعتباری پیشنهاد شده است. روش‌های نظارت‌نشده شامل تکنیک‌های تشخیص نابه‌هنجاری است که هر معامله‌ای را که با اکثریت مطابقت ندارد، تقلب در نظر می‌گیرد. قابل توجه است که یک DDM بدون نظارت در یک FDS می تواند مستقیماً از تراکنش های بدون برچسب پیکربندی شود. یک روش معروف، تجزیه و تحلیل گروه همتا است که مشتریان را بر اساس مشخصات آنها خوشه بندی می کند و کلاهبرداری ها را به عنوان تراکنش هایی که از رفتار معمول دارنده کارت خارج می شوند، شناسایی می کند. رفتار معمولی دارنده کارت نیز با استفاده از نقشه های خودسازماندهی مدل شده است.

روش‌های نظارت شده جزء محبوب‌ترین روش‌ها در کشف تقلب هستند و از تراکنش‌های برچسب‌گذاری‌شده برای آموزش یک طبقه‌بندی کننده استفاده می‌کنند. تقلب ها با طبقه بندی بردارهای ویژگی تراکنش های مجاز یا احتمالاً با تجزیه و تحلیل قسمت های پسین طبقه بندی کننده شناسایی می شوند. چندین الگوریتم طبقه‌بندی بر روی تراکنش‌های کارت اعتباری برای شناسایی تقلب‌ها آزمایش شده‌اند، از جمله قوانین انجمن رگرسیون لجستیک شبکه‌های عصبی که از ماشین‌های برداری پشتیبانی می‌کنند که تجزیه و تحلیل تفکیک فیشر و درخت‌های تصمیم را اصلاح کرده‌اند. چندین مطالعه جنگل تصادفی (RF) را برای دستیابی به بهترین عملکرد گزارش کرده اند: این یکی از دلایلی است که ما RF ها را در آزمایشات خود به کار می گیریم.

B. معیار عملکرد برای کشف تقلب

معیار عملکرد معمولی برای مشکلات کشف تقلب، AUC است. AUC را می توان با استفاده از آمار Mann-Whitney تخمین زد و مقدار آن را می توان به عنوان احتمال اینکه طبقه بندی کننده تقلب ها را بالاتر از تراکنش های واقعی رتبه بندی می کند تفسیر کرد. یکی دیگر از معیارهای رتبه‌بندی که اغلب در تشخیص تقلب استفاده می‌شود، دقت متوسط است که با ناحیه زیر منحنی فراخوانی دقیق مطابقت دارد. در حالی که این معیارها به طور گسترده در مشکلات تشخیص استفاده می‌شوند، معیارهای مبتنی بر هزینه به طور خاص برای اهداف کشف تقلب طراحی شده‌اند. معیارهای مبتنی بر هزینه، زیان پولی کلاهبرداری را با استفاده از ماتریس هزینه که هزینه را با هر ورودی ماتریس سردرگمی مرتبط می‌کند، تعیین می‌کند. الکان نشان می دهد که یک ماتریس

هزینه ممکن است گمراه کننده باشد زیرا حداقل/حداکثر از دست دادن مشکل می تواند در طول زمان تغییر کند. برای جلوگیری از این مشکل، هزینه عادی یا صرفه جویی برای ارزیابی عملکرد با توجه به حداکثر ضرر استفاده می شود.

ما استدلال می کنیم که معیارهای عملکرد باید در دسترس بودن محققین را نیز در نظر بگیرند، زیرا آنها باید تمام هشدارهای ارائه شده توسط FDS را بررسی کنند. با توجه به زمان محدودی که محققین در اختیار دارند، فقط چند هشدار را می توان هر روز تأیید کرد، و بنابراین یک FDS موثر باید تعداد کمی هشدار قابل اعتماد را به محققان ارائه دهد. به همین دلیل است که ما اقدامات دقیق هشدار شرح داده شده در بخش 3 را معرفی کرده ایم.

C. چالش های عمده ای که باید در یک FDS دنیای واقعی پرداخته شوند

همانطور که در بخش اول پیش‌بینی می‌شود، چالش‌های عمده‌ای که در طراحی FDS باید مورد توجه قرار گیرد عبارتند از: 1) رسیدگی به عدم تعادل کلاس، زیرا تعداد تراکنش‌های قانونی بسیار بیشتر از تراکنش‌های تقلبی است. 2) مدیریت مفهوم رانش از آنجایی که ویژگی های آماری تقلب ها و معاملات واقعی با گذشت زمان تکامل می یابد. و 3) فعالیت با تعداد کمی از تراکنش‌های نظارت شده اخیر، که در قالب بازخورد محققین ارائه شده است.

1) *عدم تعادل طبقاتی*: توزیع طبقاتی در تراکنش های کارت اعتباری بسیار نامتعادل است، زیرا کلاهبرداری ها معمولا کمتر از 1٪ از کل تراکنش ها هستند. یادگیری در شرایط عدم تعادل کلاس اخیراً توجه زیادی را به خود جلب کرده است، زیرا روش‌های یادگیری سنتی طبقه‌بندی‌کننده‌هایی را ارائه می‌دهند که عملکرد ضعیفی در کلاس اقلیت دارند، که قطعاً کلاس مورد علاقه در مشکلات تشخیص است. چندین تکنیک برای مقابله با عدم تعادل طبقاتی پیشنهاد شده است و برای بررسی جامع، خواننده را به آن ارجاع می دهیم. دو رویکرد اصلی برای مقابله با عدم تعادل طبقاتی عبارتند از: 1) روش های نمونه گیری و 2) روش های مبتنی بر هزینه. روش‌های نمونه‌گیری برای متعادل کردن توزیع کلاس در مجموعه آموزشی قبل از اجرای یک الگوریتم یادگیری سنتی استفاده می‌شود، در حالی که روش‌های مبتنی بر هزینه، الگوریتم یادگیری را تغییر می‌دهند تا هزینه طبقه‌بندی اشتباه بزرگ‌تری را به کلاس اقلیت اختصاص دهند.

روش‌های نمونه‌گیری به دو دسته تقسیم می‌شوند که با حذف نمونه‌ها از کلاس اکثریت، نسبت‌های کلاس را در مجموعه آموزشی متعادل می‌کند، و روش‌های نمونه‌گیری بیش‌ازحد که با تکرار نمونه‌های آموزشی کلاس اقلیت به همین هدف دست می‌یابند. روش‌های پیشرفته نمونه‌برداری بیش از حد، مانند

SMOTE، به جای تکرار نمونه، نمونه‌های آموزشی مصنوعی را از کلاس اقلیت با درون‌یابی تولید می‌کنند.

روش‌های مبتنی بر هزینه نیازی به متعادل کردن نسبت داده‌های آموزشی ندارند، زیرا آنها ضررهای متفاوتی را برای خطاهای طبقه‌بندی در نمونه‌های متعلق به کلاس اقلیت و اکثریت در نظر می‌گیرند. در تشخیص کلاهبرداری کارت اعتباری، هزینه کلاهبرداری از دست رفته اغلب متناسب با مبلغ تراکنش فرض می‌شود و این هزینه طبقه‌بندی اشتباه بزرگ‌تری را به کلاهبرداری‌ها اختصاص می‌دهد، بنابراین طبقه‌بندی کننده را به ترجیح دادن هشدارهای نادرست به جای پذیرش خطر از دست دادن یک کلاهبرداری هدایت می‌کند. در نتیجه، این الگوریتم‌ها ممکن است بسیاری از موارد مثبت کاذب را ایجاد کنند در حالی که محققان به هشدارهای دقیق نیاز دارند.

2) رانش *مفهومی*: دو عامل اصلی ایجاد تغییرات/تحول در جریان تراکنش‌های کارت اعتباری هستند که در ادبیات معمولاً به عنوان رانش مفهومی شناخته می‌شوند. در ابتدا، تراکنش‌های واقعی به این دلیل تکامل می‌یابند که دارندگان کارت معمولاً رفتارهای خرج کردن خود را در طول زمان تغییر می‌دهند (به عنوان مثال، در طول تعطیلات، خریدشان بیشتر و متفاوت از بقیه سال است). دوم، کلاهبرداری ها در طول زمان تغییر می کنند، زیرا فعالیت های کلاهبرداری جدید انجام می شود. در آزمایش‌های خود (به بخش 6-D مراجعه کنید)، ماهیت در حال تحول تراکنش‌های کارت اعتباری را در دو مجموعه داده بزرگ از معاملات تجارت الکترونیک دنیای واقعی مشاهده می‌کنیم. یادگیری تحت انحراف مفهومی یکی از چالش‌های عمده‌ای است که روش‌های مبتنی بر داده باید با آن مواجه شوند، زیرا طبقه‌بندی‌کننده‌هایی که در این شرایط کار می‌کنند در عمل باید به‌طور مستقل مرتبط‌ترین اطلاعات نظارت‌شده به‌روز را شناسایی کنند و در عین حال اطلاعات منسوخ را نادیده بگیرند. رویکردهای سازگاری رانش مفهومی را می توان به دو خانواده تقسیم کرد: 1) سازگاری فعال و 2) سازگاری غیرفعال.

رویکردهای فعال از آزمون تشخیص تغییر یا سایر محرک های آماری برای نظارت بر داده های دریافتی با تجزیه و تحلیل خطای طبقه بندی و/یا توزیع داده ها استفاده می کنند. به محض اینکه تغییری در داده‌های دریافتی شناسایی شد، سازگاری فعال می‌شود و طبقه‌بندی‌کننده بر روی نمونه‌های نظارت‌شده اخیر که منسجم با وضعیت فعلی فرآیند در نظر گرفته می‌شوند، به‌روزرسانی/بازآموزی می‌شود. به این ترتیب، رویکردهای فعال بیشتر زمانی مناسب هستند که توزیع داده ها به طور ناگهانی تغییر می کند، و فرآیند تولید داده ها از طریق دنباله ای از حالت های ثابت جابجا می شود.

در رویکردهای غیرفعال، طبقه‌بندی‌کننده به‌طور پیوسته به‌روزرسانی می‌شود که نمونه‌های تحت نظارت جدید در دسترس قرار می‌گیرند، بدون اینکه هیچ مکانیزم تحریک آشکاری در آن دخالت داشته باشد.

روش‌های مجموعه و طبقه‌بندی‌کننده‌های آموزش‌دیده بر روی یک پنجره کشویی از نمونه‌های نظارت شده اخیر (مانند STAGGER و FLORA) احتمالاً گسترده‌ترین راه‌حل‌های غیرفعال هستند. رویکردهای غیرفعال در محیط‌های در حال حرکت تدریجی و زمانی که اطلاعات نظارت شده به صورت دسته‌ای ارائه می‌شوند، مناسب‌تر هستند.

هنگامی که جریان های داده با رانش مفهومی و توزیع های نامتعادل مشخص می شوند، تطبیق اغلب با ترکیب روش های مجموعه و تکنیک های نمونه گیری مجدد حاصل می شود. یک رویکرد جایگزین عبارت است از انتشار نمونه‌های آموزشی طبقه اقلیت در طول زمان، احتمالاً نمونه‌برداری کمتر از طبقه اکثریت. چن و او REA را پیشنهاد کردند که نمونه هایی را فقط از طبقه اقلیت که به مفهوم فعلی تعلق دارد، منتشر می کند.

3) *تعامل هشدار-بازخورد و سوگیری انتخاب نمونه:* اکثر طبقه‌بندی‌کننده‌های مورد استفاده برای تشخیص تقلب کارت اعتباری در ادبیات، در آزمایش‌هایی آزمایش می‌شوند که قرار است برچسب‌های تراکنش از روز بعد از زمان مجاز شدن تراکنش در دسترس باشند. در یک FDS دنیای واقعی (بخش C-2)، تنها اطلاعات نظارت شده اخیر، بازخوردهای F_t است که توسط محققین ارائه می شود، در حالی که اکثریت قریب به اتفاق تراکنش های مجاز روزانه برچسبی در مدت کوتاهی دریافت نمی کنند ($|F_t| \ll |D_t|$). بازخوردها به دو دلیل عمده نشان دهنده تراکنش‌هایی نیستند که هر روز پردازش می‌شوند: 1) بازخوردها حاوی تراکنش‌هایی هستند که با احتمال زیاد کلاهبرداری مشخص می‌شوند و 2) نسبت تقلب‌ها در بازخوردها با نسبت تقلب‌هایی که روزانه رخ می‌دهند متفاوت است. بنابراین، بازخوردها نوعی مجموعه آموزشی مغرضانه را نشان می‌دهند: این مشکل چیزی را که در ادبیات به عنوان SSB شناخته می‌شود، تداعی می‌کند.

یک مجموعه آموزشی مغرضانه ممکن است عملکرد الگوریتم های یادگیری را مختل کند، زیرا داده های آموزشی با توزیع نمونه های آزمایشی مطابقت ندارند. در اینجا به سادگی اشاره می کنیم که سه نوع مختلف SSB وجود دارد! (SSBs!): سوگیری کلاس قبلی، سوگیری ویژگی (همچنین تغییر متغیر نامیده می شود)، و سوگیری کامل. یک راه حل استاندارد برای SSB، وزن دهی اهمیت است، یعنی تکنیک های وزن دهی مجدد نیمه نظارتی که وزن های بزرگ تری را به نمونه های تمرینی که شباهت بیشتری به توزیع داده ها در مجموعه آزمون دارند، اختصاص می دهد. ایده اصلی وزن دهی اهمیت، کاهش تأثیر مغرضانه ترین نمونه ها در فرآیند یادگیری است. مجموعه هایی از طبقه بندی کننده ها نیز برای تصحیح SSB پیشنهاد شده اند.

تعامل بین FDS (افزایش هشدارها) و محققین (ارائه برچسب‌های واقعی) سناریوی یادگیری فعال را به یاد می‌آورد، که در آن می‌توان نمونه‌های بسیار آموزنده‌ای را انتخاب کرد و برچسب‌های آن‌ها را برای یک اوراکل جستجو کرد که در FDS محققین هستند. . با این حال، این در یک FDS در دنیای واقعی امکان پذیر نیست، زیرا بازرسان باید روی مشکوک ترین تراکنش ها تمرکز کنند تا بیشترین تعداد تقلب ها را شناسایی کنند. درخواست‌ها برای بررسی تراکنش‌های (احتمالاً واقعی) برای دریافت نمونه‌های اطلاعاتی نادیده گرفته می‌شوند. با توجه به تعداد محدودی از تراکنش‌هایی که محققین می‌توانند بررسی کنند، پرداختن به این سؤالات لزوماً به این معنی است که برخی از تراکنش‌های پرخطر کنترل نمی‌شوند و در نتیجه عملکرد شناسایی از دست می‌رود.

5-استراتژی یادگیری پیشنهادی

مهم است که تاکید کنیم بازخوردها (F_t) و نمونه های تاخیری ($D_{t-\delta}$) مجموعه های بسیار متفاوتی از نمونه های نظارت شده هستند. اولین تفاوت کاملاً مشهود است: F_t اطلاعات به روز اخیر را ارائه می دهد در حالی که $D_{t-\delta}$ ممکن است برای آموزش طبقه بندی کننده ای که برای تجزیه و تحلیل تراکنش هایی که روز بعد مجاز می شوند منسوخ شده باشد. تفاوت دوم مربوط به درصد تقلب ها در F_t و $D_{t-\delta}$است: در حالی که نسبت کلاس در $D_{t-\delta}$ به شدت به سمت کلاس واقعی منحرف می شود (نسبت های تقلب ها را در جدول 1 ببینید)، تعداد تقلب ها در F_t در واقع به این بستگی دارد. عملکرد تشخیص $\mathcal{K}_{t-1}$ و مقادیر دقت بالا حتی ممکن است منجر به انحراف F_t به سمت تقلب شود. سومین و احتمالاً ظریف‌ترین تفاوت این است که زوج‌های تحت نظارت در F_t به طور مستقل ترسیم نمی‌شوند، بلکه تراکنش‌هایی از کارت‌هایی هستند که توسط $\mathcal{K}_{t-1}$ به‌عنوان کارت‌هایی انتخاب شده‌اند که به احتمال زیاد تقلب شده‌اند. به این ترتیب، F_t تحت تأثیر SSB قرار می گیرد و هر طبقه بندی کننده ای که در F_t آموزش دیده باشد، اصولاً یاد می گیرد که چگونه تراکنش هایی را که به احتمال زیاد تقلبی هستند برچسب گذاری کند. بنابراین، این ممکن است در اصل در اکثریت قریب به اتفاق معاملات واقعی دقیق نباشد.

شهود ما این است که بازخوردها و نمونه‌های تاخیری نشان‌دهنده دو مشکل طبقه‌بندی متفاوت هستند، و بنابراین باید به طور جداگانه مورد بررسی قرار گیرند. بنابراین، استراتژی یادگیری ما شامل آموزش یک طبقه‌بندی‌کننده منحصراً بر روی بازخوردها (یعنی F_t) و یک طبقه‌بندی کننده منحصراً بر روی نمونه‌های نظارت شده با تأخیر (یعنی D_t) و با جمع‌آوری احتمالات پسین آنها هنگام تعریف $\mathcal{P}_{\mathcal{K}_t}(+|x_i)$ برای تعیین اینکه کدام تراکنش‌ها، برای هشدار دادن است.

در ادامه، استراتژی یادگیری پیشنهادی را به تفصیل شرح می‌دهیم، جایی که انطباق بر اساس یک رویکرد غیرفعال انجام می‌شود و طبقه‌بندی‌کننده هر روز بر روی دسته‌ای حاوی آخرین زوج‌های تحت نظارت موجود، بازخورد یا نمونه‌های تاخیری، به‌روزرسانی می‌شود. همانطور که در بخش 3، ما تأخیر تأیید ثابت δ روز را در نظر می گیریم. به ویژه، برای پردازش تراکنش‌های مجاز در روز t + 1، ما به Q روز بازخورد $\{F_t, \ldots, F_{t-(Q-1)}\}$ و M روز از نمونه های نظارت شده با تاخیر $\{D_{t-\delta}, \ldots, D_{t-(\delta+M-1)}\}$، و این دومی آشکارا شامل بازخوردهای دریافت شده در همان روزها می شود (یعنی $F_i \subset D_i, i \leq t-\delta$). استراتژی یادگیری ما، که در الگوریتم 1 به تفصیل آمده است، شامل آموزش جداگانه طبقه‌بندی کننده $\mathcal{F}_t$ بر روی بازخوردها است.

$$\mathcal{F}_t = \text{TRAIN}(\{F_t, \ldots, F_{t-(Q-1)}\}) \qquad (7)$$

و یک طبقه‌بندی کننده در نمونه‌های نظارت شده با تاخیر

$$\mathcal{D}_t = \text{TRAIN}(\{D_{t-\delta}, \ldots, D_{t-(\delta+M-1)}\}) \qquad (8)$$

و برای شناسایی تقلب‌ها توسط طبقه‌بندی‌کننده تجمع $\mathcal{A}_t$، که احتمال بعدی آن به صورت تعریف شده است.

$$\mathcal{P}_{\mathcal{A}_t}(+|x) = \alpha \mathcal{P}_{\mathcal{F}_t}(+|x) + (1-\alpha)\mathcal{P}_{\mathcal{D}_t}(+|x) \qquad (9)$$

که در آن $0 \leq \alpha \leq 1$ پارامتر وزنی است که سهم $\mathcal{F}_t$ و $\mathcal{D}_t$ را متعادل می کند. بنابراین، احتمال پسین طبقه‌بندی‌کننده $\mathcal{K}_t$، که به تراکنش‌های مجاز در روز t + 1 هشدار می‌دهد، با (9) داده می‌شود.

پارامترهای Q و M که به ترتیب تعیین می‌کنند چند روز بازخورد و نمونه‌های نظارت شده با تأخیر برای آموزش طبقه‌بندی‌کننده‌های ما استفاده می‌شوند، باید با در نظر گرفتن تعداد کلی بازخوردها و درصد تقلب‌ها تعریف شوند. مجموعه آموزشی $\mathcal{F}_t$ تقریباً حاوی $|F_t|$ نمونه ها (تعداد متفاوتی از بازخوردها ممکن است هر روز ارائه شود) و این تعداد باید به اندازه کافی بزرگ باشد تا طبقه بندی کننده ای را آموزش دهد که به یک مشکل طبقه بندی چالش برانگیز در ابعاد بالا رسیدگی کند. با این حال، Q را نمی توان به طور دلخواه بزرگ کرد، بدون اینکه بازخوردهای قدیمی را شامل شود. ملاحظات مشابهی در هنگام تنظیم M، تعداد روزهای در نظر گرفته شده حاوی تراکنش های تاخیری، که باید شامل تعداد کافی تقلب باشد، وجود دارد. توجه داشته باشید که با این وجود امکان گنجاندن بازخوردهای $\mathcal{F}_t$ قبل از δ روز ($Q \geq \delta$) در مجموعه آموزشی وجود دارد و به ویژه در آزمایش‌های خود از $Q = \delta + M$ استفاده کردیم.

منطق پشت استراتژی یادگیری پیشنهادی دو جنبه دارد. در ابتدا، با آموزش یک طبقه‌بندی‌کننده (7) منحصراً بر روی بازخوردها، ما ارتباط بیشتر با این نمونه‌های نظارت‌شده را تضمین می‌کنیم، که در غیر این صورت تعداد نمونه‌های نظارت شده با تأخیر، بیشتر می‌شوند. دوم، ما فقط به تراکنش‌هایی هشدار می‌دهیم که هم $\mathcal{F}_t$ و هم $\mathcal{D}_t$ به احتمال زیاد تقلب در نظر گرفته می‌شوند: این از این واقعیت ناشی می‌شود که، در عمل، به دلیل تعداد زیادی تراکنش‌هایی که روزانه پردازش می‌شوند، هشدارها با مقادیر $\mathcal{P}_{\mathcal{A}_t}$ که بسیار نزدیک به یک هستند مطابقت دارد. بیایید به یاد بیاوریم که $\mathcal{F}_t$ و در نتیجه $\mathcal{A}_t$ نیز به دلیل تعامل هشدار-بازخورد تحت تأثیر SSB قرار می گیرد. تنها نمونه‌های آموزشی که تحت تأثیر SSB قرار نمی‌گیرند، نمونه‌های نظارت شده با تأخیر هستند که، با این حال، ممکن است به دلیل رانش مفهومی منسوخ شوند.

Algorithm 1 Proposed Learning Strategy

Require: M and Q, i.e., the number of days of delayed samples and feedbacks to use, respectively; $\mathcal{F}_t$ and $\mathcal{D}_t$ classifiers previously trained.
$\mathrm{T}_{t+1} \leftarrow$ transactions at day $t+1$.
for each transaction $x \in \mathrm{T}_{t+1}$ **do**
  compute $\mathcal{P}_{\mathcal{F}_t}(+, x)$
  compute $\mathcal{P}_{\mathcal{D}_t}(+, x)$
  compute $\mathcal{P}_{\mathcal{A}_t}(+, x)$ as in (9)
rank T_{t+1} according to $\mathcal{P}_{\mathcal{A}_t}(+, \cdot)$,
generate alerts A_t.
if update the classifier **then**
  $\mathrm{F}_{t+1} \leftarrow$ feedbacks from cards alerted in A_t.
  $\mathcal{F}_{t+1} \leftarrow \mathrm{TRAIN}(\{\mathrm{F}_{t+1}, \ldots, \mathrm{F}_{t-Q}\})$
  $\mathrm{D}_{t+1-\delta} \leftarrow$ transactions authorized at $t+1-\delta$
  $\mathcal{D}_{t+1} \leftarrow \mathrm{TRAIN}(\{\mathrm{D}_{t+1-\delta}, \ldots, \mathrm{D}_{t-(\delta+M)}\})$
return $\mathcal{F}_t, \mathcal{D}_t$ and $\mathcal{A}_t$ defined as in (9).

A. اجرای استراتژی یادگیری پیشنهادی

در آزمایش‌های خود، استراتژی یادگیری پیشنهادی را در دو سناریو مختلف اجرا می‌کنیم که با دو رویکرد اصلی برای یادگیری $\mathcal{D}_t$ مطابقت دارد. در اولی، $\mathcal{D}_t$ یک طبقه‌بندی‌کننده پنجره کشویی است که آن را با $\mathcal{W}_t^D$ نشان

می‌دهیم، در حالی که در دومی، $\mathcal{D}_t$ مجموعه‌ای از طبقه‌بندی‌کننده‌ها است که ما با $\mathcal{E}_t^D$ نشان دهید. هر دو طبقه بندی کننده $\mathcal{W}_t^D$و $\mathcal{E}_t^D$بر روی نمونه های تاخیری آموزش داده شده اند $\{D_{t-\delta}, \ldots, D_{t-(\delta+M-1)}\}$. با این حال، در حالی که $\mathcal{W}_t^D$ از یک مدل منحصر به فرد برای این منظور استفاده می کند، $\mathcal{E}_t^D$ مجموعه ای از M طبقه بندی کننده $\{\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_M\}$ که در آن هر طبقه‌بندی‌کننده $\mathcal{M}_i$ جداگانه روی نمونه‌های تاخیری یک روز متفاوت آموزش داده می‌شود، یعنی $D_{t-\delta-i}$،i=0,…,M-1 ، خلفی $\mathcal{P}_{\mathcal{E}_t^D}(+|\mathrm{x})$ با میانگین‌گیری احتمالات خلفی طبقه‌بندی‌کننده‌های منفرد، یعنی $\mathcal{P}_{\mathcal{E}_t^D}(+|\mathrm{x}) = (\frac{\sum_i^M \mathcal{P}_{\mathcal{M}_i}(+|x)}{M})$ به دست می‌آید.

در مورد پنجره کشویی، استراتژی یادگیری پیشنهادی شامل تجزیه و تحلیل قسمت عقبی طبقه‌بندی‌کننده $\mathcal{A}_t^W$ است که $\mathcal{F}_t$ و $\mathcal{W}_t^D$را تجمیع می‌کند، یعنی $\mathcal{P}_{\mathcal{A}_t^W}(+|\mathrm{x}) = \alpha\mathcal{P}_{\mathcal{F}_t}(+|\mathrm{x}) + (1-\alpha)\mathcal{P}_{\mathcal{W}_t^D}(+|\mathrm{x})$ مانند (9). معیار مقایسه با $\mathcal{A}_t^W$ طبقه‌بندی‌کننده $\mathcal{W}_t$ است که در مورد تمام تراکنش‌های نظارت‌شده با اشاره به بازه زمانی یکسان (در نتیجه ترکیب نمونه‌های تاخیری و بازخوردها) آموزش دیده است: $\{F_t, \ldots, F_{t-(Q-1)}, D_{t-\delta}, \ldots, D_{t-(\delta+M-1)}\}$.

به طور مشابه، در مورد مجموعه، استراتژی یادگیری پیشنهادی شامل تجزیه و تحلیل قسمت‌های پسین طبقه‌بندی‌کننده $\mathcal{A}_t^E$ است که با تجمیع قسمت‌های خلفی $\mathcal{F}_t$ و $\mathcal{E}_t^D$ به دست می‌آید، یعنی $\mathcal{P}_{\mathcal{A}_t^E}(+|\mathrm{x}) = \alpha\mathcal{P}_{\mathcal{F}_t}(+|\mathrm{x}) + (1-\alpha)\mathcal{P}_{\mathcal{E}_t^D}(+|\mathrm{x})$، مانند (9). معیار مقایسه با $\mathcal{A}_t^E$ طبقه بندی کننده $\mathcal{E}_t$ است که افراد آن $\{\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_M, \mathcal{F}_t\}$ و خلفی آن $\mathcal{P}_{\mathcal{E}_t}(+|\mathrm{x})$ با میانگین‌گیری احتمالات خلفی همه افراد آن تخمین زده می‌شود، یعنی $\mathcal{P}_{\mathcal{E}_t}(+|\mathrm{x}) = (\frac{\sum_i^M \mathcal{P}_{\mathcal{M}_i}(+|x)+\mathcal{P}_{\mathcal{F}_i}(+|\mathrm{x})}{M+1})$

در هر دو تجمیع $\mathcal{A}_t^W$ و $\mathcal{A}_t^E$، α = 0.5 را تنظیم کردیم تا سهم برابری در بازخورد و طبقه‌بندی‌کننده تاخیری داشته باشیم، همانطور که در بخش 6-F بهتر بحث خواهد شد. برای همه طبقه‌بندی‌کننده‌های پایه درگیر (به عنوان مثال، $\mathcal{F}_t, \mathcal{W}_t^D, \mathcal{W}_t, \mathcal{M}_i, i = 1, \ldots, M$)، ما RF را که هر کدام 100 درخت دارد، اتخاذ می‌کنیم. هر درخت بر روی یک نمونه راه‌انداز متعادل آموزش داده می‌شود، که با کم‌نمونه‌سازی تصادفی طبقه اکثریت و حفظ تمام نمونه‌های کلاس اقلیت در مجموعه آموزشی مربوطه به دست می‌آید. به این ترتیب، هر درخت در مورد تراکنش‌های واقعی به‌طور تصادفی انتخاب شده و بر روی نمونه‌های تقلب مشابه آموزش داده می‌شود. این استراتژی کم‌نمونه‌سازی به فرد اجازه می‌دهد تا درختان را با توزیع متعادل یاد بگیرد و از بسیاری از زیرمجموعه‌های کلاس، اکثریت بهره‌برداری کند. در عین حال، زمان آموزش این دسته بندی کننده ها به طور معقولی کم است. یک اشکال کم‌نمونه‌گیری این است که ما به طور بالقوه نمونه‌های آموزشی مرتبط را از مجموعه داده‌ها حذف می‌کنیم، اگرچه این مشکل با این واقعیت کاهش می‌یابد که ما 100 درخت مختلف را برای هر طبقه‌بندی کننده پایه یاد می‌گیریم.

6-آزمایش

آزمایشات ما به شرح زیر سازماندهی شده است. در بخش 6-A، مجموعه داده ها را توصیف می کنیم و در بخش 6-B، تنظیمات آزمایشی را به تفصیل شرح می دهیم. بخش 6-C اولین آزمایش ما را ارائه می کند که از طبقه بندی کننده های شرح داده شده در بخش 5-A برای ارزیابی اثربخشی استراتژی یادگیری پیشنهادی استفاده می کند. در آزمایش دوم (بخش 6-D)، ما بیش از 54 میلیون تراکنش کارت اعتباری را که در طی 10 ماه به دست آمده‌اند، تجزیه و تحلیل می‌کنیم و نشان می‌دهیم که این جریان به طور جدی تحت تأثیر رانش مفهومی قرار گرفته است. سپس، برای بررسی توانایی انطباق استراتژی یادگیری پیشنهادی، ما به طور مصنوعی یک رانش مفهومی ناگهانی را در مکان‌های خاصی از جریان تراکنش معرفی می‌کنیم و عملکرد طبقه‌بندی را ارزیابی می‌کنیم. در آزمایش سوم (بخش 6-E)، سوگیری انتخاب نمونه معرفی شده توسط تعامل هشدار-بازخورد را بررسی می‌کنیم، و نشان می‌دهیم که وزن‌دهی اهمیت یک تکنیک مرسوم برای اصلاح SSB در مجموعه‌های آموزشی موثر نیست. بازخوردها در نهایت، در بخش 6-F، مهم ترین پارامترهای موثر بر استراتژی یادگیری پیشنهادی را مورد بحث قرار می دهیم.

Id	Start day	End day	# Days	# Instances	# Features	% Fraud Trx
2013	2013-09-05	2014-01-18	136	21'830'330	51	0.19%
2014-2015	2014-08-05	2015-05-31	296	54'764'384	51	0.24%

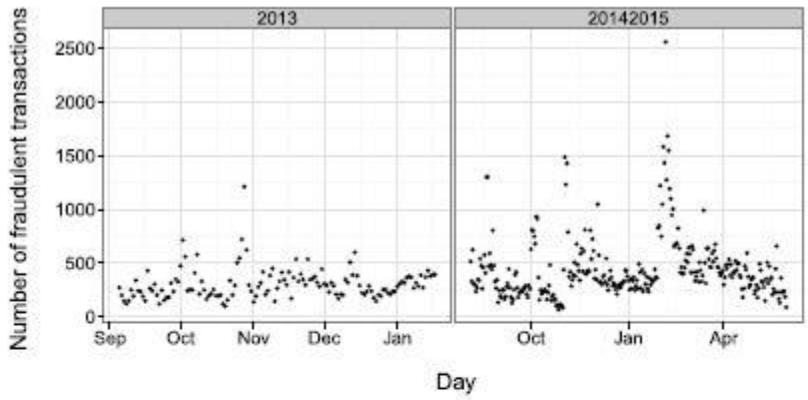
جدول 1: DATA SETS

A. مجموعه داده های ما

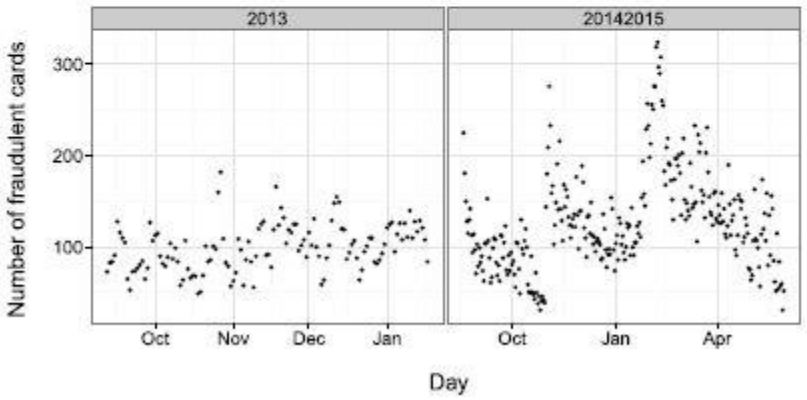
ما از دو مجموعه داده بزرگ از تراکنش های تجارت الکترونیک آنلاین از دارندگان کارت اعتباری اروپایی که توسط شریک صنعتی ما ارائه شده است استفاده می کنیم. حتی اگر این تراکنش‌ها از یک پایانه فیزیکی شروع نشده‌اند، اما تحت فرآیند مشابهی قرار می‌گیرند که در شکل 1 توضیح داده شده است. در جدول 1، ما تمام اطلاعات مربوط به این مجموعه داده‌ها را ارائه می‌کنیم، که به عنوان 2013 و 2014-2015، و به طور خاص مشخص می‌کنیم. ، ما بر عدم تعادل طبقاتی شدید تأکید می کنیم زیرا تقلب ها حدود 0.2٪ از کل معاملات را تشکیل می دهند. همانطور که در شکل 3 نشان داده شده است، تعداد کلاهبرداری ها در هر روز به طور قابل توجهی در طول زمان متفاوت است و تراکنش های کلاهبرداری بیشتر از کارت های متقلبانه وجود دارد که نشان می دهد گاهی اوقات کلاهبرداری های متعددی در یک کارت انجام می شود.

برای ارزیابی قابل اعتماد عملکرد تشخیص تقلب بر حسب P_k، مؤلفه CARD_ID را از همه بردارهای ویژگی حذف کردیم. این در هنگام آزمایش یک طبقه‌بندی کننده بر روی مجموعه داده‌ای از تراکنش‌های تاریخی بسیار

مهم است، زیرا طبقه‌بندی‌کننده‌ای که متغیر CARD_ID ورودی را دریافت می‌کند ممکن است این را به عنوان یک ویژگی متمایز برای شناسایی تقلب‌های متعدد از یک کارت در روزهای مختلف یاد بگیرد (در نتیجه عملکرد بسیار خوش‌بینانه ارائه می‌کند.). با این حال، در یک FDS دنیای واقعی، پس از شناسایی اولین مورد، امکان تقلب های متعدد از یک کارت وجود ندارد، زیرا همانطور که در بخش دوم بحث شد، آن کارت بلافاصله مسدود می شود. یک گزینه متفاوت حذف تمام تراکنش های یک کارت پس از شناسایی اولین تقلب است. با این حال، این تعداد تقلب‌های موجود را کاهش می‌دهد و عدم تعادل طبقاتی در مجموعه داده‌های ما را بدتر می‌کند. بنابراین، ما CARD_ID را منحصراً برای محاسبه ویژگی‌های انبوه در نظر می‌گیریم و آن را در بردارهای ویژگی لحاظ نمی‌کنیم.



(a)



(b)

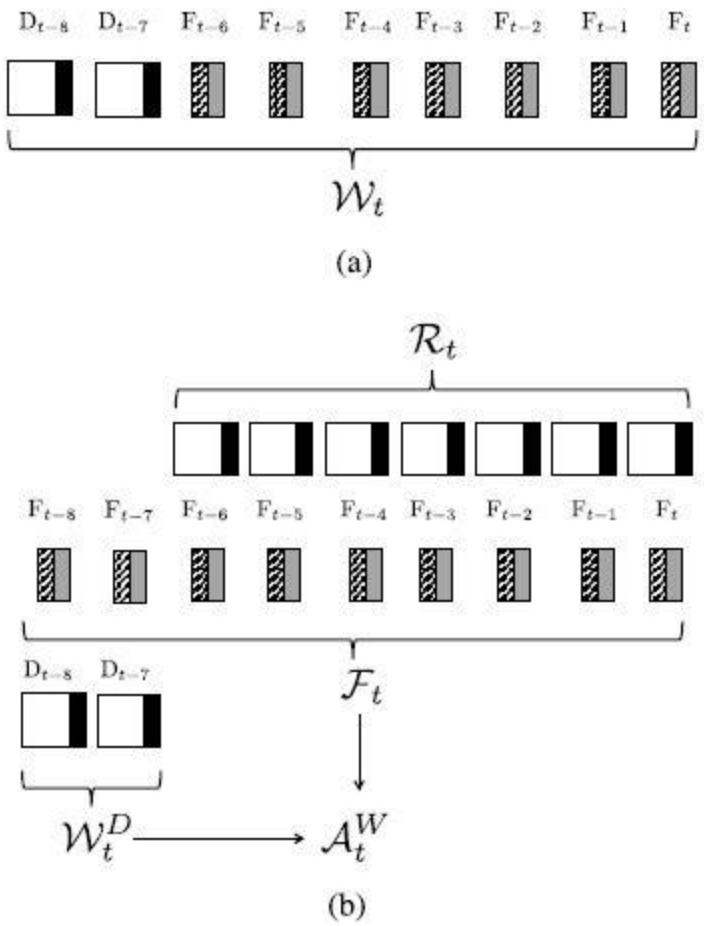
شکل 3: تعداد تراکنش‌ها و کارت‌های تقلبی در روز در مجموعه داده‌های شرح داده شده در جدول 1. مشخص می‌شود که تراکنش‌های کلاهبرداری بیشتر از کارت‌ها وجود دارد، به این معنی که برخی از کارت‌ها بیش از یک کلاهبرداری دریافت کرده‌اند. a) تعداد معاملات متقلبانه. b) تعداد کارتهای تقلبی.

B. تنظیمات آزمایشی

در توافق با شریک صنعتی خود، ما فرض کردیم که بازرسان می توانند هر روز حداکثر 100 کارت هشدار داده شده توسط DDM را بررسی کنند. بنابراین، F_t هر روز در طول Q روز آموزش داده می شود که شامل هر تراکنش هشدار از 100 دارنده کارت مختلف است. به یاد بیاوریم که بازخوردها به طبقه بندی کننده واقعی که برچسب ها را درخواست می کند بستگی دارد. به این ترتیب، مجموعه آموزشی F_t ممکن است هنگام استفاده در $\mathcal{A}_t$و زمانی که به طور مستقل استفاده می شود متفاوت باشد: در واقع، در مورد اول، هشدارها به خلفی(قسمت عقبی) D_t نیز بستگی دارند، در حالی که در دومی، هشدارها به طور منحصر به فرد توسط F_t تعیین می شوند.

ما عملکرد کلی تشخیص تقلب را در مجموعه داده‌های خود با میانگین معیارهای عملکرد روزانه (P_k، CP_k، و AUC) و همچنین با تجزیه و تحلیل مجموع رتبه‌های طبقه‌بندی‌کننده در هر روز ارزیابی می‌کنیم. به ویژه، در هر روز j، طبقه‌بندی‌کننده‌های آزمایش‌شده S را از بهترین تا کم‌بازده رتبه‌بندی می‌کنیم و با $r_{\mathcal{K},j} \in \{1, \dots, S\}$، نشان می‌دهیم. رتبه طبقه‌بندی‌کننده K در روز j: وقتی K بهترین طبقه‌بندی‌کننده است، رتبه آن حداکثر است، یعنی ، $r_{\mathcal{K},j} = S$، در حالی که وقتی بدترین است، ، $r_{\mathcal{K},j} = 1$. آزمون فریدمن را انجام می‌دهیم و این فرضیه صفر را رد می‌کنیم که همه طبقه‌بندی‌کننده‌ها عملکرد یکسانی دارند. سپس، با جمع کردن تمام رتبه‌های روزانه، یک رتبه‌بندی جهانی را تعریف می‌کنیم (جدول 2 را ببینید): هر چه مجموع رتبه‌ها بزرگتر باشد، طبقه‌بندی‌کننده بهتر است، و از آزمون‌های t زوجی برای تعیین اینکه آیا تفاوت‌ها در رتبه‌بندی جهانی معنی‌دار هستند یا خیر استفاده می‌کنیم. در عمل، برای هر جفت طبقه‌بندی‌کننده K و H، از آزمون t برای مقایسه رتبه‌های آنها در تمام روزها استفاده می‌شود (یعنی $r_{\mathcal{K},j} - r_{\mathcal{H},j}, j \in \{1, \dots, J\}$). j تعداد روزها.

هر آزمایش 10 بار تکرار می شود تا تغییرپذیری عملکرد کاهش یابد، و هنگام مقایسه طبقه بندی کننده ها در چند روز، شاخص t را از نماد طبقه بندی حذف می کنیم. در بیشتر آزمایش‌هایمان، یک هفته تأخیر تأیید $\delta = 7$ و $M = 8$ را در نظر می‌گیریم، به طوری که تعداد کلی بازخوردهای مورد استفاده $Q = M + \delta = 15$ است. در بخش 6-F، آزمایش‌ها را تکرار می‌کنیم. با در نظر گرفتن تاخیر تایید طولانی تر $\delta = 15$ و $M = 15$، $Q = 30$.



شکل 4: اطلاعات نظارت شده که توسط طبقه‌بندی‌کننده‌ها در نظر گرفته شده در آزمایش‌های ما استفاده می‌شود. در این مثال گویا، ما $\delta = 7$، $M = 2$ و $Q = 7 + 2 = 9$ را تنظیم کردیم . a) ادغام تمام تراکنش های برچسب دار. (b) تفکیک بازخوردها و نمونه های تاخیری.

C. جداسازی بازخوردها از نمونه های نظارت شده با تاخیر

برای ارزیابی اثربخشی استراتژی یادگیری پیشنهادی، عملکرد طبقه‌بندی‌کننده‌های پیشنهادی $\mathcal{A}^W$ (مثلا $\mathcal{A}^E$) را با معیارهای مربوطه معرفی‌شده در بخش 5-A و طبقه‌بندی‌کننده‌های مورد استفاده برای تعریف پسین آنها، یعنی $\mathcal{F}$ و $\mathcal{W}^{\mathcal{D}}$ (مثلا $\mathcal{E}^{\mathcal{D}}$) مقایسه می‌کنیم.). شکل 4 مجموعه آموزشی مربوط به استفاده از $\mathcal{A}_t^W$ و طبقه‌بندی‌کننده‌های مرتبط را نشان می‌دهد، در حالی که جدول 3 مهم‌ترین پارامترها و نمونه‌های آموزشی مورد استفاده توسط طبقه‌بندی‌کننده‌های در نظر گرفته شده را خلاصه می‌کند.

در این آزمایش، طبقه‌بندی‌کننده ایده‌آل $\mathcal{R}_t$ را نیز گنجانده‌ایم که در تمام تراکنش‌های مجاز بین روزهای t و t-δ آموزش داده شده است. این طبقه‌بندی‌کننده یک همتای ایده‌آل برای طبقه‌بندی‌کننده‌های پنجره کشویی

در نظر گرفته می‌شود، که به طور غیرواقعی فرض می‌کنند که محققین می‌توانند هر روز برچسب صحیح را به هر تراکنش مجاز اختصاص دهند. به طور خاص، مجموعه آموزشی $\mathcal{R}_t$ تحت تأثیر تعامل هشدار-بازخورد قرار نمی‌گیرد.

Classifier	Dataset	Average P_k			Average CP_k			Average AUC		
		mean (std)	sum of ranks	comparison	mean (std)	sum of ranks	comparison	mean (std)	sum of ranks	comparison
$\mathcal{A}^W$	2014-2015	0.77 (0.21)	1796.50	a	0.37 (0.18)	1824.00	a	0.94 (0.02)	1396.00	b
$\mathcal{F}$	2014-2015	0.73 (0.23)	1632.00	b	0.32 (0.17)	1505.00	b	0.87 (0.05)	409.00	e
$\mathcal{R}$	2014-2015	0.63 (0.24)	1156.00	c	0.30 (0.18)	1354.50	c	0.96 (0.02)	1822.00	a
$\mathcal{W}$	2014-2015	0.61 (0.25)	1055.50	d	0.25 (0.14)	955.00	d	0.91 (0.04)	865.00	d
$\mathcal{W}^D$	2014-2015	0.57 (0.26)	889.00	e	0.25 (0.14)	885.00	e	0.94 (0.03)	1315.00	c
$\mathcal{A}^W$	2013	0.75 (0.20)	732.00	a	0.35 (0.12)	754.50	a	0.94 (0.03)	631.00	b
$\mathcal{F}$	2013	0.73 (0.21)	693.00	b	0.32 (0.13)	670.50	b	0.89 (0.05)	229.00	e
$\mathcal{R}$	2013	0.58 (0.22)	493.50	c	0.25 (0.11)	514.00	c	0.96 (0.01)	736.00	a
$\mathcal{W}$	2013	0.54 (0.25)	434.00	d	0.22 (0.11)	387.00	d	0.91 (0.05)	355.00	d
$\mathcal{W}^D$	2013	0.50 (0.23)	345.00	e	0.21 (0.09)	330.00	e	0.93 (0.03)	539.00	c
$\mathcal{A}^E$	2014-2015	0.77 (0.21)	981.50	a	0.39 (0.17)	940.00	a	0.94 (0.03)	873.00	b
$\mathcal{F}$	2014-2015	0.73 (0.23)	827.50	b	0.36 (0.17)	800.50	b	0.87 (0.06)	294.00	d
$\mathcal{E}$	2014-2015	0.66 (0.25)	637.50	c	0.26 (0.14)	533.50	c	0.94 (0.03)	943.00	a
$\mathcal{E}^D$	2014-2015	0.54 (0.26)	323.50	d	0.23 (0.12)	276.00	d	0.93 (0.03)	660.00	c
$\mathcal{A}^E$	2013	0.76 (0.20)	410.50	a	0.37 (0.14)	335.00	a	0.94 (0.02)	380.00	a
$\mathcal{F}$	2013	0.73 (0.21)	354.00	b	0.35 (0.15)	285.00	b	0.89 (0.04)	129.00	c
$\mathcal{E}$	2013	0.62 (0.23)	246.50	c	0.24 (0.11)	193.00	c	0.93 (0.03)	374.00	a
$\mathcal{E}^D$	2013	0.48 (0.24)	119.00	d	0.20 (0.11)	97.00	d	0.93 (0.03)	247.00	b

جدول 2: عملکرد تشخیص تقلب هنگام استفاده از 15 روز تراکنش ($\delta = 7$، $M = 8$، و $Q = 15$)

جدول 2 میانگین P_k، CP_k و AUC را در تمام دسته‌ها برای دو مجموعه داده به طور جداگانه نشان می‌دهد. مقایسه ستون ها نتایج آزمون t زوجی را در رتبه های شرح داده شده در بالا گزارش می دهد. طبقه بندی کننده هایی که حرف یکسانی دارند نمی توانند به طور قابل توجهی متفاوت در نظر گرفته شوند. در هر دو مجموعه داده، $\mathcal{A}^W$ از نظر P_k و CP_k از W بهتر عمل می کند، و این نشان می دهد که جداسازی بازخوردها و نمونه های تاخیری در واقع یک استراتژی یادگیری خوب است. همین نتیجه برای گروه های در نظر گرفته شده، یعنی $\mathcal{A}^E$ و E صدق می کند. از آنجایی که هر دو $\mathcal{A}^E$ و $\mathcal{E}$ میانگین قسمت های خلفی افراد خود را دارند، تفاوت آنها فقط در وزن های تجمع است: در $\mathcal{A}^E$، 50٪ از وزن کل به $\mathcal{P}_{\mathcal{F}}(+|x)$ اختصاص می یابد. و 50٪ باقیمانده به طور مساوی بین افراد دیگر توزیع می شود. در مقابل، در $\mathcal{E}$ همه افراد به طور مساوی مشارکت دارند. همین رابطه بین $\mathcal{A}^W$ و W که به صورت پنجره کشویی به روز می شوند برقرار نیست. با این حال، در این مورد نیز می‌توان نتیجه گرفت که بازخوردها بسیار آموزنده هستند و برای افزایش دقت هشدار باید به دقت در نظر گرفته شوند. این نیز با این واقعیت تأیید می‌شود که $\mathcal{F}$ از $\mathcal{W}^{\mathcal{D}}$ و W بهتر عمل می‌کند. به عنوان یک نظر کلی، ما متذکر می‌شویم که CP_k معمولاً کمتر از P_k است، زیرا اغلب تقلب‌های متعدد روی یک کارت انجام می‌شود.

جدول 2 همچنین نتایج را بر حسب AUC گزارش می‌کند، یک معیار رتبه‌بندی جهانی که پسین طبقه‌بندی‌کننده را در تمام نمونه‌ها و نه تنها در k بالا (متفاوت از CP_k و P_k) ارزیابی می‌کند. از نظر AUC،

طبقه‌بندی‌کننده ایده‌آل $\mathcal{R}$ به‌طور قابل‌توجهی بهتر از $\mathcal{A}^W$ است و $\mathcal{F}$ به مراتب بدتر است، که نشان می‌دهد $\mathcal{F}$ هنگام رتبه‌بندی همه تراکنش‌ها مؤثر نیست.

ما این نتایج را به صورت زیر تفسیر می کنیم: زمانی که هدف به دست آوردن یک رتبه بندی دقیق از مشکوک ترین کارت ها است (به عنوان مثال، حداکثر کردن CP_k)، باید وزن های بزرگ تری را به تراکنش هایی که به اندازه تراکنش هایی که می خواهیم پیش بینی کنیم مخاطره آمیز هستند، اختصاص دهیم، بنابراین از $\mathcal{A}^W$ استفاده می کنیم. . برعکس، یک طبقه‌بندی‌کننده آموزش‌دیده بر روی تمام تراکنش‌های روزانه (که عمدتاً واقعی هستند) در رتبه‌بندی همه تراکنش‌ها بهتر است، زیرا از ناحیه زیر منحنی $\mathcal{R}$ ROC (AUC) بیرون می‌آید. در جدول 2، همچنین می‌توانیم ببینیم که $\mathcal{R}$ از نظر P_k، CP_k و AUC از $\mathcal{W}^{\mathcal{D}}$ بهتر عمل می کند. این نتیجه نشان می دهد که جریان تراکنش های کارت اعتباری غیر ثابت است. در واقع، هر دو مجموعه آموزشی $\mathcal{R}$ و $\mathcal{W}^{\mathcal{D}}$ شامل تمام معاملات مجاز در $\delta = 7$ و $M = 8$ روز متوالی هستند. تفاوت عمده آنها در این است که $\mathcal{R}$ در آخرین تراکنش ها آموزش دیده است، در حالی که تراکنش ها در $\mathcal{W}^{\mathcal{D}}$ با تاخیر δ روز انجام می شوند. این واقعیت که $\mathcal{R}$ بهتر از $\mathcal{W}^{\mathcal{D}}$ عمل می کند نشان می دهد که جدیدترین تراکنش ها برای کشف تقلب ها در روزهای آینده اطلاعات بیشتری دارند و بنابراین توزیع تراکنش غیر ثابت است.

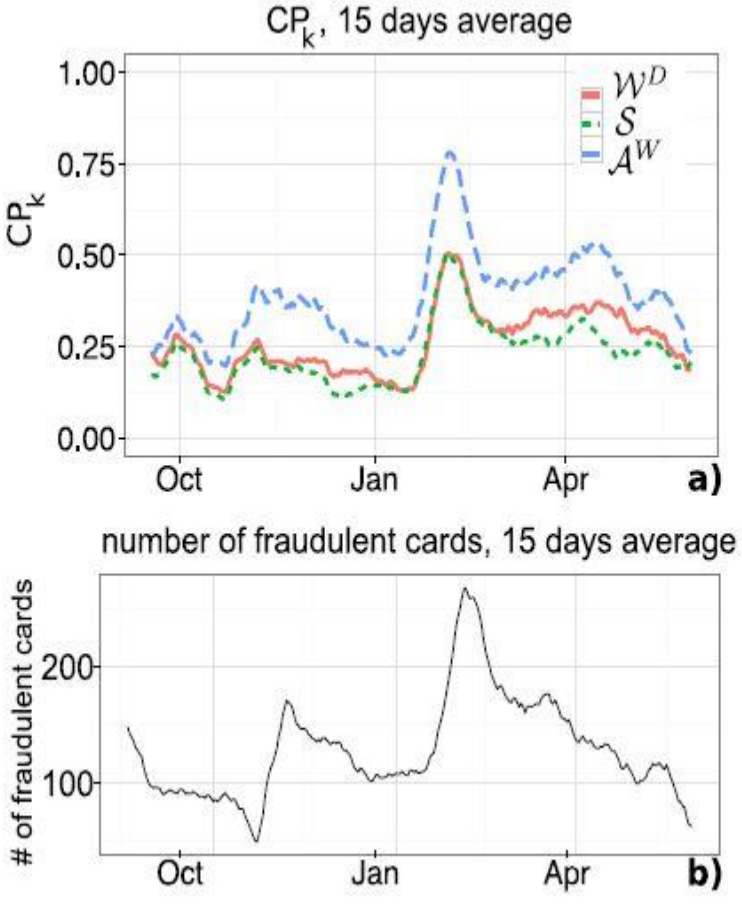
انحراف استاندارد P_k و CP_k که در جدول 2 گزارش شده است، به ویژه در مقایسه با AUC بسیار زیاد است. همانطور که در بخش 3 بحث کردیم، و همانطور که در شکل 5 نشان داده شده است، مقادیر CP_k (و همچنین P_k) به شدت تحت تاثیر تعداد تقلب هایی است که هر روز رخ می دهد. از آنجایی که این عدد در طول زمان به شدت در نوسان است (شکل 3 را ببینید)، انتظار چنین پراکندگی بزرگی منطقی است. ما خاطرنشان می‌کنیم که مقایسه بین طبقه‌بندی‌کننده‌ها در جدول 2 نشان می‌دهد که تفاوت‌ها از نظر عملکرد، با وجود چنین انحراف استاندارد زیاد، همیشه قابل توجه است. توجه داشته باشید که مقادیر NCP_k (به جدول 4 مراجعه کنید) کمتر تحت تأثیر چنین نوساناتی قرار می گیرند.

Symbol	supervised samples	adaptation	# days training
$\mathcal{F}$	feedbacks	sliding	Q
$\mathcal{W}^D$	delayed	sliding	M
$\mathcal{W}$	feedbacks + delayed	sliding	$\delta + M$
$\mathcal{A}^W$	feedbacks + delayed	sliding	$Q + M$
$\mathcal{R}$	all the recent	sliding	δ
$\mathcal{E}^D$	delayed	ensemble	M
$\mathcal{E}$	feedbacks + delayed	ensemble	$\delta + M$
$\mathcal{A}^E$	feedbacks + delayed	ensemble	$Q + M$

جدول 3: طبقه‌بندی‌کننده‌ها در آزمایش‌های ما در نظر گرفته شده‌اند

D. رانش مفهومی

در این بخش، ابتدا مجموعه داده‌های 2014-2015 را که شامل بیش از 54 میلیون تراکنش مجاز طی 10 ماه است، تجزیه و تحلیل می‌کنیم و نشان می‌دهیم که این جریان تحت تأثیر رانش مفهومی است. برای این منظور از طبقه‌بندی‌کننده استاتیک S_t استفاده می‌کنیم که در ابتدا در روز M آموزش داده می‌شود و هرگز به‌روزرسانی نمی‌شود (به‌طوری که در ابتدا با $\mathcal{W}_t^D$ مصادف می‌شود) و آن را با $\mathcal{W}_t^D$ (که در عوض مرتب به‌روزرسانی می‌شود) و $\mathcal{A}_t^W$ (که همچنین از نمونه های نظارت شده به روز شده استفاده می کند) مقایسه می کنیم. در یک مسئله طبقه بندی ثابت، دو طبقه بندی کننده S و $\mathcal{W}^{\mathcal{D}}$ عملکرد مشابهی دارند. این واقعیت که S_t در طول زمان از $\mathcal{W}_t^D$ بهتر عمل می کند [به شکل 5(a) مراجعه کنید] تأیید می کند که این مجموعه داده تحت تأثیر رانش مفهومی قرار گرفته است. اگرچه ممکن است تعجب آور به نظر نرسد که جریان تراکنش های کارت اعتباری غیر ثابت است، تا جایی که می دانیم، تحلیل ما اولین تحلیل در مورد تأثیر رانش مفهومی بر چنین مجموعه داده تراکنش بزرگی است.



classifier	mean	sd	sum of ranks	comparison	k
$\mathcal{A}^W$	0.48	0.09	506.00	a	300
$\mathcal{F}$	0.46	0.10	448.00	b	300
$\mathcal{W}$	0.38	0.11	283.00	c	300
$\mathcal{W}^D$	0.35	0.10	172.50	d	300
$\mathcal{A}^W$	0.41	0.10	519.50	a	150
$\mathcal{F}$	0.38	0.10	441.50	b	150
$\mathcal{W}$	0.29	0.10	272.50	c	150
$\mathcal{W}^D$	0.27	0.09	179.50	d	150
$\mathcal{A}^W$	0.40	0.13	518.50	a	100
$\mathcal{F}$	0.37	0.13	443.00	b	100
$\mathcal{R}$	0.29	0.10	342.50	c	100
$\mathcal{W}^D$	0.26	0.11	249.00	d	100

جدول 4: میانگین NCP_k هنگامی که $k \geq 100$ در مجموعه داده 2013 ($\delta = 15$)

شکل 5 : (الف) مقادیر CP_k برای S، $\mathcal{W}^{\mathcal{D}}$، و $\mathcal{A}^{W}$ در مجموعه داده 2014-2015. (ب) تعداد کارتهای تقلبی در همان دوره. به منظور تجسم، این مقادیر به طور متوسط در یک پنجره کشویی 15 روزه محاسبه شده اند. اوج CP_k در (a) مطابق با اوج تعداد کارت های تقلبی در (b) است. این نتیجه تأیید می‌کند که طبقه‌بندی‌کننده‌ها در آن روزهایی که با تعداد زیادی کارت‌های تقلبی مشخص می‌شد، دقیق‌تر می‌شوند.

شکل 5(a) همچنین نشان می‌دهد که $\mathcal{A}^{W}$ پیشنهادی همیشه از نظر CP_k به عملکرد برتر دست می‌یابد، که انطباق بهتری با رانش مفهومی را نشان می‌دهد. شایان ذکر است که عملکرد همه طبقه‌بندی‌کننده‌ها در شکل 5 (الف) کاملاً نوسان دارد و اوج خود را در فِوریه 2015 گزارش می‌کند. این در واقع ماهی است که بیشترین تعداد کارت‌های تقلبی را در مجموعه داده ما دارد [که در گزارش شده است. شکل 5 (ب)]. در مقابل، در اکتبر 2014 (دوره ای که کمترین تعداد کارت های تقلبی را در مجموعه داده های ما نشان می دهد)، همه طبقه بندی کننده ها به مقادیر پایین CP_k دست می یابند. بنابراین، شکل 5 تأیید می کند که دقت هشدار به شدت به تعداد کارت های تقلبی در یک روز بستگی دارد.

برای بررسی بیشتر عملکرد انطباق $\mathcal{A}^{W}$ در محیط‌های غیر ثابت، توانایی‌های انطباق آن را با توجه به یک رانش مفهومی معرفی شده مصنوعی ارزیابی می‌کنیم. به طور خاص، ما به طور مصنوعی تغییراتی را در مکان‌های شناخته شده معرفی می‌کنیم و یک جابجایی ناگهانی را در بالای (تدریجی) آنکه بر جریان تراکنش تأثیر می‌گذارد، اضافه می‌کنیم، که قبلاً در مورد آن بحث کردیم. ما 10 جریان کوتاه را با کنار هم قرار دادن معاملات مجاز در دو ماه غیر متوالی آماده کردیم. هر یک از این جریان‌ها شامل یک رانش مفهومی ناگهانی در وسط است، که وقتی فاصله زمانی بین ماه‌های کنار هم افزایش می‌یابد، باید به وضوح قابل درک باشد. برای ارزیابی توانایی انطباق استراتژی یادگیری پیشنهادی، عملکرد $\mathcal{A}^{W}$ و $\mathcal{W}^{\mathcal{D}}$ را از نظر CP_k مقایسه می‌کنیم. به طور خاص، ما افت عملکرد نسبی ناشی از رانش مفهوم را به عنوان تفاوت بین CP_k در ماه اول و دوم، تقسیم بر مقدار CP_k در ماه اول اندازه‌گیری می‌کنیم. آزمایش‌های ما نشان می‌دهد که در این 10 مجموعه داده، 7.7% ،CP_k از $\mathcal{A}^{W}$کاهش می‌یابد، در حالی که 12.5%،CP_k از $\mathcal{W}^{\mathcal{D}}$کاهش می‌یابد که عملکرد انطباق برتر استراتژی یادگیری پیشنهادی را تایید می‌کند.

E. سوگیری انتخاب نمونه به دلیل تعامل هشدار-بازخورد

در اینجا ما بررسی می کنیم که آیا وزن دهی اهمیت، یک راه حل اصلی برای اصلاح SSB، می تواند با موفقیت SSB معرفی شده توسط تعامل هشدار-بازخورد را جبران کند یا خیر؟ برای این منظور، طبقه‌بندی بازخورد $\mathcal{F}_t$

را در نظر می‌گیریم، زیرا این طبقه‌بندی‌کننده عمدتاً تحت تأثیر SSB به دلیل تعامل هشدار-بازخورد قرار می‌گیرد، و از پیاده‌سازی حساس به وزن RFها بر اساس درخت‌های استنتاج شرطی استفاده می‌کنیم.

وزن دهی مهم شامل وزن دهی مجدد هر نمونه تمرین بر حسب فوت با استفاده از وزن زیر است:

$$w = \frac{\mathcal{P}(\mathbf{s} = 1)}{\mathcal{P}(\mathbf{s} = 1|x, y)} \qquad (10)$$

که در آن s یک متغیر انتخابی است که به هر نمونه در T_t مقدار 1 را در صورتی که تراکنش بر حسب F_t باشد و 0 را در غیر این صورت مرتبط می کند. بنابراین، P(s = 1|x,y) مربوط به احتمال قرار گرفتن نمونه (x,y) در مجموعه آموزشی F_t است. تعریف اوزان در (10) از قضیه بیز و این واقعیت ناشی می شود که می توان توزیع پیوستگی بی طرف P(x, y) را با توجه به توزیع مشترک بایاس P(x) بیان کرد.P(x,y| s = 1) به عنوان:

$$\mathcal{P}(x, y) = \frac{\mathcal{P}(\mathbf{s} = 1)}{\mathcal{P}(\mathbf{s} = 1|x, y)}\mathcal{P}(x, y|\mathbf{s} = 1) = w\mathcal{P}(x, y|\mathbf{s} = 1).$$

جدول 5 عملکرد به دست آمده در هنگام تصحیح SSB با استفاده از وزن های ارائه شده توسط (10) را گزارش می کند و مشخص می شود که این وزن ها از عملکرد به دست آمده توسط $\mathcal{F}$ در جدول 2 کمتر است. وزن دهی اهمیت در واقع عملکرد $\mathcal{F}$ را بهبود نمی بخشد، که ما آن را به عنوان یک شکست در هنگام جبران SSB معرفی شده توسط تعامل هشدار-بازخورد تفسیر می کنیم.

ما معتقدیم که وزن‌دهی اهمیت به‌دلیل تعامل هشدار-بازخورد، بی‌اثر می‌شود، زیرا P(s = 1|x,y) و P(+|x) در (10) همبستگی بالایی دارند. این بدان معناست که هر چه تراکنش بیشتر به عنوان ریسک در نظر گرفته شود، احتمال P(s = 1|x, y) بیشتر است و وزن آن در (10) کمتر است. بنابراین، وزن‌دهی اهمیت، تأثیر آن نمونه‌ها را در بازخوردهایی که احتمال تقلب دارند، کاهش می‌دهد و این بر دقت هشدار تأثیر منفی می‌گذارد.

به عنوان یک بررسی عقلانی، ما این آزمایش را در چارچوبی تکرار کردیم که در آن نمونه‌های نظارت شده اخیر با تعامل هشدار-بازخورد ارائه نمی‌شوند، بلکه به‌طور تصادفی (در همان تعداد و نسبت‌های کلاس آزمایش فوق) از میان تراکنش‌هایی که مبلغی بزرگ‌تر از AC500 دارند، انتخاب می‌شوند. این شکل از SSB به عنوان تغییر متغیر نامیده می شود زیرا ما P(s|y, x) = P(s|x) داریم، یعنی با توجه به ورودی x، متغیر انتخابی s مستقل از کلاس y است. در این مورد، وزن‌دهی اهمیت توانست این سوگیری را به درستی جبران کند و طبقه‌بندی‌کننده منحرف از طبقه‌بندی‌کننده مشابهی که بدون اصلاح SSB آموزش داده شده است، بهتر عمل می‌کند.

metric	mean	sd	dataset
P_k	0.68	0.26	2014-2015
P_k	0.59	0.26	2013
CP_k	0.26	0.16	2014-2015
CP_k	0.25	0.13	2013
AUC	0.85	0.06	2014-2015
AUC	0.85	0.06	2013

جدول 5: میانگین P_k، CP_k و AUC برای $\mathcal{F}_t$ وقتی $Q = 15$

classifier	mean	sd	sum of ranks	comparison	dataset
$\mathcal{A}^W$	0.38	0.17	1671.00	a	2014-2015
$\mathcal{F}$	0.36	0.17	1482.50	b	2014-2015
$\mathcal{R}$	0.31	0.17	1234.50	c	2014-2015
$\mathcal{W}$	0.25	0.13	850.50	d	2014-2015
$\mathcal{W}^D$	0.24	0.12	705.50	e	2014-2015
$\mathcal{S}$	0.23	0.12	605.50	f	2014-2015
$\mathcal{A}^W$	0.38	0.14	609.00	a	2013
$\mathcal{F}$	0.35	0.14	541.00	b	2013
$\mathcal{R}$	0.27	0.11	411.50	c	2013
$\mathcal{W}$	0.25	0.13	325.50	d	2013
$\mathcal{W}^D$	0.24	0.12	281.00	e	2013
$\mathcal{S}$	0.20	0.12	198.00	f	2013

جدول 6: میانگین CP_k هنگام استفاده از 30 روز ($\delta = 15$، $M = 15$، و $Q = 30$)

F. تاثیر پارامترها

در اینجا نشان می‌دهیم که چگونه عملکرد $\mathcal{F}_t$ و $\mathcal{A}_t^W$ تحت تأثیر: 1) تعداد روزهای بازخورد در نظر گرفته شده برای آموزش طبقه‌بندی‌کننده‌های ما (یعنی Q) قرار می‌گیرد. 2) تعداد کارت هایی که هر روز توسط بازرسان کنترل می شوند. و 3) پارامتر α که طبقه بندی کننده تجمع را در (9) تنظیم می کند. برای این منظور، ما δ = 15 روز تأخیر تأیید را در نظر می گیریم، به طوری که $\mathcal{F}_t$ در 30 روز بازخورد آموزش داده می شود (Q = 30، M = 15، و δ = 15) و نمونه های نظارت شده با تأخیر پس از 15 روز می آیند. جدول 6 نشان می دهد که F از نظر CP_k زمانی که با استفاده از Q = 30 روز بازخورد آموزش داده شود نسبت به Q = 15 بهتر است (جدول 2 را ببینید). همین امر برای $\mathcal{A}^W$، به عنوان یک نتیجه از عملکرد برتر به دست آمده توسط $\mathcal{F}$ ، صدق می کند. بنابراین، مقدار بیشتر بازخوردهای استفاده شده در طول آموزش به خوبی در این مورد افزایش تأخیر تأیید را جبران می کند.

ما این آزمایش را با در نظر گرفتن تعداد بیشتری بازخورد در روز تکرار می کنیم تا نشان دهیم این پارامتر چگونه بر عملکرد $\mathcal{F}$ و $\mathcal{A}^W$ تأثیر می گذارد. در جدول 4، فرض می‌کنیم که محققان می‌توانند بیش از 100 کارت را بررسی کنند و عملکرد تشخیص تقلب را بر حسب NCP_k گزارش کنند تا دقت هشدار را زمانی که بتوان کارت‌های بیشتری را کنترل کرد، به درستی ارزیابی کرد. این نتیجه تأیید می‌کند که داشتن بازخوردهای بیشتر، عملکرد برتر در تشخیص تقلب را تضمین می‌کند. این تجزیه و تحلیل می تواند به عنوان یک دستورالعمل برای شرکت هایی در نظر گرفته شود که باید تصمیم بگیرند که آیا هزینه های استخدام محققان بیشتر با بهبود مورد انتظار در عملکرد کشف تقلب جبران می شود یا خیر.

یکی دیگر از پارامترهای مهم در استراتژی یادگیری ما α است که سهم بازخورد و طبقه بندی کننده های تاخیری را در (9) متعادل می کند. این به طور تجربی پس از بررسی استراتژی های متعدد برای تطبیق این پارامتر به صورت روزانه روی 0.5 تنظیم شد. ایده ما این بود که دقت (یا سایر معیارهای عملکرد) به دست آمده در طول روز t-1 توسط $\mathcal{F}_{t-1}$ و $\mathcal{D}_{t-1}$ را در نظر بگیریم و سپس وزن هایی را به $\mathcal{F}_t$ و $\mathcal{D}_t$ نسبت دهیم (بهترین طبقه بندی کننده در طول روز t-1 بود. ، وزن در طول روز t بزرگتر است). متأسفانه، به نظر می‌رسد هیچ یک از راه‌حل‌های پیاده‌سازی‌شده از میانگین دو مورد پسین، یعنی $\alpha_t = 0.5 \forall t$بهتر عمل نمی‌کند.

بنابراین، ما یک شبیه‌سازی گسترده را روی راه‌حل پنجره کشویی اجرا کردیم، جایی که هر روز $\alpha_t \in \{0.1, 0.2, \ldots, 0.9\}$ را ، آزمایش کردیم و سپس α_t^* را به عنوان یکی از آنها انتخاب می کنیم که تجمع را در بهترین حالت بر حسب P_k انجام می دهد. چنین انتخاب بهینه ای از وزن ها البته در یک FDS در دنیای واقعی امکان پذیر نیست، زیرا نیاز به درخواست بازخورد برای هر$\alpha_t \in \{0.1, 0.2, \ldots, 0.9\}$ است. با این حال، تنظیم α_t^* روزانه حداقل بهبود را با توجه به تنظیم $\alpha_t = 0.5 \forall t$ به همراه داشت. این را می توان با این واقعیت توضیح داد که α_t^* توزیع اوج در حدود 0.5 داشت که میانگین $(\alpha_t^*) \approx 0.52$ داشت. مقدار P_k با نزدیک شدن به α = 0.1 و α = 0.9 به طور پیوسته کاهش می یابد، که نشان می دهد مقادیر شدید α به ندرت بهترین گزینه هستند. در این موارد شدید، $\mathcal{A}_t$ به D_t یا F_t نزدیک می شود (که نشان داده شده است بهترین گزینه نیستند) و طبقه بندی کننده که کمترین وزن را دریافت می کند، شانس کمی برای درخواست بازخورد به منظور بهبود عملکرد و افزایش وزن خود دارد.

نتیجه

اکثر کارهایی که به مشکل کشف تقلب در تراکنش‌های کارت اعتباری می‌پردازند، به‌طور غیرواقعی فرض می‌کنند که کلاس هر تراکنش بلافاصله برای آموزش طبقه‌بندی‌کننده ارائه می‌شود. در اینجا ما شرایط کاری دنیای واقعی FDS را به تفصیل تجزیه و تحلیل می‌کنیم و یک توصیف رسمی از مشکل طبقه‌بندی مفصلی ارائه می‌کنیم. به طور خاص، ما تعامل هشدار-بازخورد را شرح داده‌ایم، که مکانیزمی است که نمونه‌های نظارت شده اخیر را برای آموزش/به‌روزرسانی طبقه‌بندی‌کننده ارائه می‌کند. ما همچنین ادعا می‌کنیم که برخلاف معیارهای عملکرد سنتی که در ادبیات استفاده می‌شود، در یک FDS دنیای واقعی، دقت هشدارهای گزارش‌شده احتمالاً معنادارترین است، زیرا محققان می‌توانند تنها چند هشدار را بررسی کنند.

آزمایش‌های ما بر روی دو مجموعه داده گسترده از تراکنش‌های دنیای واقعی نشان می‌دهد که برای دریافت هشدارهای دقیق، دادن اهمیت بیشتری به بازخوردها در طول مشکل یادگیری الزامی است. جای تعجب نیست که بازخوردها نقش اصلی را در استراتژی یادگیری پیشنهادی ایفا می‌کنند، که شامل آموزش جداگانه طبقه‌بندی

کننده در مورد بازخوردها و طبقه‌بندی کننده بر روی نمونه‌های نظارت شده با تأخیر، و سپس جمع‌آوری پسین آنها برای شناسایی هشدارها است. آزمایش‌های ما همچنین نشان می‌دهد که راه‌حل‌هایی که تأثیر بازخوردها را در فرآیند یادگیری کاهش می‌دهند (به‌عنوان مثال، طبقه‌بندی‌کننده‌هایی که بازخوردها و نمونه‌های نظارت شده با تأخیر را ترکیب می‌کنند یا طرح‌های وزن‌دهی نمونه را اجرا می‌کنند) اغلب هشدارهای دقیق‌تری را ارائه می‌دهند.

کار آینده مربوط به مطالعه روش‌های تجمع تطبیقی و احتمالاً غیرخطی برای طبقه‌بندی‌کننده‌های آموزش‌دیده بر روی بازخوردها و نمونه‌های نظارت شده با تاخیر است. ما همچنین انتظار داریم که دقت هشدار را با اجرای رویکرد یادگیری برای رتبه بندی افزایش دهیم که به طور خاص برای جایگزینی تجمع خطی احتمالات پسین طراحی شده است. در نهایت، یک جهت تحقیقاتی بسیار امیدوارکننده مربوط به روش‌های یادگیری نیمه‌نظارت‌شده برای بهره‌برداری در فرآیند یادگیری است، همچنین چند تراکنش بدون برچسب اخیر.

منابع

[1] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, “Credit card fraud detection and concept-drift adaptation with delayed supervised information,” in Proc. Int. Joint Conf. Neural Netw., 2015,.pp. 1–8