دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی هوش مصنوعی

تشخیص بدافزار با استفاده از یادگیری فعال نیمه‌نظارتی

نگارنده: رضا رحیمیان

استاد راهنما

دکتر هدی مشایخی

استاد مشاور

دکتر محسن رضوانی

شهریور ۱۳۹۷

شماره: ۵۷۹ /ف.ک
تاریخ: ۹۷/۶/۲۶

باسمه‌تعالی

دانشگاه صنعتی شاهرود

مدیریت تحصیلات تکمیلی

فرم شماره (۳) صورتجلسه نهایی دفاع از پایان نامه دوره کارشناسی ارشد

با نام و یاد خداوند متعال، ارزیابی جلسه دفاع از پایان نامه کارشناسی ارشد آقای رضا رحیمیان با شماره دانشجویی ۹۵۰۶۷۲۴ رشته مهندسی کامپیوتر گرایش هوش مصنوعی تحت عنوان تشخیص بدافزار با استفاده از یادگیری فعال نیمه‌نظارتی که در تاریخ ۱۳۹۷/۶/۱۹ با حضور هیأت محترم داوران در دانشگاه صنعتی شاهرود برگزار گردید به شرح ذیل اعلام می‌گردد:

قبول (با درجه: بسیار خوب) ☑ **مردود** ☐

نوع تحقیق: **نظری** ☑ **عملی** ☐

عضو هیأت داوران	نام ونام خانوادگی	مرتبهٔ علمی	امضاء
۱ـ استادراهنمای اول	دکتر هدی شاخنی	استادیار	
۲- استادراهنمای دوم	—		
۳- استاد مشاور	دکتر محسن رضوانی	استادیار	
۴- نماینده تحصیلات تکمیلی	دکتر منصور مفاخ	استادیار	
۵- استاد ممتحن اول	دکتر اسعد حانیان	استادیار	
۶ـ استاد ممتحن دوم	دکتر میثاقی	دانشیار	

نام و نام خانوادگی رئیس دانشکده:

تاریخ و امضاء و مهر دانشکده:

تبصره: در صورتی که کسی مردود شود حداکثر یکبار دیگر (در مدت مجاز تحصیل) می تواند از پایان نامه خود دفاع نماید (دفاع مجدد نباید زودتر از ۴ ماه برگزار شود).

تقدیم اول به

پدر و مادر عزیزم که مهر آسمانی شان آرامش بخش

و راه و روش شان چراغ راه زندگانی ام است

و تقدیم دوم

به همه افرادی ست که درست اندیشیدن را در این مسیر به من آموختند.

تشکر و قدردانی

سپاس خداوند یکتای عزتمندی که رحمت و دانش او در سراسر گیتی گسترده شده، آسمان ها و زمین همه از آن اوست و علم و دانش حقیقی را بر هر که بخواهد موهبت می فرماید. رحمت و لطف او را بی نهایت سپاس می گویم چرا که فهم و درک مطالب این پژوهش را بر من ارزانی داشت و مرا به این اصل رساند که علم و ایمان دو بال یک پرواز ند. توفیق تلاش به من داد، تا با امید، راه تازه ای را آغاز کنم و به خواست او به نتیجه ی مطلوب نائل آیم. به راستی که همه چیز از آن و به خواست اوست.

همچنین از استاد گرامی، سرکار خانم دکتر مهدی مشایخی بسیار سپاسگزارم که در تمامی دشواری های این مسیر، راهنمایی های بی دریغشان چاره ساز کارم بود و از آقای دکتر محسن رضوانی بابت کمک هایشان قدردانی به عمل می آورم.

تعهدنامه

اینجانب **رضا رحیمیان** دانشجوی دوره کارشناسی ارشد رشته **مهندسی کامپیوتر** دانشکده مهندسی کامپیوتر دانشگاه صنعتی شاهرود نویسنده پایان‌نامه **تشخیص بدافزار با استفاده از یادگیری فعال نیمه‌نظارتی** تحت راهنمائی **دکتر هدی مشایخی** متعهد می‌شوم.

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است .
- مطالب مندرج در پایان‌نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می‌باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « Shahrood University of Technology » به چاپ خواهد رسید .
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان‌نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان‌نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان‌نامه ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ

امضای دانشجو

چکیده

امروزه ضرورت استفاده از اینترنت و تبدیل شدن آن به عنوان بخش مهمی از زندگی افراد، موضوعی غیر قابل اغماض است. از سویی دیگر متناسب با رشد چشم‌گیر شبکه‌ها و زیرساخت‌های رایانه‌ای و همچنین طراحی بدافزارهای پیچیده و پویایی که دائم در حال به روز رسانی خود هستند، حفظ امنیت و نظارت بر ترافیک شبکه‌ها یکی از مهم‌ترین ملزومات فضای سایبری می‌باشد. به طور کلی بدافزارها می‌توانند پس از ورود به سیستم، اقداماتی نظیر سرقت اطلاعات، ایجاد هرزنامه و یا تولید شبکه‌ای از بات‌ها را به همراه داشته باشند. بنابراین ایجاد روشی که بتواند به صورت کارا به شناسایی و جلوگیری از نفود آنها بپردازد، همواره مورد نیاز خواهد بود. در سال‌های اخیر بات‌نت‌ها به عنوان یکی از خطرناک‌ترین بدافزارهای شناخته شده در بستر اینترنت مطرح می‌شوند که قابلیت تخریب رایانه‌های سالم و تبدیل آنها به بات‌هایی برای انتقال ویروس، اسپم و غیره را دارند. تاکنون روش‌های مختلفی به منظور شناسایی بات‌نت‌ها ارائه شده است که در این بین، رده‌بندی ترافیک شبکه به کمک رویکردهای یادگیری با توجه به کارایی و قدرت توسعه‌پذیری آنها، به عنوان یکی از شناخته‌شده‌ترین راهکارهای امنیتی به شمار می‌آید. با این وجود، تشخیص بات‌نت با استفاده از روش‌های یادگیری، چالش‌های متعددی دارد که از میان آنها می‌توان به کمبود داده‌های برچسب‌گذاری شده و تشخیص بات‌نت جدید اشاره نمود. به منظور تخفیف این مشکلات می‌توان از روش یادگیری فعال نیمه‌نظارتی استفاده کرد که کمتر در زمینه تشخیص بات‌نت مورد توجه قرار گرفته است.

در این پژوهش یک رویکرد مبتنی بر یادگیری فعال نیمه نظارتی به صورت گروهی و با استفاده از رده‌بندهای رگرسیون لجستیک، ماشین بردار پشتیبان خطی و بیز ساده به منظور تشخیص بات‌نت‌ها ارائه شده است. آموزش در این روش به صورت تعاملی انجام شده و سیستم در حین اجرا دائما رده‌بندهای پایه را با توجه به نمونه‌های انتخابی خود، که برچسب آنها درخواست می‌شود، به روز رسانی می‌نماید.

برای انجام آزمایش‌ها از مجموعه داده‌ای حاوی انواع مختلف باتنت استفاده کرده و پنج مجموعه ویژگی مختلف را استخراج می‌کنیم. نتایج بدست آمده، کارایی مدل را در تشخیص باتنت‌های دیده نشده و دقت رده‌بندی ۸۹/۸۵ درصد را نشان می‌دهد.

کلمات کلیدی : یادگیری فعال نیمه‌نظارتی، بدافزار، باتنت، رده‌بندی ترافیک شبکه، رده‌بندی گروهی، امنیت اطلاعات

لیست مقالات مستخرج از پایان نامه

۱-**رحیمیان،ر. مشایخی،ه. رضوانی**،م. (۱۳۹۷)، "تشخیص بدافزار به کمک یادگیری فعال نیمه نظارتی" کنفرانس بین المللی انجمن رمز ایران، سال پانزدهم،تهران،ایران.

فهرست مطالب

فهرست جداول **م**

فهرست اشکال **ن**

فصل۱ : مقدمه **۱**

۱-۱ مقدمه ۲

۱-۲ شرح مسئله ۹

۱-۳ اهمیت انجام پژوهش ۱۴

۱-۴ هدف پژوهش ۱۵

۱-۵ مروری بر فصل‌ها ۱۷

فصل۲ : ادبیات پژوهش **۱۹**

۲-۱ بدافزارها ۲۰

۲-۲ رده‌بندی ترافیک شبکه ۲۳

۲-۳ بات‌نت ۲۴

۲-۳-۱ اجزای بات‌نت ۲۶

۲-۳-۲ انواع بات‌نت‌ها ۲۷

۲-۴ روش‌های تشخیص بات‌نت ۲۹

۲-۵ سیستم‌های تشخیص نفوذ ۳۰

۲-۵-۱ انواع سیستم‌های تشخیص نفوذ ۳۱

۲-۵-۲ انواع روش‌های برخورد و پاسخ به نفوذ ۳۲

۲-۶ یادگیری نیمه‌نظارتی ۳۳

۲-۷ یادگیری فعال ۳۹

۲-۸ یادگیری فعال نیمه‌نظارتی ۴۱
۲-۹ بررسی پژوهش‌های انجام شده ۴۳
فصل۳: روش پیشنهادی برای تشخیص بدافزار **۵۱**
۳-۱ ساز و کار سیستم تشخیص ۵۲
۳-۲ مجموعه ویژگی‌ها ۵۴
۳-۲-۱ مجموعه ویژگی اول (پایه-Qiu2017) ۵۴
۳-۲-۲ مجموعه ویژگی دوم(ISCX2014) ۶۱
۳-۲-۳ مجموعه ویژگی سوم (Milcom2015) ۶۲
۳-۲-۴ مجموعه ویژگی چهارم (Li2009) ۶۳
۳-۲-۵ مجموعه ویژگی پنجم (CIC2018) ۶۵
۳-۳ فرآیند یادگیری فعال نیمه‌نظارتی ۶۵
۳-۳-۱ مجموعه داده آموزشی برچسب‌دار ایستا ۶۶
۳-۳-۲ یادگیری مدل و مدل آموزش دیده شده ۶۷
۳-۳-۳ داده‌های مبتنی بر جریان بدون برچسب ۶۷
۳-۳-۴ انتخاب نمونه‌های یادگیری فعال نیمه‌نظارتی ۶۸
۳-۳-۵ برچسب‌گذاری توسط خبره ۶۹
۳-۳-۶ پیش‌بینی برچسب نمونه‌ها توسط رده‌بندها ۷۰
۳-۳-۷ مجموعه داده آموزشی برچسب‌دار پویا ۷۰
۳-۳-۸ فرآیند به روز رسانی مدل ۷۰
۳-۴ رده‌بندهای پایه ۷۴
۳-۴-۱ رده‌بند ماشین بردار پشتیبان خطی ۷۴
۳-۴-۲ رده‌بند رگرسیون لجستیک ۷۶

۳-۴-۳ رده‌بند بیز ساده ۷۷

فصل۴ :پیاده‌سازی و ارزیابی روش پیشنهادی **۷۹**

۴-۱ تنظیمات و راه‌اندازی سیستم ۸۰

۴-۱-۱ مجموعه داده بات‌نت ۸۰

۴-۱-۲ پیاده‌سازی فرآیند یادگیری فعال نیمه‌نظارتی ۸۵

۴-۲ آزمایش‌ها و ارزیابی نتایج ۸۷

۴-۳ مقایسه ۹۸

۴-۳-۱ مقایسه نتایج مجموعه ویژگی‌ها در اجرای آزمایش‌ها ۹۸

۴-۳-۲ مقایسه با پژوهش مشابه ۱۰۱

فصل۵ :نتیجه‌گیری و پژوهش‌های آینده **۱۰۳**

۵-۱ نتیجه‌گیری ۱۰۴

۵-۲ پژوهش‌های آینده ۱۰۶

مراجع **۱۱۰**

فهرست واژگان **۱۱۴**

فهرست جداول

جدول ۲-۱. خلاصه‌ای از پژوهش‌های انجام شده..... ۴۷
جدول ۳-۱. بازنمایی مجموعه ویژگی‌های پایه(Qiu2017)..... ۵۶
جدول ۳-۲. مجموعه ویژگی ISCX2014..... ۶۲
جدول ۳-۳. مجموعه ویژگی Milcom2015..... ۶۳
جدول ۳-۴. مجموعه ویژگی Li2009..... ۶۴
جدول ۳-۵. مجموعه ویژگی CIC2018..... ۶۵
جدول ۳-۶. پارامترهای موجود در الگوریتم یادگیری فعال نیمه‌نظارتی..... ۷۱
جدول ۴-۱. نحوه‌ی توزیع بات‌نت‌ها در مجموعه‌ی آموزش ISCX..... ۸۲
جدول ۴-۲. نحوه‌ی توزیع بات‌نت‌ها در مجموعه‌ی آزمون ISCX..... ۸۲
جدول ۴-۳. نحوه‌ی توزیع بات‌نت‌ها در مجموعه‌ی آموزش و آزمون ISCX در مجموعه ویژگی پایه. ۸۴
جدول ۴-۴. اطلاعات مجموعه ویژگی‌های استخراجی(Qiu2017) بر روی مجموعه بات‌نت ISCX..... ۸۵
جدول ۴-۵. مقادیر پارامترها در راه‌اندازی سیستم..... ۸۷
جدول ۴-۶. شرح ارزیابی آزمایش‌هاس..... ۹۰
جدول ۴-۷. ماتریس درهم‌ریختگی..... ۹۱
جدول ۴-۸. مقایسه دقت پژوهش با سایر مجموعه ویژگی‌ها در آزمایش اول..... ۹۹
جدول ۴-۹. مقایسه دقت پژوهش با سایر مجموعه ویژگی‌ها در آزمایش دوم..... ۱۰۰
جدول ۴-۱۰. مقایسه دقت پژوهش با سایر مجموعه ویژگی‌ها دیگر در آزمایش سوم..... ۱۰۱

فهرست اشکال

شکل ۳-۱. فلوچارت نحوه‌ی ساخت مجموعه ویژگی‌های پایه (Qiu2017)..... ۶۰
شکل ۳-۲. شمای کلی سیستم پیشنهادی مبتنی بر یادگیری فعال نیمه‌نظارتی ۶۶
شکل ۳-۳. الگوریتم یادگیری فعال نیمه‌نظارتی..... ۷۳
شکل ۳-۴. نمایش به روز رسانی افزایشی در الگوریتم SGD..... ۷۵
شکل ۴-۱. نمودار دقت و معیار F در آزمایش اول..... ۹۲
شکل ۴-۲. نمودار نرخ تشخیص درست(بات‌نت) در آزمایش اول..... ۹۲
شکل ۴-۳. نمودار دقت رده‌بندی و معیار F در آزمایش دوم..... ۹۴
شکل ۴-۴. نمودار نرخ تشخیص درست(بات‌نت) در آزمایش دوم..... ۹۴
شکل ۴-۵. نمودار دقت رده‌بندی و معیارF در آزمایش سوم..... ۹۶
شکل ۴-۶. نمودار نرخ تشخیص درست(بات‌نت) در آزمایش سوم..... ۹۷

فصل۱ : مقدمه

۱-۱ مقدمه

در دنیای امروزی ضرورت استفاده از اینترنت و تبدیل شدن آن به عنوان بخش مهمی از زندگی افراد، موضوعی غیر قابل اغماض است. در واقع رشد فزاینده و استفاده‌ی همگانی افراد از اینترنت به عنوان یک سوژه‌ی جذاب برای انجام کارهای خرابکارانه توسط مهاجمان تبدیل شده و انگیزه آنان برای نفوذ در شبکه و ایجاد حملات اینترنتی گسترده‌تر، همواره در حال شدت یافتن است. بنابراین به علت افزایش تهدیدات و طراحی بدافزارهای پیچیده و پویایی که دائما در حال به روز رسانی هستند، لزوم برقراری امنیت اطلاعات و نظارت بر ترافیک شبکه‌ها و همچنین ایجاد سیستم‌های تشخیص نفوذ پویا، به عنوان مهم‌ترین راه‌حل‌های امنیتی به شمار می‌آید.

به طور کلی بدافزارها را می‌توان گونه‌ای از نرم‌افزارهای معمول دانست که با اهداف تخریب‌کارانه ایجاد شده‌اند و به عنوان یکی از ابزارهای اقدامات ضد امنیتی به شمار می‌آیند و کارهای ناخواسته و خرابکارنه‌ای را در سیستم فرد قربانی انجام می‌دهند. در واقع بدافزارها، به قطعه کدهایی اطلاق می‌شود که توسط برنامه‌نویسان تولید شده و هدف آنها از ایجاد این کدها، آلوده کردن، خرابکاری و کارهای مجرمانه بدون اطلاع مالک سیستم می‌باشد. بنابراین هر کد یا برنامه‌ای که در سیستم فرد قربانی بدون اطلاع وی اجرا شود و یک سری عملیات را به صورت ناخواسته به انجام برساند به عنوان بدافزار شناخته می‌شود [۱].

اصطلاح بدافزار از ترکیب دو واژه‌ی تخریب و نرم‌افزار بدست می‌آید که نمایانگر هر نرم‌افزار مخربی خواهد بود که مورد استفاده قرار می‌گیرد. همچنین به ویروس‌ها یا به اصطلاح عمومی‌تر تروجان‌ها، جاسوس‌افزارها و دیگر کدهای مخرب نیز این اصطلاح اطلاق می‌شود. امروزه تشخیص و شناسایی این

فرآیندها و نحوه‌ی استفاده مهاجم از راه‌های نفوذ همانند درهای پشتی[1]، پویش صفحه کلید[2]، سرقت رمزهای ورود و سایر توابع بدافزاری، همواره پیچیده‌تر و به مسئله‌ای دشوارتر تبدیل شده است [۲].

به طور کلی، دسترسی آزاد به ابزارهای مخرب موجود در اینترنت، میزان مهارت لازم برای توسعه‌ی بدافزارها را به شدت کاهش داده است. از سوی دیگر وجود تکنیک‌های ضد تشخیص و همچنین توانایی خرید نرم‌افزارهای مخرب در بازار سیاه، این فرصت را برای تبدیل شدن هر فرد مبتدی به مهاجم می‌دهد. مطالعات کنونی نشان می‌دهد که اکثر حملات توسط برنامه‌های اجرایی ساده[3] انجام می‌شوند. این کدهای مخرب می‌توانند پس از ورود به سیستم اقداماتی نظیر سرقت اطلاعات، ایجاد هرزنامه[4] و یا تولید شبکه‌ای از بات‌ها را داشته باشند [۳].

در سال‌های اخیر، افزایش انگیزه تولید بدافزارها، سبب ایجاد گونه‌ی جدیدی از تهدیدات شد که زیر ساخت هزاران شبکه در سراسر دنیا را در معرض خطر قرار داد. این نوع از بدافزارها با نام بات‌نت‌ها شناخته می‌شوند که روندی رو به رشد داشته است و به عنوان یکی از بزرگ‌ترین تهدیدات امنیتی به شمار می‌روند. این گونه از بدافزارها رایانه‌های سالم را به بات‌هایی تبدیل کرده و برای انتقال ویروس و هرزنامه از آنها استفاده می‌کنند، همچنین این قابلیت را خواهند داشت که به صورت خودکار وظیفه‌ی حمله به سایر رایانه‌ها را نیز داشته باشند [۴].

در واقع بات‌نت‌ها توانایی انجام محاسبات توزیع‌شده و اشتراک‌گذاری منابع در شبکه‌های رایانه‌ای را دارا هستند؛ به این صورت که وظایف توزیع شده بر روی این شبکه‌ها، امکان اجرای فرآیندهای کاری گوناگون را برای یک رایانه‌ی یکتا (بات) ایجاد می‌نماید. همچنین از طریق تقسیم یک وظیفه به چندین زیر وظایف کاری مجزا، قادر هستند که سرعت پردازش اطلاعات را افزایش داده و به صورت همزمان آن وظیفه را بر روی چندین رایانه اجرا نماید. علاوه بر اینکه در این رایانه‌های شبکه شده، یک گره مرکزی

[1] Backdoors
[2] Keystroke logging
[3] Scripts-kiddies
[4] Spam

به نام رئیس وجود دارد که بات‌ها به منظور هماهنگی و کنترل به آن نیاز خواهند داشت. حال از آنجایی که اینترنت شامل حجم وسیعی از منابع پردازشی و پهنای باند بدون استفاده است، فعالان خرابکار و مهاجمان راهی را به منظور استفاده از این ماشین‌ها پیدا کرده‌اند. این راهکار از طریق به‌کارگیری ماشین‌های مخرب به همراه نرم‌افزارهای خرابکار یا به اصطلاح بدافزار است که سبب ایجاد بات‌نت‌های تخریب‌کننده‌ای می‌شود که از ماشین‌های آسیب دیده به منظور انجام محاسبات مختلف تحت فرمان خود استفاده می‌نماید؛ به عبارتی دیگر بات یک رایانه آلوده شده به بدافزار است که بدون آگاهی و اراده‌ی کاربر و از راه دور توسط یک یا چند عامل انسانی یا ماشین کنترل می شود که به این عامل کنترل کننده، بات مرکزی یا چوپان‌بات[1] گفته می‌شود. علت اصلی خطرناک بودن این گونه شبکه‌ها وجود تعداد زیادی از رایانه‌ها است که چوپان‌بات می‌تواند از پهنای باند، قدرت ذخیره‌سازی و پردازش هر یک از این رایانه‌ها در راستای اهداف مخرب خود استفاده نماید و تهدیدات بزرگی را به وجود آورد. حملات ممانعت از سرویس‌دهی توزیع شده[2] فعالیت‌های فریب‌کارانه همانند تولید هرزنامه، شنود[3]، سرقت هویت[4]، کلاه‌برداری‌های مالی، نشر اطلاعات[5] و همچنین کلاه‌برداری با کلیک[6] از جمله حملاتی است که توسط بات‌نت‌ها صورت می‌پذیرد [۵].

تاکنون تکنیک‌های مختلفی به منظور شناسایی بدافزارها و به طور ویژه بات‌نت‌ها، ارائه شده است که در تمامی آنها برای دست‌یابی به نتیجه‌ی مطلوب، لازم است تا به طور دقیق بدافزار را شناسایی کرده و از نظام کاری آن شناخت کاملی بدست آورده شود. بنابراین ایجاد روشی که بتواند به صورت کارا به شناسایی و جلوگیری از نفوذ بپردازد، همواره مورد نیاز خواهد بود. از جمله روش‌های شناخته شده‌ای که به منظور تشخیص حملات و رفتار بدافزارها ارائه شده است، رده‌بندی ترافیک شبکه می‌باشد. این

[1] Bot master (Bot herder)
[2] Distributed denial-of-service (DDoS) attacks
[3] Phishing
[4] Identity theft
[5] Information exfiltration
[6] Click fraud

راهکار با هدف شناسایی وقوع حملات و تمایز آن از جریان‌های سالم، نقش اساسی را در مدیریت و ایجاد ساز و کارهای امنیتی به همراه خواهد داشت. به طور کلی مدیریت عملکرد ترافیک شبکه برای تمامی مراکز ارائه‌دهنده‌ی خدمات اینترنتی[1] امری بسیار حیاتی می‌باشد، پس رده‌بندی ترافیک به عنوان اولین گام در جهت تعیین و طبقه‌بندی کلاس‌های ناشناخته شبکه به منظور شناسایی حملات در نظر گرفته شده است که نقش مهمی را در برقراری امنیت و مدیریت شبکه‌ها همانند تشخیص نفوذ و کیفیت سرویس‌دهی[2] ایفا می‌نماید. از این رو متصدیان شبکه با استفاده از این راهکارها، می‌توانند اقداماتی نظیر مسدود کردن جریان‌های مشکوک را با هدف جلوگیری از وقوع حملات و مدیریت منابع پردازشی به انجام برسانند [۶].

به طور کلی نظارت بر ترافیک شبکه با اهداف پیش‌گیرانه خود به دنبال تحلیل و شناسایی رفتارهای ناهنجار[3] در بستر اینترنت است. ترافیک شبکه می‌تواند به صورت بسته‌هایی با اهداف مخرب و یا با اهدافی سالم ایجاد شده باشند. در دو دهه‌ی گذشته تکنیک‌های زیادی به منظور رده‌بندی ترافیک شبکه با هدف تعیین و طبقه‌بندی کلاس‌های ناشناخته ارائه شده است که در یک تقسیم بندی کلی می‌توان روش‌های کلاسیک و مدرن را نام برد.

در روش رده‌بندی جریان ترافیک کلاسیک، پیش بینی مبتنی بر پورت و بررسی مبتنی بر محموله[4] صورت می‌پذیرد. تکنیک مبتنی بر پورت بر اساس شماره پورتی است که توسط نهاد آیانا[5] ثبت می‌شود. این نهاد وظیفه‌ی تخصیص نام و شماره مجوزهای یکتا برای استفاده‌ی از منابع و پروتکل‌های اینترنتی همانند آدرس‌های IP، پورت سیستم‌های خودکار[6] و غیره را دارد [۷]. این تکنیک امروزه به علت افزایش برنامه‌های نظیر به نظیر[7] که از شماره پورت‌های پویا استفاده می‌کنند دارای محدودیت بوده و کارایی

[1] Internet service provider (ISP)
[2] Quality of service (QoS)
[3] Anomaly treats
[4] Payload-based Inspection
[5] Internet Assigned Numbers Authority (IANA)
[6] Autonomous system (AS)
[7] Peer-to-peer

چندان مطلوبی به همراه نخواهد داشت. لازم به ذکر است که استفاده از پورت‌های پویا به معنای به‌کارگیری شماره پورت‌هایی می‌باشد که توسط آیانا ثبت نشده‌اند و حالتی غیر استاندارد دارند.

دومین روش این راهکار که مبتنی بر محموله است، می‌تواند نتایج دقیقی را در رده‌بندی ترافیک شبکه ارائه دهد، اما امروزه به علت وجود برنامه‌های رمزگذاری شده و استفاده‌ی این دسته از برنامه‌ها از تکنیک‌های مختلف رمزنگاری به منظور جلوگیری از شناسایی داده‌های شبکه، با شکست همراه بوده است و کارایی چندانی ندارد. این روش که با نام بازرسی عمیق بسته[1] نیز شناخته می‌شود، از سوی دیگر نیاز به یک سخت افزار قدرتمند به منظور کشف الگوهای موجود در قسمت محموله بسته‌های شبکه دارد که در نتیجه بار هزینه‌ای زیادی را به همراه خواهد داشت. بنابراین این روش نیز نتوانسته است، انتظارات مورد نظر را در بحث رده‌بندی ترافیک شبکه برآورده نماید [۸].

بنابراین پژوهشگران به دنبال ارائه راهکارهایی هستند که مشکلات مربوط به روش‌های کلاسیک را نداشته باشند. از این رو روش‌های مدرن به منظور رفع اشکالات راهکارهای گذشته پیشنهاد شدند که شامل روش‌های مبتنی بر یادگیری ماشین، روش‌های آماری و مبتنی بر رفتار هستند [۲]. روش‌های مبتنی بر یادگیری ماشین که راهکار پیشنهادی این پژوهش نیز بر اساس آن ارائه شده است، می‌تواند به خوبی نوع برنامه‌های موجود در جریان ترافیک شبکه را ارزیابی و شناسایی نماید. این روش‌ها نتایج خود را بر اساس رده‌بندی و استفاده از مجموعه داده‌های آموزشی و آزمون ارائه می‌دهند و می‌توانند در تشخیص جریان‌های ناشناخته ترافیک شبکه موثر واقع شوند.

از جمله ساختارهایی که با استفاده از روش‌های یادگیری ماشین برای شناسایی حملات مورد استفاده قرار می‌گیرد، سیستم‌های تشخیص نفوذ[2] است که به عنوان یکی از راهکارهای اصلی برای مقابله با تهدیدات و شناسایی رفتارهای ناشناخته مبتنی بر ترافیک شبکه در نظر گرفته می‌شود. به طور کلی سیستم‌هایی که به کمک آنها می‌توانیم رفتارهای مخرب و ناهنجاری‌های موجود در بستر ترافیک شبکه

[1] Deep Packet Inspection (DPI)
[2] Intrusion Detection Systems (IDS)

را مورد ارزیابی قرار دهیم و به کمک روش‌ها و تکنیک‌های خاصی مانع از رشد این گونه رفتارها در شبکه‌ها و تشخیص زودهنگام شویم، سیستم‌های تشخیص نفوذ نامیده می‌شود. سیستم‌های مدرن تشخیص نفوذ باید قادر به پردازش سریع اطلاعات و از سوی دیگر قابل اعتماد باشند که اغلب این موضوع با توجه به ویژگی زمان واقعی مورد نیاز خواهند بود. الگوریتم‌های یادگیری مبتنی بر روش‌های افزایشی[1]، گروهی(تجمیعی)[2]، فعال نیمه‌نظارتی و پیاده‌سازی توزیع شده‌ی آنها یک رویکرد امیدوارکننده نسبت به این گونه مسائل خواهد بود [۹].

در حالت کلی می‌توان هدف اصلی سیستم‌های تشخیص نفوذ را کشف حملات به صورت موثر دانست؛ به عبارتی دیگر قابلیت شناسایی در این سیستم‌ها باید همراه با تشخیص حملات در مراحل ابتدایی باشد، به این منظور که میزان آثار تخریبی حملات کاهش یابد. از سوی دیگر مهم‌ترین مشکلاتی که سیستم‌های تشخیص نفوذ کنونی با آن مواجه هستند، عدم توزیع متعادل کلاس‌ها، کمبود داده‌های برچسب خورده، حجم وسیع جریان‌های ترافیکی و تغییر رفتار و افزایش ناهنجاری‌های موجود در ترافیک شبکه می‌باشد؛ به علاوه با توجه به طبیعت جریان‌های شبکه‌ای، اعمال مدل‌های یادگیری ثابت سبب کاهش کارایی مورد انتظار فرآیند تشخیص در طول زمان خواهد شد [۱۰].

به طور کلی مسئله رده‌بندی ترافیک شبکه به خصوص برای سیستم‌های تشخیص نفوذ و بات‌نت هنوز هم با چالش‌های زیادی همراه است. اینکه یک سیستم تشخیص با توجه به ماهیت پویای فضایی که در آن فعالیت دارد، دارای کارایی مطلوب و بازخورد بلادرنگ باشد، همواره به عنوان یکی از مهم‌ترین خواسته‌های پژوهشگران حیطه‌ی امنیت بوده است که در همین راستا نیز باید تلاش‌های تازه‌ای صورت بپذیرد. بنابرین سیستم‌های تشخیص می‌بایست، قابلیت شناسایی رفتارهای غیر طبیعی در داده‌های ترافیکی شبکه را در اسرع وقت و با حداقل مداخله کاربر داشته باشند. از سوی دیگر با گسترش حجم داده‌های موجود در شبکه و افزایش قدرت ذخیره‌سازی و پردازش داده‌ها، همواره نیاز به روش‌هایی

[1] Incremental learning
[2] Ensemble learning

خواهد بود که بتواند استخراج دانش را از منابع داده‌ای کلان به انجام برساند. یک مساله اساسی در الگوریتم‌های یادگیری تشخیص بدافزارها این است که برای رسیدن به دقت مطلوب، نیاز به نمونه‌های آموزشی فراوان داریم که این خواسته مستلزم، صرف هزینه‌های گزاف و به کارگیری نیروی انسانی متخصص جهت برچسب زدن نمونه‌ها می‌باشد. از سوی دیگر ایجاد یک مجموعه ویژگی مناسب از طریق انتخاب ویژگی‌های پراهمیت به منظور آموزش رده‌بند به گونه‌ای که کارایی مناسبی را برای سیستم تشخیص ایجاد نماید، از دیگر اهداف پژوهشگران به شمار می‌آید [۱۱].

بنابراین در این پژوهش به منظور رفع مشکلات بیان شده و بهبود کارایی از یک روش یادگیری فعال نیمه‌نظارتی برای ایجاد رده‌بند استفاده شده است. به این معنی که ابتدا با تعداد کمی اسناد برچسب‌دار اولیه، رده‌بند ساخته می‌شود و به جای برچسب زدن به کل اسناد در دسترس، ابتدا میزان مفید بودن اطلاعات آنها اندازه‌گیری می‌شود. در واقع یادگیری فعال به ما این امکان را می‌دهد تا نمونه‌های آموزشی خود را به صورت هدفمند انتخاب کنیم و بدین ترتیب، تعداد نمونه‌های مورد نیاز برای برچسب زدن را تا اندازه قابل توجهی کاهش دهیم. از سوی دیگر ما نسبت به ساخت یک مجموعه ویژگی با هدف بهبود کارایی و استفاده از ویژگی‌های موثر نیز اقدام کردیم و بر پایه‌ی آنها روند یادگیری را انجام دادیم.

در واقع یادگیری فعال نیمه‌نظارتی گونه‌ی خاصی از الگوریتم‌های یادگیری است که در آن از طریق تعامل با کاربر (خبره[1]) و استفاده از یک سری پرس‌وجو یا منابع اطلاعاتی گوناگون، فرآیند یادگیری انجام می‌پذیرد. به عبارتی دیگر در این روش به جای آنکه انتخاب نمونه‌ها از یک مجموعه تصادفی انجام پذیرد، یک سری داده‌های بدون برچسب توسط سیستم انتخاب شده و سپس شخص خبره بر اساس الگوهای محموله بسته‌ها، اطلاعات بدست آمده از شبکه و غیره، فرآیند برچسب‌گذاری را انجام می‌دهد و عملیات آموزش دوباره از سر گرفته می‌شود. در این الگوریتم یادگیر این قابلیت را دارد که با استفاده از داده‌های برچسب خورده‌ی محدود، فرآیند یادگیری و به روز رسانی را به انجام برساند و از طریق

[1] Oracle

تشخیص متوالی مثال‌هایی که به احتمال بیش‌تری مفید هستند، بتواند به عملکرد بهتری دست یابد. به طور کلی این روش زمانی استفاده می‌شود که برچسب نمونه‌ها کمیاب و یا انجام چنین عملیاتی بسیار هزینه‌بر باشد [۱۲].

حال از آنجایی در میان بدافزارهای موجود، ایجاد بات‌نت‌ها روندی رو به رشد داشته و به عنوان یکی از بزرگ‌ترین تهدیدات امنیتی به شمار می‌رود، این پژوهش نخست تلاش می‌کند تا انواع بدافزارها را معرفی کرده و سپس به طور دقیق در خصوص گونه‌های مختلف بات‌نت‌ها و همچنین چگونگی کارکرد و وجه تمایز آن با سایر بدافزارها تحلیل مناسبی را به انجام برساند. سپس به بررسی روش‌ها و سیستم‌های تشخیص نفوذ کنونی برای کشف شبکه‌های بات خواهد پرداخت و کاستی‌های آنها را بیان می‌کند. در نهایت نتیجه‌ی این‌کار به‌کارگیری عملیات رده‌بندی برای تشخیص بات‌نت خواهد بود که جریان ترافیک شبکه را با استفاده از تکنیک‌های یادگیری فعال نیمه‌نظارتی طبقه‌بندی می‌نماید و می‌تواند پاسخ مناسبی نسبت به مشکلات موجود در سیستم های تشخیص نفوذ کنونی ارائه دهد و به طور کل در این امر موثر واقع شود. بنابراین به‌کارگیری روش‌های یادگیری نیمه‌نظارتی فعال راهکاری خواهد بود که می‌تواند در عملکرد یک سیستم تشخیص، با توجه به بالا بردن کارایی و قدرت تشخیص خود، نقش به سزایی را داشته باشد. در این پایان‌نامه نیز سعی در جهت افزایش نرخ تشخیص، کاهش هزینه‌های برچسب‌گذاری، افزایش کارایی، اعتبار ارزیابی سیستم و همچنین پاسخ‌گویی مناسب به ماهیت پویای ترافیک شبکه شده است.

۱-۲ شرح مسئله

جریان‌های داده‌ای به دنباله‌ای از داده‌ها گفته می‌شود که از منابع اطلاعاتی مختلف به صورت پیوسته و سریع در طول زمان تولید می‌شوند. این جریان داده‌ها در کاربردهای مختلفی همچون بررسی

تراکنش‌های مالی، بررسی ترافیک شبکه، داده‌های بدست آمده از حسگر بی‌سیم[1] و.. کارایی دارند. ترافیک شبکه به عنوان یکی از انواع جریان‌های داده‌ای در شبکه‌های سوئیچینگ بسته[2] مطرح است. در واقع جریان ترافیک شبکه، دنباله‌ای از بسته‌های یک منبع رایانه‌ای به یک مقصد خاص می‌باشد که ممکن است برای یک میزبان و یا چند شبکه به طور هم زمان اقدام به فرستادن اطلاعات نماید. به عبارتی دیگر جریان[3] در مفهوم شبکه، توالی از ارتباطات دو طرفه بین یک جفت گره در شبکه می‌باشد که طی آن مجموعه‌ای از بسته‌ها در یک فاصله زمانی مشخص، منتقل می‌شوند [۱۳].

جریان‌های ترافیک شبکه با اهداف مختلفی ایجاد می‌شوند. این اهداف می‌توانند در راستای کاربردهای عادی و استفاده‌ی معمول از اینترنت و یا به صورت مخرب و به منظور حمله به شبکه‌ها و اقدامات خرابکارانه صورت پذیرد. از مهم‌ترین اهداف تحلیل ترافیک شبکه، رده‌بندی جریان است تا بتوان به کمک روش‌های مناسبی، نفوذ و حملات گوناگون را شناسایی نمود. از سوی دیگر تنوع گونه‌های بدافزاری، همواره به عنوان یکی از دغدغه‌های پژوهشگران حیطه‌ی امنیت به شمار می‌آید که در این بین بات‌نت‌ها به علت گستردگی ایجاد تهدیدات، لزوم شناسایی این شبکه‌ها را در کمترین زمان ممکن، به طور ویژه واضح ساخته است.

تا به امروز روش‌ها و راهکارهای متعددی در جهت طراحی سیستم‌های تشخیص بات‌نت پیشنهاد شده است که یکی از آنها، بررسی دوره‌ای الگوها در جریان‌های ترافیکی شبکه می‌باشد. در واقع نحوه‌ی ارتباط بات‌ها در زمانی که به صورت پیوسته نسبت به اجرا و به روز رسانی دستورات خود اقدام می‌کنند، ممکن است دارای الگوهای یکنواختی باشد. در این وضعیت جریان‌های ارتباطی بات‌ها با ارسال تعداد زیادی از بسته‌های کوچک و یکسان TCP یا UDP همراه است که با بررسی آن در سیستم تشخیص، می‌توان به شناسایی موفقیت‌آمیزی دست یافت. بنابراین راهکار تجزیه و تحلیل ویژگی‌های آماری جریان

[1] Wireless sensor
[2] Packet Switching
[3] Flow

ترافیکی شبکه در یک محیط کنترل شده، می‌تواند در تشخیص بات‌نت‌ها سود بخش باشد [۱۴]. به طور کلی فرآیند نظارت بر ترافیک شبکه، تمایل زیادی به کشف الگوهای مشکوک و جلوگیری از نفوذ بات‌نت‌ها قبل از وقوع حملات واقعی دارد. حال اینکه سیستم تشخیصی بتواند به این مقصود دست یابد، نیاز به رفع چالش‌ها و بهبود تلاش‌های صورت گرفته خواهد داشت.

اولین مسئله چالش برانگیزی که سیستم‌های تشخیص بات‌نت با آن مواجه هستند، نحوه‌ی ارزیابی سیستم است که باید با استفاده از مجموعه داده‌ی جامعی انجام شود و طراحی سیستم، مبتنی بر حجم متنوعی از بات‌نت‌های متمرکز و غیر متمرکز به همراه پروتکل‌های مختلف، باشد. در واقع این موضوع نیازمند جنبه عملی پیدا کردن راهکار و استفاده از مجموعه داده واقعی خواهد بود که از بستر اینترنت بدست آمده است. علاوه بر اینکه می‌بایست داده‌های آموزشی و داده‌هایی که در جهت ارزیابی در نظر گرفته شده اند، تا حد امکان با هم همپوشانی نداشته باشند. بنابراین سیستم تشخیص بات‌نتی که تولید می‌شود، لازم است که عملکرد آن در بستر دنیای واقعی مورد ارزیابی قرار گرفته شود [۱۵].

دومین چالش این سیستم‌ها، کمبود داده‌های برچسب خورده به منظور رده‌بندی می‌باشد. در واقع در بسیاری از مسائل یادگیری واقعی، بدست آوردن نمونه‌های بر چسب‌دار در مرحله آموزش بسیار پرهزینه است. از سوی دیگر به منظور آنکه بتوان در سیستم‌های تشخیص بات‌نت به دقت مطلوبی دست یافت. نیاز به نمونه‌های آموزشی زیادی خواهد بود که با به کارگیری نیروی انسانی متخصص در جهت برچسب زدن نمونه‌ها می‌توان اقدام نمود اما فرآیندی بسیار زمان‌بر و غیر بهینه‌ای را در پی خواهد داشت [۱۶].

سومین چالشی که در سیستم‌های تشخیص بات‌نت وجود دارد، نحوه‌ی آموزش آنها با مجموعه ویژگی‌های مورد اطمینان و با ابعاد کمتر است. در واقع یکی از خواسته‌های مورد انتظار در شبکه‌های تشخیص نفوذ توسعه یافته کنونی، شناسایی گروهی از حملات ناشناخته (همانند بات‌نت روز صفرم[1]) و

[1] Zero-day botnet

جریان‌های بسته‌ای[1] به همراه آشکارسازی میزان ناهمگونی[2] آنها (به نسبت آنچه که به عنوان مدل عادی یا تهی[3] در نظر گرفته می شود) بر روی زیر مجموعه‌ای از ویژگی‌های استخراجی با ابعاد کوچکتر خواهد بود؛ به عبارتی دیگر اگر در ابتدا تمام نمونه‌ها (جریان‌ها) را عادی فرض کنیم (فرض تهی) و سپس به کمک یکی از آزمون‌های آماری، فرض تهی را بتوانیم رد کنیم، آنگاه می‌گوییم که دو نمونه دارای ناهمگونی معناداری هستند وگرنه دو نمونه را یکسان (عادی) می‌خوانیم. لازم به ذکر است این مجموعه کوچک‌تر از طریق مجموعه ویژگی کاملی با ابعاد بزرگ استخراج می‌گردد. همچنین بحثی دیگری که شناسایی ناهنجاری در این سیستم‌ها را به طور کامل به چالش اساسی تبدیل می‌سازد، این است که سنجش[4] مشخصی برای تمایز زیر مجموعه‌ای از ویژگی‌های مشترک با یک رفتار ناشناخته وجود ندارد. علاوه بر این اینکه در حال حاضر رفتار متفاوت بات‌نت‌ها باعث عدم شناسایی آنها توسط سیستم‌های تشخیص نفوذ مبتنی بر امضا[5] نیز شده است [۱۷].

از سوی دیگر همانطور که بیان شد، ترافیک شبکه یک جریان داده است، به این معنی که امضای ترافیک در طول زمان به احتمال زیاد تغییر خواهد کرد. در این سیستم‌ها جریان وسیع داده‌ها، نیاز به قدرت تعمیم‌پذیری بالایی برای شناخت حملات جدید دارد. به این صورت که بر خلاف بسته‌های اطلاعاتی کلاسیک که بطور ذاتی ایستا هستند، جریان داده‌ای، جریان پیوسته‌ای از داده‌ها به شمار می‌آیند که نمی‌توانند ذخیره‌سازی شوند و می‌بایست به عنوان یک واحد مجزا در لحظه مورد تحلیل قرار گیرند [۱۶]. علاوه بر اینکه، بات‌ها تمایل دارند که رفتار خود را در طول زمان بر اساس دستوراتی که از سمت بات مرکزی می‌رسد تغییر داده و نسخه‌ی جدیدی را جایگزین برنامه‌ی خود نمایند، که این موضوع سبب ایجاد مشکل رانش مفهومی[6] برای چارچوب تشخیص خواهد شد. به عبارت دیگر بر خلاف

[1] Packet-flows
[2] Atypicality
[3] Null model
[4] Priori
[5] Signature-based IDS
[6] Concept drift

برنامه‌های مشروع شبکه، بات‌نت‌های جدید می‌توانند در هر زمانی بر روی اینترنت پخش شوند و مدل تشخیص، ممکن است ویژگی‌های بات‌های جدید را در فاز آموزش مشاهده نکرده باشد [۱۷].

چالش بعدی، افزایش حجم اطلاعات تولید شده توسط شرکت‌ها و رسانه‌های اجتماعی مبتنی بر اینترنت است که سبب رشد چشم‌گیر داده‌ها شده‌اند. بنابراین در مقابل، تکنیک‌های تشخیص نفوذ و ناهنجاری نیز می‌بایست قابلیت اجرا و پردازش این حجم وسیع از داده‌ها را در ابعاد بزرگ دارا باشند. یک سیستم تشخیص نفوذ کارآمد که قادر به شناسایی حملات بالقوه است، تعمیم‌پذیری و تشخیص با بیشترین سرعت ممکن را نیاز خواهد داشت [۱۸].

در نهایت چالش نهایی، امکان آموزش مجدد سیستم و به روز رسانی آن به منظور بالا بردن کارایی و قدرت تشخیص سیستم خواهد بود که این امر منجر به تطابق سیستم با ماهیت پویای اینترنت در دنیای واقعی خواهد شد [۱۹]. در واقع دانش کسب شده توسط داده‌های آموزشی در یک سیستم تشخیص در طول زمان، ضروری است تا در قبال حملات جدید و ترافیک نرمال شبکه به روز رسانی شود. به عبارتی دیگر یک سیستم تشخیص کارا باید بتواند مجموعه آموزشی خود را به طور مداوم به روز رسانی کرده تا قابلیت اجرا در دنیای واقعی را داشته باشد. به طور کلی اگر یک سیستم تشخیص در مواجه با گونه‌های جدید حملات (بات‌نت مشاهده نشده)، نرخ تشخیص بالایی را داشته باشد ولی نتواند از این نمونه‌ها برای ارزیابی در مراحل بعدی استفاده نماید، دارای ارزش عملیاتی چندانی نخواهد بود [۲۰].

بنابراین در این پایان‌نامه سعی شده است که با ارائه‌ی راهکاری مبتنی بر یادگیری فعال نیمه‌نظارتی که به صورت افزایشی اقدام به روز رسانی مدل خود می‌کند، بتواند چالش‌های سیستم‌های تشخیص نفوذ کنونی را برای شناسایی بدافزار بات حل و فصل کرده و به سیستمی کارا با نرخ تشخیص مناسب دست یابد.

۱-۳ اهمیت انجام پژوهش

امروزه تهدیدات و حملات در فضای سایبری گسترده‌تر و ساختار آنها از حالت متمرکز به توزیع شده تغییر وضعیت پیدا کرده است. بدافزارها به طور کلی در حال تحول و به روز رسانی هستند و پیوسته از روش‌های پیچیده‌تری به منظور عدم شناسایی توسط سیستم‌های تشخیص استفاده می‌کنند. در مقابل امنیت که به معنای محافظت از دارایی‌ها در برابر طیف وسیعی از تهدیدات است، به دنبال به حداقل رساندن میزان خطرات احتمالی، کاهش تهدیدات و تضمین در فعالیت‌های تحت کنترل خود می‌باشد. به تعبیری دیگر امنیت، فرایند کشف و شناسایی رخدادهایی است که به نوعی می‌توانند به طور بالقوه ضرر ایجاد نمایند. بنابراین برقراری امنیت در بستر اینترنت و جلوگیری از نفوذ خرابکاران و همچنین شناسایی بدافزارها از مهم‌ترین ملزومات فضای سایبری به حساب می‌آید [۲۱].

در حال حاضر یکی از مهم‌ترین گونه‌هایی که در طبقه‌بندی بدافزارها مورد توجه مهاجمان قرار گرفته است، بات‌ها هستند. در واقع بات‌ها دسته‌ای از نرم‌افزارهای مخرب شناخته می‌شوند که با ایجاد شبکه‌ای از چندین بات مختلف به علت انجام حملات گروهی و در ابعاد وسیع، جزء خطرناک‌ترین تهدیدات امنیتی بر شمرده می‌شوند. به این شبکه‌ی ایجاد شده که شامل چندین بات قربانی[1] و یک بات مرکزی است، باتنت گفته می‌شود. باتنت مجموعه‌ای از میزبان‌ها و یا زامبی‌های[2] آسیب دیده است که از طریق یک کانال فرماندهی و کنترل[3] از راه دور توسط یک مهاجم به نام بات مرکزی کنترل می‌شود. با توجه به حجم عظیم تولید باتنت‌ها و مشارکت در انواع حملات اینترنتی، آنها را به عنوان یک تهدید جدی برای امنیت سایبری، تبدیل ساخته است [۴]. بنابراین با توجه به تهدیدات وسیع این دسته از بدافزارها و بالا بودن تنوع ساختاری آنها، نیاز به طراحی سیستمی است که بتواند به صورت کارا و با قدرت تعمیم‌پذیری مناسب به تشخیص و شناسایی بپردازد. همچنین با توجه به حجم وسیع جریان‌های

[1] Slaves
[2] Zombies
[3] Command and Control(C&C)

داده‌ای ترافیک شبکه و کمبود برچسب نمونه‌های آموزشی، نیاز به راهکاری می‌باشد که علاوه بر رفع چالش‌های سیستم‌های تشخیص سابق، بتواند نرخ تشخیص بالا و کار با حجم وسیعی از جریان‌های ترافیکی را داشته باشد. از سوی دیگر عملکرد سیستم طراحی شده نیاز است که با مجموعه داده جامعی مورد ارزیابی قرار گیرد تا پاسخی مناسب به ماهیت بات‌نت‌ها و رفتار واقعی ترافیک شبکه داده شود.

۱-۴ هدف پژوهش

هدف اصلی این پایان‌نامه طراحی یک سیستم تشخیص بات‌نت است که تحلیل جریان‌های ترافیکی شبکه در آن به کمک بردارهای ویژگی می‌باشد که بر اساس مشخصه‌های جریان‌های عادی و حمله استخراج شده‌اند و با استفاده از رویکرد یادگیری فعال نیمه‌نظارتی، اقدام به آموزش و با مشاهده‌ی نمونه‌های جدید مدل خود را به روز رسانی می‌نمایند. در واقع در این سیستم هر جریانی که بر اساس مشخصه‌های تخریب شکل گرفته باشد به عنوان حمله، شناسایی شده و به همین صورت چنانچه دارای اهداف سالم باشد، به عنوان ترافیک معمولی در نظر گرفته می‌شود. اما از سوی دیگر این امکان نیز وجود دارد که در بین بردارهای ویژگی استخراج شده، رده‌بند نتواند به صورت قطعی اقدام به شناسایی جریان‌های سالم از حملات نماید. همچنین از آنجایی در کاربردهای واقعی فرآیند برچسب‌گذاری به منظور آموزش، بسیار هزینه‌بر خواهد بود؛ بنابراین لازم است که راهکاری مناسبی در نظر گرفته شود. در واقع رویکرد ما برای حل مشکلات بیان شده در خصوص این سیستم تشخیص و فضای داده‌ای جریان‌های ترافیکی شبکه، استفاده از روش یادگیری فعال نیمه‌نظارتی است که بتواند از طریق حجم وسیعی از نمونه‌های بدون برچسب و تعداد کمی نمونه‌های برچسب‌دار در جامعه‌ی داده‌های بزرگ به صورت کارا و تعمیم‌پذیر مورد استفاده قرار گیرد و به کمک پرسش از خبره نسبت به تعیین برچسب نمونه‌هایی که رده‌بند نتوانسته به صورت قطعی رده‌بندی کند، اقدام نماید. لازم به ذکر است که این روش جزء اولین روش‌هایی است که برای تشخیص بات‌نت از یادگیری فعال استفاده می‌کند. همچنین

بهره‌گیری از مجموعه داده‌ی جامع و به کارگیری ویژگی‌های موثر جهت شناسایی بات‌نت‌ها در این سیستم می‌تواند پاسخ مناسبی به ماهیت پویای ترافیک شبکه در نظر گرفته شود.

به طور کلی در این سیستم از یک سو به کمک مجموعه نمونه‌های برچسب‌دار اولیه، جریان‌های ترافیکی سالم و حمله مدل‌سازی و آموزش داده می‌شوند و از سویی دیگر جریان‌های بدون برچسب مورد بررسی قرار می‌گیرند و بر حسب اینکه جریان مورد نظر دارای اهدافی مخرب (مشخصه‌هایی مشابه با ویژگی‌های بات‌نت دارند) و یا اینکه جزء جریان‌های سالم مدل‌سازی شده باشند، به دو دسته سالم یا بات‌نت دسته‌بندی می‌نماید. حال در این بین ممکن است، حین رده‌بندی جریان‌های ترافیکی، رده‌بند نتواند با اطمینان دسته‌ی مورد نظر را برای جریان ارسال شده اعلام نماید. این جریان‌های ترافیکی به صورت جریان‌های مشکوک در نظر گرفته می‌شوند. رویکردی که ما برای بهبود کارایی در طراحی سیستم تشخیص خود در نظر گرفته‌ایم، استفاده از چرخه‌ی انسانی و اعلام نظر توسط متخصص(خبره) می‌باشد. در واقع این فرد در خصوص بسته‌های مشکوک تحلیل و ارزیابی به عمل می‌آورد و در نهایت با برچسب‌گذاری مناسب، فرآیند یادگیری دوباره از سر گرفته می‌شود. رده‌بندهای مورد استفاده به صورت گروهی و بر پایه الگوریتم‌های رگرسیون لجستیک، بیز ساده و ماشین بردار پشتیبان خطی[1] می‌باشد که به صورت فعال عمل می‌کند. آموزش در این روش پیشنهادی به صورت تعاملی و سیستم در حین اجرا دائما رده‌بندهای خود را با توجه نمونه‌های جدیدی که مشاهده می‌کند به روز رسانی می‌نماید. علاوه بر اینکه همانند روش‌های بلادرنگ، همواره روند یادگیری ادامه می‌یابد و سیستم قادر خواهد بود تا بدون داشتن برچسب واقعی همه‌ی نمونه‌های جدید، با در نظر گرفتن میزان مفید بودن اطلاعات نمونه‌ها، سعی در به حداقل رساندن هزینه‌های به دست آوردن برچسب داده‌ها نماید و با در اختیار داشتن یک سری از این نوع نمونه‌ها، برچسب سایرین را پیش‌بینی نماید. همچنین، به منظور دستیابی به یک ارزیابی معتبر از عملکرد واقعی سیستم، که در میان پژوهش‌های انجام شده کمتر

[1] Linear Support vector machine (SVM)

مشاهده شده است، تحلیل سیستم به کمک یک مجموعه داده‌ی جامع و معتبر است که دارای درجه بالایی از تنوع بانت‌ها می باشد. بنابراین این سیستم تشخیص بات‌نت سطح بالایی از تعمیم‌پذیری را ارائه می‌دهد.

۱-۵ مروری بر فصل‌ها

در ادامه‌ی این پایان‌نامه و پس از بیان مقدماتی که در این فصل داده شد، موضوعاتی به منظور دریافت بهتر مطالب در خصوص کارهای پیشین و مرتبطی که تاکنون در زمینه بدافزارها، بات‌نت و سیستم‌های تشخیص به انجام رسیده است، در فصل دوم ارائه می‌گردد. در فصل سوم به طور کامل راهکار پیشنهادی این پژوهش شرح داده می‌شود. روش پیشنهادی، مدل پایه‌ای را در اختیار پژوهشگران قرار می‌دهد که می‌تواند در پیاده‌سازی‌های گوناگون این حطیه‌ی کاری موثر واقع شود. در فصل چهارم نتایج و بیان نظری و عملی پژوهش پرداخته می‌شود و ارزیابی‌های صورت گرفته گزارش خواهد شد و در نهایت در فصل پنجم نتیجه‌گیری به عمل می‌آید.

فصل ۲ : ادبیات پژوهش

۲-۱ بدافزارها

در گذشته‌های دور مهاجمان و مجرمان اینترنتی، درهای پشتی را بر روی سیستم‌های مختلف شناسایی و به آن نفوذ می‌کردند ولی پس از آن به این نتیجه رسیدند که به جای نفوذ مستقیم، بدافزارها را به سیستم هدف ارسال کرده و با فریب کاربر، او را نسبت به نصب در پشتی ترغیب نمایند و سپس از طریق راه‌های مختلف همانند ورود از راه دور[1] به سیستم مورد نظر حمله کنند. منظور از در پشتی همان راه نفوذی می‌باشد که اجازه ورود به افراد غیرمجاز از طریق آن داده می‌شود و به خودی خود موجب آسیب نشده اما بستری را برای سطح گسترده‌ای از حملات برای مهاجمان فراهم می‌سازد. مزیت این نوع حملات این‌گونه است که مهاجم در هر زمانی که اراده کند، می‌تواند وارد سیستم هدف شده و کارهای خرابکارانه خود را به انجام برساند [۲۲].

در واقع این روزنه‌های نفوذ به عنوان مسیری برای توسعه و ایجاد نرم‌افزارهایی شدند که بتوانند به صورت خودکار یک سری دستورالعمل‌ها و وظایف تخریبی را به اجرا بگذارند. به طور کلی نرم‌افزارهای رایانه‌ای می‌توانند خود به صورت اهداف سالم و یا مخرب ایجاد شوند؛ از همین رو به نرم‌افزارهایی که با هدف خرابکارانه، اقداماتی نظیر تخریب، جاسوسی، حمله‌ی توزیع شده و کارهای مجرمانه ایجاد می‌شوند، بدافزار گفته می‌شود. به طور کلی بدافزارها با خصوصیات تکثیر، انتشار سریع، خودمختاری و آلوده کردن شناخته می‌شوند که می‌توانند قابلیت اطمینان، صحت و خدمات‌دهی رایانه‌های تحت کنترل خود را سلب نماید. قابلیت تکثیر بدافزارها به عنوان مهم‌ترین خصیصه برای آنها به شمار می‌آید به گونه‌ای که در صورت شناسایی آن در هر سیستمی، نمایانگر وجود گونه‌ای از بدافزار خواهد بود. این قابلیت به حدی مخرب است که در بعضی از موارد سبب اجرای عملیاتی بی‌پایان خواهد شد که در نهایت با تخریب منابع رایانه‌ای (همانند حافظه‌ی اصلی) قربانیان خود همراه خواهد شد [۲۳].

[1] Remote entry

به طور کلی بدافزارها شامل گونه‌های مختلفی هستند که در ادامه به منظور درک بهتر ساختار و عملکرد هر یک از آنها سعی شده است، مطالبی مطرح گردد.

۱. **ویروس**: اولین یا به عبارتی ساده‌ترین نوع بدافزارها ویروس‌ها هستند. در واقع ویروس‌ها به فایل‌هایی گفته می‌شود که خود را افزایش داده و به این طریق، خود را به دیگر فایل‌ها و برنامه های اجرایی، بدون مجوز کاربر، سرایت می‌دهند [۲۴].
۲. **کرم**: به فایل‌هایی اطلاق می‌شوند که از راه آسیب‌پذیر بودن شبکه‌های رایانه‌ای، به آنها رخنه می‌کنند و اغلب پس از نفوذ، فعالیت‌های مخرب یا سودجویانه‌ای را بر روی سیستم‌ها انجام می‌دهند. در واقع کرم‌ها عملکردی مشابه با ویروس‌ها خواهند داشت با این تفاوت که کرم می‌تواند بر روی شبکه پخش شده و به سیستم‌های دیگر انتشار پیدا کند [۲۵].
۳. **تروجان**: به فایل‌هایی گفته می‌شود که به نرم‌افزارهای دیگر می‌پیوندند و زمانی که کاربر، نرم‌افزار را درون سیستم خود نصب می‌کند، سیستم را آلوده می‌سازد. این دسته از بدافزارها همواره سعی دارند تا خود را به صورت یک نرم‌افزار مشروع جلوه دهند [۲۶].
۴. **بات**: این دسته از بدافزارها که ما نیز در این پژوهش نسبت به شناسایی آنها اقدام می‌کنیم، در واقع برنامه‌های نرم‌افزاری هستند که برای اجرای عملیاتی خاص به صورت خودکار، طراحی و به کار برده می‌شوند. اگر این بات‌ها با هدف انجام یک سری وظایف تخریب‌کارانه به صورت گروهی به کار گرفته شوند، گونه‌ی خطرناکی از بدافزارهای تحت فرمان را به نام بات‌نت‌ها ایجاد می‌کنند. همانطور که در فصل اول نیز عنوان شد، علت اصلی خطرناک بودن این گونه شبکه‌ها وجود تعداد زیادی از رایانه‌هایی است که چوپان‌بات می‌تواند از پهنای باند، قدرت ذخیره‌سازی و پردازش هر یک از این رایانه‌ها بهره برده و برای اهداف مخرب خود، استفاده نماید [۲۷].

۵. **آگهی‌افزار**[1]: این دسته از بدافزارها به طور خودکار یک سری تبلیغات و هرزنامه را ارائه می‌دهند که بسیاری از آن‌ها همراه با جاسوس‌افزارها برای ردیابی فعالیت‌های کاربران و سرقت اطلاعات به کار برده می‌شوند [۲۷].

۶. **جاسوس‌افزار**[2]: این بدافزار همانطور که از نامش بر می‌آید، نرم‌افزارهای مخربی هستند که برای انجام فعالیت‌های جاسوسی به کار برده می‌شوند. اقدامات همچون ردیابی سابقه جستجوی واژه‌ها و تصاویر، موقعیت مکانی، سرقت اطلاعات و ارسال آنها به اشخاص ثالث از جمله مهم‌ترین اهداف این بدافزارها به شمار می‌آید [۲۸].

۷. **باج‌افزار**[3]: نوع دیگر از بدافزارها هستند که از طریق رمزگذاری داده‌های سامانه، برای دسترسی به اطلاعات محدودیت ایجاد می‌کنند و در ازای برداشتن این انحصار، از فرد قربانی درخواست باج می‌نمایند. به سامانه محدود شده توسط این بدافزار، یخزده[4] نیز می‌گویند، زیرا کاربر نمی‌تواند هر فایلی را در آن باز و اجرا نماید [۲۹].

۸. **پویشگر کلید**[5] این بدافزار از طریق پویش، تمامی کلیدهای استفاده شده توسط صفحه کلید کاربر اقدام به کار می‌کند. بنابراین تمام داده‌ها را ذخیره‌سازی می‌کند و به رمزهای عبور، شماره کارت‌های بانکی و سایر اطلاعات حساس دسترسی پیدا می‌نماید [۳۰].

۹. **روت‌کیت**[6] نوعی از نرم‌افزارهای مخرب هستند که برای دسترسی از راه دور و یا کنترل رایانه بدون تشخیص کاربر یا برنامه‌های امنیتی طراحی شده‌اند. زمانی که یک روت‌کیت نصب می‌شود، امکان اجرای دستورات از راه دور، سرقت اطلاعات، تغییر تنظیمات پیکربندی سامانه، جایگزینی نرم‌افزارها، نصب بدافزارهای مخفی‌شونده و یا کنترل رایانه به عنوان بخشی از یک بات‌نت را می‌توانند اجرا نمایند؛ که به همین دلیل تشخیص این بدافزار دشوار می‌باشد [۲۷].

---

[1] Adware
[2] Spyware
[3] Ransomware
[4] Frozen
[5] Keylogger
[6] RootKit

۲-۲ رده‌بندی ترافیک شبکه

تعداد کاربران شبکه جهانی اینترنت به طور پیوسته رو به افزایش است، به گونه‌ای که هر روز شاهد ورود برنامه‌های کاربردی جدید و متنوع مبتنی بر آن برای استفاده‌ی کاربران هستیم. بازی‌های برخط، کارافزارهای[1] به اشتراک‌گذاری فایل، ویدئو کنفرانس‌ها، مکالمات مبتنی بر شبکه IP و غیره، به مرور سهم بیشتری از ظرفیت خطوط ارتباطی اینترنت و ترافیک شبکه را به خود اختصاص می‌دهند. بر اساس تحقیقی که در سال ۲۰۱۷ در ارتباط با نرخ نفوذ اینترنت صورت پذیرفت، نشان داده شده است که بیش از نیمی از کل جمعیت جهان، از اینترنت استفاده می‌کنند و بیش از ۳ میلیارد و ۷۷۳ میلیون کاربر فعال در اینترنت حضور دارند. لازم به ذکر است که نرخ نفوذ اینترنت مربوط به درصد کل جمعیت یک کشور یا منطقه خاص (بدون احتساب نوزادان و بی‌سوادان) است که از امکانات آن بهره می‌برند [۳۱].

بنابراین متناسب با این رشد ظرفیت‌های ارتباطی، تولید انواع ترافیک‌های مخرب و تهدیدات امنیتی نیز در فضای سایبری رو به افزایش است که می‌تواند امنیت اطلاعات کاربران را به خطر بیاندازد. تقاضای رو به رشد برای استفاده از پهنای باند بیشتر، از یک سو و محدودیت ظرفیت‌های فیزیکی خطوط ارتباطی شبکه از سوی دیگر، سرویس‌دهندگان اینترنت را بر آن می‌دارد تا در پی یافتن راهکارهایی جهت بهبود کیفیت بهره‌برداری کاربران از منابع شبکه‌ای باشند. یکی از این راهکارها، تخصیص پهنای باند مشخص به هر یک از برنامه‌ها و سرویس‌های موجود در شبکه و اولویت‌دهی به آن‌ها در استفاده از ظرفیت خطوط ارتباطی و منابع پردازشی تجهیزات شبکه است که گام نخست در نیل به این هدف، شناسایی و رده‌بندی ترافیک برنامه‌ها و سرویس‌های موجود در شبکه می‌باشد. همچنین با توجه به افزایش تولید بدافزارها و تلاش آن‌ها برای پنهان‌سازی ترافیک مورد استفاده‌ی خود به منظور گریز از سیستم‌های تشخیص نفوذ و دور زدن دیوارهای آتش، رده‌بندی ترافیک شبکه به عنوان یک گام اولیه در تشخیص نفوذ و تأمین

[1] Application

امنیت اطلاعات به شمار می‌آید که در مقابل تهدیدات سایبری دارای اهمیت ویژه‌ای می‌باشد. به طور خلاصه می‌توان رده‌بندی ترافیک را مقدمه‌ای لازم برای بسیاری از وظایف امنیتی، مدیریتی، کنترلی و بهبود کیفیت سرویس‌دهی در شبکه دانست [۶].

رده‌بندی ترافیک در شبکه‌های رایانه‌ای، کاربردهای امنیتی، کنترلی و مدیریتی مختلفی دارد و به کمک استخراج ویژگی‌های ذاتی جریان‌ها، بررسی محتویات بسته‌ها و با استفاده از الگوریتم‌های یادگیری ماشین انجام می‌پذیرد. به طور کلی رده‌بندی برخط ترافیک، برای سیستم‌های تشخیص نفوذ به عنوان یک اصل محسوب می‌شود و از سوی دیگر برای نظارت در شبکه، اطلاعات آماری لازم را فراهم می‌سازد. انواع مختلفی از کاربردهای شبکه در اینترنت وجود دارد که دارای مشخصه‌های آماری متفاوتی هستند. بنابراین به دلیل وجود این سطح از تنوع در مشخصه‌های آماری، معمولا به منظور رده‌بندی ترافیک، از رده‌بندی‌های آماری استفاده می‌شود [۳۲]. از جمله کاربردهای رده‌بندی ترافیک شبکه در حیطه‌ی امنیت اطلاعات، رده‌بندی بر اساس کاربرد جریان‌ها جهت تشخیص حملات اینترنتی می‌باشد. پس همانطور که در فصل قبل نیز عنوان شد، جریان‌های ترافیکی دارای مشخصه‌های مختلفی برای میزبان‌ها هستند که در یک طبقه‌بندی کلی این مشخصه‌ها به دو دسته‌ی جریان‌های سالم و حمله تقسیم‌بندی می‌شوند.

۲-۳ بات‌نت

بات‌نت‌ها، شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از رایانه‌های مختلف به نام بات، شکل می‌گیرند و توسط یک و یا چند مهاجم به نام بات مرکزی یا چوپان‌بات، با هدف انجام فعالیت‌های مخرب کنترل می‌شوند. به عبارت بهتر مهاجم با انتشار ویروس‌ها و برنامه‌های مخرب به صورت غیرقانونی و بدون اطلاع صاحب رایانه، کنترل آن را در دست می‌گیرند و با استفاده از مجموعه‌ای از این رایانه‌ها، درخواست‌های جعلی زیادی را به سمت سرور یا سایت قربانی ارسال می‌کنند که در نهایت منجر به

انجام یک حمله ممانعت از سرویس‌دهی می‌شوند. به طور کلی بات‌نت‌ها می‌توانند شامل هزاران و یا حتی میلیون‌ها بات آلوده‌کننده باشند که این خود به عنوان تهدید بزرگی برای نرم‌افزارهای اینترنتی و ارتباطات برخط است. بر طبق گزارشات سال ۲۰۱۵ که توسط موسسه IMPERVA در خصوص ترافیک بات جهانی صورت پذیرفت، سهم استفاده از ترافیک شبکه را می‌توان به سه گروه عمده تقسیم‌بندی کرد که در این میان، حدود ۵۱/۵ درصد سهم انسان‌ها، ۲۹درصد سهم بات‌های مخرب و ۱۹/۵درصد بات‌نت‌های غیرمخرب را شامل می‌شود. همچنین این گزارش توابع اصلی بات‌های مخرب یعنی اسپم‌ها، سودجویان و برهم زنندگان امنیتی را نیز برجسته ساخته که نمایانگر تهدید بزرگ این بدافزار در سال‌های آینده خواهد بود [۳۳].

از نظر تاریخی بات‌نت‌ها برگرفته شده از یک پروتکل گفت‌وگوی اینترنتی[1] هستند که یک سیستم مبتنی بر متن بود و ارتباطات درون کانال‌ها سازماندهی می‌گشت. همچنین فرآیند گفت‌وگو در این سیستم‌ها در غالب یک مدل سرور - مشتری و از بات‌نت‌ها با هدف کنترل فعالیت‌های موجود در اتاق‌های گفت‌وگوی IRC بهره گرفته می‌شد. این بات‌ها می‌توانستند دستورات ساده را اجرا کرده، بازی‌های ساده و سرویس‌های مختلف را به کاربران گفت‌وگو پیشنهاد داده و اطلاعاتی در مورد سیستم عامل‌ها، گزارش‌های ورود به سیستم، آدرس‌های ایمیل و مانند آنها را استخراج نمایند. اولین بات IRC، به اسم Eggdrop در سال ۱۹۹۳ ارائه شد و پس از آن توسعه پیدا کرد. در ادامه بات‌های IRC مختلفی با اهداف مخرب اعم از حمله به کاربران IRC و یا تخریب همه‌ی سرورها، ایجاد شدند [۳۴].

به طور کلی بات‌های جدید از ساز وکارهای پیچیده‌ای برای ارتباط با بات مرکزی استفاده می‌کنند که این خود سبب بهره‌گیری از پروتکل‌ها و تکنیک‌های متعددی می‌شود و در نهایت منجر به پیچیده شدن روزافزون ساختار این بات‌ها و سخت‌تر شدن تشخیص و مقابله با آنها می‌گردد. همچنین آنها می‌توانند مانند کرم‌ها منتشر شوند، مثل یک ویروس مخفی بمانند و حملات گسترده و سازمان یافته‌ای

[1] Internet Relay Chat (IRC)

را شکل دهند. نسل جاری بات‌ها می‌توانند از طریق شبکه‌های اشتراک فایل، شبکه‌های نظیر به نظیر و پیوست‌های ایمیل و سایت‌های آلوده نیز منتشر شوند [۳۵].

۲-۳-۱ اجزای بات‌نت

اجزای یک بات‌نت شامل بات، کانال فرمان و کنترل، بات مرکزی، بات‌نت و قربانیان می‌باشد که در ادامه در خصوص هر یک از آنها جزییاتی را بیان می‌کنیم.

۱. **بات**: یک برنامه‌ی نرم‌افزاری به صورت بدافزار است که بر روی یک میزبان آسیب‌پذیر نصب می‌شود. این بدافزار می‌تواند حتی از طریق مشاهده‌ی یک وب‌سایت آلوده نیز به رایانه‌ی میزبان نفوذ کرده و به نحوی پیکربندی شود که با هر بار روشن شدن رایانه قربانی، بات نیز فعال گردد.

۲. **کانال فرمان و کنترل**: اقداماتی که بات‌ها انجام می‌دهند بر اساس فرمان‌هایی هستند که توسط بات مرکزی و از طریق یک کانال کنترلی ارسال می‌شوند. بات‌ها آسیب‌پذیری‌های سیستم‌های عامل و یا برنامه‌های کاربردی نیستند؛ بلکه برنامه‌هایی هستند که برای نصب کردن برنامه‌های درهای پشتی بر روی ماشین قربانی مورد استفاده قرار می‌گیرند. در واقع چیزی که بات‌ها را از سایر بدافزارها متمایز می‌کند، همین کانال فرمان و کنترل است.

۳. **بات‌نت**: مجموعه‌ای از بات‌هایی که به یک کانال کنترل و فرمان متصل شده‌اند و منتظر دریافت دستورات برای انجام فعالیت‌های تخریب‌کننده هستند، گفته می‌شود.

۴. **بات مرکزی(چوپان‌بات)**: کاربران مخربی هستند که با ارسال فرمان‌هایی برای انجام فعالیت‌های مضر، بات‌ها را کنترل و در راستای اهداف مختلف خود آنها را هدایت می‌کنند.

۵. **قربانیان(اهداف)**: به ماشین‌هایی که بعد از آلوده شدن تبدیل به زامبی شده و می‌توانند اهداف مخرب مختلفی را دنبال کنند، گفته می‌شود.

به طور کلی مهم‌ترین جزء بات‌نت زیر بنای کانال کنترل و فرمان است که شامل بات‌ها و یک واحد کنترل خواهد بود. بات‌های مرکزی از پروتکل‌های ارتباطی مختلفی برای برقراری ارتباط با قربانی‌ها و ارسال دستورات به آن‌ها استفاده می‌کنند. با توجه به اینکه کانال C&C عموما به عنوان تنها راه کنترل بات‌ها محسوب می‌شود و کارایی بات‌نت وابسته به ارتباط پایدار با این کانال می‌باشد، معماری آن می‌تواند تعیین کننده‌ی میزان مقاومت، پایداری و زمان واکنش نیز باشد. در حالت کلی بات‌ها به دو دسته‌ی متمرکز و غیر متمرکز تقسیم‌بندی می‌شوند [۴].

۲-۳-۲ انواع بات‌نت‌ها

بات‌نت‌ها را می‌توان بر اساس معیار کانال فرمان و کنترل به دو بخش کلی، شامل ساختار و پروتکل طبقه‌بندی نمود. همچنین بر اساس ساختار کانال فرمان و کنترل به سه دسته‌ی متمرکز و غیر متمرکز و ترکیبی و بر اساس پروتکل مورد استفاده در این کانال‌ها، به سه نوع مبتنی بر IRC، مبتنی بر HTTP و نظیر به نظیر دسته‌بندی می‌شوند. در ادامه به صورت مختصر ویژگی این بات‌نت‌ها شرح داده می‌شود.

۱. **بات‌نت متمرکز**[1]: ساختار مبتنی بر مدل مشتری - سرویس‌دهنده است به طوری که همه‌ی بات‌ها به طور مستقیم به یک یا تعداد کمی از سرویس‌دهنده‌های کنترل و فرمان متصل هستند. این سرویس‌دهنده‌ها بات‌ها را با یکدیگر هماهنگ کرده و همچنین به بات‌ها برای انجام عملیات فرمان می‌دهند [۳۶].
۲. **بات‌نت غیرمتمرکز**[2]: در این نوع معماری، سرویس‌دهنده‌ی کنترل و فرمان متمرکزی وجود ندارد، بلکه در آن بات‌نت‌هایی مختلف از طریق پروتکل‌های نظیر به نظیر با یکدیگر در ارتباط هستند. به عبارت دیگر، بات‌ها هم به عنوان مشتری و هم سرویس‌دهنده‌ی کنترل و فرمان عمل می‌کنند [۳۷].

[1] Centralized botnet
[2] Decentralized botnet

۳. **بات‌نت ترکیبی**[1]: معماری ترکیبی بات‌نت‌ها از مزایای هر دو نوع معماری متمرکز و غیر متمرکز بهره می‌برد. به این معنی که در این ساختار، بات‌ها عملکردی متفاوتی را از خود نشان می‌دهند. برخی از آن‌ها به صورت موقت نقش سرویس‌دهنده‌ی کنترل و فرمان را به عهده می‌گیرند و عمل هماهنگ‌سازی بات‌نت و نیز انتشار فرمان‌ها را انجام می‌دهند در حالی که سایر بات‌ها منتظر فرمان می‌مانند [۳۸].

۴. **بات‌نت مبتنی بر**IRC: در این گونه از بات‌نت‌ها هر سرویس‌دهنده‌ی IRC، کانال‌های متنوعی را میزبانی می‌کند. در این نوع از بات‌نت‌ها، کانال کنترل و فرمان در سرویس‌دهنده‌ی IRC ایجاد می‌شود و بات‌ها عضو این کانال می‌گردند. در این ساختار بات مرکزی سعی در حفظ ارتباط خود با قربانیان و به روز رسانی برنامه‌ها و دستورات را خواهد داشت [۱۷].

۵. **بات‌نت مبتنی بر** HTTP: در این گونه از بات‌نت‌ها، پروتکل HTPP برای انتشار دستورات در وب سرورهای خاص استفاده می‌شود. در واقع بات مرکزی از این پروتکل برای مخفی کردن فعالیت‌های خود در میان جریان‌های عادی ترافیک شبکه بهره می‌گیرد و به راحتی فعالیت خود را از سیستم‌های تشخیصی و دیوار آتش پنهان می‌سازد [۳۷].

۶. **بات‌نت نظیر به نظیر**[2]: در این گونه از بات‌نت‌ها همانند بات‌نت‌های با ساختار غیر متمرکز، اغلب از پروتکل‌های ارتباطی نظیر به نظیر استفاده می‌گردد و همانند شبکه‌های مبتنی بر آن که نسبت به تغییرات پویا انعطاف پذیرند، ارتباطات این بات‌نت نظیر به نظیر نیز، با از دست دادن تعدادی از بات‌ها مختل نخواهد شد. از سوی دیگر این بات‌نت‌ها در حالت پیشرفته از رمزگذاری استفاده می‌کنند تا ارتباطات بین خود را پنهان کنند [۳۷].

[1] Hybrid botnet
[2] Peer to peer botnet

۲-۴ روش‌های تشخیص بات‌نت

روش‌های تشخیص بات‌نت را می‌توان بر اساس سه معیار گروه‌بندی کرد. معیار اول موقعیت بات‌نت در چرخه حیات[1] به هنگام تشخیص است. معیار دوم و سوم به ترتیب، رویکرد یادگیری و میزان سطح همبستگی می‌باشد. بر اساس معیار اول، تشخیص می‌تواند در مراحل آغازین، یعنی در زمان شکل‌گیری بات‌نت و ایجاد کانال کنترل و فرمان و یا در مرحله‌ی حمله بات‌نت صورت گیرد. به طور کلی، دقت روش‌هایی که در این مرحله شناسایی را انجام می‌دهند بالاتر است. اما از طرفی تشخیص بات‌نت‌ها در مراحل آغازین، از حضور آن‌ها در فعالیت‌ها و حمله‌های مخرب جلوگیری به عمل می‌آورد و امکان تحلیل رفتاری و الگو جریان‌های مربوط به آنها دیگر وجود نخواهد داشت [۸].

بر اساس معیار دوم، رویکرد یادگیری می‌تواند به صورت با ناظر یا بدون ناظر انجام پذیرد. به طور کلی در یادگیری بر خط، اغلب به دلیل محدودیت نیاز به داده‌های برچسب‌گذاری شده، از رویکردهای با ناظر استفاده نشده و به جای آن از رویکردهای بدون ناظر که نیازی به اطلاعات پیشینی از بات‌نت‌ها و داده‌های برچسب‌گذاری شده ندارند، استفاده می‌شود. بنابراین برای به‌کارگیری روش‌های با ناظر، لازم است که این محدودیت‌ها با استفاده از شیوه‌های نوینی برطرف شود [۳۷].

در نهایت بر اساس معیار سوم، روش‌های تشخیص بات‌نت می‌توانند بر اساس دو سطح مختلف از تحلیل همبستگی[2] که به صورت گروهی یا انفرادی هستند، به کار برده شوند. در تحلیل سطح انفرادی، شناسایی بر اساس رفتارهای فردی هر سیستم صورت می‌گیرد و رفتار سایر سیستم‌های آلوده در نظر گرفته نمی‌شود. مزیت کلی این روش‌ها در این است که اگر شبکه مورد نظر، دارای تنها یک گونه بات باشد، آن را به درستی تشخیص دهند. از سوی دیگر روش‌های مبتنی بر تحلیل سطح گروهی بر اساس یافتن الگوی مشابه بین دو یا چند سیستم عمل می‌کنند و آن‌ها را به عنوان اعضای بات‌نت، تشخیص

[1] Life cycle
[2] Correlation analysis

و معمولا دقت در این روش‌ها نسبت به حالت قبل بالاتر ولی تنها قادر به شناسایی بات‌نت‌هایی با عضویت مشترک خواهند بود [۸].

به طور کلی، روش تشخیص بات‌نت در این پژوهش یک رویکرد مبتنی بر یادگیری فعال نیمه‌نظارتی، تحلیل انفرادی و تشخیص در مرحله آغازین را ارائه می‌دهد و سیستم می‌تواند در حین اجرا دائما رده‌بندهای پایه‌ی خود را با توجه نمونه‌های جدیدی که مشاهده می‌کند، به روز رسانی نماید.

۲-۵ سیستم‌های تشخیص نفوذ

به صورت کلی سه روش برای شناسایی و تشخیص نفوذ به شبکه وجود دارد که بر اساس آنها سیستم‌های تشخیص شکل گرفته و فعالیت می‌کنند. این روش‌ها شامل شناسایی مبتنی بر امضا، تشخیص ناهنجاری و تشخیص پروتکل ناهنجاری می‌باشد که در ادامه توضیحاتی را در خصوص آنها ارائه می‌دهیم.

۱. **تشخیص مبتنی بر امضاء**[1]: در این روش که همانند کاری است که یک آنتی‌ویروس انجام می‌دهد، سیستم تشخیص نفوذ دارای یک پایگاه داده است که در آن نوع و روش فعالیت برخی از حملات مشخص شده‌اند و به محض اینکه موردی را تشخیص دهد آن را با اطلاعات پایگاه داده مربوطه مقایسه کرده و در صورت بروز تطابق اعلام هشدار می‌کند.
۲. **تشخیص مبتنی بر رفتار ناهنجار**[2]: در این روش سیستم با توجه به رفتاری که در شبکه عادی وجود دارد و ترافیکی که در اثر یک عمل غیر عادی ایجاد شده است، تصمیم می‌گیرد که در مورد این نوع ترافیک اعلام هشدار دهد. در واقع سیستم از طریق ارزیابی و مقایسه بین ترافیک طبیعی و غیرعادی اقدام به کار می‌کند.

[1] Signature based detection
[2] Anomaly based detection

۳. **تشخیص پروتکل غیرعادی**[1]: در این نوع تشخیص، مدل‌ها بر اساس مشخصات پروتکل TCP/IP تجزیه و تحلیل می‌شوند و در صورت مشخص شدن تغییرات در مشخصات این پروتکل، سیستم هشدار فعال می‌شود [۱۸].

۲-۵-۱ انواع سیستم‌های تشخیص نفوذ

امروزه سیستم‌های تشخیص نفوذ مختلفی در ارتباط با شناسایی حملات، باتنت‌ها و ناهنجاری‌ها ارائه شده‌اند که در یک تقسیم‌بندی کلی می‌توان به موارد زیر اشاره کرد:

۱. **سیستم‌های تشخیص نفوذ تحت شبکه**[2]: این سیستم‌ها به کمک کارت شبکه‌ای که در حالت بی‌قید[3] قرار می‌گیرد، تمامی ترافیک شبکه را دریافت و تجزیه و تحلیل می‌نماید. مانند نرم‌افزار SNORT در سیستم عامل لینوکس؛ به این صورت که بسته‌های شبکه را در برابر امضاهای شناخته شده مطابقت داده و اگر یک حمله شناسایی شود، هشدار می‌دهد.

۲. **سیستم‌های تشخیص نفوذ تحت میزبان**[4]: این سیستم‌ها به کمک اطلاعات فایل‌های پایشی[5] مربوط به یک رخداد خاص بر روی هر سیستم، فعالیت کرده و این رویدادها را تجزیه و تحلیل می‌کنند. اما از سوی دیگر به دلیل ایجاد بار کاری زیاد برای پردازنده‌ها، معمولا کمتر استفاده می شوند. نرم‌افزار منتسب به این سیستم تشخیص، به صورت انفرادی بر روی تمامی سیستم‌ها نصب می‌شود و در نهایت فعالیت مجزایی را در پیش می‌گیرد. همانند نرم‌افزار CSA شرکت سیسکو[6]. ساز وکار حفاظتی این سیستم، سبب می‌شود تا

[1] Protocol Anomaly detection
[2] Network Based IDS
[3] Unconditional mode
[4] Host Based IDS
[5] Log file
[6] Cisco Security Agent

بهره‌برداری از راه‌های آسیب‌پذیر ناشناخته یا ناخواسته‌ی موجود در نرم‌افزار کاهش پیدا کرده، اما به گونه‌ای اتفاق می‌افتد که با شناسایی هر حمله، فعالیت برنامه نیز خاتمه می‌یابد.

۳. **سیستم بررسی یکپارچگی فایل**[1]: معمولا برای تشخیص انواع تروجان و نرم‌افزارهایی به کار می‌روند که باعث ایجاد تغییرات اساسی در سیستم‌ها شده‌اند. در این روش از هر فایل بر روی سیستم یک درهم[2] گرفته شده و در پایگاه داده مرکزی نگهداری می‌شود. حال در صورت بروز مشکل، این درهم با درهم فایل جدید مقایسه می‌گردد و اگر عدم تطابق وجود داشته باشد، اعلام اخطار داده می‌شود. همانند نرم‌افزار Tripwire و AFICK که نوعی تصدیق‌کننده‌ی یک‌پارچگی سیستم[3] به شمار می‌آید و از طریق نظارت بر فایل‌های سیستم، عملیات حفاظت از داده‌ها و تشخیص نفوذ را انجام می‌دهند.

۴. **سیستم نظارت بر فایل‌های پایشی**[4]: در این نوع سیستم از تمامی رخدادهای حاصل شده در سیستم‌ها رویداد برداری[5]می‌شود و همه آنها به سمت سروری بر روی شبکه منتقل شده و از طریق آن مورد تجزیه و تحلیل قرار می‌گیرند. این روش در تشخیص سوء استفاده از نرم افزارها، نقض قوانین و همچنین کشف فعالیت‌های مخرب مفید است [۳۹].

۲-۵-۲ انواع روش‌های برخورد و پاسخ به نفوذ

به طور کلی سیستم‌ها تشخیص نفوذ، دارای نحوه‌ی برخورد متفاوتی با حملات هستند که در یک تقسیم‌بندی کلی می‌توان به رویکردهای فعال و غیرفعال اشاره نمود. در رویکرد فعال عملکرد سیستم به صورت خودکار صورت می‌پذیرد ولی در رویکرد غیر فعال منتظر پاسخ از مدیر شبکه باقی خواهد ماند. در ادامه توضیحاتی را در این رابطه ارائه می‌دهیم.

[1] File Integrity Checker system
[2] Hash
[3] System Integrity Verifier (SIV)
[4] Log File Monitoring system
[5] Log events

۱. **پاسخ فعال در سیستم تشخیص نفوذ**: در این گونه از روش‌ها، سیستم به محض تشخیص مورد خاصی به صورت برخط، نسبت به تحلیل و بررسی آن اقدام کرده و در صورت یافتن نشانه‌هایی از حمله، اقدام به اعلام هشدار به مدیر شبکه می‌نماید. همچنین ممکن است این اعلام به صورت یک رویداد در فایل‌های پایشی در نظر گرفته شود.

۲. **پاسخ غیر فعال در سیستم تشخیص نفوذ**: در این روش به کمک ارسال پیامک یا ایمیل، اطلاعاتی را در خصوص حمله برای مدیر شبکه ارسال می‌شود. این اطلاعات می‌تواند شامل آدرس‌های IP منبع و مقصد حمله، ابزار یا راهکار مطلوب برای مهار و مقابله با حمله، گزارش‌های مربوط به ارتباطات حمله و غیره باشد [۳۹].

۲-۶ یادگیری نیمه‌نظارتی

یادگیری نیمه‌نظارتی یک روش ما بین یادگیری بدون ناظر و یادگیری با ناظر است. به عبارت دیگر، این روش یادگیری با مقدار کمی داده‌های برچسب خورده آموزش می‌بیند و اطلاعات بدست آمده را با مجموعه بزرگی از داده‌های بدون برچسب، برای انجام یک تقریب مناسب در الگوریتم یادگیری ترکیب می‌سازد [۴۰]. یادگیری نیمه نظارتی در سیستم‌های امنیتی بیشتر به منظور یادگیری و به‌روز رسانی مدل فراگرفته شده توسط سیستم است که می‌بایست با حجم محدودی از داده‌های بر چسب خورده به انجام برسد. در واقع هدف یادگیری نیمه نظارتی استخراج یک مدل از نمونه‌های برچسب خورده محدود است [۴۱]. این الگوریتم‌ها به طور خاص برای جامعه داده‌های بزرگ قابل توجه است چرا که مجموعه بسیار بزرگی از داده‌های بدون برچسب وجود دارند که به خوبی توسط الگوریتم‌های یادگیری با ناظر سنتی مورد بهره‌برداری و استفاده مناسب قرار نگرفته‌اند. در روش یادگیری نیمه‌نظارتی بعضی از داده‌ها دارای برچسب بوده و بعضی نیز برچسب ندارند. به علت اینکه در خیلی از برنامه‌های کاربردی عملیات برچسب‌گذاری هزینه‌بر و زمان‌بر می‌باشد؛ برای اینکه کارایی را افزایش داده و از کل توان در حل مسئله

برای بهبود دقت استفاده کرد، می‌توان از داده‌های بدون برچسب به گونه‌ای سود برد که کمترین هزینه را برای سیستم داشته باشند؛ به این صورت که به کمک نمونه‌های برچسب‌دار مدلی از رده‌بند ساخته شود و سپس هر نمونه بدون برچسب بر اساس مدل‌های شکل گرفته، به کلاس شبیه‌تر تعلق پیدا کند. در یادگیری نیمه‌نظارتی هدف یافتن روش‌هایی است که با استفاده از آن به حل یک مسئله پرداخته و در نتیجه کارایی الگوریتم مورد نظر را نسبت به قبل افزایش و همچنین از سوی دیگر میزان نرخ خطا را در فرآیندهای یادگیری به شکل مطلوبی کاهش داد [۴۲].

به طور کلی در یادگیری نیمه‌نظارتی علامت نمونه‌های بدون برچسب با توجه به نمونه‌های برچسب خورده تعیین می‌شود و نتیجه‌ی این کار ایجاد یک رده‌بند مطلوب‌تر خواهد بود. در یک دسته‌بندی جامع، این روش یادگیری را می‌توان به رویکردهای خودآموز (خودفراگیر)[۱]، آموزش توأم[۲]، ماشین‌های بردار پشتیبان انتقالی[۳]، بیشینه‌سازی امید[۴] به همراه مدل‌های مخلوطی مولد[۵] و روش‌های مبتنی بر گراف[۶] تقسیم‌بندی نمود که توجه بسیاری از پژوهشگران را به خود جلب کرده‌اند [۱۰]. ما در ادامه در خصوص هر یک از این رویکردهای یادگیری نیمه‌نظارتی به طور خلاصه، مطالبی را مطرح می‌کنیم.

۱. **خود آموز:** ایده‌ی اصلی این راهکار آموزش رده‌بند به کمک نمونه‌های برچسب خورده است. سپس رده‌بند به منظور پیش‌بینی کلاس نمونه‌های بدون برچسب اعمال می‌گردد. در این روش زیر مجموعه‌ای از قابل اعتمادترین نمونه‌های بدون برچسب با برچسب‌های پیش بینی شده انتخاب و سپس به مجموعه آموزشی اضافه خواهند شد. رده‌بند دوباره بر روی مجموعه نمونه‌های جدید، آموزش مجدد می‌بیند و این رویه تکرار می‌شود. راهکار خودآموزی با این واقعیت که رده‌بند از پیش‌بینی‌های انجام شده برای آموزش خود استفاده می‌کند، مشخص می‌شود [۴۰].

---

[1] Self-training
[2] Co-training
[3] Transudative Support Vector Machines (TSVMs)
[4] Expectation maximization (EM)
[5] Generative mixture models
[6] Graph-based methods

۲. **آموزش توأم:** در این روش با دو رده‌بند مختلف که نیاز به دو مجموعه ویژگی متفاوت از نمونه‌های برچسب خورده دارند، اقدام به کار می‌شود. هر رده‌بند به کمک مجموعه ویژگی‌ها آموزش می‌بیند و سپس به منظور رده‌بندی نمونه‌های بدون برچسب مورد استفاده قرار می‌گیرد. به طور کلی آموزش توأم یک روش یادگیری نیمه نظارتی است که نیاز به دو نما از داده‌ها دارد؛ یعنی هر نمونه، دو مجموعه از ویژگی‌هایی که مختلف و مکمل یکدیگر هستند را برای توصیف یک واقعیت ارائه می‌دهد. در حالت ایده‌آل، هر نمونه، به صورت شرطی از کلاس تعلق یافته به آن مستقل و کلاس هر نمونه نیز به تنهایی و با دقت بالا قابل پیش‌بینی می‌باشد. آموزش توأم در سنجش کیفیت هوای شهری و دسته‌بندی رایانامه‌ها به کار گرفته شده است. نتایج بدست آمده از این مطالعات، مزیت بالای این روش را نسبت به سایر روش‌های یادگیری نیمه‌نظارتی نشان می‌دهد [۴۰و۴۳].

۳. **مدل‌های مخلوطی مولد:** در روش‌های مولد ابتدا یک مدل پارامتری برای تابع توزیع نقاط(مثلا توزیع گاوسی) انتخاب می‌شود که آن را با $P(x|y,\theta)$ نشان می‌دهیم و θ نمایانگر مدل است. سپس $P(y)$ از روی داده‌های برچسب‌دار تخمین زده می‌شود. احتمال وقوع نقاط با توجه به تابع توزیع هر دسته، بر حسب پارامترهای مدل، به صورت تحلیلی محاسبه می‌شود. سپس با اعمال قانون بیز می‌توان تابع توزیع برچسب در هر نقطه را محاسبه کرد. در روش‌های مولد معمولاً هدف بیشینه کردن این احتمال وقوع یا به طور معادل درست‌نمایی بیشینه[1] آن‌ها نسبت به پارامترهای مدل است. از روش‌های مختلفی می‌توان برای بهینه‌کردن پارامترهای مدل نسبت به میزان راست‌آزمایی استفاده کرد. در مقابل روش‌های مولد، روش‌هایی نیز وجود دارند که به طور مستقیم به یادگیری $P(y|x)$ می‌پردازند، این روش‌ها با نام روش‌های تمایزی[2] شناخته می‌شوند. توجیهات نظری وجود دارد که نشان می‌دهد که روش‌های مولد نیاز به داده‌های

[1] Maximum Likelihood
[2] Discriminative

بیشتری نسبت به روش‌های تمایزی جهت یادگیری دارند. همچنین در عمل روش‌های تمایزی موفقیت بیشتری را داشته‌اند. بنابراین تحقیقات روی روش‌های مولد کم‌رنگ بوده است [۴۴].

۴. **روش‌های مبتنی بر گراف:** در این روش، گرافی تعریف می‌شود که در آن رئوس نمایانگر نمونه‌های برچسب خورده و بدون برچسب هستند و یال‌های بدون جهت بین دو راس، بیانگر شباهت[1] بین آن دو نمونه خواهد بود. در سال‌های اخیر بیشترین بخش مورد توجه پژوهشگران در زمینه‌ی یادگیری نیمه‌نظارتی، راهکارهای مبتنی بر گراف می‌باشد که از طریق ساخت یک گراف از نمونه‌های آموزشی ایجاد می‌شود [۴۰]. به طور کلی این روش در صورتی مؤثر است که پیش‌فرض هموار و پیش‌فرض خمینه، هم‌زمان برقرار باشند (لازم به ذکر است که در خصوص پیش‌فرض‌های مذکور در انتهای این بخش نکاتی مطرح می‌گردد). برای استفاده از پیش‌فرض خمینه در فضایی با بعد بالا، باید ساختار گراف به نحو مناسبی بیان شود که یکی از این راه‌ها ، استفاده از گراف‌های همسایگی است. در گراف همسایگی، رئوس همان نقاط هستند و میان نقاط نزدیک به هم روی خمینه یال، وزن متناسب قرار داده می‌شود. در روش‌های نیمه‌نظارتی مبتنی بر گراف، ابتدا گراف همسایگی روی نقاط ساخته می‌شود و سپس به کمک روش‌های استنتاجی نسبت به تعیین برچسب نقاط بدون برچسب اقدام می‌شود. به عبارت دیگر، هر الگوریتم نیمه‌نظارتی مبتنی بر گراف شامل گام‌های کلی زیر است:

- پیش‌پردازش داده‌ها که شامل استخراج ویژگی‌ها، کاهش بعد، حذف نویز و موارد دیگر می‌باشد.
- ایجاد گراف همسایگی روی نقاط که معمولا لازمه‌ی آن محاسبه‌ی فاصله‌ی بین نقاط است.
- استنتاج برچسب نقاط بدون برچسب به کمک یکی از روش‌های استنتاج [۴۴].

۵. **بردارهای پشتیبان انتقالی:** این روش جز راهکارهای انتقال یادگیری به شمار می‌آید و بر اساس فرض خوشه که معادل با فرض جداسازی کم چگالی است، عمل می‌نماید. به طور کلی

[1] Similarity

در بسیاری از الگوریتم‌های یادگیری ماشین و داده‌کاوی فرض عمده بر این است که داده‌های آموزش و داده‌های مورد بررسی باید دارای فضای ویژگی و همچنین توزیع یکسانی باشند، درصورتی که در بسیاری از کاربردهای واقعی داده‌های انبوه بدست آمده از منابع گوناگون، دارای عدم تجانس هستند که این خود سبب رد این فرضیه می‌شود. به عنوان مثال، ما گاهی فرآیند رده‌بندی مرتبط با حوزه‌ی خاصی را در نظر داریم، ولی داده‌های آموزشی حوزه‌ی دیگری به صورت کافی در دسترس هستند که در آن داده‌ها ممکن است از یک فضا با ویژگی‌های مختلف و یا توزیعی متفاوت پیروی کنند. جهت غلبه بر این مسئله، انتقال یادگیری پیشنهاد شده است که اجازه می‌دهد تا حوزه، وظایف و توزیع بین داده‌ها متفاوت باشد. این روش، دانش را از یک یا چند منبع وظایف استخراج و به یک وظیفه‌ی هدف انتقال می‌دهد. در چنین مواردی اگر انتقال دانش بدست آمده قبلی با موفقیت و هوشمندانه انجام گیرد، تا حد زیادی یادگیری را تسریع و با دوری جستن از برچسب زدن پرهزینه داده‌ها، حل مسائل جدید را بهبود می‌بخشد. به طور کلی بر اساس شرایط مختلف حوزه‌ها و وظایف بین منبع و هدف داده شده، انتقال یادگیری به سه شیوه قیاسی، ارسالی و بدون نظارت انجام می‌گیرد. در مورد انتقال یادگیری قیاسی، وظایف منبع مبدأ و هدف مقصد متفاوت هستند، بدون توجه به آنکه حوزه‌های مبدا و مقصد همان است یا نه. در مقابل، در انتقال یادگیری ارسالی، حوزه هدف از حوزه منبع فرق می‌کند، در صورتی که وظایف آن‌ها یکسان هستند. در نهایت، در انتقال یادگیری بدون نظارت، وظیفه هدف با وظیفه منبع فرق دارد، ولی به آن مرتبط است. بنابراین در راهکار ماشین بردار پشیبان نیمه نظارتی که به ماشین‌های بردار پشتیبان انتقالی نیز شهرت دارد، هدف اصلی استفاده از داده‌های برچسب‌دار و بدون برچسب برای پیدا کردن یک مرز خطی مناسب و دارای حداکثر حاشیه، خواهد بود [۴۰و۴۳].

حال‌که دسته‌بندی مناسبی از روش‌های نیمه‌نظارتی انجام پذیرفت، می‌توان در خصوص زمان به‌کارگیری و استفاده از این راهکار برای مسائل مختلف بحث نمود. پرسش اصلی در زمینه یادگیری نیمه نظارتی این است که اصولا تحت چه شرایطی باید از این روش استفاده کرد. به عبارتی دیگر آیا با استفاده از داده‌های بدون برچسب واقعا می‌توان کارایی را بهبود بخشید؟. نگاهی به حجم مقالات ارائه شده در این زمینه نشان می‌دهد پاسخ مثبت است، اما یک شرط اساسی وجود دارد و آن هم اینکه باید توزیع نمونه‌هایی که به کمک داده‌های بدون برچسب بدست می‌آیند، مناسب مسئله جداسازی باشند.

در حقیقت داده‌های بدون برچسب کمک می‌کند تا دانش اولیه درمورد توزیع داده‌ها کسب شود. به بیان دقیق‌تر، در صورتی استفاده از داده‌های بدون برچسب مفید واقع خواهد شد که دانش بدست آمده از داده‌های بدون برچسب درمورد توزیع داده‌ها، یعنی $P(x)$ حاوی اطلاعات مفیدی برای استنتاج در مورد $p(y|x)$ باشد. اگر این موضوع در یک مسئله خاص برقرار نباشد، روش نیمه‌نظارتی کمکی در بهبود تعمیم‌پذیری جداساز نخواهد داشت، حتی ممکن است داده‌های بدون برچسب با اطلاعات نادرستی که در مورد توزیع داده‌ها می‌دهند، موجب افزایش خطای جداسازی شوند. بر این اساس واضح است برای استفاده از روش‌های نیمه‌نظارتی، پیش‌فرض‌های بخصوصی باید برقرار باشد که این پیش‌فرض‌ها همان دانش پیشین هستند. همان طور که گفته شد استفاده از داده‌های بدون برچسب درحقیقت معادل با یادگیری توزیع داده‌ها است و هر فرآیند یادگیری برای همگرا شدن نیاز به یک دانش پیشین دارد [۴۵]. اما پیش فرض‌هایی که در یادگیری نیمه‌نظارتی باید وجود داشته باشند، شامل موارد زیر خواهد بود:

۱. **پیش‌فرض هموار**[1]: اگر دو نقطه x1 و x2 در یک منطقه با چگالی بالا نزدیک به هم باشند، برچسب‌های متناظر آن‌ها یعنی y1 و y2 هم باید به هم نزدیک باشند. به عبارت دیگر مرز تصمیم‌گیری مناطق کم تراکم، نقاط نزدیک به یکدیگر کمتری خواهد داشت و نقاط، دارای کلاس‌های متفاوتی خواهند بود.

[1] Smoothness assumption

۲. **پیش‌فرض خوشه**[1] : داده‌های موجود در یک خوشه احتمالا برچسب‌های مشابهی دارند.

۳. **پیش‌فرض خمینه**[2] : در فضای ورودی با بُعد بالا، داده‌ها روی یک خمینه تقریبا با بُعد پایین‌تری قرار دارند و تابع جداساز روی خمینه‌ی داده‌ها هموار است. در این وضعیت می‌توان با استفاده از داده‌های برچسب‌دار و بدون برچسب نسبت به یادگیری اقدام کرده و همزمان از چالش ابعاد زیاد[3] نیز جلوگیری نمود [۴۴].

۲-۷ یادگیری فعال

یادگیری فعال گونه‌ای از روش‌های یادگیری به شمار می‌آید که در آن الگوریتم یادگیری قادر به تعامل با کاربر، پرس‌وجو از وی و یا برخی منابع اطلاعاتی دیگر خواهد بود و برای دستیابی به نتایج مطلوب، بر اساس نقاط داده‌ای جدید اقدام به کار می‌کند. در ادبیات آماری گاهی اوقات این روش با نام طراحی تجربی مطلوب[4] نیز نامیده می‌شود. ایده‌ی کلیدی یادگیری فعال، این است که الگوریتم یادگیری ماشین می‌تواند همواره با مجموعه داده‌های کمتر، آموزش بهتری ببیند؛ البته در صورتی که مجاز به انتخاب داده‌های موردنظر خود به منظور یادگیری باشد [۴۶]. به عبارتی دیگر یادگیری فعال یک تکنیک یادگیری ماشین است که هدف آن دستیابی به دقت بیشتر با استفاده از نمونه‌های آموزشی کمتر خواهد بود. این نمونه‌ها به صورت فعال انتخاب شده و رده‌بند بر اساس آنها، آموزش و به روز رسانی می‌شود. در مقابل این راهکار، یادگیری غیرفعال[5] است که به طور تصادفی نسبت به انتخاب نمونه‌ها برای برچسب‌گذاری اقدام می‌کند؛ در صورتی که الگوریتم‌های فعال نمونه‌هایی با بیشترین ارزش اطلاعاتی را انتخاب می‌کنند (با توجه به تابع اندازه‌گیری و راهبرد فعال) و سپس برچسب آنها را از متخصص و یا رده‌بند درخواست می‌نماید [۴۷].

[1] Cluster assumption
[2] Manifold assumption
[3] Curse of dimensionality
[4] Desirable experimental design
[5] Passive learning

یک یادگیرنده فعال ممکن است که پرس‌وجوها را به طور معمول در قالب یک سری نمونه داده‌های بدون برچسب توسط یک شخص خبره (به عنوان مثال یک فرد آگاه انسانی) که با ماهیت مسئله آشنایی دارد، برچسب‌گذاری نماید. این نوع رویکرد در بسیاری از برنامه‌های یادگیری ماشین مدرن و برنامه‌های کاربردی داده‌کاوی به خوبی محقق می‌شود. در واقع جایی که داده‌های بدون برچسب ممکن است فراوان و یا به راحتی قابل دسترسی باشند، اما برچسب‌های آموزشی آنها دشوار، وقت‌گیر و گران است که در بسیاری از کاربردهای دنیای واقعی نیز، ما با چنین وضعیتی مواجه هستیم که داده‌ها دارای حجم بالایی هستند ولی برچسب کمیاب یا به دست آوردن آن گران است. بنابراین در چنین شرایطی یادگیری فعال می‌تواند موثر واقع شود. به عبارت دیگر در یادگیری فعال تلاش می‌گردد تا با انتخاب یک زیر مجموعه مهم و حیاتی برای برچسب زدن به این موضوع رسیدگی شود. در این راه، یادگیرنده فعال با هدف دستیابی به دقت بالا و کاهش هزینه‌ها با استفاده از چند نمونه برچسب ممکن، فرآیند یافتن برچسب داده‌ها را دنبال می‌کند که این طبقه‌بندی را می‌تواند با چند نمونه برچسب‌دار و از طریق پرس‌وجو، به جای یادگیری منفعل معمولی با عملکردی رضایت‌بخش به دست آورد [۱۱].

سه شیوه اصلی یادگیری فعال عبارتند از: ترکیب پرس‌وجوی عضویت[1]، نمونه‌برداری گزینشی مبتنی بر جریان[2] و نمونه‌برداری مبتنی بر استخر[3]. امروزه روش یادگیری فعال به طور گسترده در زمینه یادگیری ماشین مورد مطالعه قرار گرفته و در بسیاری از کاربردهای پردازش داده‌ها همانند طبقه‌بندی تصویر، شناسایی بیولوژیکی DNA، تشخیص خودکار گفتار و بازیابی چندرسانه ای استفاده می‌شود [۴۸].

[1] Membership Query Synthesis
[2] Stream Based Selective Sampling
[3] Pool Based Sampling

در ساختار یک فرآیند یادگیری فعال بخش‌های مختلفی در کنار هم مورد استفاده قرار می‌گیرند که از این بخش‌ها می‌توان به سناریوها[1] یا شیوه‌های یادگیری فعال، راهبردهای پرس‌وجو[2]، خبره مورد استفاده و تعداد مراحل اجرا الگوریتم نام برد [۱۱].

با توجه به ویژگی‌هایی بیان شده در خصوص این روش، به طور کلی یک مساله اساسی در الگوریتم‌های یادگیری تشخیص بدافزارها این است که برای رسیدن به دقت مطلوب، نیاز به نمونه‌های آموزشی فراوان داریم که این نیاز به صرف هزینه فراوان و به کارگیری نیروی انسانی متخصص جهت برچسب زدن نمونه ها دارد. به همین دلیل در این پژوهش از روش یادگیری فعال برای ساختن رده‌بندها استفاده شده است؛ به این معنی که ابتدا با تعداد کمی اسناد برچسب‌دار رده‌بندهای اولیه ساخته می شود و به جای برچسب زدن به کل اسناد در دسترس، ابتدا میزان مفید بودن اطلاعات آنها اندازه‌گیری می‌شود.

۲-۸ یادگیری فعال نیمه‌نظارتی

هر چند که راهبرد یادگیری فعال به تنهایی می‌تواند تا حد زیادی باعث کاهش زمان کار و تنزل هزینه‌های برچسب‌گذاری و همچنین منجر به بهبود عملکرد شود، اما با این وجود، برای برخی از شرایط که در آن حجم زیادی از تفسیر انسانی و پرسش از خبره وجود دارد، در عمل غیر قابل اجرا و یا اصلا نشدنی است؛ بنابراین احتمال رخداد چنین وضعیتی باید به حداقل برسد. با توجه به این که یادگیری نیمه‌نظارتی نیز به دنبال استفاده از داده‌های بدون برچسب در یک حالت کارآمد اما بدون مداخله‌ی چرخه‌ی انسانی است، بنابراین ترکیب این دو راهکار که با نام یادگیری فعال نیمه‌نظارتی معروف است، می‌تواند در چنین شرایطی موثر واقع شود. به این صورت که به جای برچسب‌گذاری تمام نمونه‌ها، ابتدا نمونه‌های مفیدی که ارزش اطلاعاتی بالایی دارند به کمک یادگیری فعال برچسب‌گذاری شده و سپس

[1] Scenario
[2] Query strategies

برچسب نمونه‌های دیگر نیز به صورت خودکار از طریق یادگیری نیمه‌نظارتی به مدل اضافه شده و در نهایت آموزش مجدد انجام پذیرد [۴۷].

به طور کلی یادگیری فعال نیمه‌نظارتی گونه‌ای از روش‌های یادگیری ماشین است که با هدفی واحد در دو جهت مختلف به یک مسئله یادگیری نگاه می‌کند. به این صورت که روش نیمه‌نظارتی آن به دنبال حدس زدن در خصوص داده‌های بدون برچسب از روی مدل ساخته شده و روش فعال به دنبال کشف جنبه‌های ناشناخته‌ی داده‌های بدون برچسب است تا موثرترین داده‌ها برای فرآیند برچسب‌گذاری انتخاب شوند. این روش در سیستم‌های امنیتی بیشتر به منظور یادگیری و به روز رسانی مدل آموزش دیده شده است که باید با حجم محدودی از داده‌های بر چسب خورده به انجام برسد. یادگیری فعال نیز همانطور که در بخش قبلی بیان شد، روشی است که در آن الگوریتم یادگیری قادر به تعامل با خبره یا کاربر، از طریق پرس‌وجو و یا برخی منابع اطلاعاتی دیگر خواهد بود و برای دستیابی به نتایج بهتر، بر اساس نقاط داده‌ای جدید اقدام به کار می‌کند [۱۲]. به عبارت دیگر یادگیری فعال نیمه‌نظارتی رویکردی است که از طریق ترکیب مشخصه‌های یادگیری این دو روش برای رده‌بندی داده‌ها اقدام به کار می‌کند و هدف اصلی آن، کاهش میزان داده‌های برچسب‌گذاری شده توسط انسان است. این روش به طور خاص، نمونه‌هایی را که رده‌بند نتوانسته به درستی رده‌بندی نماید؛ یعنی همان‌هایی که درجه‌ی اطمینان بالایی برای آنها وجود ندارد، توسط الگوریتم فعال تعیین و سپس توسط خبره برچسب‌گذاری می‌کند. در حالی که نمونه‌های باقی مانده یعنی آنهایی که بیشترین درجه‌ی اطمینان را داشتند، به طور خودکار توسط الگوریتم نیمه‌نظارتی برچسب‌گذاری می‌شوند. در نهایت، هر دو گروه از نمونه‌ها با هم ترکیب شده و مورد استفاده قرار می‌گیرند تا رده‌بند، مجدد فرآیند آموزش را از سر بگیرد [۴۷].

به طور کلی در روش یادگیری فعال نیمه نظارتی با دو دسته مجموعه داده مواجه خواهیم بود. به این صورت که ما به کمک نمونه‌های برچسب خورده اقدام به ساخت مدلی از رده‌بند خواهیم کرد و برای برخورد مناسب با نمونه‌های بدون برچسب اقدام به مقایسه نمونه‌ها با مدل‌های شکل گرفته خواهیم

داشت. اگر مدل شکل گرفته مربوط به کلاس خاصی باشد و الگوی نمونه‌های بدون برچسب شبیه به آنها باشد در نتیجه برچسب همان کلاس نیز، برای آن اعمال خواهد شد [۱۱].

این پژوهش نیز یک رویکرد فعال نیمه‌نظارتی را ارائه می‌دهد که در واقع ترکیبی بین روش خود آموز نیمه‌نظارتی و راهکار یادگیری فعال می‌باشد. به این صورت که در ابتدا نسبت به آموزش اولیه نمونه‌های برچسب‌دار اقدام شده و سپس از یک سو به کمک راهکار یادگیری فعال، از بین نمونه‌های بدون برچسب، نمونه‌هایی با ارزش اطلاعاتی بالاتر انتخاب شده و برای پرسش از خبره ارسال و سپس برچسب آنها اعلام می‌گردد. لازم به ذکر است که فرآیند تعامل با خبره به منظور بهبود کارایی تا جایی ادامه می‌یابد که رده‌بند به تنهایی نتوانسته برچسب نمونه‌های موثر انتخاب شده را با قطعیت پیش بینی نماید به همین دلیل برای پرسش از وی اقدام می‌کند. از سوی دیگر به کمک راهکار یادگیری نیمه‌نظارتی، نمونه‌هایی که برچسب آنها توسط خود رده‌بند به صورت قطعی پیش‌بینی می‌شوند نیز به مدل اضافه می‌گردد تا با ترکیب این نمونه‌های برچسب خورده با یکدیگر در نهایت برای به روز رسانی مدل فرا گرفته شده و آموزش مجدد اقدام شود.

۲-۹ بررسی پژوهش‌های انجام شده

تاکنون روش‌های مختلفی به منظور شناسایی بات‌نت‌ها ارائه شده است. استفاده از انواع رده‌بندهای مبتنی بر یادگیری ماشین به صورت با ناظر و بدون ناظر، استفاده از شبکه‌های عصبی، مباحث یادگیری عمیق[1]، یادگیری‌های نیمه‌نظارتی و فعال از جمله مهم‌ترین راهکارهای پیشنهادی در خصوص شناسایی بات‌نت‌ها می‌باشد که به عنوان رویکردهای نوین در این زمینه شناخته می‌شوند. از سوی دیگر یک چالش اساسی در سیستم‌های تشخیص بات‌نت، توانایی شناسایی بات‌نت‌های نوع جدید و تاکنون مشاهده نشده می‌باشد. از آنجایی که یادگیری ماشین قادر به توسعه‌ی الگوریتم‌ها و تکنیک‌های کاراتری

[1] Deep learning

برای مقابله و تشخیص درست باتنت‌های جدید بوده است، اخیرا از میان رویکردهای مختلف شناسایی، روش‌های مبتنی بر یادگیری ماشین بیشتر مورد توجه پژوهشگران واقع شده است.

به عنوان مثال یک تکنیک مبتنی بر یادگیری ماشین با ناظر برای شناسایی ترافیک باتنت توسط Stevanovic و همکاران ارائه شد که در آن زمینه‌ی واقعی برچسب نمونه‌ها در دسترس می‌باشد [۴۹]. به طور کلی در روش‌های با ناظر هر چند که نرخ تشخیص اعلام شده اغلب در سطح بالایی می‌باشد، اما همگی بر اساس این فرض ارائه شده‌اند که ما نسبت به زمینه‌ی واقعی داده‌ها حتی آنهایی که ناشناخته هستند، نیز اطلاع کامل داریم که این موضوع توسعه‌پذیری سیستم‌های تشخیص را با محدودیت همراه می‌کند و از سوی دیگر نیاز به بهبود بیشتر به منظور به کارگیری آنها در دنیای واقعی، همچنان احساس می‌شود و می‌بایست راهکارهای نوینی در این زمینه ارائه گردد.

همچنین یک روش یادگیری بدون ناظر توسط Qiu و همکاران به کمک ترافیکی از بات‌های ناشناخته برای آموزش اولیه به کار گرفته شد [۵۰]. آنها با توسعه‌ی راهکار تشخیص ناهنجاری گروهی[1] و خوشه‌بندی نسبت به شناسایی نمونه‌های ناهنجار و انتخاب زیر مجموعه‌ای از ویژگی‌های موثر در تولید خوشه‌های ناهنجار اقدام کردند که نتایج آنها با درصد کمی از باتنت‌های ناشناخته همراه بوده است.

یک سیستم تشخیص ناهنجاری بر پایه یادگیری بدون ناظر توسط Dromard و همکاران ارائه شد [۲۰]. به طور کلی سیستم‌های تشخیص نفوذ دارای پایگاه داده‌ای هستند که الگوهایی از ترافیک حمله در آن نگهداری می‌شود؛ اما با توجه به اینکه این گونه از پایگاه‌های داده مدام در حال به روز رسانی از طریق منابع مختلف جریان داده‌ای هستند، پس نیاز به راهکاری به منظور رفع آن خواهند بود که نویسندگان برای حل این مشکل، یک روش بلادرنگ بدون ناظر ارائه می‌دهند. سیستم پیشنهادی به نام ORUNADA بر پایه‌ی یک پنجره‌ی زمانی گسسته و پویا عمل می‌کند. این پنجره وظیفه‌ی به روز رسانی پیوسته در فضای ویژگی‌ها را به کمک یک روند خوشه‌بندی شبکه‌ای افزایشی[2] به منظور تشخیص

[1] Group anomaly detection (GAD)
[2] Incremental grid clustering

سریع ناهنجاری‌ها بر عهده خواهد داشت. کاربرد در سیستم‌های تشخیص نفوذ برخط و ارائه‌ی راه‌حلی به منظور بهبود کارایی در تشخیص حملات از جمله اهدافی است که توسط نویسندگان دنبال شده است اما در مقابل کاهش سرعت اجرا در هنگام افزایش تعداد جریان‌ها و همچنین عدم استفاده از مجموعه داده‌ی جامعی که دارای گونه‌های جدیدی از حملات باشد، از جمله ضعف‌های راهکار پیشنهادی بوده است.

نتایج حاصل از بررسی روش‌های مختلف یادگیری ماشین و داده‌کاوی به منظور رده‌بندی ترافیک شبکه با هدف کشف حملات و ناهنجاری‌ها در یک سیستم تشخیص نفوذ توسط Nadiammai و Hemalatha به کار گرفته شد [۵۱]. مقایسه میزان پیچیدگی و زمان اجرای الگوریتم‌های مختلف و دست‌یابی به مجموعه داده برچسب‌دار اولیه با هدف کاهش هزینه‌ها از جمله مهم‌ترین اهداف نویسندگان در این مرجع بوده است. به طور کلی آنها چهار موضوع رده‌بندی داده‌ها، سطح بالای تعامل با انسان، نقصان داده‌های برچسب خورده و شناسایی حملات ممانعت از سرویس‌دهی، جزء محورهای تحت پوشش رویکرد پیشنهادی آنها می‌باشد. در این مرجع یک روش نیمه‌نظارتی به کمک مدل‌های ترکیبی تشخیص نفوذ ارائه می‌شود که علاوه بر رفع چهار موضوع مطرح شده، توانسته نرخ هشدار نادرست را کاهش دهد اما از سوی دیگر کاهش کارایی سیستم و فقدان منابع اطلاعاتی مناسب لازم برای استفاده در سیستم‌های تشخیص نفود برخط را در پی داشته است.

روشی به منظور رده‌بندی جریان‌های داده‌ای ترافیک شبکه به کمک یادگیری نیمه‌نظارتی توسط Noorbehbahani و همکاران ارائه شد [۴۱]. از آنجایی که افزایش استفاده از رایانه‌ها و اینترنت، لزوم جلوگیری از خرابکاری و نفوذ توسط بدافزارها را برای تمامی رسانه‌ها بیش از پیش آشکار ساخته است؛ از این رو نفوذ به عنوان یک کلید اساسی در حل و فصل میزان دسترس‌پذیری، صحت و اعتبار منابع رایانه‌ای به شمار می‌رود. در تشخیص نفوذ، مهم‌ترین محدودیت‌ها شامل توزیع نامتعادل کلاس‌ها، کمبود داده‌های برچسب‌گذاری شده و مقادیر زیادی از جریان‌های ترافیکی شبکه می‌باشد. علاوه بر این، به

دلیل ماهیت پویای جریان‌های شبکه‌ای، استفاده از مدل‌های آماری ایستا، عملکرد سیستم را در طول زمان به طور قابل توجه‌ای کاهش می‌دهد. در این مرجع، یک روش رده‌بندی جدید مبتنی بر جریان‌های داده‌ای به صورت نیمه‌نظارتی برای تشخیص نفوذ پیشنهاد شده است که می تواند با استفاده از اطلاعات یک سری داده‌های برچسب خورده، به روز رسانی افزایشی داشته باشد. در واقع آنها از یادگیری مبتنی بر نمونه استفاده می‌کنند که به صورت بُرون‌خط در طول مدت زمانی که مجموعه داده جدید در دسترس است، اقدام به روزرسانی می‌کند. اما از جمله مشکلات سیستم پیشنهادی، می‌توان به افزایش هزینه‌های برچسب‌گذاری و عدم انتخاب نمونه‌های مناسب اشاره نمود.

ارائه یک مجموعه داده باتنت جامع توسط Beigi و همکاران صورت پذیرفت [۱۵]، که در آن ویژگی‌هایی در جهت شناسایی باتنت انتخاب شدند که وابستگی زیادی به انواع محدود و مشخصی از باتنت‌ها نداشتند و تا حد زیادی قابل تعمیم به گونه‌های مختلف موجود در آن بودند. نویسندگان به منظور ارزیابی مجموعه داده خود از یک رویکرد یادگیری با ناظر به کمک درخت تصمیم C.45 بهره بردند و نرخ تشخیص قابل قبولی را بدست آوردند و نشان دادند که وجود یک مجموعه داده‌ی جامع به منظور ارزیابی سیستم باتنت بسیار تاثیر گذار است. با این حال رویکرد آنها به علت عدم آموزش در محیط پویا و کاربردهای دنیای واقعی نمی‌تواند چندان قابل اتکا باشد.

یک رویکرد مبتنی بر یادگیری فعال با هدف اصلاح مشکلات کنونی در سیستم‌های تشخیص نفوذ توسط Menahem و همکاران مورد استفاده قرار گرفت [۵۲]. در این سیستم از طریق انجام یک فرآیند به روز رسانی فعال سعی در کاهش هزینه‌های برچسب‌گذاری جریان‌های ترافیکی شبکه شد، اما به دلیل عدم استفاده از ترافیک واقعی شبکه و مجموعه داده‌ی جامع، نتایج قابل اطمینانی را به همراه نداشت.

از سوی دیگر Qiu و همکاران نیز به منظور یافتن برچسب تعداد محدودی از نمونه‌های حمله که دارای ارزش اطلاعاتی بالایی بودند از یک رویکرد مبتنی بر آنتروپی تحت یک چارچوب یادگیری فعال و آموزش نیمه‌نظارتی استفاده کردند [۴۶]. آنها به کمک این رویکرد و بهره‌گیری از فرآیندهای پرس‌وجو

نسبت به انتخاب نمونه‌های موثر و سپس تمیز دادن جریان‌های سالم از حمله و برچسب‌گذاری کل نمونه‌های ناشناخته اقدام کردند که در نهایت با کمبود تنوع حملات، به خصوص تشخیص بات‌نت‌های جدید همراه گشت.

همچنین Zhu و همکاران نیز یک روش راهبرد یادگیری فعال نیمه‌نظارتی برای اجرای در مجموعه جویبار داده‌ها پیشنهاد کردند [۵۳]. راهبرد آنها مبتنی بر یک روش رده‌بندی وزن‌دار گروهی و با هدف کاهش واریانس انجام پذیرفت. از آن جایی محققان نشان داده‌اند که با کاهش میزان واریانس هر رده‌بند گروهی، میزان خطای کلی آنها نیز کاهش می‌یابد. بنابراین، در این مرجع یک اصل به نام واریانس حداقلی معرفی شد، به گونه‌ای که تنها برچسب نمونه‌هایی که دارای واریانس گروهی بالایی هستند، از خبره پرسش می‌شود. با این حال کاهش کارایی سیستم در قبال حملات جدید از جمله مشکلات سیستمی پیشنهادی توسط آنها می‌باشد.

آقای Qiu و همکاران در مقاله‌ی دیگری یک رویکرد مبتنی بر یادگیری فعال نیمه‌نظارتی را ارائه دادند که در آن برچسب نمونه‌ها طی یک سناریوی مبتنی بر استخر از مدیر شبکه پرسش می‌شود و به کمک گونه‌ای از رده‌بند رگرسیون لجستیک نسبت به رده‌بندی جریان‌های بات و سالم اقدام می‌نماید [۱۱]. عدم کارایی در مقابله با بات‌نت‌های گونه‌ی جدید و عدم توانایی در کاربردهای واقعی از جمله مشکلات راهکار آنها می‌باشد.

حال به منظور آنکه بتوانیم مقایسه‌ی جامعی بین پژوهش‌های انجام شده در این حیطه داشته باشیم، در جدول ۲-۱ خلاصه‌ای از روش‌های مختلف به همراه شرح و معایب هر یک از آنها ارائه شده است.

جدول ۲-۱. خلاصه‌ای از پژوهش‌های انجام شده

روش	شرح مختصر	معایب
۱- رویکرد مبتنی بر یادگیری با ناظر	یک رویکرد با ناظر با استفاده از الگوریتم‌های ماشین بردار پشتیبان خطی و بیز ساده به کار برده شده است. هدف اصلی این مرجع مقایسه چهار عامل تاثیرگذار در شناسایی بات‌نت یعنی تعمیم‌پذیری، توانایی پنهان ماندن، نرخ تشخیص بالا و استحکام، بر روی الگوریتم‌های مختلف یادگیری ماشین بوده است [۴۹].	ایجاد محدودیت در توسعه‌پذیری سیستم‌های تشخیص و عدم کارایی در کاربردهای واقعی
۲- رویکرد مبتنی بر یادگیری بدون ناظر	به کمک توسعه‌ی روش تشخیص ناهنجاری گروه، زیر مجموعه‌ای از ویژگی‌های موثر با ابعاد کم را انتخاب کرده و سپس نسبت به خوشه‌بندی اقدام می‌کند تا ناهنجاری‌های موجود در ترافیک شبکه را مورد بررسی قرار دهد [۵۰].	دارای نرخ پایین تشخیص در مواجه با نمونه بات‌نت‌های جدید
۳- ارائه‌ی یک سیستم تشخیص نفوذ مبتنی بر یادگیری بدون ناظر به نام ORUNADA	یک روش بلادرنگ بدون ناظر بر پایه‌ی یک پنجره‌ی زمانی گسسته و پویا ارائه می‌شود. این پنجره وظیفه‌ی به روز رسانی پیوسته در فضای ویژگی‌ها و خوشه‌بندی افزایشی را به منظور تشخیص سریع ناهنجاری‌ها بر عهده خواهد داشت [۲۰].	کاهش عملکرد سیستم و افزایش زمان اجرا و عدم بهره‌مندی از مجموعه داده جامع
۴- ارائه‌ی روشی مبتنی بر یادگیری نیمه‌نظارتی برای تشخیص نفوذ	یک روش نیمه‌نظارتی به کمک مدل‌های ترکیبی تشخیص نفوذ ارائه شده است که توانسته رده‌بندی داده‌ها، سطح بالای تعامل با انسان، نقصان داده‌های برچسب خورده و شناسایی حملات ممانعت از سرویس‌دهی را پوشش و از سوی دیگر نرخ هشدار نادرست را کاهش دهد [۵۱].	کاهش عملکرد و کارایی سیستم و فقدان منابع اطلاعاتی لازم در کاربردهای برخط
۵- ارائه یک سیستم	یک روش رده‌بندی جدید مبتنی بر جریان‌های داده‌ای به صورت نیمه نظارتی برای تشخیص نفوذ پیشنهاد شده	افزایش هزینه‌های برچسب‌گذاری و عدم

تشخیص نفوذ مبتنی بر یادگیری نیمه‌نظارتی افزایشی به نام ISF-NIDS	است که می‌تواند با استفاده از اطلاعات یک سری داده‌های برچسب خورده، آموزش ببیند و سپس به کمک یادگیری مبتنی بر نمونه به صورت بُرون‌خط در طول مدت زمانی که مجموعه داده جدید در دسترس است، اقدام به روزرسانی نماید [۴۱].	انتخاب نمونه‌های مناسب
۶- یافتن مجموعه ویژگی‌های موثر و رویکرد مبتنی یادگیری با ناظر	چهار معیار مهم در انتخاب ویژگی‌ها به منظور تشخیص بات‌نت‌ها ارائه شده است. این چهار معیار بر اساس مشخصه‌های مبتنی بر زمان، بسته، بایت و رفتار هر جریان ترافیکی در نظر گرفته می‌شوند و سپس طی روند یادگیری مبتنی بر درخت تصمیم C.45 آموزش داده می‌شوند [۱۵].	کاهش عملکرد سیستم در کاربردهای واقعی
۷-ارائه روشی مبتنی بر یادگیری فعال	به کمک یادگیری فعال سعی در کاهش هزینه‌های برچسب‌گذاری نمونه‌ها در شناسایی حملات شده است [۵۲].	عدم بهره‌مندی از داده‌های بدست آمده از ترافیک واقعی شبکه
۸-رویکردی مبتنی بر یادگیری فعال نیمه‌نظارتی	کاهش هزینه‌های برچسب‌گذاری نمونه‌ها و رده‌بندی آنها به کمک رویکردهای یادگیری فعال نیمه‌نظارتی با هدف شناسایی حملات و جریان‌های سالم از یکدیگر [۴۴].	کمبود تنوع حملات به خصوص تشخیص بات‌نت‌های جدید
۹- رویکردی مبتنی بر یادگیری فعال برای اجرا در جویبار داده	راهبردی مبتنی بر یک روش رده‌بندی وزن‌دار گروهی و با هدف کاهش واریانس بین رده‌بندها انجام شده است. در واقع هدف اصلی این راهکار ارائه‌ی راهبرد پرس‌وجو مبتنی بر کاهش واریانس می‌باشد تا به کمک آن نمونه‌هایی با ارزش اطلاعاتی بالاتر برای پرسش از خبره مورد استفاده قرار گیرند [۵۳].	کاهش تعمیم‌پذیری سیستم در شناخت حملات جدید

۱۰- رویکرد مبتنی بر یادگیری فعال نیمه‌نظارتی	برچسب نمونه‌ها طی یک سناریوی مبتنی بر استخر از مدیر شبکه پرسش می‌شود و به کمک گونه‌ای از رده‌بند لجستیک نسبت به رده‌بندی جریان‌های بات و سالم اقدام می‌نماید [۱۱].	عدم کارایی در مقابله با بات‌نت‌های گونه‌ی جدید و در کاربردهای مبتنی بر ترافیک واقعی شبکه

بنابراین در این پژوهش با در نظر گرفتن چالش‌های مطرح شده و بررسی مراجع مختلف این حیطه، یک رده‌بند فعال نیمه‌نظارتی برای تشخیص بات‌نت‌ها طراحی می‌شود. از آنجایی که مطالعات اخیر نشان داده‌اند که ویژگی‌های مبتنی بر جریان در سیستم‌های تشخیص بات‌نت و نیز رده‌بندی ترافیک، کارایی بهتری را نسبت به سایر ویژگی‌ها به ارمغان می‌آورند [۱۱]، در این پژوهش نیز از این نوع ویژگی‌ها استفاده شده است. در واقع سیستم طراحی شده با استفاده از مجموعه ویژگی‌هایی که توانایی رویارویی و تشخیص ترافیک‌های رمزگذاری شده را دارد اقدام به فعالیت می‌نماید و به دلیل اینکه ویژگی‌های مبتنی بر جریان، محتوای درون بسته‌ها را مورد تحلیل قرار نمی‌دهند و فقط از قسمت سرآیند استفاده می‌کنند، به کارگیری این ویژگی‌ها میزان نفوذ به حریم محرمانه‌ی اطلاعات بسته‌ها را کاهش داده و هزینه‌های محاسباتی کمتری نیز به دنبال خواهند داشت. همچنین از سوی دیگر، استفاده از ویژگی‌های موثر با تعداد محدود در ساخت مجموعه ویژگی با هدف کاهش محاسبات و پیچیدگی‌های مسئله نیز از دیگر نکات تاثیرگذاری است که در این پایان‌نامه به آن توجه شده است. بهره‌مندی از یک مجموعه داده جامع با گونه‌های مختلفی از بات‌نت که از بستر اینترنت بدست آمده‌اند و در نهایت استفاده از روش یادگیری فعال نیمه‌نظارتی با هدف کاهش هزینه‌های برچسب‌گذاری و آموزش مجدد، از دیگر نکات مورد توجه ما می‌باشد. به طور کلی در این پایان‌نامه سعی در جهت افزایش نرخ تشخیص، کارایی، اعتبار ارزیابی سیستم و همچنین پاسخ‌گویی مناسب به ماهیت پویای ترافیک شبکه شده است.

فصل ۳ : روش پیشنهادی برای تشخیص بدافزار

۳-۱ ساز و کار سیستم تشخیص

با توجه به کمبود نمونه‌های برچسب خورده در کاربردهای دنیای واقعی، ماهیت پویای ترافیک شبکه و همچنین افزایش تنوع بات‌نت‌ها در سال‌های اخیر، ضرورت ایجاد سیستم‌های تشخیص بات‌نتی که بتوانند به صورت کارا عملیات یادگیری و شناسایی را انجام دهند، بیش از پیش احساس می‌شود. بنابراین در این پژوهش به منظور رسیدگی به این موضوعات یک سیستم تشخیص بات‌نت با استفاده از رویکرد یادگیری فعال نیمه‌نظارتی ارائه شده است. در واقع روند یادگیری در این روش به صورت تعاملی و خودفراگیر است و سیستم پس از برچسب‌گذاری نمونه‌های مناسب، رده‌بندهای پایه‌ی خود را به روز رسانی می‌کند و فرآیند آموزش مجددا آغاز می‌شود. الگوریتم پایه در این سیستم، الگوریتم گروهی و با استفاده از فرآیند رای‌گیری بین رده‌بندهای رگرسیون لجستیک، بیز ساده و ماشین بردار پشتیبان خطی صورت می‌پذیرد. بر اساس ساختار سیستم، رده‌بند مورد استفاده می‌بایست قابلیت اجرای یک روند افزایشی را به منظور به روزسانی مدل‌های خود داشته باشد و در هر لحظه با اضافه شدن نمونه‌ی جدید، آموزش مجدد ببیند.

از آنجایی هزینه‌های برچسب‌گذاری داده‌ها در روش‌های یادگیری با ناظر بسیار زیاد است، الگوریتم مورد استفاده در این سیستم در جهت رفع این چالش حرکت می‌کند و به صورت فعال نیمه‌نظارتی، تنها نمونه‌هایی با ارزش اطلاعاتی مناسب را برای تعیین برچسب انتخاب و به مدل ساخته شده، اضافه می‌نماید. به طور کلی در این سیستم، از یک سو خبره به کمک یادگیری فعال، برچسب این نمونه‌های انتخابی را تعیین می‌کند و از سوی دیگر به کمک یادگیری نیمه‌نظارتی نمونه‌هایی که برچسب آنها توسط خود رده‌بند تعیین می‌شوند نیز به مدل اضافه می‌گردد تا مدل مفروض از گرایش یافتن به نمونه‌هایی که فقط خبره آنها را انتخاب می‌کند (نمونه‌های کمیاب)، محفوظ بماند. در نهایت با ترکیب نمونه‌های برچسب خورده انتخابی با یکدیگر، نسبت به اجرای فرآیند به روز رسانی و آموزش مجدد، اقدام می‌شود. این الگوریتم برخلاف رویکردهای یادگیری با ناظر، به گونه‌ای می‌باشد که می‌تواند در

سیستم‌های تشخیص برخط نیز مورد استفاده قرار گیرد. بنابراین با توجه به نیاز مبرم سیستم‌های تشخیص به بلادرنگ بودن، این سیستم بر پایه‌ی یادگیری فعال نیمه‌نظارتی و به روز رسانی افزایشی می‌تواند نسبت به این موضوع پاسخ‌گو باشد و بدین صورت یکی از مهم‌ترین چالش‌های حال حاضر در این سیستم‌ها را رفع نماید.

از سوی دیگر استفاده از مجموعه داده‌ی جامعی که دارای بات‌نت‌های گونه‌ی جدید باشد، از دیگر نیازهای سیستم‌های تشخیص مبتنی بر جریان است تا بتوانند بر اساس آن قابلیت توسعه‌پذیری و کارایی مناسبی را از خود نشان دهند. همچنین در این مجموعه داده لازم است که داده‌های آموزشی و داده‌هایی که در جهت ارزیابی در نظر گرفته شده‌اند، تا حد امکان با هم، همپوشانی نداشته باشند. از این رو سیستم تشخیص بات‌نتی که تولید می‌شود لازم است که بر پایه‌ی یک مجموعه داده مبتنی بر ترافیک واقعی شبکه طراحی و توسعه داده شده باشد. بنابراین در این پژوهش از یک مجموعه داده‌ی جامع با بات‌نت‌های متنوع و با حداقل هم‌پوشانی استفاده شده است تا بتواند تضمین کننده‌ی خوبی برای این موضوع باشد. به عبارت دیگر این سیستم برای افزایش تعمیم‌پذیری از مجموعه داده‌هایی با بات‌نت‌های جدید استفاده می‌نماید که پاسخ مناسبی به ماهیت ترافیک شبکه داده باشد.

ما در ادامه نحوه‌ی ساخت مجموعه ویژگی‌ها که بر اساس مشخصه‌های جریان‌های ترافیکی بدست می‌آیند، را شرح می‌دهیم. مجموعه ویژگی پایه در این پژوهش بر اساس مدل ارائه شده توسط Qiu و همکاران [۱۱] پیاده‌سازی شده است که در آن به کمک دو ویژگی اندازه و جهت ارسال بسته‌ها نسبت به رده‌بندی و آموزش سیستم اقدام می‌شود. سایر مجموعه ویژگی‌ها نیز به منظور مقایسه و آزمایش استخراج شده‌اند. لازم به ذکر است که فرآیند ساخت مجموعه ویژگی‌ها به کمک مجموعه داده بات‌نت ISCX دانشگاه UNB کانادا صورت پذیرفته است که در حال حاضر جزء کامل‌ترین مجموعه داده‌ها از نظر تنوع بات‌نت می‌باشد. ما پس از معرفی مجموعه ویژگی‌ها، شمای کلی سیستم طراحی شده و فرآیند یادگیری فعال نیمه‌نظارتی به همراه جزییات کاری آن را ارائه خواهیم داد. به طور کلی راهکار پیشنهادی

این پژوهش، به عنوان یکی از نخستین روش‌های مبتنی بر یادگیری فعال‌نیمه‌نظارتی در بحث سیستم‌های تشخیص باتنت به شمار می‌آید.

۳-۲ مجموعه ویژگی‌ها

به طور کلی در مطالعات اخیر، نشان داده شده است که همواره انتخاب ویژگی‌ها و انجام مراحل پیش‌پردازشی به منظور آموزش در سیستم‌های تشخیص باتنت و نیز رده‌بندی ترافیک شبکه، نقش به‌سزایی را در کارایی و کاهش پیچیدگی‌های زمانی ایفا می‌کند. همچنین طراحی این مجموعه ویژگی می‌تواند در بی اثر کردن برخی از خصوصیات باتنت‌ها نیز موثر واقع شود [۱۱].

بنابراین با توجه به نقش مهم ویژگی‌ها در سیستم‌های تشخیص باتنت، می‌توان به کمک رویکردهای مختلفی، نسبت به ساخت بردارهای ویژگی از روی جریان‌های ترافیکی شبکه، مبادرت ورزید. در این پژوهش، پنج مجموعه ویژگی مختلف ارائه می‌شود که در ادامه به معرفی آنها خواهیم پرداخت.

۳-۲-۱ مجموعه ویژگی اول (پایه-Qiu2017)

در این مجموعه ویژگی که ما نام آن را Qiu2017 یا پایه می‌نامیم، نویسندگان به کمک رویکرد نوینی نسبت به محاسبه و ساخت بردارهای ویژگی حاصل از جریان‌های ترافیکی مختلف اقدام می‌کنند [۱۱]. همانطور که پیش‌تر نیز بیان شد، این مجموعه ویژگی، به عنوان مجموعه ویژگی پایه در این پژوهش مورد استفاده قرار می‌گیرد و آزمایشات و نتایج حاصل از آن به منظور به کارگیری در سیستم تشخیص باتنت پیشنهادی به کار گرفته می‌شود. ما در ادامه توضیحات روند پیاده‌سازی و مراحل ساخت این مجموعه ویژگی و در پایان روش پیشنهادی خود، به منظور ساخت بردارهای ویژگی مبتنی بر آن و در نهایت مجموعه ویژگی نهایی را شرح خواهیم داد.

به طور کلی از آنجایی که اکثر حجم ترافیک شبکه را جریان‌های TCP با طولی بزرگ‌تر از ۱۰ تشکیل می‌دهند و از سوی دیگر پورت مقصد برای تمایز جریان‌های سالم از حمله، بر روی ۸۰ قرار گرفته است. در این مجموعه ویژگی نیز به منظور استخراج و ساخت بردارهای ویژگی، در ابتدا نسبت به انتخاب و تولید جریان‌هایی با پورت مقصد ۸۰ و اندازه‌ی بزرگ‌تر از ۱۰ اقدام می‌شود. همانطور که مشهود است، جریان‌های مبتنی بر پروتکل TCP از طریق ارسال یک سری بسته‌های خاص شروع به کار می‌کنند که به این مراحل در مفاهیم شبکه، عملیات دست‌تکانی سه مرحله‌ای[1] گفته می‌شود. بنابراین در این مجموعه ویژگی پس از انتخاب جریان‌های مذکور، نسبت به انتخاب ۱۰ بسته‌ی اول ارسالی هر جریان پس از عملیات دست‌تکانی اقدام می‌شود.

با انتخاب این جریان‌های خاص، در ادامه برای تعیین اندازه و وضعیت ارسال هر بسته از طریق آدرس منبع و مقصد، سعی در بازنمایی جهت ارسال آنها می‌گردد. به عبارتی دیگر از هر ۱۰ بسته‌ی نخست هر جریان، دو ویژگی جهت ارسال و اندازه‌ی بسته‌ها استخراج می‌گردد. حال از آنجایی که جهت ارسال یک ویژگی رسته‌ای[2] و اندازه یک ویژگی عددی پیوسته[3] است، برای آنکه بتوان ویژگی رسته‌ای را به عددی تبدیل کرد از یک روش بازنمایی خاص بهره می‌گیرد. این روش بازنمایی به این صورت است که برای جهت ارسال جریان‌های ترافیکی موجود، فرض می‌نماید که بین مشتری به سرور (CS) و سرور به مشتری (SC) متناوب باشد. بنابراین برای هر جریان CS و SC اندازه بسته را در نظر گرفته و برای بسته‌هایی پشت سرهم که به صورت CC یا SS ارسال می‌شوند، یک بسته با اندازه صفر وارد فضای ویژگی‌ها می‌کند تا نشان دهنده‌ی عدم وجود بسته در جهت عکس آن باشد. بنابراین با در نظر گرفتن بازنمایی بسته‌ها، بردار ویژگی با ابعاد 2N بر روی هر N بسته‌ی نخست جریان‌های منتخب اعمال می‌گردد. به عنوان مثال در جدول ۳-۱ سه حالت از فرآیندهای ارسالی به همراه نحوه‌ی بازنمایی بردارهای ویژگی نشان داده شده است. در این مثال، تعداد بسته‌ها (N) چهار و ابعاد (D) هشت است،

[1] Three-way handshake
[2] Categorical
[3] Continuous numerical

C_i نشان‌دهنده‌ی اندازه‌ی بسته‌ی i ام از سمت مشتری به سرور و بلعکس S_i نمایانگر اندازه‌ی بسته‌ی i ام از سمت سرور به مشتری می‌باشد.

جدول ۳-۱. بازنمایی مجموعه ویژگی‌های پایه(Qiu2017)

ترتیب بسته‌های هر جریان	بازنمایی ویژگی‌ها							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
$C_1S_1C_2S_2$	C_1	S_1	C_2	S_2	0	0	0	0
$C_1C_2S_1S_2$	C_1	0	C_2	S_1	0	S_2	0	0
$S_1S_2S_3S_4$	0	S_1	0	S_2	0	S_3	0	S_4

به طور کلی این بازنویسی 2N بُعدی اندازه بسته‌ها، سبب حفظ اطلاعات جریان‌های TCP دو جهته به منظور تشخیص بات‌نت و ترافیک معمولی شبکه از هم خواهد شد. در این مجموعه ویژگی از آنجایی که ۱۰ بسته‌ی نخست هر جریان انتخاب می‌گردد، پس ابعاد ویژگی‌ها ۲۰ در نظر گرفته می‌شود. حال با اجرای این فرآیند بر روی هر جریان ورودی، مجموعه ویژگی مطلوبی استخراج می‌شود که ما نام آن را داده‌های خام[1] می‌نامیم. لازم به ذکر است که این مجموعه ویژگی برای استفاده در سیستم تشخیص بات‌نت پیشنهادی به کار برده می‌شود. اما از سوی دیگر همانطور که اشاره شد، از آنجایی که اندازه بسته‌ها و جهت ارسال آنها، می‌تواند در شناسایی ترافیک بات مفید باشد؛ بنابراین مجموعه‌ای از امتیازات ناهنجاری[2] نیز برای اندازه‌گیری در چنین شرایطی تعریف می‌شود که در ادامه به نحوه‌ی تولید این مجموعه ویژگی می‌پردازیم.

در این مرحله بردارهای ویژگی D بُعدی یا هر سطر از مجموعه داده‌های خام به تابعی به نام I (اگر I(x)>0 برابر یک، در غیر این صورت صفر) اعمال می‌گردد تا مقادیر بسته‌های متوالی هر جریان به صورت بردارهای ویژگی دودویی تغییر وضعیت دهد.

[1] Raw-data
[2] Anomaly scores

در واقع اگر بردار ویژگی D بُعدی به صورت $x = (x_1, x_2, x_3, \dots x_D)^T$ در نظر گرفته شود، آنگاه تابع I به صورت $I(x) = (I(x_1), I(x_2), I(x_3), \dots I(x_D))^T$ بر روی هر ویژگی اعمال خواهد شد. به عنوان مثال در جدول ۳-۱ برای ورودی اول، بردار ویژگی آن به صورت ۱۱۱۱۰۰۰۰ تبدیل می‌شود.

حال در مرحله‌ی بعد، به منظور کاهش تعداد پارامترهای مورد نیاز در مدل‌سازی توزیع مشترک[1] برای تابع I، مدل مفروض به یک شبکه بیزی[2] اعمال می‌گردد که در آن با محاسبه‌ی درست‌نمایی بیشینه بر روی مدل ساخته شده، احتمال بسته‌های تکی و همچنین جفت شده‌ی شرطی، از طریق شمارش تکرار نمونه‌ها بدست آورده می‌شود. بنابراین احتمال تابع I به صورت (رابطه ۳-۱) محاسبه می‌شود.

$$P[I(x)] = P[I(x_{j1})]P[I(x_{j2})|I(x_{j1})] \dots P[I(x_{jD})|I(x_{jD-1})] \quad \text{(رابطه ۳-۱)}$$

که در آن j_1 نشان‌دهنده‌ی اندیس گره ریشه در شبکه بیزی آموزش دیده می‌باشد و در ادامه به منظور ساده‌نویسی به جای $I(x_j)$ از I_j استفاده می‌شود.

از سوی دیگر برای تخمین احتمالات و جلوگیری از صفر شدن آنها از روش هموارسازی لاپلاس[3] استفاده می‌شود. مثلا در جدول ۳-۱ احتمال ویژگی x_1 اگر کل جریان‌ها را سه در نظر بگیریم، مقدار $\frac{۲}{۳}$ و با اعمال روش هموارسازی لاپلاس برای تک ویژگی (صورت به اضافه یک و مخرج به اضافه دو) حاصل نهایی $\frac{۳}{۵}$ بدست می‌آید. لازم به ذکر است که همین وضعیت برای جفت ویژگی‌ها نیز اعمال می‌شود؛ البته با این تفاوت که روش هموارسازی لاپلاس از طریق اضافه شدن مقدار یک به صورت و مقدار چهار به مخرج انجام می‌پذیرد.

[1] Joint distribution
[2] Bayesian network
[3] Laplacian smoothing

در مرحله بعدی با استفاده از تک ویژگی و جفت ویژگی‌هایی بدست آمده که دارای مقادیر مثبت و مخالف صفر هستند، نسبت به مدل‌سازی داده‌ها به کمک مدل مخلوطی گوسی[1] اقدام می‌شود. لازم به ذکر است، برای جفت ویژگی‌های موجود که به صورت $Y = (X_i, X_j), 1 \leq i \neq j \leq D$ هستند، از یک مدل مخلوطی گوسی دو مقداره[2] استفاده می‌شود. در نهایت خروجی این مدل‌ها مقادیر ارزش- P [3]یا همان امتیاز ناهنجاری را ایجاد می‌کند که نمایانگر نحوه‌ی توزیع احتمالی کلاس‌های مختلف در بین جریان‌های ورودی می‌باشد؛ در واقع مدل GMM پارامترهای موجود در بین داده‌های درون یک جریان را شناسایی می‌کند و احتمال آن که یک بردار ویژگی دو بعدی یا تک بعدی، چقدر نسبت به پراکندگی و چگالی کل داده‌های موجود پرت هستند را بازگو می‌نماید. در نهایت با انجام مراحل بیان شده، بردارهای ویژگی مشتق شده (z) به صورت (رابطه ۳-۲) بدست می‌آید که در سیستم پیشنهادی به صورت بردارهای ویژگی برچسب‌دار (z_l) و بدون برچسب (z_u) در نظر گرفته می‌شود.

$$z = (P(I_{j1}), P(I_{jk}|I_{jk-1}), p_i(x_i), p_{ij}(y) \quad \forall\, i,j,k\,, 1 < k \leq D, 1 \leq i \leq j \leq D) \in (0,1]^{2D+\binom{D}{2}}$$

(رابطه ۳-۲)

که در آن $P(I_{j1})$ احتمال بدست آمده از گره ریشه در شبکه بیزی و$P(I_{jk}|I_{jk-1})$ احتمال گره k ام به ازای پدر آن گره می‌باشد؛ در واقع همانطور که می‌دانیم از آنجایی که در شبکه بیزی احتمال هر گره به ازای پدرانش محاسبه می‌گردد، در رابطه‌ی مذکور نیز به همین صورت در نظر گرفته شده است. همچنین $p_i(x_i)$ مقدار ارزش p، برای تک ویژگی‌ها و $p_{ij}(y)$ مقدار ارزش p برای جفت ویژگی‌ها می‌باشد که نحوه‌ی محاسبه‌ی آنها به ترتیب در (رابطه ۳-۳) و (رابطه ۳-۴) آورده شده است.

$$p_i(x_i) = \begin{cases} {p_i}^+(x_i) & I_i = 1 \\ 1 & otherwise \end{cases}$$

(رابطه ۳-۳)

[1] Gaussian mixture model (GMM)
[2] Bivariate Gaussian Mixture Model
[3] P-Value

$$p_{ij}(y) = \begin{cases} {p_{ij}}^{+}(y) & I_i = 1, I_j = 1 \\ 1 & otherwise \end{cases}$$ (رابطه ۳-۴)

که در این رابطه‌ها مقادیر ${p_i}^{+}(x_i)$ ، ارزش- p مبتنی بر مخلوط[1] برای تک ویژگی‌ها و ${p_{ij}}^{+}(y)$ مقدار ارزش - p مورد انتظار[2] برای جفت ویژگی‌ها می‌باشد که طریقه استخراج آنها در (رابطه ۳-۶) و (رابطه ۳-۷) آورده شده است. البته با فرض اینکه احتمال پیشین مولفه‌های چندگانه برای K_{ij} به صورت (رابطه ۳-۵) تعریف شده و $\alpha_k = (\mu_k, \sum_k)$ بیانگر میانگین و ماتریس کواریانس برای چگالی k ام باشد.

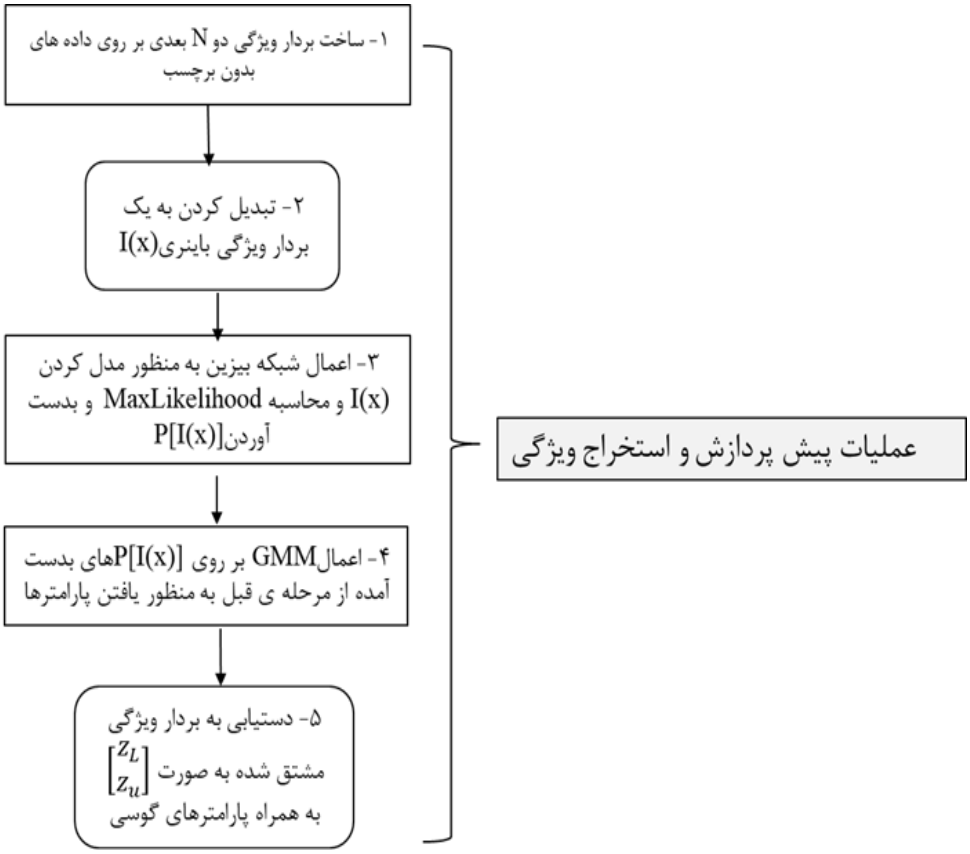
$$\{\alpha_k, k = 1 \dots K_{ij}\}, 0 \le \alpha_k \le k, \sum_{k=1}^{K_{ij}} \alpha_k = 1$$ (رابطه ۳-۵)

$${p_i}^{+}(x_i) = \frac{\alpha_k f(y|\theta_k)}{\sum_{m=1}^{k_{ij}} \alpha_m f(y, \theta_m)}$$ (رابطه ۳-۶)

$${p_{ij}}^{+}(x_i) = \frac{\alpha_k f(y|\theta_k)}{\sum_{m=1}^{k_{ij}} \alpha_m f(y, \theta_m)} e^{-r_k^2(y)/2}$$ (رابطه ۳-۷)

لازم به ذکر است که در روابط مفروض $f(y|\theta_k)$ همان تابع توزیع گوسی معروف و $r_k^2(y)$ مربع فاصله‌ی ماهالانوبیس[3] بین y و μ_k برای مولفه‌ی k ام مدل گوسی می‌باشد. خروجی این مجموعه ویژگی که ما نام آن را داده‌های امتیازی می‌نامیم، دارای ۲۳۰ ویژگی خواهد شد که ۴۰ ویژگی اول توسط شبکه بیزی و ۱۹۰ ویژگی بعدی توسط مدل‌های گوسی(GMM تکی و دو گانه) بدست می‌آید. فلوچارت ساخت بردارهای ویژگی در شکل ۳-۱ آورده شده است. در واقع با انتخاب دو ویژگی اندازه بسته و جهت ارسال و سپس انجام مراحل ذکر شده به مجموعه ویژگی ۲۳۰ بُعدی خواهیم رسید.

[1] Mixture-based p-values
[2] Expected p-value
[3] Mahalanobis distance



شکل ۳-۱. فلوچارت نحوه‌ی ساخت مجموعه ویژگی‌های پایه (Qiu2017)

حال به شرح تغییرات و نحوه‌ی استفاده از مجموعه ویژگی مفروض در سیستم پیشنهادی خود می‌پردازیم. همانطور که پیش‌تر عنوان شد؛ از آنجایی که فرآیندهای یادگیری نیمه‌نظارتی و فعال شامل دو دسته از نمونه‌ها یعنی برچسب‌دار و بدون برچسب هستند، لذا در ساخت مجموعه ویژگی‌ها برای استفاده در چنین سیستمی نیز باید این نکته رعایت گردد.

ما در طراحی سیستم خود ۱۰ درصد از کل نمونه‌ها یا همان بردارهای ویژگی (z) را به عنوان نمونه‌های برچسب‌دار اولیه و مابقی را به صورت بدون برچسب در نظر می‌گیریم. علت اصلی انتخاب درصد کمی از داده‌ها نیز، لحاظ کردن کمبود نمونه‌های برچسب‌دار در کاربردهای دنیای واقعی و از سوی دیگر ارزیابی کارایی با سیستم با تعداد محدودی از نمونه‌های آموزشی اولیه و رفع مشکلات سیستم‌های نظارتی می‌باشد. بنابراین در هنگام ساخت مجموعه ویژگی مفروض، در ابتدا تمامی مراحل ساخت مجموعه ویژگی داده‌های امتیازی را برای کل نمونه‌های برچسب‌دار اجرا کردیم و سپس برای

نمونه‌های بدون برچسب، عملیات محاسبه‌ی احتمالات و شمارش تکرار نمونه‌ها (مرحله سوم در شکل ۱-۳) را صرفا از روی پارامترهای بدست آمده از مجموعه داده‌های امتیازی به کار بردیم. به عنوان مثال اگر مجموعه اولیه برچسب‌دار دارای ۴۰۹۵ نمونه باشد و ما کل فرآیند پیش پردازشی را بر روی آنها اجرا کرده باشیم، حال به منظور ساخت بردار ویژگی ۴۰۹۶ که عضو نمونه‌های بدون برچسب است، لازم خواهد بود تا صرفا محاسبه‌ی احتمالات و ساخت بردار ویژگی ۲۳۰ بعدی، از روی همان نمونه‌های اولیه انجام پذیرد؛ البته با فرض اینکه نمی‌خواهیم هیچ نمونه‌ی جدیدی را به مجموعه برچسب‌دار اولیه اضافه کنیم. لازم به ذکر است که علت اصلی این کار تطابق رویکرد پیشنهادی با راهکار برخط در سیستم‌های تشخیص مبتنی بر یادگیری ماشین می‌باشد. چرا که هیچ‌گاه کل اطلاعات جریان‌های ترافیکی در پایگاه داده‌ها وجود ندارد، بلکه فرآیند از طریق آموزش با مجموعه محدودی از آنها انجام می‌پذیرد و سپس با مشاهده‌ی جریان‌های جدید، فرآیند استخراج ویژگی و ساخت بردار و در نهایت رده‌بندی و تشخیص صورت می‌گیرد. در فصل بعدی نتایج حاصل از پیاده‌سازی و اجرای این روش و همچنین مجموعه ویژگی‌های استخراج شده از آن بر روی یک مجموعه داده‌ی جامع در زمینه بات‌نت شرح داده می‌شود.

۳-۲-۲ مجموعه ویژگی دوم(ISCX2014)

به طور کلی ما به منظور ساخت سایر مجموعه ویژگی‌ها با توسعه‌ی ابزار CICFlowMeter [۵۴] نسبت به استخراج و محاسبه‌ی سایر ویژگی‌های ذکر شده در مقالات مختلف اقدام می‌کنیم.

مجموعه ویژگی دوم که نام آن را ISCX2014 می‌نامیم، شامل چهار ویژگی موثر در تشخیص بات‌نت می‌باشد که بر اساس معیارهای مبتنی بر زمان، مبتنی بر بسته، مبتنی بر رفتار و مبتنی بر بایت طی یک سری آزمایشات متوالی به کمک رده‌بند درخت تصمیم C.45 انتخاب می‌شوند. به طور کلی این

ویژگی‌ها وابستگی زیادی به انواع محدود و مشخصی از باتنت‌ها نداشته و تا حد زیادی قابل تعمیم به گونه‌های مختلف باتنت خواهند بود. مشخصات این مجموعه ویژگی در جدول ۳-۲ مشاهده می‌شود.

جدول ۳-۲. مجموعه ویژگی ISCX2014

نام ویژگی	توضیحات
Flow duration	طول مدت زمان جریان (μ_s)
IOPR	نسبت بین تعداد بسته‌های دریافتی بر تعداد بسته‌های ارسالی
APL	میانگین طول بسته‌ها
BS	میانگین بیت بر ثانیه بسته‌ها(سرعت بسته‌ها b/s)

۳-۲-۳ مجموعه ویژگی سوم (Milcom2015)

مجموعه ویژگی سوم Milcom2015 نام دارد [۵۵] که نویسندگان در آن برای ساخت این مجموعه ویژگی، تعداد ۱۰ ویژگی موثری که در تشخیص باتنت تاثیرگذار هستند را از بین ۲۴۸ ویژگی که در مقاله [۵۶] ارائه شده است، انتخاب کردند. ویژگی‌های مشتق شده، حاصل اعمال فیلتر مبتنی بر همبستگی[1] بین ویژگی‌ها بر روی مجموعه داده‌های مختلف بوده است که به عنوان مجموعه ویژگی‌های نهایی ارائه می‌شود. نام هر ویژگی به همراه توضیحات مرتبط با آن در جدول ۳-۳ نمایش داده شده است. لازم به ذکر است که منظور از بسته‌ها رو به جلو در واقع همان بسته‌هایی است که از سمت مشتری به سرور ارسال می‌شوند و بسته‌های رو به عقب به صورت بالعکس، از سمت سرور به مشتری در نظر گرفته می‌شود.

[1] Correlation-based filtering

جدول ۳-۳. مجموعه ویژگی Milcom2015

نام ویژگی	توضیحات
Flow duration	طول مدت زمان جریان (μ_s)
Cnt_data_pkt	تعداد کل بسته‌ها با حداقل یک بایت از محموله (رو به جلو[1])
Min_data_size	کمترین اندازه محموله مشاهده شده (رو به جلو)
Mean_Bytes	میانگین بایت داده‌های رو به عقب[2] (داده بر حسب بایت به تعداد کل بسته ها)
Int_data_Len	تعداد کل بایت‌های ارسالی قبل از مشاهده‌ی اولین بسته تصدیق (به صورت دو طرفه[3])
RTT samples	تعداد کل نمونه‌های RTT یافت شده در کل بسته‌ها (رو به جلو)
Med_Bytes	میانه طول بایت بسته‌ها (رو به جلو)
Var_Bytes	واریانس طول بایت بسته‌ها (رو به عقب)
IP_ratio	نسبت بین بزرگ‌ترین اندازه بسته به کوچکترین اندازه بسته(دو طرفه)
Goodput	حاصل تقسیم تعداد کل بایت‌های فریم به مدت زمان جریان(دو طرفه)

۳-۲-۴ مجموعه ویژگی چهارم (Li2009)

مجموعه ویژگی چهارم که Li2009 می‌نامیم [۵۷]، دارای ۱۲ ویژگی موثر و و پایدار در زمان است که طی اجرای یک سری آزمایشات متوالی به کمک الگوریتم‌های C.45، Adaboost و بیز ساده از بین ۲۴۸

[1] Forwarding
[2] Backwarding
[3] Bidirectional

ویژگی انتخاب شده‌اند، با این هدف که به بیشترین دقت رده‌بندی و کمترین هزینه به کمک معیار عدم قطعیت متقارن[1] دست یابند. این مجموعه ویژگی در جدول ۳-۴ آورده شده است.

جدول ۳-۴. مجموعه ویژگی Li2009

نام ویژگی	توضیحات
Push_pkt_serv	تعداد کل بسته‌ها با مجموعه بیت PSH در سرآیند TCP (رو به عقب)
Int_win_bytes	تعداد کل بایت‌های ارسال شده در پنجره نخست (رو به عقب)
Int_win_bytes	تعداد کل بایت‌های ارسال شده در پنجره نخست (رو به جلو)
Avg_seg_size	میانگین اندازه سگمنت (داده بر حسب بایت به تعداد کل بسته‌ها) رو به عقب
IP_bytes_med	میانه کل بایت بسته‌ها (رو به جلو)
Act_data_pkt	تعداد کل بسته‌ها با حداقل یک بایت از محموله TCP (رو به جلو)
Data_bytes_var	واریانس طول بایت بسته‌ها (رو به عقب)
Min_seg_size	کمترین اندازه سگمنت مشاهده شده (رو به جلو)
RTT samples	تعداد کل نمونه‌های RTT یافت شده در کل بسته‌ها (رو به جلو)
Push_pkt_clnt	تعداد کل بسته‌ها با مجموعه بیت PSH در سرآیند TCP (رو به جلو)
Serv_port	پورت سرور
Clnt_port	پورت مشتری

[1] Symmetric uncertainty

۳-۲-۵ مجموعه ویژگی پنجم (CIC2018)

در نهایت مجموعه ویژگی پنجم که CIC2018 نامیده می‌شود [۵۸]، دارای چهار ویژگی موثر برای تشخیص باتنت‌ها می‌باشد که توسط الگوریتم جنگل تصادفی[1] انتخاب و معرفی شده است. نام هر ویژگی به همراه توضیحات مرتبط با آن در جدول ۳-۵ مشاهده می‌شود.

جدول ۳-۵. مجموعه ویژگی CIC2018

نام ویژگی	توضیحات
Flow duration	طول مدت زمان جریان (μ_s)
Total Len F.Packets	کل طول بسته‌های رو به جلو
SubFlow F.Bytes	تعداد بایت در زیر جریان رو به جلو
B.Packers/s	تعداد بسته‌های رو به عقب در ثانیه

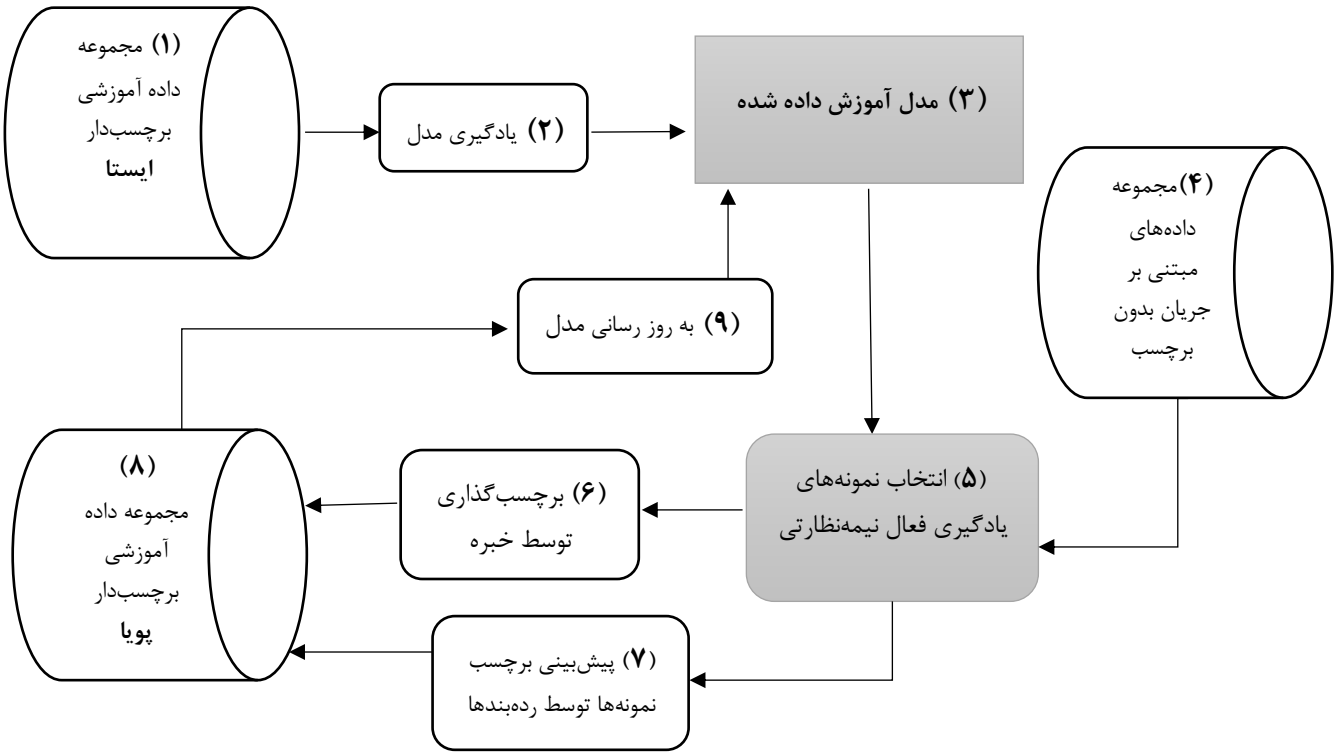
۳-۳ فرآیند یادگیری فعال نیمه‌نظارتی

ما پس از استخراج و تولید مجموعه ویژگی پایه نسبت به آموزش داده‌ها طی یک فرآیند یادگیری فعال نیمه‌نظارتی اقدام می‌کنیم. همانطور که در بخش ۳-۲-۱ بیان شد، ما در ابتدا ۱۰ درصد از کل نمونه‌ها را به عنوان مجموعه برچسب‌دار و مابقی را به عنوان مجموعه بدون برچسب در نظر می‌گیریم. با استفاده از مجموعه برچسب‌دار، آموزش اولیه سیستم را به کمک الگوریتم گروهی انجام داده و مدلی از نمونه‌های رده‌بندی شده تشکیل می‌دهیم. سپس طی فرآیند یادگیری فعال نسبت به انتخاب نمونه‌های مفید از مجموعه‌ی بدون برچسب که به صورت جریان داده‌ای هستند، مبادرت می‌ورزیم. سپس با تعیین برچسب نمونه‌های انتخابی و افزودن آنها به مجموعه نمونه‌های برچسب‌دار جدید در جهت به روز رسانی مدل آموزش داده شده اقدام می‌کنیم. لازم به ذکر است که الگوریتم گروهی شامل رده‌بندهای رگرسیون

[1] Random forest

لجستیک و ماشین بردار پشتیبان خطی و همچنین بیز ساده می‌باشد و در آن دو رده‌بند اول بر اساس الگوریتم گرادیان نزولی تصادفی نسبت به بهینه‌سازی وزن‌ها و به روز رسانی مدل اقدام کرده و بیز ساده نیز به صورت افزایشی و مستقل این فرآیند را اجرا می‌کند.

سیستم یادگیری فعال نیمه‌نظارتی پیشنهاد شده در این پژوهش دارای روال کلی است که در شکل ۳-۲ مشاهده می‌شود. ما در ادامه توضیحاتی را در خصوص بخش‌های مختلف در آن و نوآوری‌های ارائه شده در سیستم پیشنهادی، شرح می‌دهیم.



شکل ۳-۲. شمای کلی سیستم پیشنهادی مبتنی بر یادگیری فعال نیمه‌نظارتی

۳-۳-۱ مجموعه داده آموزشی برچسب‌دار ایستا

در این بخش از نمونه‌های برچسب‌دار ایستا برای یادگیری مدل استفاده می‌شود. منظور از مجموعه داده‌های ایستا در واقع همان نمونه‌های اولیه برچسب‌دار ثابتی هستند که در فرآیند یادگیری فعال

نیمه‌نظارتی برای آموزش در نظر گرفته شده‌اند و سیستم بر اساس آن، آموزش اولیه می‌بیند تا در مراحل بعدی اجرای الگوریتم نسبت به روز رسانی مدل اقدام شود.

۳-۳-۲ یادگیری مدل و مدل آموزش دیده شده

در این مرحله نسبت به رده‌بندی نمونه‌ها و در نهایت ساخت مدل آموزش دیده شده اقدام می‌شود. از آنجایی که رده‌بند مورد استفاده در این سیستم بر اساس یک روند گروهی و با رای‌گیری اکثریت است، بنابراین هر یک از رده‌بندها در بخش یادگیری مدل، نسبت به رده‌بندی داده‌ها و ساخت مدل‌های خود اقدام می‌کند. حال پس از اعلام نظر در خصوص کلاس هر نمونه، در بخش مدل آموزش دیده شده، با انجام عملیات رای‌گیری مدل نهایی از داده‌های سالم و باتنت توسط الگوریتم آموخته می‌شود. به طور کلی ما به منظور رده‌بندی داده‌ها در این سیستم از رده‌بندهای رگرسیون لجستیک، ماشین بردار پشتیبان خطی و بیز ساده بهره می‌گیریم که در بخش ۳-۴ به معرفی آنها به طور دقیق خواهیم پرداخت. نحوه‌ی تعلق کلاس پیش‌بینی شده توسط رده‌بندها در (رابطه ۳-۸) نشان داده شده است. در رابطه مذکور، e یک نوع کلاس خاص موجود در مجموعه کل کلاس‌ها (E) و g یک گونه از رده‌بندهای گروهی G می‌باشد که کلاس جریان ورودی c یا بردار ویژگی مرتبط با آن را پیش‌بینی می‌نماید.

$$predicted\_label(c) = \underset{e \in E}{\operatorname{argmax}} \sum_{g \in G} 1\{classify(G, c) = e\} \qquad \text{(رابطه ۳-۸)}$$

۳-۳-۳ داده‌های مبتنی بر جریان بدون برچسب

در این بخش فرآیند خواندن نمونه‌ها از مجموعه داده‌های بدون برچسب آغاز می‌شود. ما به منظور انجام این کار نمونه‌ها را طی یک فرآیند جویبار داده‌ای[1] اجرا کردیم. یعنی در هر مرحله از اجرای الگوریتم،

[1] Data Stream

پنجره‌ای بر روی نمونه‌ها حرکت داده شده و از هر پنجره نمونه‌های برتر استخراج می‌شود. ما نام این سناریو مبتنی بر یادگیری فعال نیمه‌نظارتی را جریان داده‌ی برخط می‌نامیم. هدف اصلی از این نحوه‌ی خواندن نمونه‌ها، ماهیت پویای ترافیک شبکه است که سیستم تشخیص می‌بایست قادر به دریافت داده‌ها به صورت جریانی پیوسته از اطلاعات باشد تا بر اساس هر جریان ترافیکی وارد شده، نسبت به استخراج ویژگی‌ها و در نهایت رده‌بندی و شناسایی حملات اقدام نماید.

۳-۳-۴ انتخاب نمونه‌های یادگیری فعال نیمه‌نظارتی

یادگیری فعال دارای راهبردهای پرس‌وجوی مختلفی می‌باشد که از مهم‌ترین آنها می‌توان به نمونه‌برداری مبتنی بر آنتروپی، نمونه‌برداری تصادفی، نمونه‌برداری مرزی[1]، واگرایی Kullbak-Liebler (KL)، اتلاف لگاریتم مورد انتظار[2]، کاهش واریانس[3] اشاره کرد که هرکدام به گونه‌ی خاصی داده‌های بدون برچسب را برای پرسش از خبره انتخاب می‌کنند [۱۲].

ما در این پژوهش از راهکار مبتنی بر آنتروپی داده‌ها استفاده کردیم. این روش به عنوان یکی از راهبردهای پرس‌وجوی نمونه‌برداری عدم اطمینان[4] می‌باشد که در آن بر اساس توزیع احتمالاتی نمونه‌ها و محاسبه‌ی مقدار آنتروپی تحت مدل ساخته شده، نسبت به انتخاب داده‌های برتر اقدام می‌شود. به طور کلی آنتروپی یک تئوری اطلاعاتی و نشان دهنده‌ی میزان دانسته‌هایی است که برای رمزگذاری یک توزیع مورد نیاز می‌باشد و اغلب به عنوان یک معیار از عدم اطمینان یا ناخالصی در یادگیری ماشین در نظر گرفته می‌شود [۵۲]. طبق فرمول اندازه‌ی آنتروپی شرطی مطابق (رابطه ۳-۹) بدست می‌آید.

$$x_H^* = \underset{x}{\operatorname{argmax}}\, H_\theta(Y|x) = \underset{x}{\operatorname{argmax}} - \sum_y P_\theta(y|x) \log P_\theta(y|x) \qquad \text{(رابطه ۳-۹)}$$

[1] Margin Sampling
[2] Expected log-loss
[3] Variance Reduction
[4] Uncertainty Sampling

که در آن (y) محدوده‌ای از تمام برچسب‌های ممکن برای نمونه‌های (x) است و $P_\theta(y|x)$ احتمال برچسب کلاس هر نمونه تحت مدل θ می‌باشد. به عبارتی دیگر در این سیستم احتمال تعلق هر نمونه بدون برچسب بر اساس میانگین مدل‌های شکل گرفته شده، محاسبه و سپس مطابق فرمول، مقدار آنتروپی برای هر نمونه بدست آورده می‌شود. این مقدار احتمال، همان خروجی حاصل شده از احتمال تعلق نمونه‌ها به میانگین مدل‌ها می‌باشد که توسط رده‌بند گروهی محاسبه شده است و با انجام این کار در واقع ما از نتایج رده‌بندها در انتخاب نمونه‌ها بهره گرفته‌ایم. ما از سوی دیگر به منظور انتخاب نمونه‌های موثر برای ارسال به خبره و همچنین استفاده در روند یادگیری نیمه‌نظارتی، آستانه‌ای به اندازه‌ی ۰/۷ را در نظر گرفتیم که در کنار سایر شروط برای انتخاب نمونه‌های برتر استفاده می‌گردد. لازم به ذکر است که مقدار آستانه‌ی انتخاب شده به صورت تجربی و بر اساس کار پژوهشگران مختلف این حوزه، بدست آمده است [۱۲].

۳-۳-۵ برچسب‌گذاری توسط خبره

در این مرحله فرآیند برچسب‌گذاری توسط خبره صورت می‌پذیرد. فرآیند پرسش از خبره می‌تواند به صورت چرخه‌ی انسانی یعنی پرسش از مدیر شبکه یا توسط رده‌بندها انجام پذیرد. به طور کلی نحوه‌ی تصمیم‌گیری خبره می‌تواند بر اساس الگوی محموله بسته‌ها، میزان شباهت جریان‌ها به بات‌نت‌های کشف شده، اطلاعات بدست آمده از هانی‌نت و غیره انجام می‌پذیرد [۱۱]. به طور کلی فرآیند تعامل و پرسش از خبره با هدف بهبود کارایی به میزانی لازم است که نمونه‌های بدون برچسب با ارزش اطلاعاتی مناسب در جریان‌های ورودی وجود داشته باشند و رده‌بند نتواند با قطعیت نسبت به تعیین برچسب آنها اقدام نماید. با تعیین برچسب این نمونه‌ها توسط خبره و اضافه شدن آنها به مجموعه آموزشی، امکان آموزش مجدد فراهم شده و کارایی الگوریتم نیز در نتیجه بهبود می‌یابد.

۳-۳-۶ پیش‌بینی برچسب نمونه‌ها توسط رده‌بندها

در این مرحله فرآیند برچسب‌گذاری توسط رده‌بندها انجام می‌پذیرد. همانطور که در بخش‌های قبلی اشاره شد. ما به منظور جلوگیری از گرایش نمونه‌ها به مدل‌های ساخته شده توسط نمونه‌های برچسب‌گذاری شده توسط خبره و همچنین ایجاد توازن بر روی مدل‌ها، یک سری نمونه‌ی دیگر نیز انتخاب کردیم تا مستقیما توسط خود رده‌بندها برچسب‌گذاری شوند.

۳-۳-۷ مجموعه داده آموزشی برچسب‌دار پویا

پس از انتخاب نمونه‌های برتر و مشخص شدن برچسب آنها در مرحله‌ی قبل، حال مجموعه داده برچسب‌دار جدیدی ایجاد می‌شود که مدل آموزش دیده شده می‌بایست توسط این نمونه‌ها به روز رسانی شود.

۳-۳-۸ فرآیند به روز رسانی مدل

با مشخص شدن کلاس نمونه‌های بدون برچسب و اضافه شدن آنها به مجموعه برچسب‌دار پویا، حال نوبت به روز رسانی مدل‌های شکل گرفته توسط رده‌بندها می‌باشد. به این صورت که هر رده‌بند نسبت به روز رسانی مدل خود اقدام کرده و سپس دوباره طی فرآیند رای گیری اکثریت، مدل نهایی به روز شده و فرآیند یادگیری دوباره از سر گرفته می‌شود.

حال که تمامی بخش‌های موجود در فرآیند یادگیری فعال نیمه‌نظارتی مورد بررسی قرار گرفت، نوبت به ارائه‌ی الگوریتم و روندی می‌باشد که به منظور تشخیص بات‌نت به کار برده شده است. به این منظور در ابتدا خلاصه‌ای از پارامترهای استفاده شده در الگوریتم طبق جدول ۳-۶ ارائه می‌شود و سپس بر اساس آن، مطابق با شکل ۳-۳ الگوریتم فعال نیمه‌نظارتی نشان داده می‌شود.

جدول ۳-۶. پارامترهای موجود در الگوریتم یادگیری فعال نیمه‌نظارتی

پارامتر	توضیحات
S	مجموعه داده‌های برچسب‌دار ایستا
R	مجموعه داده‌های خام برچسب‌دار ۲۰ بعدی
D	مجموعه داده‌های برچسب‌دار پویا
U	مجموعه داده‌های مبتنی بر جریان بدون برچسب ۲۳۰ بعدی
T	مقدار آستانه
Q	پرس‌وجو یادگیری فعال نیمه‌نظارتی برای انتخاب نمونه‌ها
O	برچسب‌گذاری توسط خبره
C	پیش‌بینی برچسب توسط رده‌بند
M	مدل آموزش داده شده
j	اندیس پنجره‌ها
i	اندیس تعداد تکرار الگوریتم یادگیری فعال نیمه‌نظارتی
k	تعداد نمونه‌های موجود در هر پنجره
o	نمونه‌های انتخابی برای پرسش از خبره
c	نمونه‌های انتخابی برای پیش‌بینی توسط رده‌بندها
instance	اندیس نمونه‌های بدون برچسب

score	امتیاز نمونه‌های بدون برچسب
Slide_window	اندازه پنجره مبتنی بر جریان
BatchSize	تعداد نمونه‌های انتخاب شده
Max_iteration_num	بیشینه تکرار الگوریتم یادگیری فعال نیمه‌نظارتی
Num_windows	تعداد پنجره‌ها

$\boldsymbol{Input}: \boldsymbol{S}, \boldsymbol{R}, \boldsymbol{U}, \boldsymbol{Slide\_window}, \boldsymbol{Max\_iteration\_num}$

$\boldsymbol{Output}$: $updated\ \boldsymbol{M}\ with\ set\ \boldsymbol{D}$

// Initial_traning phase

1: $Init\_TrainingSet \leftarrow \boldsymbol{S}$

2: $\boldsymbol{M} \leftarrow Training\ on\ Init\_TrainingSet\ \ by\ Ensemble\ learning$

3: $\boldsymbol{unlabeled\_instances\_r} \leftarrow \boldsymbol{R}$

// Semi-supervised active learning phase

4: $\boldsymbol{set\ \ i}\ and\ \boldsymbol{Max\_iteration\_num}\ of\ semi-supervised\ active\ learning\ //i = 0$

5: $\boldsymbol{num\_window} \leftarrow\ \boldsymbol{unlabeled\_instances\_r}\ /\ \boldsymbol{Slide\_window}$

6: $\boldsymbol{For}\ each\ \ \boldsymbol{j}\ window\ of\ \boldsymbol{num\_window}$

7: $\boldsymbol{If}(\boldsymbol{i}\ == \boldsymbol{Max\_iteration\_num})$

8: $\boldsymbol{break}\ form\ \boldsymbol{for}//j$

9: $end\ If$

10: $\boldsymbol{For}\ each\ \boldsymbol{k}\ \ instances\ in\ \boldsymbol{Slide\_window}$

11: $\boldsymbol{instance} \leftarrow ((j * Slide\_window) + k)$

12: $\boldsymbol{score} \leftarrow calculate\ informative\ of\ \boldsymbol{instance}$ by $\mathbf{Q} = \underset{instance}{\operatorname{argmax}} H_\theta(Y|instance)$

$$= \underset{instance}{\operatorname{argmax}} - \sum_a P_\theta(y_a|\ instance) \log P_\theta(y_a|\ instance)$$

13: $\boldsymbol{If}(\boldsymbol{score} < \boldsymbol{T}\ )$

14: $\boldsymbol{unlabeled\_instances} \leftarrow \boldsymbol{U}$

15: ***and*** *select* ***o*** *instances of* ***unlabeled_instances*** *with the highest informative* $< \boldsymbol{T}$

16: *end if*

17: ***Else if*** $(score > \boldsymbol{T})$

18: $\boldsymbol{unlabeled\_instances} \leftarrow \boldsymbol{U}$

19: ***and*** *select* ***c*** *instances of* ***unlabeled_instances*** *with the highest informative* $> \boldsymbol{T}$

20: *end esle if*

21: *Defined lables of* $\boldsymbol{o}, \boldsymbol{c}$ *form* ***unlabeled_instances*** *by* ***O*** *and* ***C*** *like as step* 22 *and* 23

22: $\boldsymbol{Predicted\ label\_active\_learning} \leftarrow Human\ //\ o$

23: $\boldsymbol{Predicted\ label\_Semi\ supervised} \leftarrow \underset{e}{\operatorname{argmax}} \sum_G 1\{classify(G, c) = e\}$ //c

24: $\boldsymbol{D} \leftarrow \boldsymbol{Predicted\ label\_active\_learning} + \boldsymbol{Predicted\ label\_Semi\ supervised}$

25: ***If*** *number of* $\boldsymbol{D} == \boldsymbol{BatchSize}$

26: $\boldsymbol{i}++$

27: ***Break*** *form* ***For***

28: *end if*

29: *end For // k*

// Incremental learning and update phase

30: *Update* ***M*** *with* ***D***

31: *end For // j*

شکل۳-۳. الگوریتم یادگیری فعال نیمه‌نظارتی

با مشخص شدن روند کلی سیستم پیشنهادی و همچنین بررسی الگوریتم یادگیری فعال نیمه‌نظارتی، حال می‌توان مهم‌ترین نوآوری‌های ارائه شده در این سیستم را یاد آورد شد که از جمله آنها می‌توان به روند جریان داده‌ای آن در هنگام ساخت مجموعه ویژگی پایه در مرحله شمارش تکرار نمونه‌ها و همچنین در هنگام خواندن نمونه‌های بدون برچسب و بهره‌گیری از یادگیری گروهی، در نظر گرفتن حد آستانه، انتخاب نمونه‌هایی با ابعاد ویژگی کمتر و در نهایت استفاده از نتایج رده‌بندها در انتخاب نمونه‌ها را اشاره کرد. در واقع مهم‌ترین ویژگی سیستم پیشنهادی روند جریان داده‌ای آن در هنگام دریافت و پردازش

داده‌ها می‌باشد که در کنار سایر مشخصه‌های پیشنهاد شده، کارایی مناسبی را برای سیستم در بر خواهد داشت.

۳-۴ رده‌بندهای پایه

به منظور رده‌بندی داده‌ها، همانطور که عنوان شد از سه رده‌بند مختلف و به صورت رای‌گیری اکثریت استفاده گشت که در ادامه به معرفی آنها خواهیم پرداخت.

۳-۴-۱ رده‌بند ماشین بردار پشتیبان خطی

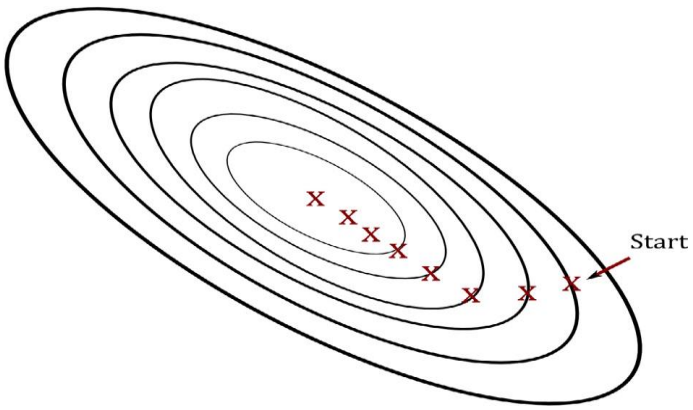
ما به منظور استفاده از یک روند افزایشی برای همگرایی خطی داده‌ها و استفاده از رده‌بند ماشین بردار پشتیبان، نسبت به کمینه ساختن تابع اتلاف Hinge[1] از طریق الگوریتم گرادیان نزولی تصادفی[2] اقدام کردیم. تابع Hinge معمولا به منظور ایجاد بیشترین حاشیه برای رده‌بندی و به طور ویژه برای ماشین بردار پشتیبان استفاده می‌شود. به طور کلی مشکل رده‌بندی و رگرسیون داده‌های بزرگ معمولا با استفاده‌ی صحیح از روش مرتبه‌ی دوم گرادیان تصادفی[3] و تکنیک‌های گرادیان تصادفی متوسط[4] برطرف می‌شود. در این روش تابع هزینه (اتلاف) با استفاده از الگوریتم گرادیان نزولی تصادفی به صورت (رابطه ۳-۱۰) کمینه می‌گردد.

$$w_{k+1} = w_k - \mu \nabla_w Q(x_k, w_k) \qquad \text{(رابطه ۳-۱۰)}$$

که در آن μ به عنوان نرخ یادگیری الگوریتم و $Q(x_k, w_k)$ به عنوان تخمین‌زننده لحظه‌ای[5] تابع اتلاف $Q(x, w)$ می‌باشد که از بردار ورودی x_k برای نمونه‌ی k ام استفاده می‌کند. بر همین اساس، مدل

[1] Loss function
[2] Stochastic gradient descent (SGD)
[3] Second order stochastic gradient
[4] Averaged stochastic gradient
[5] Instantaneous estimator

پارامترها یا ویژگی‌ها w_k با استفاده از هر بردار ورودی، به صورت افزایشی اقدام به روز رسانی می‌نماید. در نهایت زمانی که μ به اندازه‌ی کافی کوچک شد، الگوریتم SGD یک همگرایی خطی برای داده‌ها به دست می‌آورد. در شکل ۳-۴ تاثیر لحظه‌ای پارامترهای مدل یعنی w_k را بر روی منحنی خطا مشاهده می‌شود [۵۹].



شکل ۳-۴. نمایش به روز رسانی افزایشی در الگوریتم SGD

حال اگر به جای تابع اتلاف (Q)، تابع Hinge را که برای ماشین بردار پشتیبان استفاده می‌شود، در نظر بگیریم، از طریق الگوریتم گرادیان نزولی می‌توان برای به روز رسانی مدل آن اقدام کرد. در واقع Hinge یک تابع محدب بوده و بسیاری از روش‌های بهینه‌سازی در یادگیری ماشین همانند گرادیان نزولی بر روی آن قابل اجرا خواهد بود. این تابع به صورت (رابطه ۳-۱۱) نشان داده شده است.

$$l(y) = \max(0,1 - t.y)$$ (رابطه ۳-۱۱)

که در آن y خروجی خام حاصل از تابع تصمیم‌گیری رده‌بند (نه برچسب پیش‌بینی شده کلاس) می‌باشد و به صورت (رابطه ۳-۱۲) در نظر گرفته می‌شود. همچنین t خروجی از قبل تعیین شده و به صورت $t= \pm 1$ است.

$$y = w.x + b$$ (رابطه ۳-۱۲)

که در آن (w,b) پارامترهای ابر صفحه و x نقطه مورد نظر برای رده‌بندی است.

۳-۴-۲ رده‌بند رگرسیون لجستیک

به منظور استفاده از رده‌بند لجستیک، ما از مدل خطی آن که بر پایه‌ی گرادیان نزولی تصادفی نسبت به بهینه‌سازی وزن‌های خود اقدام می‌کند، استفاده کردیم. رده‌بند مفروض با نام SGD همانطور که در بخش قبلی معرفی شد، می‌تواند بر پایه‌ی تابع اتلاف رگرسیون لجستیک نیز عمل کند. بنابراین فرآیند افزایشی آن همانند بخش قبلی اتفاق می‌افتد با این تفاوت که تابع اتلاف این روش، رگرسیون لجستیک می‌باشد. به طور کلی رگرسیون لجستیک به طور موفق آمیزی برای مسائل رده‌بندی در نظر گرفته می‌شود. این الگوریتم دو کلاس با برچسب‌های Y=0 و Y=1 را ارائه می‌نماید که N نماینده‌ی n بُعد ویژگی، شامل $\{X_1, X_2, X_3, .., X_N\}$ خواهد بود و هر نمونه از ویژگی‌ها به عنوان یک بردار تصادفی، متشکل از متغیرهای تصادفی گسسته به کار گرفته می‌شود. رگرسیون لجستیک یک رده‌بند دو کلاسه خطی است که احتمال کلاس را بر پایه‌ی تابع سیگموئید به صورت (رابطه ۳-۱۳) تخمین می‌زند:

$$P(Y = 1|y) = \frac{1}{1 + e^{-y}} \qquad \text{(رابطه ۳-۱۳)}$$

$$P(Y = 0|y) = 1 - P(Y = 1|y) = \frac{e^{-y}}{1 + e^{-y}}$$

که در آن y خروجی مدل و w وزن برای ورودی‌های x به صورت تابع خطی همانند (رابطه ۳-۱۴) در نظر گرفته می‌شود:

$$y = w_0 + w_1 x_1 + w_2 x_2 + \cdots + w_n x_n \qquad \text{(رابطه ۳-۱۴)}$$

در نهایت پارامترهای مدل لجستیک با روش درست‌نمایی بیشینه محاسبه می‌شوند [۵۹].

۳-۴-۳ رده‌بند بیز ساده

رده‌بند بیز به عنوان یکی از معروف‌ترین الگوریتم‌های حوزه‌ی داده کاوی می‌باشد که در مسائل رده‌بندی مورد استفاده قرار می‌گیرد. سادگی، تاثیرگذاری و قدرت در مسائل رده‌بندی، آن را به عنوان الگوریتم مناسبی در این حیطه به وجود آورده است. بیز ساده یک رویکرد احتمالاتی است که مبتنی بر فرضیه‌هایی خواهد بود که در آن ویژگی‌ها از یکدیگر استقلال داشته و وزن ویژگی‌ها نیز در آن دارای درجه‌ی اهمیتی یکسانی می‌باشد. با توجه به قضیه بیز، توزیع پسین یک نمونه نسبتی بر اساس توزیع پیشین و بیشترین شباهت خواهد بود که فرمول بیز ساده بر اساس (رابطه ۳-۱۵) در نظر گرفته می‌شود.

$$P(C_k|X) = \frac{P(C_k)\mathrm{P}(\mathrm{X}|C_k)}{P(X)} \qquad \text{(رابطه ۳-۱۵)}$$

که در آن C_k مربوط به کلاس‌های واقعی نمونه‌ها به صورت k=0,1 و$\mathrm{X}=(x_1, x2, \dots x_n)$ بیانگر مقادیر نمونه‌ها خواهد بود [۶۰]. در این پژوهش ما نسخه‌ی افزایشی بیز ساده را که در آن از یک کرنل تخمین چگالی غیر پارامتریک برای متغیرهای پیوسته استفاده می‌شود، به کار بردیم و به صورت (رابطه ۳-۱۶) در نظر گرفته می‌شود.

$$P(X = x|C = c) = \frac{1}{n}\sum_i g(x, \mu_i, \sigma_i) \qquad \text{(رابطه ۳-۱۶)}$$

که در آن i بازه‌ی نقاط آموزشی حاصل از ویژگی X در کلاس C_i و $\mu_i = x_i$ و g تابع چگالی احتمال برای یک توزیع نرمال گوسی به صورت (رابطه ۳-۱۷) می‌باشد.

$$g(x, \mu, \sigma) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \qquad \text{(رابطه ۳-۱۷)}$$

فصل ۴ : پیاده‌سازی و ارزیابی روش پیشنهادی

۴-۱ تنظیمات و راه‌اندازی سیستم

در این فصل به بیان پیاده‌سازی و ارزیابی راهکار پیشنهادی و جزییات مربوط به آن پرداخته می‌شود. ما در ادامه به معرفی مجموعه داده بات‌نت با هدف اجرای آن در ساخت مجموعه ویژگی مطابق روشی که در فصل سوم بررسی شد و همچنین مراحل راه‌اندازی و انجام تنظیمات مورد نیاز برای ارائه‌ی یک روش یادگیری فعال نیمه‌نظارتی می‌پردازیم. انجام آزمایش‌ها و ارزیابی نتایج و در نهایت مقایسه‌ی راهکار پیشنهادی با تعدادی از روش‌های مشابه نیز در انتهای این فصل صورت می‌پذیرد. لازم به ذکر است که تمامی مراحل پیاده‌سازی (ساخت مجموعه ویژگی‌ها و سیستم پیشنهادی) به زبان برنامه‌نویسی جاوا و در محیط eclipse انجام پذیرفت.

۴-۱-۱ مجموعه داده بات‌نت

همانطور که در فصل اول اشاره شد، یکی از مهم‌ترین چالش‌های پیش‌رو در سیستم‌های تشخیص، نیاز آنها به وجود یک مجموعه داده با حملات گوناگون و الگوهای متفاوت است تا در برابر حملات نوع جدید بتواند به خوبی فرآیند شناسایی را به انجام برساند. از سوی دیگر طراحی یک سیستم تشخیص بات‌نت نیازمند وجود بات‌نت‌های دیده نشده در مجموعه آزمون است، تا بدین صورت کارایی سیستم در قبال تشخیص انواع مختلف بات‌نت‌های جدید سنجیده شود. علاوه بر اینکه می‌بایست داده‌های آزمون و آزمایش تا حد ممکن هم‌پوشانی زیادی با یکدیگر نداشته باشند تا نتایج استخراج شده، قابلیت اطمینان بالایی را به خود اختصاص دهند. در واقع انجام یک ارزیابی اطمینان‌بخش از سیستم‌های تشخیص بات‌نت، نیازمند وجود مجموعه داده‌ی جامعی است که سیستم مبتنی بر آن، شامل حجم متنوعی از بات‌نت‌های متمرکز و غیر متمرکز به همراه پروتکل‌های متفاوت باشد. این موضوع زمینه‌ساز جنبه عملی پیدا کردن راهکار و نیازمند وجود مجموعه داده واقعی خواهد بود که از بستر اینترنت بدست آمده است.

بنابراین در این پژوهش، به منظور برآوردن نیازمندی‌های بیان شده و همچنین رفع مشکلات، از مجموعه داده باتنت ISCX استفاده شده است که تاکنون در بین مجموعه داده‌های مرتبط با باتنت‌ها دارای جامعیت و سطح تنوع بالایی از گونه‌های مختلف باتنت خواهد بود. این مجموعه داده توانسته، با ارائه‌ی یک مجموعه جامع، همراه با ترافیک واقعی باتنت و جمع‌آوری سایر جریان‌های واقعی و نرمال ترافیک شبکه، چالش‌های موجود در این حوزه را تاحد قابل قبولی برطرف سازد [۱۵].

از سوی دیگر اعمال یک دوره‌ی زمانی کافی در جمع‌آوری مجموعه داده که با هدف نمایان ساختن عملکردهای خاموش باتنت‌های مختلف صورت پذیرفته است و همچنین وجود داده‌های ناهمگن و جامع، تا حد زیادی شبیه‌سازی واقعی از ترافیک شبکه در این مجموعه داده را دلالت می‌کنند. بنابراین کارایی سیستم طراحی شده در این پایان‌نامه، نیز می‌تواند درجه‌ی قابل قبولی از اطمینان را به خود اختصاص دهد. این مجموعه داده در آزمایشگاه CIC دانشگاه UNB کانادا[1] تهیه و توسعه داده شده است. مجموعه داده باتنت ISCX دارای ۷ گونه بانتنت مختلف در مجموعه‌ی آموزش با حجمی معادل۵/۳ گیگابایت و دارای ۱۶ گونه باتنت در مجموعه آزمون به حجم ۸/۵ گیگابایت می‌باشد. علت اصلی تنوع بیشتر در مجموعه آزمون ارزیابی دقیق‌تر و سنجش میزان توسعه‌پذیری و توانایی سیستم‌های تشخیص باتنت در مقابله با باتنت‌های گونه‌ی جدید خواهد بود.

در جدول ۴-۱ نام، گونه‌ی باتنت‌ها و سهم حضور در جریان‌های ترافیکی در مجموعه‌ی آموزش و در جدول ۲-۴ موارد مفروض، برای مجموعه‌ی آزمون شرح داده شده است. لازم به ذکر است که سایر جزییات و نحوه‌ی جمع‌آوری و همچنین لیست آدرس‌هایIP باتنت‌ها در مجموعه آزمون و آموزش در صفحه‌ی وب‌سایت آزمایشگاه CIC و در مرجع [۱۵] قابل دسترس می‌باشد.

[1] http://www.unb.ca/cic/datasets/botnet.html

جدول ۴-۱. نحوه‌ی توزیع بات‌نت‌ها در مجموعه‌ی آموزش ISCX

نام بات‌نت	نوع بات‌نت	درصد سهم حضور در جریان
Neris	IRC	۲۱۱۵۹ (٪ ۱۲)
Rbot	IRC	۳۹۳۱۶ (٪ ۲۲)
Virut	HTTP	۱۶۳۸ (٪ ۰/۹۴)
NSIS	P2P	۴۳۳۶ (٪ ۲/۴۸)
SMTP Spam	P2P	۱۱۲۹۶ (٪ ۶/۴۸)
Zeus	P2P	۳۱ (٪ ۰/۰۱)
Zeus control(C&C)	P2P	۲۰ (٪ ۰/۰۱)

جدول ۴-۲. نحوه‌ی توزیع بات‌نت‌ها در مجموعه‌ی آزمون ISCX

نام بات‌نت	نوع بات‌نت	درصد سهم حضور در جریان
Neris	IRC	۲۵۹۶۷ (٪ ۵/۶۷)
Rbot	IRC	۸۳ (٪ ۰/۰۱۸)
Menti	IRC	۲۸۷۸ (٪ ۰/۶۲)
Sogou	HTTP	۸۹ (٪ ۰/۰۱۹)
Murlo	IRC	۴۸۸۱ (٪ ۱/۰۶)
Virut	HTTP	۵۸۵۷۶ (٪ ۱۲/۸۰)

NSIS	P2P	٪ ۰/۱۶۵) ۷۵۷
Zeus	P2P	٪ ۰/۱۰۹) ۵۰۲
SMTP Spam	P2P	٪ ۴/۷۲) ۲۱۶۳۳
UDP Strom	P2P	٪ ۹/۶۳) ۴۴۰۶۲
Tbot	IRC	٪ ۰/۲۸۳) ۱۲۹۶
Zero Access	P2P	٪ ۰/۲۲۱) ۱۰۱۱
Weasel	P2P	٪ ۹/۲۵) ۴۲۳۱۳
Smoke Bot	P2P	٪ ۰/۰۱۷) ۷۸
Zeus Control (C&C)	P2P	٪ ۰/۰۰۶) ۳۱
ISCX IRC bot	P2P	٪ ۰/۳۸۷) ۱۸۱۶

حال مطابق با راهکار پیشنهادی که برای ساخت مجموعه ویژگی پایه در بخش ۳-۲-۱ شرح داده شد، ما نسبت به تولید جریان‌هایی از ترافیک شبکه اقدام کردیم که دارای شرایط خاصی بودند. به طور کلی در این جریان‌ها اندازه‌ی بسته‌ها می‌بایست بزرگ‌تر از ۱۰، پروتکل ارتباطی آنها به صورت TCP و از سوی دیگر پورت مقصد برای تمامی جریان‌ها ۸۰ در نظر گرفته شده باشد. بنابراین با اعمال این شرایط و در نهایت اجرای راهکار مذکور بر روی مجموعه داده ISCX، اطلاعات مربوط بات‌نت‌ها و نحوه‌ی توزیع آنها در مجموعه آموزش و آزمون همانند جدول ۴-۳ بدست آورده شد.

جدول ۴-۳. نحوه‌ی توزیع بات‌نت‌ها در مجموعه‌ی آموزش و آزمون ISCX در مجموعه ویژگی پایه

نام بات‌نت	نوع بات‌نت	مجموعه آموزش	مجموعه آزمون
Neris	IRC	✓	✓
Rbot	IRC	✓	✓
Virut	HTTP	✓	✓
NSIS	P2P	✓	✓
SMTP Spam	P2P	✓	✓
Menti	IRC	_	✓
Sogou	HTTP	_	✓
Murlo	IRC	_	✓
Virut	HTTP	_	✓
Zeus	P2P	_	✓
Tbot	IRC	_	✓
Zero Access	P2P	_	✓
Weasel	P2P	_	✓
Smoke Bot	P2P	_	✓
ISCX IRC bot	P2P	_	✓

۴-۱-۲ پیاده‌سازی فرآیند یادگیری فعال نیمه‌نظارتی

پس از معرفی شدن مجموعه داده‌ی مورد استفاده، ما در این بخش به بیان مراحل پیاده‌سازی یادگیری فعال نیمه‌نظارتی و همچنین نتایج بدست آمده از اجرای آن، مطابق با الگوریتمی که در فصل سوم ارائه شد، می‌پردازیم.

به طور کلی ما به منظور آموزش اولیه سیستم، در ابتدا نسبت به ساخت مجموعه داده‌های برچسب‌دار و بدون برچسب به کمک یک فرآیند نمونه‌برداری تصادفی با ناظر و بدون جایگزینی اقدام کردیم که در جدول ۴-۴ خلاصه‌ای از مشخصات مجموعه ویژگی‌های استخراج شده از راهکار پیشنهادی و اجرای آن بر روی مجموعه داده باتنت ISCX به همراه اندازه مجموعه‌های برچسب‌دار و بدون برچسب آورده شده است.

جدول ۴-۴. اطلاعات مجموعه ویژگی‌های استخراجی از (Qiu2017) بر روی مجموعه باتنت ISCX

نام مجموعه ویژگی‌های استخراج شده	تعداد ویژگی‌ها	اندازه مجموعه آموزش	اندازه مجموعه آزمون	تعداد نمونه‌های مجموعه برچسب‌دار	تعداد نمونه‌های مجموعه بدون برچسب
مجموعه ویژگی داده‌های خام	۲۰	۴۰۹۵۷	۱۸۱۷۱	۴۰۹۵	۳۶۸۶۲
مجموعه ویژگی داده‌های امتیازی	۲۳۰	۴۰۹۵۷	۱۸۱۷۱	۴۰۹۵	۳۶۸۶۲

پس از ساخت مجموعه داده‌های معرفی شده، حال سیستم تشخیص ما با دو دسته داده مواجه خواهد بود؛ به این صورت که به کمک مجموعه داده‌ی برچسب‌دار نسبت به ساخت مدل اولیه اقدام می‌کند و در ادامه به منظور به روز رسانی مدل و پاسخ به ماهیت واقعی ترافیک شبکه، با انتخاب مناسب نمونه‌ها

از مجموعه داده‌ی بدون برچسب طی یک فرآیند یادگیری افزایشی، آموزش مجدد می‌بیند. به این صورت که در هر تکرار از فرآیند یادگیری فعال نیمه‌نظارتی، نسبت به انتخاب ۲۰ نمونه با بیشترین ارزش اطلاعاتی از هر پنجره، اقدام شده که در این میان، ۱۰ نمونه انتخاب شده برای پرسش از خبره ارسال و برچسب آنها استعلام می‌شود و به همین ترتیب ۱۰ نمونه‌ی دیگر نیز طی یک فرآیند نیمه‌نظارتی توسط رای اکثریت رده‌بندها، برچسب‌گذاری می‌گردد. در واقع با انتخاب نمونه‌های مناسب، یکی از مهم‌ترین چالش‌های موجود در سیستم‌های تشخیص بات‌نت که همان کاهش هزینه‌های برچسب‌گذاری نمونه‌ها می‌باشد، برطرف خواهد شد.

همچنین ما در انتخاب نمونه‌های برتر علاوه بر بهره‌گیری از راهبرد آنتروپی یادگیری فعال و اعمال حد آستانه، به منظور کاهش محاسبات و افزایش کارایی سیستم از مجموعه ویژگی داده‌های خام نیز استفاده کردیم که در آن به جای بررسی بردارهای ۲۳۰ بعدی از هر نمونه، تنها کافی است، بردارهای ۲۰ بعدی حاصل شده از داده‌های خام را در نظر بگیریم. حال اگر آنتروپی هر بردار موجود در آن مناسب پرسش از خبره و اعمال برچسب توسط رده‌بند باشد؛ در این صورت نسبت به ساخت بردار ویژگی ۲۳۰ بعدی متناظر با آن اقدام کرده و فرآیند انتخاب نمونه‌های برتر انجام می‌پذیرد. بنابراین در این سیستم نحوه‌ی انتخاب به این صورت است که از بین تمام نمونه‌های بدون برچسب در مجموعه داده‌های خام، آنهایی که ارزشی نزدیک به یک و کوچکتر از آستانه دارند، ۱۰ نمونه‌ی متناظر با آن در مجموعه داده‌های امتیازی (۲۳۰ بعدی) برای پرسش از خبره (در واقع همان نمونه‌های مشکوک) استفاده می‌شود و آنهایی که بزرگ‌تر از آستانه هستند؛ به همین صورت، متناظر آنها در مجموعه داده‌های امتیازی برای رده‌بندها ارسال می‌شوند تا برچسب پیش‌بینی‌شده توسط آنها اعمال گردد. به صورت ساده‌تر می‌توان گفت از آنجایی که هر بردار از مجموعه داده‌های خام همان ۲۰ ویژگی اول از مجموعه داده‌های امتیازی است، بنابراین می‌توان تعداد ویژگی‌های کمتری را برای بررسی شروط سیستم در نظر گرفت. لازم به ذکر است که تعداد تکرار فرآیند یادگیری فعال نیمه‌نظارتی نیز ۵۰ دور در نظر گرفته شد. در نهایت با

تعیین برچسب نمونه‌ها و افزودن آنها به مجموعه برچسب‌دار پویا، فرآیند به روز رسانی مدل طی یک فرآیند یادگیری افزایشی اتفاق می‌افتد. در جدول ۴-۵ خلاصه‌ای از مقادیر پارامترهای مورد نیاز برای راه‌اندازی الگوریتم یادگیری فعال نیمه‌نظارتی که در فصل قبل معرفی شد، نشان داده شده است. همچنین ما مقدار پارامتر نرخ یادگیری الگوریتم گرادیان نزولی تصادفی در رده‌بندهای رگرسیون لجستیک و ماشین بردار پشتیبان خطی را ۰/۰۱ و تعداد تکرار آن را ۵۰۰ در نظر گرفتیم.

جدول ۴-۵. مقادیر پارامترها در راه‌اندازی سیستم

نام پارامتر	مقدار در نظر گرفته شده
T	۰/۷
Slide_window	۵۰۰
BatchSize	۲۰
Max_iteration_num	۵۰
o	۱۰
c	۱۰

۴-۲ آزمایش‌ها و ارزیابی نتایج

طبیعت داده‌ها در فضای ترافیک شبکه و همچنین ورود جریان‌های داده‌ای که به طور پیوسته در حال تولید هستند، طراحی سیستم‌های تشخیص را ملزم به ایجاد شرایطی مناسب برای برخورد با چنین وضعیتی می‌نماید. به این صورت که در چنین محیطی، ممکن است در هر لحظه داده‌های مشابه و یا جدیدی وارد شده و سیستم می‌بایست در مورد جریان‌های ورودی به درستی تصمیم‌گیری نماید و در

صورت نیاز آنها را در مجموعه آموزشی پویای خود ذخیره کرده و یا تنها به منظور به روزرسانی مدل در هر مرحله از یادگیری استفاده نماید. ما در طراحی سیستم تشخیص باتنت خود با ایجاد چارچوبی متفاوت، نسبت به برآوردن این نیاز اقدام کردیم؛ در واقع تعدادی دادهی آزمون طی مراحل مختلف به منظور ارزیابی کارایی سیستم به کار برده شد که این دادهها همانند نمونههایی خواهند بود که در محیط واقعی وارد سیستم تشخیص میشوند. از سوی دیگر بحث جامعیت نمونههای آموزشی، کمبود دادههای برچسب خورده به منظور ردهبندی و رفع مشکل محدودیت در روشهای نظارتی، قابلیت توسعهپذیری سیستم در قبال باتنتهای گونه جدید و پیشتر از آن ساخت مجموعه ویژگیها بر اساس انتخاب ویژگیهای موثر از دیگر مواردی است که سیستم طراحی شده، میتواند تا حد قابل قبولی تامین کنندهی آنها باشد.

به طور کلی آزمایشها به این صورت میباشد که در یک حلقهی تکرار، هر سری نمونههایی ۵۰۰تایی (به اندازه پنجره) وارد سیستم شده و سپس بر اساس فرآیند یادگیری فعال نیمهنظارتی نسبت به انتخاب نمونههای برتر و برچسبگذاری آنها اقدام میشود. نمونههای برچسبگذاری شده از سوی خبره و ردهبندها با هم ترکیب شده و در نهایت برای به روزرسانی سیستم مورد استفاده قرار میگیرد. حال ما به منظور ارزیابی راهکار خود، سه وضعیت کلی را در نظر میگیریم که در ادامه به بیان آنها پرداخته میشود و سپس برای هر یک توضیحات تکمیلی را ارائه خواهیم داد.

حالت نخست، اجرای الگوریتم بر روی مجموعه ویژگیهای استخراج شده توسط راهکار پیشنهادی و بر اساس نحوهی شکلگیری بردارهای ویژگی موجود در مجموعهی آموزش و آزمون میباشد. به این صورت که به کمک مجموعه آموزش و بر اساس ترتیب تصادفی که در هنگام تولید بردارهای ویژگی وجود داشته است، سیستم تعلیم میبیند و سپس بر اساس کل مجموعه آزمون مورد ارزیابی قرار میگیرد.

در حالت بعدی ما به منظور سنجش کارایی روش خود و پاسخ به چالش تغییر رفتار در ترافیک شبکه، نحوه‌ی شکل‌گیری نمونه‌ها و داده‌های ورودی را همانند حالت نخست در نظر می‌گیریم ولی برای ارزیابی عملکرد سیستم خود، نمونه‌های باتنت آزمونی که در مجموعه‌ی آموزش دیده نشده‌اند را به کار برده و سیستم طراحی شده را در قبال این نحوه‌ی ورود داده‌ها و مواجه با نمونه‌های دیده نشده (باتنت‌های گونه‌ی جدید) استفاده می‌کنیم. در واقع تا حدود ۴۴۰۰ نمونه‌ی اول مجموعه آموزشی، مشابه حالت اول به کار برده می‌شود، ولی برای نمونه‌های بعد از آن در میان داده‌ها، باتنت‌های نوع جدید در نظر گرفته می‌شود. بنابراین عملیات برچسب‌گذاری از بین نمونه‌های باتنت نوع جدیدی اتفاق می‌افتد که قبلا تنها در میان داده‌های آزمون وجود داشته‌اند.

در نهایت، حالت سوم به این صورت انجام می‌پذیرد که ما سیستم را بر اساس یک روند یادگیری فعال دیگر مورد ارزیابی قرار می‌دهیم. در واقع با تغییر در فرآیند یادگیری فعال و استفاده از سناریو مبتنی بر استخر تحت شرایط موجود در آزمایش دوم این حالت را اجرا می‌کنیم. رویکرد مورد استفاده در این روش این گونه است که از بین تمامی نمونه‌های بدون برچسب در هر تکرار از الگوریتم فعال نسبت به انتخاب ۲۰ نمونه‌ی برتر به صورت بدون جایگزینی اقدام شده و برای به‌روزرسانی مدل از آنها استفاده می‌نماید؛ به عبارتی دیگر در این آزمایش نحوه‌ی ورود داده‌های بدون‌برچسب به سیستم را طوری تغییر داده‌ایم که فرض در دسترس بودن تمام داده‌ها موجود و نمونه‌های انتخابی توسط سیستم حالت یکتایی داشته باشند. در واقع تفاوت اصلی این آزمایش با دو حالت قبلی در روند کلی سیستم تشخیص خواهد بود؛ به این صورت که فرض می‌کنیم استخری از نمونه‌های بدون برچسب داریم و از بین تمامی آنها خبره اقدام به تصمیم‌گیری می‌نماید. در جدول ۶-۴ خلاصه‌ای از نحوه‌ی انجام آزمایش‌های مختلف به منظور ارزیابی سیستم ارائه شده است.

جدول ۴-۶. شرح ارزیابی آزمایش‌ها

آزمایش	توضیحات
آزمایش اول	خواندن نمونه‌ها بر اساس نحوه‌ی شکل‌گیری بردارهای ویژگی موجود در مجموعه‌ی آموزش و آزمون می‌باشد به گونه‌ای که بات‌نت‌های جدید در مجموعه آزمون وجود دارند.
آزمایش دوم	تعدادی از نمونه‌های بات‌نت در مجموعه آزمون برای سنجش کارایی سیستم به کار برده می‌شود تا در قبال گونه‌های جدید مورد ارزیابی قرار گیرد و روند افزایشی در بستر راهکار پیشنهادی نشان داده شود.
آزمایش سوم	با تغییر روند یادگیری فعال و استفاده از سناریوی مبتنی بر استخر، تحت شرایط موجود در آزمایش دوم از بین تمامی نمونه‌های بدون برچسب، در هر تکرار از الگوریتم، نسبت به انتخاب ۲۰ نمونه‌ی برتر به صورت بدون جایگزینی اقدام می‌شود.

معیار ارزیابی در این پژوهش دو معیار معمول دقت رده‌بندی و معیارF می‌باشد، که به ترتیب در (رابطه ۴-۱) و (رابطه ۴-۳) مشاهده می‌شود. همانطور که مشخص است، معیارF خود از (رابطه ۴-۲) بدست می‌آید که در آن صحت (دقت)[1] از طریق حاصل تقسیم تعداد نمونه‌های بات‌نتی که به درستی شناسایی شده‌اند به کل شناسایی درست و نادرست نمونه‌های بات بوده و معیار فراخوانی (یادآوری)[2] که به عنوان نرخ تشخیص درست[3] نیز از آن یاد می‌شود، بیانگر نسبت تعداد بات‌نت‌های به درستی شناسایی بر تعداد بات‌نت‌های موجود، خواهد بود که در اغلب مقالات نیز از این رابطه به منظور تشخیص بات‌نت استفاده می‌گردد. در واقع این معیار میانگینی بین دقت و یادآوری می‌باشد که در ارزیابی سیستم‌ها کارایی دارد. لازم به ذکر است که دقت رده‌بندی نیز بر اساس ماتریس درهم‌ریختگی ایجاد می‌شود که نسبت موارد

[1] Presision
[2] Recall
[3] True Positive Rate

حقیقی به کل حالات در نظر گرفته شده می‌باشد و در جدول ۴-۷ جزییات مربوط به آن آورده شده است.

$$Accuracy = \frac{TN + TP}{TN + FN + TP + FP}$$ (رابطه ۴-۱)

$$Precision = \frac{TP}{TP + FP}, Recall = \frac{TP}{TP + FN}$$ (رابطه ۴-۲)

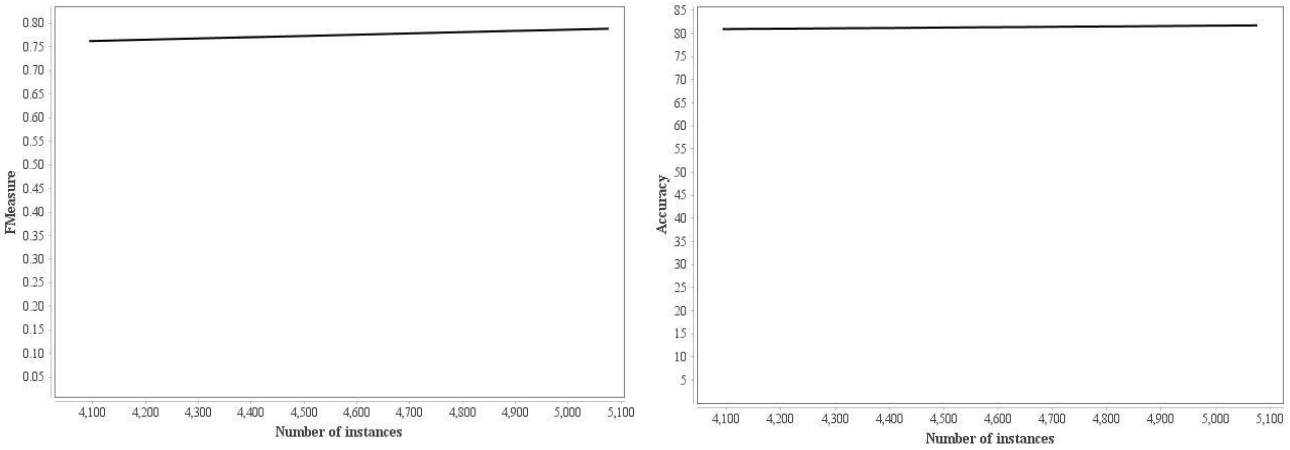
$$Fmeasure = 2 * \frac{Percision * Recall}{Percision + Recall}$$ (رابطه ۴-۳)

جدول ۴-۷. ماتریس درهم‌ریختگی

		کلاس تخصیص یافته توسط مدل	
		مثبت	منفی
کلاس واقعی	مثبت	مثبت حقیقی (TP)	منفی کاذب (FN)
	منفی	مثبت کاذب (FP)	منفی حقیقی (TN)

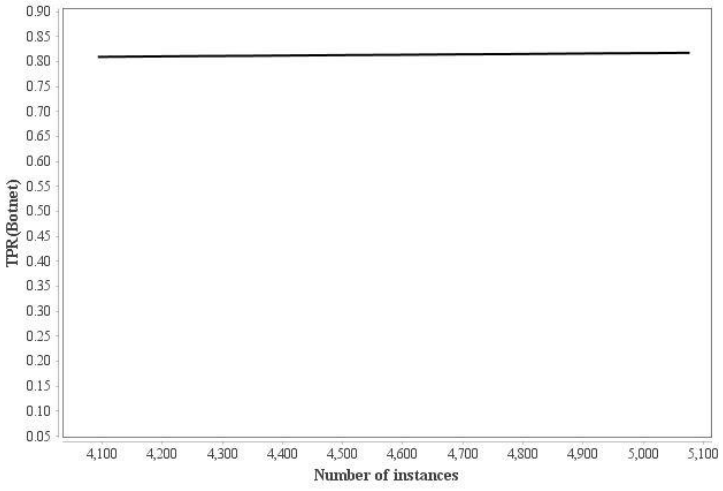
آزمایش اول: همانطور که توضیح داده شد، نحوه‌ی ورود نمونه‌ها به سیستم بر اساس همان ترتیبی خواهد بود که بسته‌ها در مجموعه‌ی آموزش و آزمون وجود داشته‌اند. در واقع پس از ورود داده‌ها به سیستم در ابتدا فرآیند نمونه‌برداری تصادفی برای ساخت دو مجموعه دارای برچسب و بدون برچسب آغاز می‌شود. بر روی مجموعه برچسب‌دار ساخت مدل اولیه انجام می‌پذیرد و سپس از بین نمونه‌های بدون برچسب آنهایی که خبره و رده‌بند کلاس آنها را مشخص می‌نماید، طی یک فرآیند افزایشی برای به روز رسانی مدل اقدام می‌شود. جهت ارزیابی روش پیشنهادی نیز مطابق با نحوه‌ی شکل‌گیری بسته‌ها در مجموعه آزمون، استفاده می‌گردد. نتایج حاصل از ارزیابی در نمودارهای شکل ۴-۱ (قسمت‌های الف

و ب) آورده شده است. میزان دقت رده‌بندی در هر تکرار الگوریتم روندی ثابت و به طور متوسط مقدار آن برابر ۸۱/۳۰٪ است و مقدار معیار F نیز با میانگین مقدار ۷۷/۲۰٪ و همچنین نرخ تشخیص ۸۱/۱۳٪ برای این آزمایش مطابق نمودار شکل ۴-۲ بدست آورده شد.



الف) نمودار دقت رده‌بندی در آزمایش اول **ب) نمودار معیار F در آزمایش اول**

شکل ۴-۱. نمودار دقت و معیار F در آزمایش اول



شکل ۴-۲. نمودار نرخ تشخیص درست(بات‌نت) در آزمایش اول

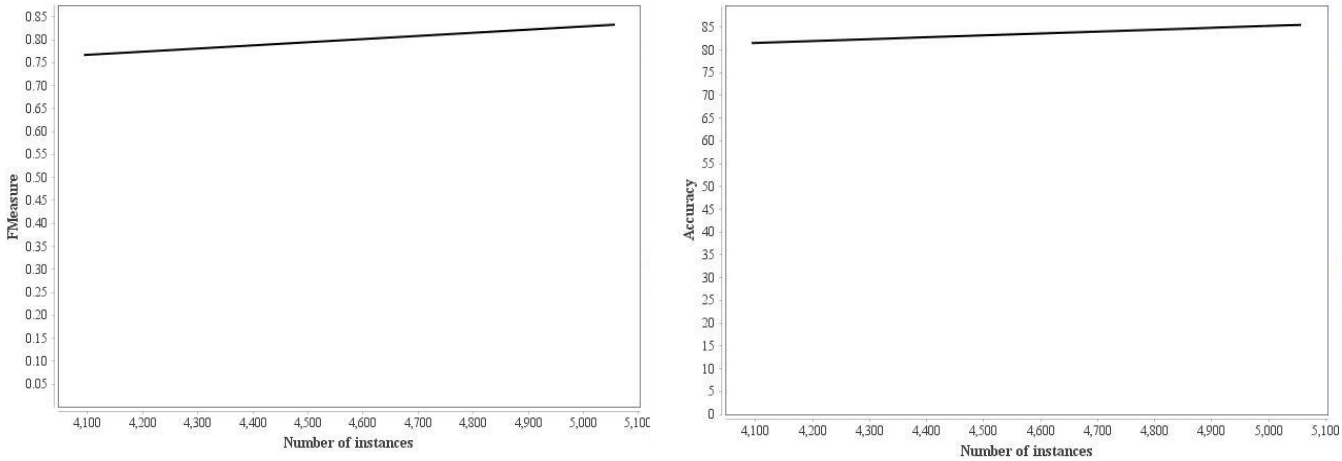
در نمودار شکل ۴-۱ قسمت الف، محور افقی تعداد نمونه‌های برچسب‌دار شده می‌باشد که سیستم در هر بار از اجرای الگوریتم فعال نیمه‌نظارتی نسبت به تعیین برچسب نمونه‌ها به کمک پرسش از خبره و

همچنین رده‌بندها اقدام می‌کند و محور عمودی دقت تشخیص نمونه‌ها (بسته‌های سالم و باتنت) را نشان می‌دهد و به همین صورت در قسمت ب محور افقی یکسان و محور عمودی نشان‌دهنده‌ی معیار F است که میانگین حالات بین دقت و یادآوری می‌باشد و توازنی را بین آنها ایجاد می‌نماید. نمودار شکل ۴-۲ بیانگر نرخ تشخیص درست باتنت است و در محور افقی تعداد نمونه‌های برچسب خورده توسط خبره و رای اکثریت رده‌بندها است و محور عمودی نیز نسبت تعداد باتنت‌های به درستی شناسایی شده بر تعداد باتنت‌های موجود خواهد بود.

همانطور که در نمودارهای مفروض مشخص است، با اضافه شدن نمونه‌ها به مدل ساخته شده، نرخ تشخیص، دقت رده‌بندی و معیارF با شیب تقریبا ثابتی ایجاد شده است؛ یعنی سیستم در همان ابتدا با آموزش نمونه‌های اولیه، کارایی قابل قبولی داشته است و با افزایش تعداد نمونه‌های برچسب خورده، حالت پایداری را ارائه می‌دهد. در واقع از مزیت‌های این سیستم آموزش با داده‌های اولیه محدود و کاهش هزینه‌های برچسب‌گذاری در روند شناسایی در سیستم‌های تشخیص می‌باشد.

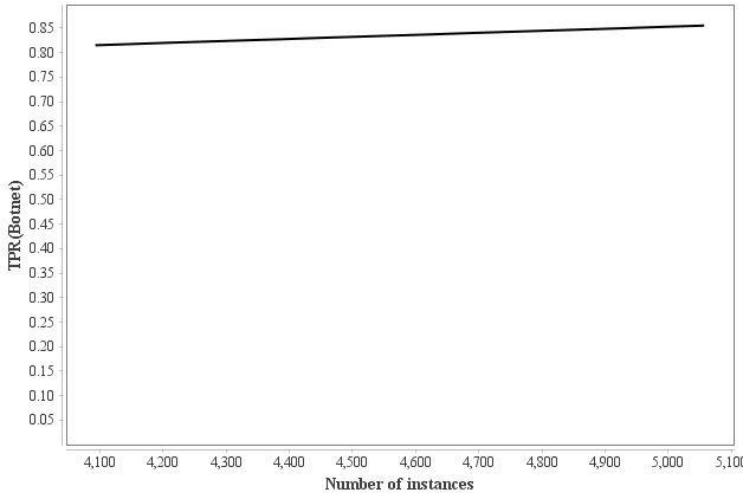
آزمایش دوم: در این آزمایش، همانطور که اشاره شد، به منظور ارزیابی کارایی سیستم، در مجموعه آموزش تعدادی از باتنت‌های جدید مجموعه آزمون استفاده می‌گردد، به عبارتی دیگر تا حدود ۴۴۰۰ نمونه‌ی اول مجموعه آموزشی، مشابه آزمایش اول به کار برده می‌شود، ولی برای نمونه‌های بعد از آن در میان داده‌ها، باتنت‌های نوع جدید در نظر گرفته می‌شود. هدف اصلی از انجام این کار سنجش میزان توسعه‌پذیری سیستم و کارایی سیستم در قبال نمونه‌های جدید است تا بتواند بر اساس یک سناریوی مبتنی جریان داده برخط، نسبت به انتخاب نمونه‌های مفید اقدام نمایید. به این صورت که با ۱۰ درصد از نمونه‌هایی که شامل گونه‌های جدید باتنت هستند برای آموزش اولیه و ساخت مدل اقدام می‌شود و از مابقی داده‌ها طی یک فرآیند فعال نیمه‌نظارتی، انتخاب به عمل آمده و سپس برای به روز رسانی مدل استفاده می‌شوند.

همانطور که در نمودارهای شکل ۴-۳ (قسمت‌های الف وب) و شکل ۴-۴ مشاهده می‌شود، دقت رده‌بندی، معیارF و نرخ تشخیص در مقایسه با حالت قبلی با شیب ملایمی رو به افزایش است که نشان‌دهنده‌ی کارایی الگوریتم یادگیری می‌باشد.



الف) نمودار دقت رده‌بندی در آزمایش دوم **ب) نمودار معیارF در آزمایش دوم**

شکل ۴-۳. نمودار دقت رده‌بندی و معیار F در آزمایش دوم



شکل ۴-۴.نمودار نرخ تشخیص درست(بات‌نت) در آزمایش دوم

همچنین از نمودارها می‌توان برداشت کرد که سیستم با مشاهده‌ی بات‌نت‌های گونه جدید نسبت به روز رسانی مدل خود اقدام کرده و در قبال حملات جدید تعمیم‌پذیری مناسبی داشته باشد و تا حد

قابل قبولی آنها را به درستی تشخیص دهد؛ یعنی با اضافه شدن نمونه‌های جدید از حدود ۴۴۰۰ به بعد که بات‌نت‌های گونه جدید هستند و خبره برچسب آنها را اعلام کرده، سیستم نسبت به حالت قبلی بهبود پیدا می‌کند و می‌تواند آنها را تشخیص دهد. مقدار دقت رده‌بندی در این حالت به طور متوسط ۸۳٪/۳۷ و مقدار معیار F مقدار ۷۹/۹۸٪ را نشان می‌دهد. همچنین نرخ تشخیص در این آزمایش مقدار ۸۳٪/۱۱ می‌باشد.

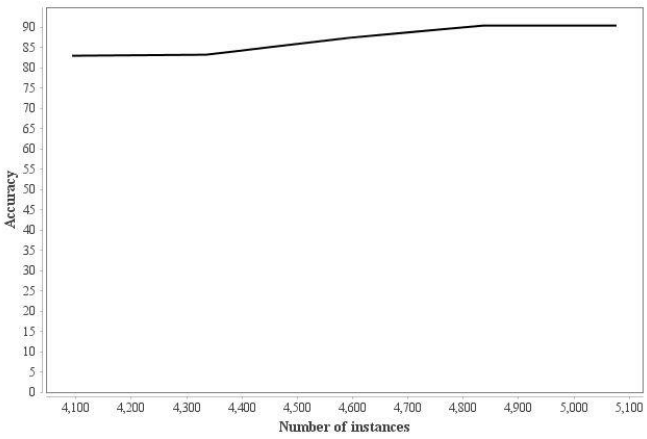
در خصوص نمودارها همانند آزمایش اول، در شکل ۴-۳ قسمت الف محور افقی تعداد نمونه‌های برچسب‌دار شده می‌باشند که سیستم در هر بار از اجرای الگوریتم فعال نیمه‌نظارتی نسبت به تعیین برچسب نمونه‌ها به کمک پرسش از خبره و همچنین رای اکثریت رده‌بند اقدام می‌کند و محور عمودی دقت تشخیص نمونه‌ها (بسته‌های سالم و بات‌نت) را نشان می‌دهد و در قسمت ب محور افقی معیار F را نشان می‌دهد. در نهایت نمودار شکل ۴-۴ که نرخ تشخیص درست بات‌نت را بازگو می‌کند و دارای محور افقی مشابه با دو نمودار قبلی و محور عمودی آن که نمایانگر دقت تشخیص بات‌نت می‌باشد.

برخلاف آزمایش اول که دقت‌های حاصل شده تقریبا روندی ثابت یا شیب کندی را داشته‌اند، در آزمایش دوم، این وضعیت متفاوت و سیستم در قبال بات‌نت‌های جدید اقدام به یادگیری می‌نماید و با به روز رسانی مدل خود کارایی بهتری را نشان می‌دهد. همچنین نتایج بدست آمده از این آزمایش بهبود دقت رده‌بندی، معیار F و نرخ تشخیص درست بات‌نت را بازگو می‌نماید. به طور کلی هدف اصلی از انجام این آزمایش ارزیابی تعمیم‌پذیری سیستم تشخیص پیشنهادی می‌باشد، به گونه‌ای که در قبال حملات جدید چگونه رفتار می‌کند. بنابراین این انتظار وجود دارد که سیستم با ذخیره‌سازی برچسب نمونه‌های جدید بتواند در صورت مشاهده‌ی دوباره این نوع از بات‌نت‌ها با دقت بیشتری نسبت به شناسایی اقدام نماید.

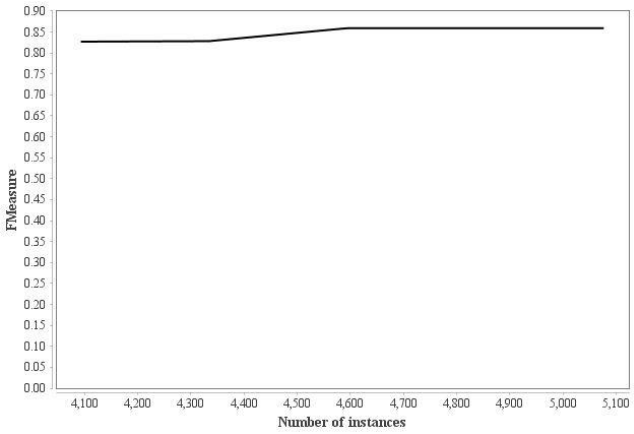
آزمایش سوم: در این آزمایش ما روند انتخاب نمونه‌ها را بر اساس یک سناریوی یادگیری فعال دیگر به کار می‌گیریم. در این رویکرد ما از سناریوی مبتنی بر استخر داده‌ها استفاده می‌کنیم، به این صورت

که از بین تمامی نمونه‌های موجود در استخر (نمونه‌های بدون برچسب)، نسبت به انتخاب ۲۰ نمونه برتر در هر تکرار از الگوریتم به صورت بدون جایگزینی اقدام کرده و سپس مدل را با توجه به نمونه‌های انتخاب جدید به روز رسانی می‌نماییم. در واقع این آزمایش همانند آزمایش دوم می‌باشد با این تفاوت که روند انتخاب نمونه‌ها بر اساس یک سناریو دیگر اتفاق می‌افتد و سیستم در قبال بات‌نت‌های جدیدی که تا به حال مشاهده نکرده است مورد ارزیابی قرار می‌گیرد. هدف اصلی از انجام این آزمایش کارایی سیستم در تغییر روند یادگیری فعال و با فرض داشتن استخری از نمونه‌های بدون برچسب است که در میان آنها بات‌نت‌های گونه‌ی جدید نیز وجود دارد و توانایی سیستم در انتخاب مناسب نمونه‌ها و برچسب‌گذاری مورد تحلیل قرار می‌گیرد.

نمودارهای بدست آمده از این آزمایش در شکل ۴-۵ (قسمت‌های الف و ب) و شکل ۴-۶ آورده شده است. همانطور که مشاهده می‌شود دقت رده‌بندی با افزایش خوبی همراه بوده است و توانسته به دقتی نزدیک به ۹۰٪ دست یابد. یعنی سیستم توانسته حملات جدید را طی یک فرآیند یادگیری فعال نیمه‌نظارتی مبتنی بر استخر داده‌ها به خوبی رده‌بندی نماید. متوسط دقت رده‌بندی در این آزمایش ۸۹٪/۸۵ و مقدار F مقدار ۸۵٪ بدست آورده شد. میزان نرخ تشخیص نیز در این آزمایش مقدار ۸۹/۷٪ بدست آورده شد.

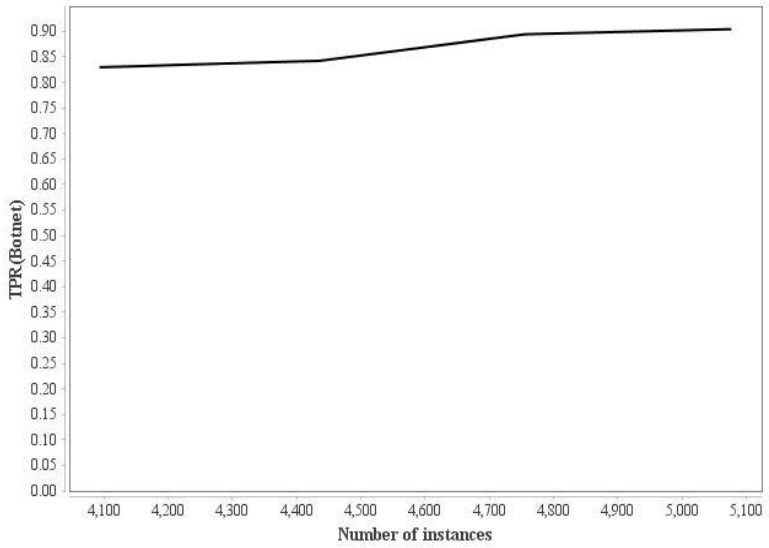


الف) نمودار دقت رده‌بندی در آزمایش سوم



ب) نمودار معیار F در آزمایش سوم

شکل ۴-۵. نمودار دقت رده‌بندی و معیار F در آزمایش سوم



شکل ۴-۶. نمودار نرخ تشخیص درست(بات‌نت) در آزمایش سوم

همانطور که در نمودارهای حاصله از روند آزمایش سوم در شکل ۴-۵ (قسمت‌های الف و ب) و شکل ۴-۶ مشاهده می‌شود، دقت رده‌بندی مقدار معیار F و نرخ تشخیص روند افزایشی بیشتری را نسبت به آزمایش دوم ارائه می‌دهد. در واقع سیستم با مشاهده‌ی بات‌نت‌های جدید، انتخاب و برچسب‌گذاری آنها توسط خبره و رای اکثریت رده‌بندها، در نهایت توانسته است با به روز رسانی مدل‌ها روند بهتری را در پی داشته باشد. به عبارتی دیگر این موضوع نشان‌دهنده‌ی توانایی سیستم در به کارگیری نمونه‌های جدیدی در راستای آزمون و شناسایی حملات می‌باشد که به گونه‌ای که با ذخیره‌سازی الگوی آنها بتواند در مراحل بعدی برای شناسایی بهره ببرد.

حال به منظور مقایسه کلی بین حالات مختلف آزمایش، مشاهده شد که دقت رده‌بندی در آزمایش اول با توجه به نمونه‌های آموزش و آزمونی که سیستم آنها را مشاهده می‌نماید با میزان رشد کمتری نسبت به آزمایش دوم وسوم همراه بوده است و با همان آموزش اولیه، توانسته نسبت به شناسایی اقدام نماید. از سوی دیگر ما به منظور نمایش کارایی سیستم خود و قابلیت رده‌بندی بات‌نت‌های جدید نسبت به انجام آزمایش دوم اقدام کردیم. نتایج حاصل از این آزمایش نشان‌دهنده‌ی رشد دقت رده‌بندی با افزایش نمونه‌های جدید برچسب‌دار همراه خواهد بود و در نهایت آزمایش سوم که در واقع همان آزمایش

دوم است با این تفاوت که از سناریوی یادگیری فعال دیگری استفاده می‌کند. در واقع در این آزمایش سعی در ارزیابی کارایی سیستم در صورت وجود مجموعه کاملی از نمونه‌های بدون برچسب می‌باشد.

به طور کلی با توجه به آزمایش‌های انجام گرفته می‌توان دقت رده‌بندی سیستم را در حالت سناریوی مبتنی بر جریان برخط ۸۳/۳۷٪ و در حالت مبتنی بر استخر داده‌ها ۸۹/۸۵٪ گزارش نمود.

۴-۳ مقایسه

با توجه به جامعیت مجموعه داده‌ی مورد استفاده در این پژوهش، سیستم‌های مشابه‌ی محدودی به منظور مقایسه با آن وجود دارد. به همین دلیل ما به منظور ارزیابی راهکار پیشنهادی خود با توجه به ساخت مجموعه ویژگی‌های مختلف که در فصل سوم، بخش ۳-۲ شرح داده شد، نسبت به مقایسه‌ی آنها با یکدیگر از طریق اجرای سیستم پیشنهادی اقدام کردیم.

لازم به ذکر است که مجموعه ویژگی‌های مفروض بر اساس اجرای تنظیماتی یکسان با سیستم طراحی شده در بخش تولید جریان‌های ترافیکی و همچنین مراحل یادگیری فعال نیمه‌نظارتی به انجام رسیدند. در واقع ما به منظور انجام مقایسه‌ای قابل اعتماد نسبت به انتخاب جریان‌های TCP به همراه پروتکل‌های مقصد ۸۰ و اندازه‌ای بزرگ‌تر از ۱۰ اقدام کردیم و خروجی‌هایی مشابه با مجموعه ویژگی پایه از نظر تعداد نمونه‌ها (بردارهای ویژگی) بدست آوریم که اطلاعات مربوط به این بردارهای ویژگی در جدول ۴-۴ مشاهده شد. در ادامه به منظور مقایسه راهکار پیشنهادی بر روی مجموعه ویژگی‌های مختلف، آزمایش‌های مطرح شده در بخش قبلی را انجام می‌دهیم.

۴-۳-۱ مقایسه نتایج مجموعه ویژگی‌ها در اجرای آزمایش‌ها

نتایج حاصل از اعمال فرآیند یادگیری فعال نیمه‌نظارتی آزمایش اول در جدول ۴-۸ آورده شده است. همانطور که مشاهده می‌گردد مجموعه ویژگی پایه وضعیت بهتری را نسبت به سایر مجموعه ویژگی‌های

دیگر در این راهکار به خود اختصاص داده است. از سوی دیگر به کارگیری سیستم پیشنهادی بر روی مجموعه ویژگی‌های مفروض دقت رده‌بندی مناسبی را نیز به همراه داشته است، هرچند که در این مقالات به جز مجموعه ویژگی ISCX2014، نویسندگان از مجموعه داده‌های بات‌نت متفاوتی در مقایسه با این پژوهش استفاده کرده‌اند که جامعیت مجموعه داده‌ی استفاده شده در این پژوهش را ندارند.

جدول ۴-۸. مقایسه دقت پژوهش با سایر مجموعه ویژگی‌ها در آزمایش اول

نام مجموعه ویژگی	دقت رده‌بندی فعال نیمه‌نظارتی	معیار امتیاز F	نرخ تشخیص (بات‌نت)
Milcom2015	۸۱/۱۰	۷۶/۳۵	۸۱
CIC2018	۸۱	۷۷	۸۱/۰۹
Li2009	۶۶/۴	۶۵/۰	۶۶/۰
ISCX2014	۸۰/۷۷	۷۲/۰	۸۰/۸
Qiu2017	۸۱/۳۰	۷۷/۲۰	۸۱/۱۳

در جدول ۴-۹ نتایج حاصل از مقایسه مجموعه ویژگی‌ها تحت اجرای آزمایش دوم ارائه گردیده است. همانطور که مشاهده می‌شود در دقت رده‌بندی مجموعه ویژگی پایه شرایطی بهتری را در این آزمایش نیز ارائه داده است و می‌تواند در بستر پویای ترافیک شبکه قابلیت بهتری را از خود نشان دهد. در واقع رویکرد اصلی در این آزمایش برخورد سیستم با نمونه‌های جدید بود که پس از آموزش و ذخیره‌سازی مشخصه‌ی آنها می‌تواند دقت عملکرد خود را در شناسایی این گونه بات‌نت‌ها افزایش دهد.

جدول ۴-۹. مقایسه دقت پژوهش با سایر مجموعه ویژگی‌ها در آزمایش دوم

نام مجموعه ویژگی	دقت رده‌بندی فعال نیمه‌نظارتی	معیار امتیاز F	نرخ تشخیص (بات‌نت)
Milcom2015	۸۲/۸۱	۸۰	۸۲
CIC2018	۸۲/۹۵	۸۱	۸۱
Li2009	۷۲/۴۰	۷۰/۵	۷۱/۲
ISCX2014	۸۱/۰۶	۸۲	۸۱
Qiu2017	۸۳/۳۷	۷۹/۹۸	۸۳/۱۱

و در نهایت نتایج حاصل از مقایسه مجموعه ویژگی‌ها تحت اجرای آزمایش سوم در جدول ۴-۱۰ ارائه گردیده است. در این رویکرد همانطور که عنوان شد، فرض بر این است که تمامی نمونه‌های بدون برچسب در دسترس هستند و ما می‌خواهیم نسبت به انتخاب تعدادی از نمونه‌های برتر و یکتا اقدام کنیم. همانطور که در جدول مذکور مشاهده می‌شود، نتایج به نسبت به حالت قبلی وضعیت بهتری را پیدا کرده است چرا که سیستم در حالتی در نظر گرفته شده که استخری از نمونه‌های بدون برچسب موجود است و فرض بر این می‌باشد که در هر مرحله از اجرای الگوریتم نمونه‌های مفید مطابق با راهبرد یادگیری فعال انتخاب شده و سپس برای به روز رسانی مدل استفاده می‌شود. اما در دو حالت قبلی رویکرد مبتنی بر جریان برخط بود که در هر مرحله تنها به اندازه پنجره در نظر گرفته شده، امکان انتخاب نمونه‌های مناسب وجود داشت.

جدول ۴-۱۰. مقایسه دقت پژوهش با سایر مجموعه ویژگی‌ها دیگر در آزمایش سوم

نام مجموعه ویژگی	دقت رده‌بندی فعال نیمه‌نظارتی	معیار امتیاز F	نرخ تشخیص (بات‌نت)
Milcom2015	۸۸/۱	۸۱/۱۵	۸۱/۳۶
CIC2018	۸۴/۱۲	۸۲	۷۶
Li2009	۷۹/۱۲	۸۰/۱	۷۹/۲
ISCX2014	۸۳/۱۱	۸۱/۲۳	۷۵/۵۵
Qiu2017	۸۹/۸۵	۸۵	۸۹/۷

۴-۳-۲ مقایسه با پژوهش مشابه

با توجه به نتایج بدست آمده از اعمال فرآیندهای مختلف یادگیری بر روی مجموعه داده ISCX ، میزان نرخ تشخیص درست بات‌نت در مرجع [۱۵] که از مجموعه داده‌ی مشابه با این پژوهش استفاده کرده است، در بالاترین حالت ۷۵ درصد گزارش شده است، همچنین مرجع [۶۱] بر روی مجموعه داده‌ای مشابه به کمک یک رویکرد افزایشی مبتنی بر نزدیک‌ترین همسایه در بالاترین حالت نرخ تشخیص ۸۸/۷۷ ارائه داده است، در صورتی که سیستم پیشنهادی در این پژوهش به کمک یادگیری فعال نیمه‌نظارتی توانست در بالاترین حالت به دقت تشخیص(۸۹/۷) درصد دست یابد.

از سوی دیگر با توجه به چالش‌های موجود در سیستم‌های تشخیص همانند کمبود داده‌های برچسب خورده، هزینه‌های زیاد عملیات برچسب‌گذاری برای تمام داده‌ها، مجموعه ویژگی‌هایی با ابعاد زیاد برای فرآیند آموزش و اعمال مراحل پیش‌پردازشی بر روی داده‌ها و همچنین مواجه با حملات گونه جدید، سیستم طراحی شده این پژوهش توانست با در نظر گرفتن آنها، راهکار مناسبی را به کمک یادگیری

فعال نیمه‌نظارتی برای بهبود شرایط فعلی ارائه دهد. این موضوع نشان‌دهنده‌ی قابلیت تعمیم‌پذیری سیستم، صرفه‌جویی در هزینه‌های برچسب‌گذاری، کاربرد در سیستم‌های برخط و ارائه‌ی یک مجموعه ویژگی متفاوت و موثر که تنها از اندازه بسته‌ها و جهت ارسال کمک می‌گیرد، خواهد بود.

فصل ۵ : نتیجه گیری و پژوهش های آینده

۵-۱ نتیجه‌گیری

داشتن یک سیستم تشخیص بات‌نت قابل اعتماد نیاز به مشخصات ویژه‌ای دارد، اینکه بتواند در زمان مناسب و با کارایی بالا، نسبت به شناسایی جریان‌های مشکوک و حملات مختلف اقدام نماید، بسیار حائز اهمیت خواهد بود. همچنین پارامترهایی مانند ویژگی‌های آموزشی و نحوه‌ی رده‌بندی داده‌ها از دیگر موارد است که باید مورد توجه قرار گیرد. برخورداری از مجموعه آموزشی جامع به منظور یادگیری مدل‌ها برای تشخیص حملات، کاهش در هزینه‌های بخش برچسب‌گذاری و تعمیم‌پذیری سیستم نیز از دیگر مشخصه‌های مورد نیاز در این سیستم‌ها به شمار می‌آید.

به طور کلی از آنجایی که عملیات برچسب‌گذاری داده‌ها در سیستم‌های تشخیص بات‌نت نیاز به یک راهکار سریع و مقرون به صرفه‌ای دارد، در این پژوهش به کمک روش فعال نیمه‌نظارتی نسبت به کاهش هزینه‌های مرتبط با آن و همچنین انتخاب نمونه‌های موثر، به منظور به کارگیری در کاربردهای دنیای واقعی اقدام کردیم. در واقع با ایجاد سیستمی که مبتنی بر جریان داده برخط فعالیت می‌کند، نسبت به انتخاب نمونه‌های مفید و آنهایی که ارزش اطلاعاتی بالاتری دارند، تحت یک سری شرایط خاص همانند حد آستانه و در نظر گرفتن بیشترین ارزش نمونه‌ها اقدام کرده و با اعمال برچسب مناسب به نمونه‌های انتخاب شده، راه‌حل بهینه‌ای را در این راستا در نظر گرفتیم. از سوی دیگر به منظور رفع چالش ماهیت پویای ترافیک شبکه، از طریق اجرای یک فرآیند جریان‌داده‌ای برخط که در آن داده‌ها به صورت پنجره‌ای وارد سیستم می‌شوند، نسبت به به روز رسانی مدل‌های یادگیری طی یک روند افزایشی اقدام کردیم که در نهایت سبب بهبود کارایی سیستم در قبال مشاهده‌ی بات‌نت‌های گونه جدید گردید.

بهره‌مندی از یک مجموعه ویژگی قابل اطمینان با هدف شناسایی موثر بات‌نت‌ها از طریق انجام مراحل پیش‌پردازشی بر روی دو ویژگی اندازه و جهت ارسال بسته‌ها، از دیگر مزیت‌های این سیستم پیشنهادی به شمار می‌آید. لازم به ذکر است که ما به منظور ساخت بردارهای ویژگی روندی مشابه به فرآیند کلی

یادگیری فعال نیمه‌نظارتی را در پیش گرفتیم که در آن دو مجموعه داده‌ی برچسب‌دار و بدون برچسب تشکیل می‌گردد و در هنگام انجام محاسبات ریاضی و شمارش تکرار نمونه‌ها این خاصیت نیز در نظر گرفته می‌شود. نتیجه‌ی کار سبب ایجاد مجموعه ویژگی متفاوت با ۲۳۰ بُعد گردید که در تشخیص موثر حملات مفید واقع شدند. استفاده از مجموعه ویژگی تحت عنوان داده‌های خام در هنگام انتخاب نمونه‌های برتر، نیز از دیگر مشخصه‌های در نظر گرفته شده در این سیستم پیشنهادی می‌باشد.

به طور کلی ما پس از ساخت مجموعه ویژگی‌هایی که مبتنی بر ویژگی‌های آماری هستند، برای اجرا در یک روند یادگیری فعال نیمه‌نظارتی استفاده کردیم. لازم به یادآوری است که رویکرد مفروض جزء نخستین راهکارهای ارائه شده در مسائل تشخیص بات‌نت به شمار می‌آید. رده‌بندی داده‌ها توسط الگوریتم گروهی و به کمک سه رده‌بند رگرسیون لجستیک و ماشین بردار پشتیبان خطی که مبتنی بر گرادیان نزولی نسبت به بهینه‌سازی وزن‌ها اقدام می‌کنند و همچنین بیز ساده افزایشی انجام پذیرفت. خروجی کار این رده‌بندها سبب می‌شود که مدل یادگیری خود را با توجه به نمونه‌های جدیدی که مشاهده می‌کند به روز رسانی نماید. ما در اجرای فرآیند یادگیری فعال نیمه‌نظارتی به منظور انتخاب نمونه‌های برتر از راهبردهای پرس‌وجو فعال استفاده کردیم و بر اساس راهبرد میزان آنتروپی بین داده‌ها، نسبت به برچسب‌گذاری داده‌ها اقدام کردیم. نتایج حاصل شده نشان‌دهنده‌ی مقبولیت این راهکار در مقایسه با سایر پژوهش‌های مشابه است. در واقع ما توانستیم که با داشتن تنها اندازه بسته‌ها، مستقل از سایر ویژگی‌ها نسبت به تشخیص بات‌نت‌ها و جریان‌های حمله در یک فرآیند یادگیری فعال نیمه‌نظارتی که با کاهش هزینه‌ها نیز همراه است، اقدام کنیم.

علاوه بر این، ما به منظور دستیابی به یک ارزیابی معتبر از عملکرد واقعی سیستم که در میان پژوهش‌های انجام شده کمتر مشاهده شده است، تحلیل سیستم خود را به کمک یک مجموعه داده‌ی جامع و معتبر که دارای درجه‌ی بالایی از تنوع بانت‌ها می‌باشد، انجام دادیم. سیستم ارائه شده در این

پژوهش به کمک یادگیری فعال نیمه‌نظارتی توانست در بالاترین حالت به دقت رده‌بندی نزدیک به ۹۰ (۸۹,۸۵) درصد دست یابد.

از مهم‌ترین مزیت‌ها و نوآوری سیستم ارائه شده، عدم وابستگی به نمونه‌های آموزشی زیاد با توجه به هزینه‌های گزاف برچسب‌گذاری و نقصان داده‌های دارای برچسب خواهد بود. همچنین از سوی دیگر رویکرد جریان داده‌ای هنگام ساخت مجموعه ویژگی و انتخاب نمونه‌های مناسب و اجرای یک فرآیند افزایشی با هدف توسعه و بهبود کارایی با توجه به مشاهده‌ی نمونه‌های جدید در مرحله آموزش از جمله مشخصه‌های حائز اهمیت سیستم پیشنهادی می‌باشد. به این صورت که سیستم در حین اجرا دائما رده‌بندهای خود را با توجه نمونه‌های جدیدی که مشاهده می‌کند، به‌روز رسانی می‌نماید. استفاده از یادگیری گروهی و سپس رای اکثریت برای ساخت مدل‌ها و در نهایت نحوه‌ی انتخاب نمونه‌های برتر که با اعمال حد آستانه، بررسی نمونه‌هایی با تعداد ویژگی کمتر و بهره‌گیری از نتایج رده‌بندها صورت می‌پذیرد، از دیگر نوآوری‌های سیستم پیشنهادی می‌باشد.

۵-۲ پژوهش‌های آینده

از آنجایی یکی از ملزومات سیستم‌های تشخیص بات‌نت، قابلیت تشخیص به صورت برخط و کارایی آن در کاربردهای دنیای واقعی می‌باشد، بنابراین طراحی سیستم‌هایی که بتوانند به خوبی در ماهیت ترافیک شبکه کار کنند، از جمله خواسته‌های پژوهشگران و طراحان نرم‌افزارهای امنیتی به شمار می‌رود. بهبود دقت تشخیص و کاهش نرخ هشدار نادرست از دیگر مواردی است که در این سیستم‌ها باید در نظر گرفته شود. از سوی دیگر با توجه به حجم وسیع داده‌ها و نیاز آنها به پاسخ سریع در مسائل رده‌بندی ترافیک شبکه، قابلیت‌های اجرای موازی و بهبود سرعت از جمله مسائلی پیش‌رو و در دست توسعه‌ی پژوهشگران این حیطه می‌باشد. به این منظور استفاده از رویکردهای پردازش موازی با هدف کاهش

زمان اجرا و بر طرف ساختن نیازمندی‌های زمانی سیستم‌های برخط، امروزه به عنوان یکی از ملزومات سیستم‌های تشخیص به شمار می‌آید.

ما در این پژوهش با طراحی سیستمی که به صورت جریان‌داده‌ای اقدام به دریافت و پردازش داده‌ها می‌نماید، نسبت به این ویژگی اقداماتی را انجام دادیم و به عنوان یکی از کارهای آینده‌ای که می‌تواند در این زمینه در نظر گرفته شود، بهبود کارایی در کاربردهای برخط و به کارگیری آن در جریان‌های ترافیکی شبکه است تا بتواند در دنیای واقعی به خوبی به کار گرفته شود. از سوی دیگر انجام پردازش‌های موازی و استفاده از چارچوب‌های توزیع شده، از دیگر مسائلی است که می‌تواند در اثربخشی سیستم نقش به سزایی داشته باشند.

از سوی دیگر دریافت داده‌ها به صورت جریان داده‌ای نیازمند مسائل مختلفی همچون شناسایی تغییرات مفهوم، داده‌های پرت و... خواهد بود که باید در نظر گرفته شوند. تعیین نقاط دارای تغییر مفهوم و تشخیص داده‌های پرت نیز می‌تواند در مسائل پیش‌پردازشی داده‌ها و ساخت مجموعه ویژگی‌های موثر در فرآیند شناسایی بات‌نت مورد استفاده قرار گیرد.

از دیگر نکاتی که به عنوان کارهای آینده می‌تواند مورد استفاده قرار گیرد، انجام فرآیندهای پیش‌پردازشی متفاوت بر روی مجموعه ویژگی‌ها می‌باشد. به عنوان مثال در نظر گرفتن جریان‌های ترافیکی بیشتر به جای انتخاب زیر مجموعه‌ای از آنها، به منظور انجام محاسبات احتمالاتی و بهره‌گیری از پروتکل‌های مختلف از جمله مهم‌ترین اقدامات در این زمینه خواهد بود. یکی از مشکلات مجموعه ویژگی‌های ارائه شده، افزایش نمونه‌هایی با اندازه صفر می‌باشد که می‌توان با بهره‌گیری از معیار کاهش ابعاد از ایجاد آنها جلوگیری نمود. همچنین استفاده از بسته‌های بیشتر از هر جریان به جای انتخاب تنها ۱۰ بسته‌ی نخست، به این صورت که از هر جریان تمامی بسته‌های بزرگ از ۱۰ انتخاب شده و سپس مقایسه‌ای بین هر ۱۰ بسته در هر جریان با یکدیگر به منظور کشف ویژگی‌های موثر به کار گرفته

شود. تمامی این اعمال به عنوان یکی دیگر از اقدامات تحت بررسی به منظور افزایش کارایی سیستم تشخیص باتنت می‌تواند مورد استفاده قرار گیرد.

در این پژوهش مجموعه ویژگی پایه با استفاده از دو ویژگی توانست به کمک مدل‌های احتمالاتی ۲۳۰ ویژگی تولید کند که نشان‌دهنده‌ی میزان اثر بخشی هر بردار ویژگی نسبت به حالت کلی داده‌ها است، به عبارت دیگر احتمال آن که یک بردار ویژگی دو بعدی یا تک بعدی، چقدر نسبت به پراکندگی و چگالی کلی داده‌ها اختلاف دارد، مدنظر خواهد بود. بنابراین انجام فرآیندهای رتبه‌بندی ویژگی‌ها و همچنین ادغام آنها با هدف کاهش ویژگی‌های تولید شده از دیگر اقدامات ما در این زمینه، می‌تواند در نظر گرفته شود. همچنین ترکیب ویژگی‌های مختلف از طریق افزودن سایر ویژگی‌های موثر در تشخیص باتنت، ایده‌ی مناسبی در بهبود کارایی سیستم در این حیطه خواهد بود.

با توجه به قابلیت توسعه‌پذیری بالای فرآیند یادگیری فعال، تغییر سناریوی فعال و همچنین نحوه‌ی پرسش خبره و راهبردهای پرس‌وجو از جمله کارهای آینده در این زمینه می‌تواند در نظر قرار گیرد. همچنین استفاده از نمونه‌های وزن‌دار برای انتخاب و ارسال برای خبره، به این صورت که اگر مقدار احتمالاتی یا فاصله‌ی نمونه‌ی بدون برچسب تا نمونه برچسب‌دار حد مناسبی را دارا باشد، مقدار وزن بالاتری به آن اختصاص یابد. استفاده از معیارهای مبتنی بر فاصله و انجام خوشه‌بندی به منظور کاهش پیچیدگی‌های محاسباتی از دیگر رویکردهای بهبود عملکرد سیستم در فرآیند یادگیری فعال خواهد بود. تعیین مقدار آستانه و انجام تنظیمات و مقایسه با فرآیندهای یادگیری بدون ناظر، با ناظر و همچنین گروهی با استفاده از رده‌بندهای مختلف از دیگر اقدامات ما برای انجام کارهای آینده می‌باشد.

از دیگر نکات مورد توجه می‌توان به کاهش نرخ تشخیص هشدار نادرست اشاره کرد که در سیستم‌های تشخیص باتنت حائز اهمیت می‌باشد. این موضوع می‌تواند با به کارگیری ویژگی‌هایی با وزن و اهمیت بیشتر به انجام برسد.

در واقع یکی از ضعف‌های سیستم پیشنهاد شده که می‌توان به آن اشاره نمود، افزایش نرخ هشدار نادرست است که از طریق نسبت داده‌های سالمی که باتنت تشخیص داده شده‌اند به کل داده‌هایی که باتنت شناسایی شده‌اند، محاسبه می‌گردد. به طور کلی افزایش نرخ هشدار نادرست، جزء چالش‌ها و مسائل موجود در سیستم‌های تشخیص می‌باشد که محققان در حال بهبود و ارائه‌ی راه‌حل‌های مختلفی به منظور کاهش آن هستند. از جمله عوامل تاثیرگذار در افزایش این موضوع بر روی سیستم پیشنهادی، می‌توان به انتخاب جریان‌های محدود شده به TCP اشاره کرد؛ چرا که این خصیصه بیشتر به منظور استفاده در تعیین و شناسایی ناهنجاری‌های موجود در بستر ترافیک شبکه کارایی دارد و بر اساس آن ترافیک سالم از ناسالم تعیین می‌گردد. از سوی دیگر ویژگی‌های اندازه و جهت ارسال هر چند که کارایی قابل قبولی را در سیستم ارائه دادند اما در کنار سایر ویژگی‌ها احتمالا تاثیرگذاری بیشتری را در بر خواهند داشت.

مراجع

[1] Zhuge, J. and Han, X. and Guo, J. and Zou, W. and Holz, T. and Zhou, Y. **(2007**), "Characterizing the IRC-based botnet phenomenon," *Peking University & University of Mannheim Technical Report*.

[2] Dhote, Y., Agrawal, S., & Deen, A. J. **(2015**). A survey on feature selection techniques for internet traffic classification. *In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on (pp. 1375-1380). IEEE.*

[3] Aliyev, V. (**2010**). Using honeypots to study skill level of attackers based on the exploited vulnerabilities in the network.

[4] Vormayr, G., Zseby, T., & Fabini, J. (**2017**). Botnet Communication Patterns. IEEE *Communications Surveys & Tutorials, 19(4), 2768-2796*.

[5] Yahyazadeh M. and Abadi M, (**2015**) "BotGrab: A negative reputation system for botnet detection," *Computer and Electrical Engineering, 41, pp 68-85.*

[6] Shafiq, M., Yu, X., Laghari, A. A., Yao, L., Karn, N. K., & Abdessamia, F. (**2016**). Network Traffic Classification techniques and comparative analysis using Machine Learning algorithms. *In Computer and Communications (ICCC), 2016 2nd IEEE International Conference on (pp. 2451-2455)*. IEEE.

[7] Zhang, J., Chen, C., Xiang, Y., & Zhou, W. (**2013**). Robust network traffic identification with unknown applications. *In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (pp. 405-414)*.

[8] ACM.Gu, G., Perdisci, R., Zhang, J., & Lee, W. **(2008**). BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection. *In USENIX security symposium (Vol. 5, No. 2, pp. 139-154).*

[9] Aburomman, A. A., & Reaz, M. B. I. (**2017**). A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & Security, 65, 135-152*.

[10] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (**2017**). Fuzziness based semi supervised learning approach for intrusion detection system. *Information Sciences, 378, 484-497*.

[11] Qiu, Z., Miller, D. J., & Kesidis, G. (**2017**). Flow based botnet detection through semi-supervised active learning. In *Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on* (pp. 2387-2391). IEEE.

[12] Settles, B. (**2012**). Active learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning, 6(1), 1-114.*

[13] Rajahalme, J., Conta, A., & Carpenter, B. (**2004**). S. Deering," IPv6 Flow Label Specification. RFC 3697, March.

[14] Kirubavathi, G., & Anitha, R. (**2016**). Botnet detection via mining of traffic flow characteristics. *Computers & Electrical Engineering, 50, 91-101*.

[15] Beigi, E. B., Jazi, H. H., Stakhanova, N., & Ghorbani, A. A. (**2014**). Towards effective feature selection in machine learning-based botnet detection approaches. *In Communications and Network Security (CNS), 2014 IEEE Conference on (pp. 247-255)*. IEEE.

[16] Alaei, P., & Noorbehbahani, F. (**2017**). Incremental anomaly-based intrusion detection system using limited labeled data. *In Web Research (ICWR), 2017 3th International Conference on (pp. 178-184)*. IEEE

[17] Saad, S., Traore, I., Ghorbani, A., Sayed, B., Zhao, D., Lu, W., ... & Hakimian, P. (**2011**). Detecting P2P botnets through network behavior analysis and machine learning.

In Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on (pp. 174-180). IEEE.

[18] Wang, W., Liu, J., Pitsilis, G., & Zhang, X. (**2016**). Abstracting massive data for lightweight intrusion detection in computer networks. *Information Sciences*.

[19] Aviv, A. J., & Haeberlen, A. (**2011**). Challenges in experimenting with botnet detection systems.

[20] Dromard, J., Roudiere, G., & Owezarski, P. (**2017**). Online and Scalable Unsupervised Network Anomaly Detection Method. *IEEE Transactions on Network and Service Management, 14(1), 34-47*.

[21] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (**2015**). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection, 9, 52-80*.

[22] Wysopal, C., Eng, C., & Shields, T. (**2010**). Static detection of application backdoors. *Datenschutz und Datensicherheit-DuD, 34(3), 149-155*.

[23] Saeed, I. A., Selamat, A., & Abuagoub, A. M. (**2013**). A survey on malware and malware detection systems. *International Journal of Computer Applications, 67(16)*.

[24] Horton, J., & Seberry, J. (**1997**). Computer Viruses An Introduction.

[25] Smith, C., Matrawy, A., Chow, S., & Abdelaziz, B. (**2009**). Computer worms: Architectures, evasion strategies, and detection mechanisms. *Journal of Information Assurance and Security, 4, 69-83*.

[26] Moffie, M., Cheng, W., Kaeli, D., & Zhao, Q. (**2006**). Hunting trojan horses. *In Proceedings of the 1st workshop on Architectural and system support for improving software dependability (pp. 12-17). ACM*.

[27] You, I., & Yim, K. (**2010**). Malware obfuscation techniques: A brief survey. *In Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on (pp. 297-300)*. IEEE.

[28] Chien, E. (**2005**). Techniques of adware and spyware. *In the Proceedings of the Fifteenth Virus Bulletin Conference, Dublin Ireland (Vol. 47)*.

[29] Savage, K., Coogan, P., & Lau, H. (**2015**). The evolution of ransomware. *Symantec, Mountain View.*

[30] Lopez, W., Guerra, H., Pena, E., Barrera, E., & Sayol, J. (**2013**). Keyloggers. *Florida International University*.

[31] Kemp, S. (**2017**). Digital in 2017: Global overview. We are social, 24.

[32] Li, W., Abdin, K., Dann, R., & Moore, A. (**2013**). Approaching real-time network traffic classification.

[33] Lashkari, A. H., Gil, G. D., Keenan, J. E., Mbah, K., & Ghorbani, A. A. (**2017**). A Survey Leading to a New Evaluation Framework for Network-based Botnet Detection. *In Proceedings of the 2017 the 7th International Conference on Communication and Network Security (pp. 59-66)*. ACM.

[34] Bejtlich, R., & Marcus J.. Ranum. (**2006**). Extrusion detection: security monitoring for internal intrusions. Addison-Wesley.

[35] Li, X., Duan, H., Liu, W., & Wu, J. (**2009**). Understanding the Construction Mechanism of Botnets. In *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on* (pp. 508-512). IEEE.

[36] Tsiatsikas, Z., Anagnostopoulos, M., Kambourakis, G., Lambrou, S., & Geneiatakis, D. (**2015**). Hidden in plain sight. SDP-Based covert channel for botnet communication. *In International Conference on Trust and Privacy in Digital Business (pp. 48-59). Springer, Cham*.

[37] Wang, P., Wu, L., Aslam, B., & Zou, C. C. (**2009**). A systematic study on peer-to-peer botnets. *In Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on (pp. 1-8)*. IEEE.

[38] Wang, P. and Sparks, S. and Zou, C.C. (**2010**), "An advanced hybrid peer-to-peer botnet," *Dependable and Secure Computing, 7, 2, pp. 113–127*.

[39] Payer, M. (**2016**). HexPADS: a platform to detect "stealth" attacks. *In International Symposium on Engineering Secure Software and Systems (pp. 138-154). Springer, Cham*.

[40] Sheikhpour, R., Sarram, M. A., Gharaghani, S., & Chahooki, M. A. Z. (**2017**). A survey on semi-supervised feature selection methods. *Pattern Recognition, 64, 141-158*.

[41] Noorbehbahani, F., Fanian, A., Mousavi, R., & Hasannejad, H. (**2017**). An incremental intrusion detection system using a new semi-supervised stream classification method. International Journal of Communication Systems, 30(4).

[42] Watkins, L., Beck, S., Zook, J., Buczak, A., Chavis, J., Robinson, W. H., ... & Mishra, S. (**2017**). Using semi-supervised machine learning to address the big data problem in DNS networks. *In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual (pp. 1-6)*. IEEE.

[43] Zhu, X., & Goldberg, A. B. (**2009**). Introduction to semi-supervised learning. *Synthesis lectures on artificial intelligence and machine learning, 3(1), 1-130*.

[44] Chapelle, O., Scholkopf, B., & Zien, A. (**2009**). Semi-supervised learning (chapelle, o. et al., eds.; 2006)[book reviews]. *IEEE Transactions on Neural Networks, 20(3), 542-542*.

[45] Zhu, X. (**2005**). Semi-supervised learning literature survey.

[46] Qiu, Z., Miller, D. J., & Kesidis, G. (**2017**). A maximum entropy framework for semisupervised and active learning with unknown and label-scarce classes. *IEEE transactions on neural networks and learning systems, 28(4), 917-933*.

[47] Han, W., Coutinho, E., Ruan, H., Li, H., Schuller, B., Yu, X., & Zhu, X. (**2016**). Semi-supervised active learning for sound classification in hybrid learning environments. *PloS one, 11(9), e0162075*.

[48] Olsson, F. (**2009**). A literature survey of active machine learning in the context of natural language processing.

[49] Stevanovic, M., & Pedersen, J. M. (**2013**). Machine learning for identifying botnet network traffic. *Aalborg University, Denmark*.

[50] Qiu, Z., Miller, D. J., & Kesidis, G. (**2015**). Detecting clusters of anomalies on low-dimensional feature subsets with application to network traffic flow data. *arXiv preprint arXiv:1511.01047*.

[51] Nadiammai, G. V., & Hemalatha, M. (**2014**). Effective approach toward Intrusion Detection System using data mining techniques. *Egyptian Informatics Journal, 15(1), 37-50*.

[52] Menahem, E., Elovici, Y., Amar, N., & Nakibly, G. (**2013**). ACTIDS: an active strategy for detecting and localizing network attacks. *In Proceedings of the 2013 ACM workshop on Artificial intelligence and security (pp. 55-66)*. ACM.

[53] Zhu, X., Zhang, P., Lin, X., & Shi, Y. (**2010**). Active learning from stream data using optimal weight classifier ensemble. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 40(6), 1607-1621.

[54] Lashkari, A. H., Draper-Gil, G., Mamun, M. S. I., & Ghorbani, A. A. (**2017**). Characterization of Tor Traffic using Time based Features. *In ICISSP (pp. 253-262)*.

[55] Celik, Z. B., Walls, R. J., McDaniel, P., & Swami, A. (**2015**). Malware traffic detection using tamper resistant features. *In Military Communications Conference, MILCOM 2015-2015 IEEE (pp. 330-335). IEEE*.

[56] Moore, A., Zuev, D., & Crogan, M. (**2013**). Discriminators for use in flow-based classification.

[57] Li, W., Canini, M., Moore, A. W., & Bolla, R. (**2009**). Efficient application identification and the temporal and spatial stability of classification schema. *Computer Networks, 53(6), 790-809.*

[58] Sharafaldin, I., Habibi Lashkari, A., Ghorbani, A. (**2018**). Toward generating a new intrusion detection dataset and intrusion traffic characterization." *Proceedings of fourth international conference on information systems security and privacy*, ICISSP.

[59] Duda, R. O., Hart, P. E., & Stork, D. G. (**2012**). **Pattern classification**. John Wiley & Sons.

[60] Arar, Ö. F., & Ayan, K. (**2017**). A feature dependent Naive Bayes approach and its application to the software defect prediction problem. *Applied Soft Computing, 59, 197-209*.

[۶۱] گلیان, مهسا و هدی مشایخی، **۱۳۹۵**، تشخیص بات نت براساس رده بندی ترافیک و یادگیری افزایشی، *کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات، تهران، دبیرخانه دایمی کنفرانس، https://www.civilica.com/Paper-CITCOMP01-CITCOMP01_292.html.*

فهرست واژگان

ا

آگهی‌افزار..... Adware

آموزش توأم..... Co-training

ارزش-P..... P-value

ارزش-P مورد انتظار ..... Expected P-value.

ارزش- p مبتنی بر مخلوط..... Mixture-based p-values

امتیازات ناهنجاری ..... Anomaly scores

اتلاف لگاریتم مورد انتظار..... Expected log-loss

ب

بات مرکزی(چوپان‌بات)..... Bot master (Bot herder)

بات‌نت روز صفرم..... Zero-day botnet

بات‌نت متمرکز..... Centralized botnet

بات‌نت غیرمتمرکز..... Decentralized botnet

بات‌نت ترکیبی..... Hybrid botnet

بات‌نت نظیر به نظیر..... Peer to Peer botnent

باج‌افزار..... Ransomware

بیشینه‌سازی امید..... Expectation Maximization

بررسی مبتنی بر محموله..... Payload-based Inspection

بازرسی عمیق بسته..... Deep Packet Inspection (DPI)

برنامه‌های اجرایی ساده..... Scripts-kiddies

پ

پیش‌فرض خمینه..... Manifold Assumption

پیش‌فرض خوشه..... Cluster Assumption

پیش‌فرض هموار ..... Smoothness assumption

پروتکل گفت‌وگوی اینترنتی..... Internet Relay Chat (IRC)

پویش صفحه کلید..... Keystroke logging

پویشگر کلید ..... Keylogger

ت

تصدیق‌کننده‌ی یک‌پارچگی سیستم..... System Integrity Verifier (SIV)

تحلیل همبستگی..... Correlation analysis

تشخیص مبتنی بر امضاء..... Signature based detection

تشخیص مبتنی بر رفتار ناهنجار..... Anomaly based detection

تشخیص پروتکل غیرعادی..... Protocol Anomaly detection

تمایزی..... Discriminative

ترکیب پرس‌وجوی عضویت..... Membership Query Synthesis

تابع اتلاف..... Loss function

تخمین‌زننده لحظه‌ای..... Instantaneous estimator

توزیع مشترک ..... Joint distribution

تشخیص ناهنجاری گروهی..... Group anomaly detection (GAD)

ج

جریان..... Flow

جریان‌های بسته‌ای..... Packet-flows

جنگل تصادفی..... Random Forest

جاسوس‌افزار..... Spyware

چ

چرخه حیات ..... Life cycle

چالش ابعاد زیاد..... Curse of dimensionality

ح

حسگر بی‌سیم..... Wireless sensor

خ

خبره.....Oracle

خوشه‌بندی شبکه‌ای افزایشی.....Incremental grid clustering

د

درهای پشتی.....Back doors

درست‌نمایی بیشینه.....Maximum Likelihood

دست‌تکانی سه مرحله‌ای.....Three-way handshaking

داده‌های خام.....Raw data

دو طرفه.....Bidirectional

دقت.....Precision

ر

رفتارهای ناهنجار.....Anomaly treats

رانش مفهومی.....Concept drift

رویداد برداری.....Log events

راهبردهای پرس‌وجو.....Query strategies

رو به جلو .....Forwarding

رو به عقب.....Backwarding

رسته‌ای.....Categorical

روش‌های مبتنی بر گراف.....Graph-based methods

س

سوئیچینگ بسته.....Packet Switching

سنجش.....Priori

سیستم تشخیص نفوذ.....Intrusion Detection Systems (IDS)

سیستم تشخیص نفوذ مبتنی بر امضاء.....Signature-based IDS

سیستم تشخیص نفوذ تحت شبکه.....Network Based IDS

سیستم تشخیص نفوذ تحت میزبان.....Host Based IDS

سیستم بررسی یکپارچگی فایل..... File Integrity Checker system

سیستم نظارت بر فایل‌های پایشی..... Log File Monitoring system

ش

شباهت.....Similarity

شنود.....Phishing

شبکه بیزی.....Bayesian network

ط

طراحی تجربی مطلوب.....Desirable experimental design

ع

عدم قطعیت متقارن.....Symmetric uncertainty

عددی پیوسته.....Continuous numerical

ف

فاصله‌ی ماهالانوبیس.....Mahalanobis distance

فیلتر مبتنی بر همبستگی.....Correlation-based filtering

فایل‌های پایشی.....Log file

ق

قربانی.....Slave

ک

کلاه‌برداری با کلیک.....Click fraud

کیفیت سرویس‌دهی.....Quality of service (QoS)

کانال فرماندهی و کنترل.....Command and Control(C&C)

کارافزار.....Application

کاهش واریانس.....Variance Reduction

گ

گرادیان نزولی تصادفی.....Stochastic gradient descent (SGD)

گرادیان تصادفی متوسط.....Averaged stochastic gradient

م

مرکز ارائه‌دهنده خدمات اینترنتی..... Internet service provider (ISP)

مدل تهی..... Null model

مدل مخلوطی گوسی.....Gaussian mixture model (GMM)

مدل مخلوطی گوسی دو مقداره..... Bivariate Gaussian Mixture Model

ماشین بردار پشتیبان خطی..... Linear Support vector machine (SVM)

مرتبه‌ی دوم گرادیان تصادفی..... Second order stochastic gradient

ن

نهاد آیانا (تخصیص شماره مجوز اینترنتی)..... IANA (Internet Assigned Numbers Authority)

ناهمگونی..... Atypicality

نمونه‌برداری گزینشی مبتنی بر جریان..... Stream Based Selective Sampling

نمونه‌برداری مبتنی بر استخر..... Pool Based Sampling

نمونه‌برداری مرزی..... Margin Sampling

نمونه‌برداری عدم اطمینان..... Uncertainty Sampling

نرخ تشخیص درست..... True Positive Rate

و

ورود از راه دور..... Remote entry

ه

هرزنامه..... Spam

هموارسازی لاپلاس..... Laplacian smoothing

ی

یادگیری افزایشی..... Incremental learning

یادگیری غیرفعال..... Passive learning

یادگیری عمیق..... Deep learning

یادآوری..... Recall

Abstract

Nowadays, the necessity of using the Internet and it becoming an important part of people's lives is unavoidable. On the other hand, in line with the dramatic growth of computer networks and infrastructures, as well as the development of complex and dynamic malware that is constantly updating itself, maintaining security and monitoring network traffic is one of the most important requirements of cyber space. In general, malware can take actions such as theft of information, spamming or the creation of a network of bots. Therefore, creating a method that can effectively detect and prevent their penetration will always be needed. In recent years, botnets have been identified as one of the most dangerous malware known on the Internet, which can destroy healthy computers and turn them into bots for the transmission of viruses, spam, and so on. So far, various methods have been developed to identify botnets. In this regard, network traffic classification is considered one of the most well-known security solutions by means of learning approaches, considering their performance and their developmental capability. However, the detection of botnets by using learning methods has several challenges, including the lack of labeled data and the detection of a new botnet. In order to mitigate these problems, an active learning method can be used which is less considered in the field of botnet detection.

In this research, a semi-supervised active learning-based approach is proposed using ensemble classifier based on logistic regression, linear support vector machine and naive Bayes for detecting botnets is presented. The training is done in an interactive manner and the system constantly updates the model of classifiers based on the requested labels of selected samples. In the experiments, we use a data set containing different types of botnets and extract five different feature sets. The results show the model's efficiency in detecting unseen botnets and the classification accuracy of 89.85.

Keywords: Semi-supervised active learning, Malware, Botnet, Network traffic classification, Ensemble classification, Information security

Shahrood University of Technology

Faculty of Computer Engineering

M.Sc Thesis in Artificial Intelligence Engineering

Malware detection using semi-supervised active learning

By: Reza Rahimian

Supervisor:

Dr. Hoda Mashayekhi

Advisor:

Dr. Mohsen Rezvani

September 2018