فصلنامه پژوهش در علوم، مهندسی و فناوری
دوره ۴، شماره ۱، بهار ۱۳۹۷
صفحات ۴۱-۵۰
ISSN: 2476-5082
www.uctjournals.com

بررسی الگوریتم بیزین برای پیشنهاد بهترین روش کارآمد در افزایش امنیت شبکه

محمد البوغبیش

گروه فناوری اطلاعات، دانشگاه آزاد اسلامی،واحد شادگان،شادگان، ایران

چکیده

با رشد سریع شبکه های کامپیوتری و فراگیر شدن اینترنت حملات روی شبکه و بخصوص اینترنت افزایش یافته است. سیستم های تشخیص نفوذ برای اطمینان از پردازش و ذخیره ی امن داده ها روی شبکه توسعه داده شده اند. یکی از مهمترین حملات روی شبکه حملات ممانعت از سرویس است. یک شبکه ی امن باید ویژگی جامعیت داده ها، در دسترس بودن داده ها و درستی داده ها را دارا باشد. که در دسترس بودن داده ها همان مقابله و شناسایی حملات ممانعت از سرویس می باشد. با توجه به روز شدن حملات باید از سیستم های یادگیری در سیستم تشخیص نفوذ استفاده کرد که قابلیت استخراج الگو از حملات قبلی را داشته و بتواند حملات جدید را تشخیص دهد. در ابتدای این پژوهش ابتدا روی مجموعه ی داده پیش پردازش را انجام داده و سپس با استفاده از طبقه بند بیزین که در ادامه آورده شده است، با توجه به پارامتر دقت، بهترین الگوریتم را پیشنهاد می کنیم.

واژه‌های کلیدی: حملات، الگوریتم های بیزین، ممانعت ، امنیت

مقدمه

با شناخت مفهوم طبقه بندی که عبارتست از تخصیص رکوردها و یا هر مجموعه ای از اشیا به مجموعه مشخصی از طبقه ها است، یکی از مهمترین ابرازها برای پیاده سازی تکنیکهای مختلف داده کاوی استدلال بیزی است. اهمیت استدلال بیزی در داده کاوی را می‌توان به دلیل زیر نسبت داد. الگوریتم‌های یادگیری بیزی که به طور صریح بر روی احتمالات فرض‌های مختلف کار می‌کنند، مانند naïve Bayes classifier که از جمله کاراترین وعملی‌ترین الگوریتم‌های ممکن برای برخی مسائل یادگیری می‌باشد . به عنوان مثال(Michie 1994) مقایسه کاملی بین این الگوریتم و سایر الگوریتم‌های یادگیری مانند درخت تصمیم و شبکه عصبی انجام داده است . این محقق نشان داد که الگوریتم naïve Bayes classifier قابل رقابت با سایر الگوریتم‌ها و در برخی موارد بهتر از آنها عمل می‌کند . در ادامه ابتدا دو الگوریتم طبقه بندی یعنی الگوریتم ساده بیزی و الگوریتم K-Mean که حالت خاصی از الگوریتم EM را توضیح می دهیم . سپس پیاده سازی خود از این الگوریتمها و نتایج تجربی و توضیح آنها و معایب و مزایای هر یک را مورد بررسی قرار می دهیم .

بیز ساده

فرض کنید A_1 و A_2 ویژگی‌های با مقادیر گسسته باشند. این مقادیر برای پیش‌بینی یک کلاس گسسته‌ی C بکار می‌روند. هدف ما از پیش‌بینی و انتخاب دسته‌ای است که رابطه‌ی ۴-۱ بیشینه شود.

$$P(C = c|A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n)$$

با استفاده از قانون بیزین داریم:

$$Beiz = \frac{P(AA_1 = \alpha_1 \cup \dots \cup A_n = \alpha_n|C = c) * p(C = c)}{P(A_1 = \alpha_1 \cup \dots \cup A_n = \alpha_n)}$$

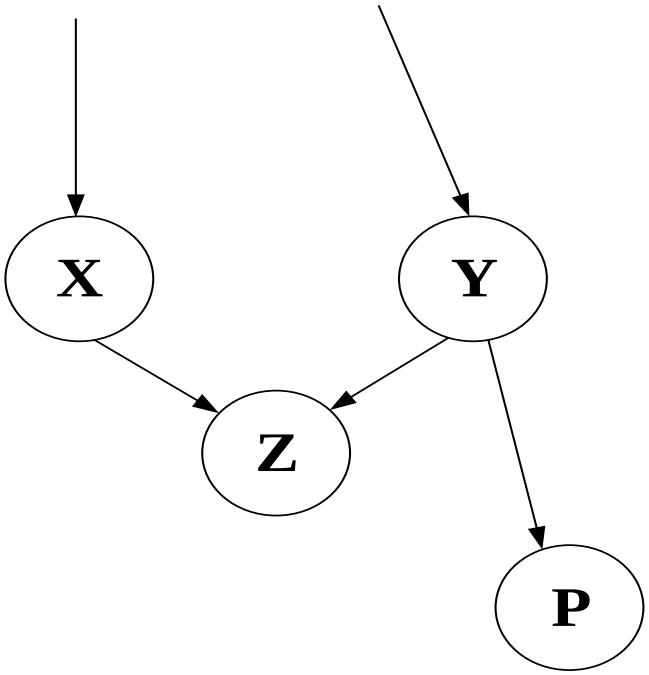
که مخرج کسر برای تصمیم‌گیری بی‌تاثیر است. زیرا که برای همه‌ی مقادیر C یکسان است از طرفی با وجه به استقلال مجموعه ویژگی‌ها داریم:

$$P(AA_1 = \alpha_1 \cup \dots \cup A_n = \alpha_n|C = c) * p(C = c) = P(A_1 = \alpha_1|C = c) * \dots * p(A_n = \alpha_n|C = c))$$

در کل برای مسائل طبقه‌بندی اگر C به عنوان صفت شاخص در نظر بگیریم، هدف حداکثر کردن مقدار $p(X|C_i) * p(C_i)$ است که x صفات دیگر هستند. از مزایای بیز ساده اجرای راحت و نتایج خوب برای بسیاری از کاربردهاست. اما از معایب آن می‌توان گفت که شاید همه‌ی ویژگی‌ها از هم مستقل نباشند و وابستگی وجود دارد که در این مورد مدل ضعیف است.

۴-۲-۲ شبکه‌های بیزین

شبکه‌های بیزین وابستگی‌های شرطی بین متغیرها را شرح می‌دهد. با استفاده از این شبکه‌ها دانش قبلی در زمینه‌ی وابستگی بین متغیرها با داده‌های آموزش مدل طبقه‌بندی ترکیب می‌شود. شکل ۴-۱ یک نمونه از شبکه‌ی بیزین را نمایش می‌دهد.



شکل ۴- ۱ یک شبکه‌ی بیزین ساده

۴-۲-۳ مفاهیم اساسی شبکه‌ی بیزین

در شبکه‌ی بیزین، گره‌ها، متغیرهایی هستند که هر کدام مجموعه‌ی مشخصی از وضعیت‌های دوبه‌دو و ناسازگار دارند. یال نشان‌دهنده‌ی وابستگی‌های متغیرها به یکدیگر می‌باشند. برای هر گره توزیع احتمال محلی وجود دارد که به گره وابسته است و از وضعیت والدین مستقل می‌باشد.

فرض مهم در روش بیزین استقلال شرطی طبقه‌ها از یکدیگر است اما در عمل این وابستگی بین متغیرها وجود دارد. شبکه‌های احتمالی بیزی این نوع احتمال‌ها را بررسی می‌کند. یک شبکه‌ی بیزی از دو بخش گراف غیرحلقوی و احتمال‌های شرطی تشکیل شده است. اگر کمانی از Y به Z وصل شود بدین

معناست که Y والد Z است. هر یال دانش علل و معلولی بین متغیرهای مرتبط را نشان می‌دهد. هر متغیر A با والدین $B_1,...,B_n$ را بصورت یک جدول فرض کنید که x با ویژگی $x_1, x_2, \dots, x_n$ است، در اینصورت:

$$p(x_1, x_2, \dots, x_n) = \prod_{i=1}^{n} p(x_1 | parents(y_i))$$

برای یادگیری این شبکه چند سناریو وجود دارد. یکی از این سناریوها استفاده از افراد خبره برای پرکرده جدول احتمال شرطی و ترسیم گراف مربوطه است. روش دیگر استفاده از روش‌های هیوریستیک است که در ادامه مورد بررسی قرار می‌گیرد.

روش‌های هیوریستیک

در روش‌های جستجوی عمقی، سطحی ، عمقی محدود شده، عمقی تکرارشونده و هزینه یکنواخت از هیچ تابعی برای تخمین میزان بهینگی هر داده استفاده نمی‌کنیم. تنها در جستجوی هزینه یکنواخت هزینه هر گام را برای سنجش میزان بهینگی داده‌ها به کار می‌بریم. اما در این روش جستجو نیز از اطلاعات مسئله برای تخمین میزان بهینگی هر داده بهره نبردیم. تابعی که عمل تخمین بهینگی هر داده را انجام می‌دهد، تابع اکتشافی می‌نامیم.

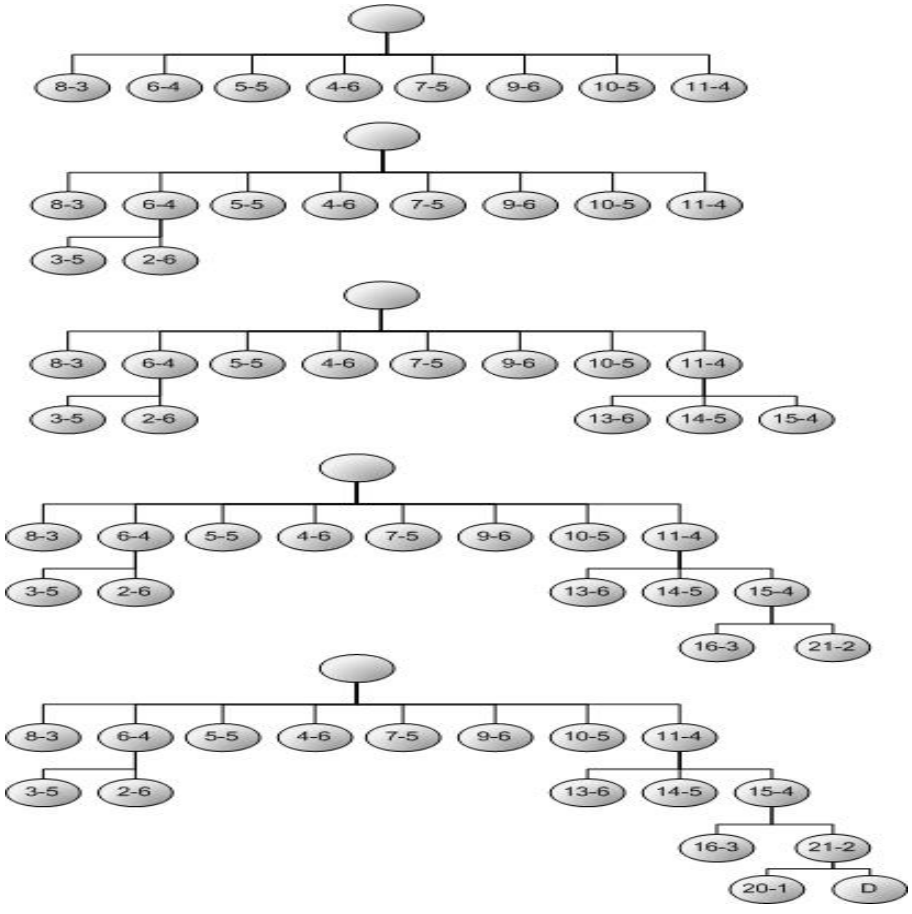
اما برای روش‌های جست‌وجوی سلسله‌مراتبی انواع مختلفی دارد که در ادامه روش‌های جست‌وجویی که مورد استفاده قرار داده‌ایم را ارائه می‌نمائیم.

جستجوی حریصانه

مسئله کلاس‌بندی بی‌تکلف مطرح شده در ارتباط با خوشه‌بندی داده‌ها بزرگ را در نظر بگیرید. می‌توانیم در این روش به جای این‌که تابع هزینه‌ی روش جست‌وجو را بصورت میزان خطا در نظر بگیریم، از روش اختلاف بین لایه‌ی داده‌ی فعلی و لایه‌ی داده‌ی بعدی به عنوان تابع هزینه استفاده کنیم. به عبارت دیگر برای هر داده از یک درخت استفاده می‌کنیم که داده‌ی بعدی کمترین میزان اختلاف را با داده‌ی فعلی داشته باشد. این فرض لازم است که هر داده تنها یک‌بار می‌تواند مورد استفاده قرار گیرد. به عبارت دیگر جست‌وجو و تشکیل درخت داده‌ها بر روی داده‌های اصلی صورت می‌گیرد و مطابق با تعریف درخت، با حرکت از ابتدای درخت به انتهای آن از هر داده تنها یک‌بار می‌توانیم عبور کنیم. بنابراین تابع اکتشافی به شکل زیر تعریف خواهد شد:

$$C = \left|X_{\text{فعلی}} - X_{\text{بعدی}}\right| + \left|Y_{\text{فعلی}} - Y_{\text{بعدی}}\right|$$

در این زیر مسئله داده‌ای برای مرحله‌ی بعدی مناسب است که مقدار هزینه‌ی آن کمتر باشد. درختی که با استفاده از این تابع اکتشافی به دست می‌آید بصورت شکل زیر خواهد بود.



درخت بدست آمده از جست‌وجوی اکتشافی

جستجوی حریصانه با گسترش داده‌های کمتر، سریعتر به جواب مساله دست پیدا می‌کند. با این حال هنگام استفاده از جستجوی حریصانه باید دقت کنیم چرا که جستجوی حریصانه با دو مشکل بزرگ همراه است. مشکل اول اینکه نمی‌توان با

استفاده از جستجوی حریصانه مطمئن بود که همیشه به جواب بهینه دست پیدا خواهیم کرد. همچنین جستجوی حریصانه ممکن است در یک حلقه بینهایت به دام افتد. به عنوان مثال در مسئله خوشه‌بندی فرض کنید از هر خانه می‌توان چندین بار عبور کرد و با این

فرض درخت جستجو را تشکیل می‌دهیم. مشاهده خواهیم نمود که گره شماره ۸ در یک حلقه بینهایت گسترش یافته و در واقع هیچگاه به جواب مسئله دست پیدا نخواهیم کرد. حال می‌توان علت نامگذاری این روش به جستجوی حریصانه را حدس زد.

الگوریتمی برای ساختن کلاس‌بندی بی‌تکلف

اگر پایگاه داده ورودی در حافظه اصلی جا گیرد می‌توانیم مستقیما طبق درخت کلاس‌بندی عمل کنیم. اما اگر داده‌ی ورودی بزرگتر از حافظه اصلی باشد چطور می‌توانیم درختان تصمیم را بسازیم؟

حال به نکته مهمی در مورد روش‌های انتخاب جداکننده می‌پردازیم که به ما کمک می‌کند تا نیازمندی‌های حافظه اصلی را کاهش دهیم. داده‌ای از درخت تصمیم را مورد ملاحظه قرار دهید. روش انتخاب جداکننده بعد از بررسی تقسیم‌بندی در مورد آن گره دو تصمیم می‌گیرد:

۱) باید صفت جداکننده را انتخاب کند.

۲) باید پیش‌گویی‌های جداکننده را برای لبه‌های خروجی انتخاب کند.

الگوریتم به صورت بازگشتی روی داده‌های فرزند اعمال می‌شود.

روش‌های انتخاب جداکننده که ضابطه جداکننده‌ای را که فقط شامل یک صفت پیشگویی کننده در هر داده است را محاسبه می‌کنند، هر صفت پیشگویی کننده را به طور انحصاری ارزیابی می‌کنند. چون هر صفت به طور مجزا امتحان می‌شود، می-توانیم روش انتخاب جداکننده را با اطلاعات جمع‌آوری شده در پایگاه داده به جای بار کامل پایگاه داده در حافظه اصلی فراهم کنیم. با انتخاب درست، این اطلاعات جمع‌آوری شده برای محاسبه بهترین ضابطه جداکننده کافی است.

چون روش انتخاب جداکننده تمامی صفات خاصه پیش‌گویی‌کننده را بررسی می‌کند، پس به اطلاعات جمع‌آوری شده در مورد هر صفت پیش گویی کننده نیاز داریم. به این اطلاعات جمع‌آوری شده مجموعه AVC صفت پیش‌گویی‌کننده می‌گوییم. مجموعه AVC صفت پیش‌گویی کننده X در داده n ، پرتویی از n قسمت پایگاه داده روی X و صفت وابسته که مقادیر منحصر به فرد در دامنه یک صفت وابسته را می‌شمارد، جمع آوری می‌کند.

توجه کنید که اندازه مجموعه AVC، صفت خاصه پیش‌گویی کننده X در داده n تنها به تعداد مقادیر منحصر به فرد صفت X و اندازه دامنه صفت وابسته دارد. برای پایگاه داده‌های بزرگ، اندازه‌ی مجموعه AVC مستقل از تعداد تاپل‌ها در پایگاه داده است، به جز وقتی که صفات خاصه با دامنه‌های بزرگ

وجود داشته باشد. به عنوان مثال، فیلدی از اعداد حقیقی که با دقت خیلی بالایی و تا تعداد ارقام زیاد بعد از نقطه اعشاری ذخیره شده‌اند.

اگر این فرض ساده را در نظر بگیریم که تمامی مجموعه های AVC گره ریشه با هم در حافظه اصلی جای می‌گیرند، سپس می‌توانیم درختان تصمیم را از پایگاه داده‌های خیلی گسترده طبق زیر بسازیم:

روی پایگاه داده جست‌جویی انجام می‌شود و گروه AVC گره ریشه در حافظه ساخته می‌شود.

سپس روش انتخاب جداکننده انتخابمان با گروه AVC به عنوان ورودی اعمال می‌شود.

بعد از اینکه روش انتخاب جداکننده صفت جداکننده و گزاره‌های جداکننده روی گره‌های خارجی را محاسبه کرد، پایگاه داده را تقسیم می‌کنیم و دوباره این عملیات تکرار می‌شود.

الگوریتم کلاس‌بندی بیز پیشنهادی

هدف از الگوریتم ارائه شده، پیاده‌سازی روشی جهت کلاس‌بندی بیز بر روی یک شبکه‌ی کامپیوتری بصورت چندگامی و به عبارت دیگر درختی می‌باشد. در این الگوریتم، توالی برای دست‌یابی به کمترین زمان پردازش بعنوان مهمترین پارامتر بهینه-سازی مورد توجه قرارگرفته است. به همین جهت این الگوریتم را، الگوریتم کلاس‌بندی بیز نام‌گذاری نموده‌اند.

دو نکته در طراحی الگوریتم مورد توجه قرارگرفته است. اول اینکه برای بهبود مقیاس‌پذیری، طبق آنچه در قسمت‌های قبل ذکر شد، روش مبتنی بر بیشترین درجه مورد استفاده قرارگرفته است. دوم اینکه جهت کاهش زمان آنالیز همانگونه که در ادامه خواهیم دید، با تعریف کلاس، زمان پردازش و خطای خوشه‌یابی را بهبود خواهیم بخشید. همانگونه که در بخش ارزیابی کارآیی خواهیم دید، این روش علاوه براینکه مقیاس‌پذیر است، دارای پایداری به مراتب بیشتر از الگوریتم‌های خوشه‌بندی دیگر می‌باشد.

در یک مساله بهینه‌سازی، مجموعه متناهی از اشیا داده شده است و یک تابع هدف که به هر شی یک مقدار هزینه مثبت نسبت می‌دهد. هدف یافتن شیئی است که مقدار هزینه را کمینه کند. توجه کنید که کمینه‌کردن تابع هدف f متناظر است با بیشینه کردن تابع f– . بنابراین، هر مساله بهینه‌سازی ترکیبی می‌تواند به صورت یک مساله کمینه‌سازی توصیف گردد.

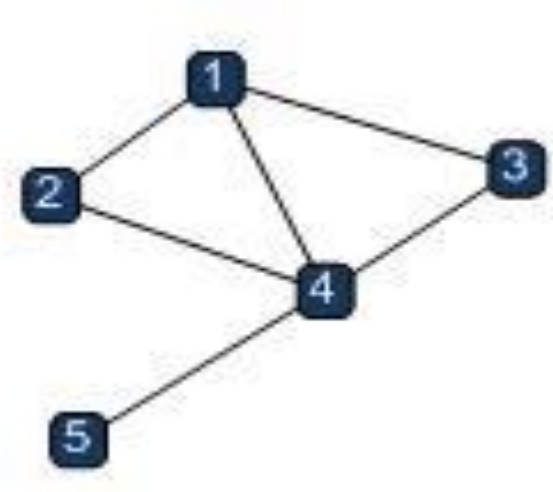
روش‌های ساختاری با این واقعیت شناخته می‌شوند که روی راه‌حل‌های جزئی کار می‌کنند. مکانیزم توسعه راه‌حل‌های جزئی، یک درخت جستجو را تعریف می‌کند. برگ‌های درخت یا شامل راه‌حل‌های نمونه مساله مورد نظر هستند و یا راه حل‌های جزئی ممکن که توسعه بیشتر آنها ممکن نیست.

اما توصیف الگوریتم کلاس‌بندی بیز سلسله‌مراتبی مورد نظر بصورت زیر است:

- ابتدا فرزندان ریشه درخت تولید شده و در سطح بعدی درخت قرار می‌گیرند.
- سپس اولین داده در سطح ۱ از درخت انتخاب شده و همه فرزندان قابل تولید آن در سطح ۲ درخت تشکیل می-شوند.
- سپس در سطح ۲ از درخت فرآیند جست‌وجو صورت می‌گیرد و همه فرزندان آن در سطح ۳ درخت تشکیل می شوند.
- در نهایت نیز سطح ۳ جست‌وجو شده و همه‌ی فرزندان آن ایجاد می‌شود. با توجه به اینکه دیگر هیچ فرزندی برای این داده وجود ندارد، بنابراین کلاس‌بندی بیز سلسله‌مراتبی که از پیمایش درخت از ریشه تا داده فعلی به دست می‌آید بررسی می‌شود تا صحیح بودن درخت را تعیین کند.

حال فرزندان در سطح ۲ تولید می‌شوند. بنابراین اگر فرزند دیگری برای داده "جست‌جو" در سطح ۳ وجود نداشته باشد، بنابراین این داده نیز به همراه گره پدر از حافظه حذف خواهد شد. سپس به سطح ۱ بازگشته و فرزندان داده"جستجو" را گسترش می دهیم. سپس فرزندادن داده "عمقی" در سطح ۲ گسترش یافته صحت و فرآیند جست‌جو مورد بررسی قرار می-گیرد.

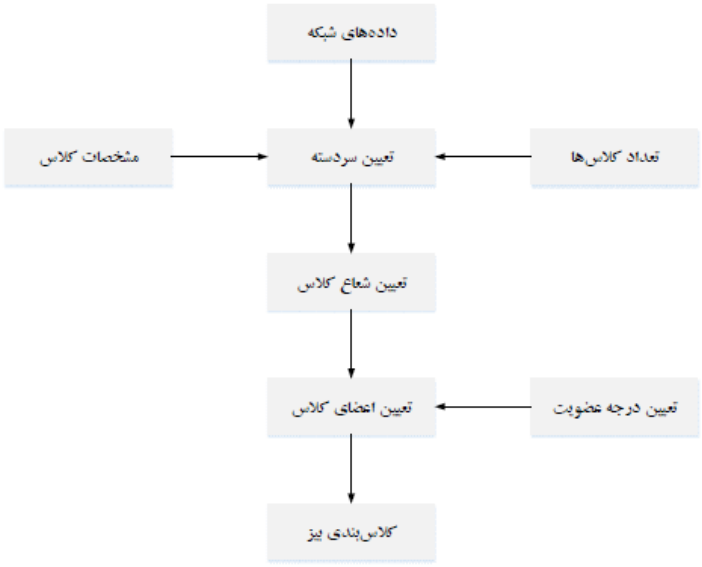
مهمترین مشکل روش جستجوی عمقی را که در برخی از مسائل با آن مواجه خواهیم بود، قرار گرفتن این روش جستجو در حلقه بینهایت می‌باشد. به عنوان مثال گراف داده شکل ۴-۳ را در نظر بگیرید:



مثالی از جست‌وجوی عمقی محدود

مراحل کلاس‌بندی بیز بصورت زیر است:

- تعیین تعداد کلاس‌ها. در این مرحله تعداد کلاس‌ها را لازم است که تعیین کنیم. تعداد کلاس‌ها اختیاری است و معمولا بوسیله‌ی کاربر تعیین می‌شود.
- تعیین سردسته. در این مرحله لازم است که برای هر کلاس، یک سرکلاس تعیین شود. در یک فایل داده معمولا عملکردهای مختلفی صورت می‌گیرد. هر عملکرد کار مشخصی را به انجام می‌رساند.
- اما در نهایت عملکردها در دسته‌هایی قرار می‌گیرند که با یکدیگر مشابهت داشته باشند. به عبارت دیگر عملکردهایی که از نظر ساختاری و مشخصه‌ای به یکدیگر نزدیک باشند، در یک کلاس قرار می‌گیرند. بنابراین در این مرحله عملکردی که نماینده‌ی یک مجموعه عملکرد مشابه است را به عنوان سردسته انتخاب می‌کنیم.
- تعیین شعاع کلاس. با توجه به سردسته‌های انتخابی و با توجه به مشخصاتی که برای کلاس‌ها در نظر گرفته‌ایم، یک محدوده برای هر کلاس در نظر می‌گیریم. این محدوده تعیین می‌کند که چه عملکردی در کلاس مورد نظر می‌توانند قرار گیرند. در مطالعه‌ی مورد نظر، زمان مورد نیاز، هزینه و خطا به عنوان شعاع کلاس‌بندی در نظر گرفته می‌شود.



بلوک دیاگرام روش کلاس‌بندی بیزی

اما با توجه به فرآیند ذکر شده، یک مجموعه‌ی داده‌ی مربوط به شبکه‌ی کامپیوتری را در نظر می‌گیریم. تعداد کلاس‌ها را برابر N منظور می‌کنیم. در مرحله‌ی بعدی لازم است که سردسته‌ها را انتخاب کنیم. ملاک انتخاب سردسته بودن، این است که تمامی مشخصات مورد نظر برای هر دسته را در بر داشته باشد.

$$classhead_i = \{t | t \in \{time_i, Cost_i, Error_i\}\}$$

رابطه‌ی فوق بیان می‌کند که سردسته عضوی از مجموعه‌ی داده‌هاست که به شرط کمترین زمان و کمترین خطا و کمترین هزینه را برآورده کند. از طرف دیگر سردسته باید عضوی از تراکنش‌ها باشد.

در مرحله‌ی بعدی لازم است که شعاع کلاس‌بندی برای هر دسته بدست آید. همانطور که ذکر کردیم برای هر دسته پارامترهایی مد نظر است. اولا این شعاع دسته باید از نظر زمان انجام وظیفه مشخص باشد.

$$0 < radial_{ci} < maxTime_i$$

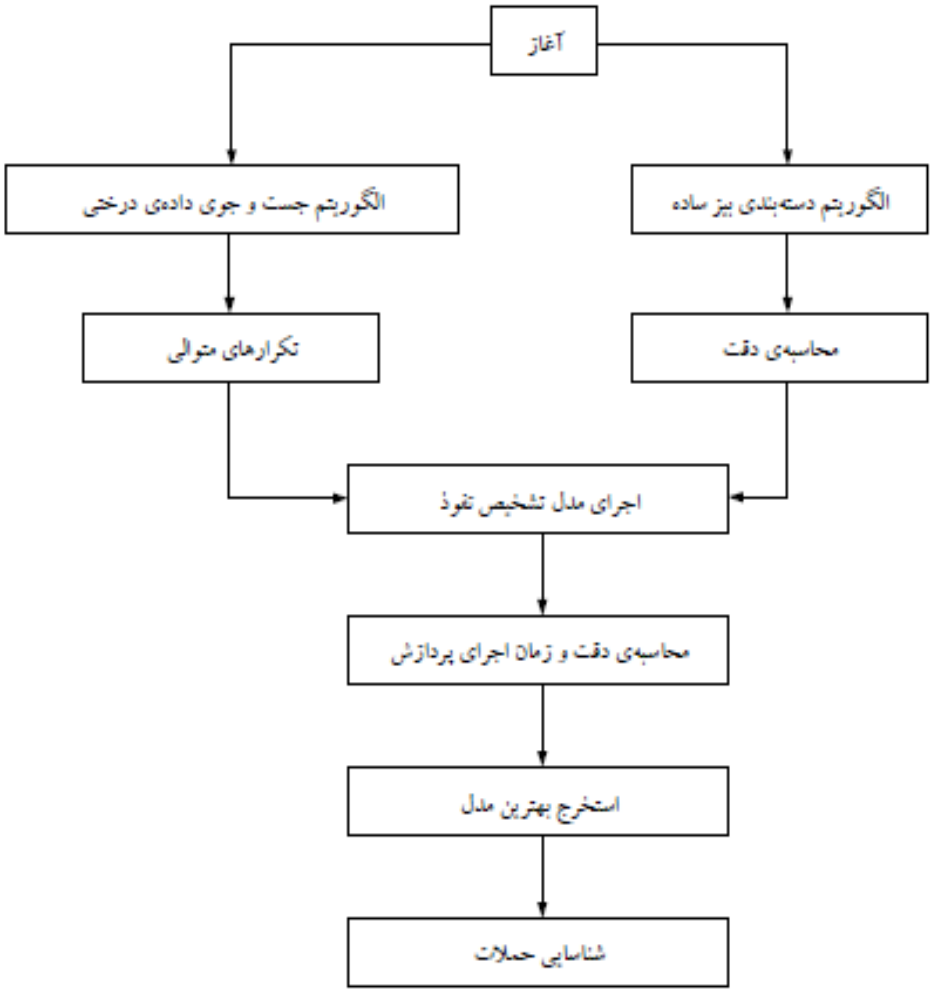
از طرف دیگر باید از نظر نوع داده و لایه‌ی قرارگیری آن مشخص باشد. به این ترتیب برای هر کلاس شعاعی باید منظور گردد.

اما بعد از اینکه شعاع کلاس‌ها مشخص گردید، لازم است که داده‌ها در این کلاس‌ها قرار گیرند. رابطه‌ی زیر چگونگی قرارگیری داده‌ها در کلاس‌ها را بیان می‌کند.

$$Task_i \in \{class_i | 0 < task_i < radial_{ci}\ , \quad i = 1,2,\dots,N\}$$

بنابراین مطابق رابطه‌ی فوق، داده‌ها به ترتیب در کلاس‌ها قرار می‌گیرند، البته به شرطی که شرایط حضور در آن کلاس را داشته باشند. این فرآیند بدین‌صورت انجام می‌شود که داده اول در کلاس قرار داده می‌شود؛ اگر شرایط این کلاس را داشته باشد در این کلاس می‌ماند و در غیر اینصورت با کلاس‌های بعدی مقایسه می‌شود و در هر کلاسی که شرایط آن را داشته باشد، قرار داده می‌شود. برای هر یک از داده‌ها این فرآیند صورت می‌گیرد تا هنگامی‌که همه‌ی داده‌ها در کلاس‌های مربوط قرار گیرند.

به منظور ایجاد یک سیستم تشخیص نفوذ با کارآیی بالا، یک چارچوب کلی مانند شکل ۴-۵ در نظر گرفته شده است. در این چارچوب فازها به ترتیب اجرا شده و نتیجه‌ی فاز قبلی به فاز جدید منتقل می‌شود. این روند تکرار می‌شود تا مدل ترکیبی پیشنهادی استخراج شود. چارچوب معرفی شده قارد خواهد بود برای کلیه‌ی مجموعه‌ها استفاده شده و باعث استخراج مدل شود.



مراحل سیستم پیشنهادی

نتیجه‌گیری

روش بهینه‌سازی کلاس‌بندی بیز که در این مقاله مورد استفاده قرار گرفته است توانسته از نظر دقت و سرعت در تشخیص نفوذ، عملکرد شبکه را بهبود بخشد.

اگر برنامه مشکوک با هر ویروس نمونه در آشکارسازی کتابخانه آشکار کننده ویروس تطبیق یابد، مقدار شباهت محاسبه می گردد. همه مقادیر برای این برنامه به عنوان یک مقدار شباهت بین برنامه و کتابخانه آشکار کننده ویروس اضافه می گردد.

نمایش داده یک تفاوت بنیادی بین مدل‌های مختلف الگوریتم‌های طبقه‌بندی ایجاد می‌کند. این تفاوت‌ها ممکن است شامل نقش‌های تطبیقی، مکانیزم‌های تولید آشکارکننده و یا فرآیندهای آشکارسازی باشد. نمایش داده بطور متداول شامل تعداد داده‌ها، دسته‌بندی داده‌ها، داده‌ی بولی و داده‌های متنی است. با در نظر گرفتن همه‌ی این احتمالات، اکثر طرح‌ها می‌تواند در دو نوع اصلی طبقه‌بندی شود: نمایش رشته‌ای و نمایش برداری. طول رشته‌ها معمولا ثابت است اما همواره به عنوان شرط اصلی مطرح نیست.

Reference

- Aycock, John Daniel, "Computer viruses and malware", United States America, December 20۱۲.

- Zhang, Pengtao,Wang, Wei, Tan, Ying, "A malware detection model based on a negative selection algorithm with penalty factor", Department of Machine Intelligence, School of Electronics Engineering and Computer Science, Peking University, P 2, 2010
- Muazzam, Ahmed Siddiqui, "Data mining methods for malware detection", College of Sciences at the University of Central Florida, 2008.
- Idris, Ismaila, "Model and Algorithm in Artificial Immune System for Spam Detection", International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.1, January 201۳.
- Zhang, Pengtao,Wang, Wei, Tan, Ying, "An immune local concentration based virus
detection approach", Department of Machine Intelligence, School of Electronics Engineering and Computer Science, Peking University, P 1, 2011.
- WU, Peifei, Zheng, Xufei, "An Improved Variable-radius Real-valued Negative Selection Algorithm", Journal of Information & Computational Science, P 1, 2012.
- F. Yuan, F.-L. Chu, Support vector machines-based fault diagnosis for turbopump rotor, Mechanical Systems and Signal Processing 20 (2006) 939–952.
- S. Zhang, T. Asakura, X. Xu, B. Xu, Fault diagnosis system for rotary machine based on Fuzzy Neural Networks, JSME International Journal 46 (2003) 1035–1041.
- N.R. Sakthivel, V. Sugumaran, S. Babudevasenapati, Comparison of decision tree-fuzzy and rough set-fuzzy methods for fault categorization of monoblock centrifugal pump, International Journal of Mechanical Systems and Signal Processing 24 (2010) 1887–1906.
- J. Sanz, R. Perera, C. Huerta, Fault diagnosis of rotating machinery based on auto associative neural networks and wavelet transforms, Journal of Sound and Vibration 302 (2007) 981–999.
- I.S. Koo, W.W. Kim, The development of reactor coolant pump vibration monitoringand a diagnostic system in the nuclear power plant, ISA Transactions 39 (2000) 309–316.
- S.-F. Yuan, F.-L. Chu, Fault diagnostics based on particle swarm optimization and support vector machines, Mechanical Systems and Signal Processing 21 (2007) 1787–1798.

- W. Sun, J. Chen, J. Li, Decision tree and PCA-based fault diagnosis of rotating machinery, Mechanical Systems and Signal Processing 21 (2007) 1300–1317.
- V. Sugumaran, V. Muralidharan, K.I. Ramachandran, Feature selection using Decision Tree and classification through Proximal Support Vector Machine for fault diagnostics of roller bearing, Mechanical Systems and Signal Processing 21 (2007) 930–942.
- N.R. Sakthivel, V. Sugumaran, B.B. Nair, Automatic rule learning using roughest for fuzzy classifier in fault categorization of centrifugal pump, International Journal of Applied soft computing 12 (2012) 196–203.