دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۱ (۳۳-۴۳)
https://monadi.isc.org.ir

ارائه‌شده در نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه گیلان، ۹ و ۱۰ شهریور ۱۴۰۱

طراحی و پیاده‌سازی دو نمونه آزمایشگاهی سامانه هوشمند شناساگر ترافیک رمز شده VoIP اسکایپ و ابزار گریز Lantern به روش یادگیری عمیق★

محمود سعیدی*، نسرین تاج و آزاده بامداد مقدم
پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
معماری پیشنهادی سامانه هوشمند شناساگر
ترافیک رمزی و ابزار گریز
یادگیری عمیق
شبکه‌ی کدگذار خودکار پیشنهادی
شبکه‌های عصبی پیچشی عمیق
ارزیابی تست‌های عملکرد سامانه

dor: 20.1001.1.24763047.1401.11.2.4.3

نوع مقاله: پژوهشی

چکیده

روش پیشنهادی جهت پیاده‌سازی سامانه‌های شناساگر ترافیک رمزی و ابزار گریز در این مقاله، روش مبتنی بر یادگیری عمیق بوده که با توجه به اهمیت استخراج بهینه و خودکار ویژگی‌ها از مجموعه دادگان ورودی، از شبکه‌ی کدگذار خودکار در فاز استخراج ویژگی استفاده شده است. سپس، خروجی لایه‌ی پنهان میانی این شبکه به یک شبکه عصبی پیچشی عمیق اعمال می‌گردد. شبکه‌های عصبی پیچشی عمیق با توجه به در نظر گرفتن ارتباطات مکانی میان ویژگی‌ها، می‌توانند در ارتقاء عملکرد سامانه نقش مؤثری ایفا نمایند. در نهایت، خروجی شبکه عصبی پیچشی عمیق نیز به منظور انجام فرایند طبقه‌بندی، به دو لایه تمام متصل اعمال می‌گردد. به گونه‌ای که تعداد نورون‌ها در لایه تمام متصل دوم، برابر با تعداد طبقه‌های مورد انتظار از سامانه خواهد بود. در قسمت اول این مقاله ابتدا به مشخصات سامانه‌های پیشنهادی پیاده‌سازی شناساگر ترافیک رمزی و ابزار گریز از نظر معماری عملیاتی و ویژگی‌ها اشاره خواهد شد. سپس به اختصار مشخصات شبکه‌های به کار رفته در پیاده‌سازی سامانه، و شیوه‌ی یکپارچه‌سازی آن‌ها جهت تشکیل سامانه‌ی شناساگر نهایی بیان می‌گردد. پس از آن، مرحله آموزشی سامانه و شیوه‌ی اجرای آن معرفی شده و در انتها، چگونگی تنظیم پارامترهای مدل و ساز و کارهای به کار رفته جهت بهبود عملکرد کلی سامانه و نتایج ارزیابی عملکرد آن ارائه خواهد شد.

© ۱۴۰۱ انجمن رمز ایران

۱ مقدمه

به منظور پیاده‌سازی نمونه آزمایشگاهی سامانه‌های هوشمند شناساگر ترافیک رمزی و ابزار گریز می‌توان از روش‌های گوناگونی از جمله روش‌های غیر خودکار و مبتنی بر یادگیری ماشین بهره برد. ولی با توجه به ضعف‌ها و چالش‌های این تکنیک‌ها از جمله نیاز به حضور کارشناس ماهر جهت استخراج ویژگی، ضعف در قابلیت تعمیم سامانه به کاربردهای دیگر، زمان زیاد لازم جهت ارائه ساز و کار جدید در مواجهه با کاربردهای نوظهوری که به طور روزافزون در حال تولید و ارائه هستند، حساسیت بالا به حدود آستانه‌ی لحاظ شده برای سامانه، وابستگی به بصری‌سازی‌های دقیق و کارشناسانه در برخی کاربردها و ... در این پژوهش از به کار بردن این روش‌ها صرف‌نظر گردیده است. علاوه بر آن با توجه به فعالیت‌های پیشین در این حوزه، در کاربردهای متنوعی نیز عملکرد سامانه‌های مبتنی بر این روش‌ها از سامانه‌های مبتنی بر روش‌های یادگیری عمیق ضعیف‌تر بوده است. لذا روش به کار گرفته شده در این مقاله مبتنی بر یادگیری

★از کمیته علمی نوزدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: msaeidi40@itrc.ac.ir (محمود سعیدی)، n_taj@itrc.ac.ir (نسرین تاج)، azadehbamdad@itrc.ac.ir (آزاده بامداد مقدم)
© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

عمیق است.

همچنین پیاده‌سازی سامانه‌ها در دو گروه توسعه ماژول‌های استخراج ویژگی و ماژول طبقه‌بندی انجام شده است. توسعه ماژول استخراج ویژگی در هر دو سامانه از طریق شبکه کدگذار خودکار انجام شده است و ماژول طبقه‌بندی از طریق شبکه های عصبی پیچشی عمیق همراه با لایه‌های تمام متصل انتهایی پیاده‌سازی شده است. در ادامه‌ی این بخش، ابتدا معماری پیشنهادی سامانه و مشخصات کامل این دو شبکه تشریح می‌گردد. پس از آن، شیوه‌ی یکپارچه‌سازی سامانه از طریق اتصال دو شبکه به یکدیگر بیان شده و در نهایت ساختار نهایی سامانه‌های شناساگر ارائه خواهد شد.

۲ سیستم‌های پیشین شناساگر ترافیك

یکی از مهمترین راه‌های شناسایی ترافیک و ناهنجاری در شبکه‌های کامپیوتری، استفاده از شماره درگاه می‌باشد. مشکلی که در مورد این روش وجود دارد، آن است که امروزه بسیاری از پروتکل‌ها را دیگر نمی‌توان از روی شماره درگاه شناسایی کرد. زیرا اغلب برنامه های کاربردی از شماره درگاه‌های پویا یا از شماره درگاه‌های ثابتی که به نام یك برنامه کاربردی دیگر بر پایه شماره درگاه ثبت شده است، استفاده می‌کنند و بدین سبب دیگر نمی‌توان تفکیك صحیح و بدون ابهام داشت این موضوع موجب عدم استفاده از این روش شده است.

از دیگر روش‌های مرسوم، روش‌های مبتنی بر نشانه می‌باشند. در این روش‌ها، که payload در سال‌های ۲۰۰۰-۲۰۰۳ به اوج تکامل خود رسید، از بخشی از داده استفاده می‌کنند؛ و قسمت مورد استفاده، عدد یا رشته ثابتی است که قابلیت تمیز دادن کاربردها از یکدیگر را دارد. این روش نیز امروزه با توجه به اینکه پروتکل‌ها غالباً مانند ابزارهای گریز و بسیاری از برنامه‌های کاربردی دیگر محتویات بسته‌ها را برای حفظ حریم خصوصی کاربران خود رمز می‌کنند، لذا امروزه این روش غیر قابل استفاده است.

امروزه رایج‌ترین روش‌ها برای استخراج اطلاعات از ترافیک و انجام دسته‌بندی روش‌های یادگیری ماشین مبتنی بر روش‌های آماری می‌باشند [۱-۳]. این روش‌ها مبتنی بر ویژگی‌های ترافیک مانند زمان بین ارسال بسته‌ها، اندازه بسته‌ها و الگوهای تکرارشونده هستند. این ویژگی‌ها پس از استخراج، به عنوان بردار ویژگی، در قالب ورودی در اختیار ابزارهای دسته‌بندی، مانند درخت تصمیم و یا شبکه‌های عصبی مصنوعی، قرار می‌گیرند. فرآیند یادگیری این مدل‌ها نمی‌باشد، در حالی که جابجایی بسته‌ها و اعمال مدل بر روی آنها، باید به شکل برخط صورت بپذیرد و استفاده از این روش‌ها و استخراج ویژگی‌های بهینه نیازمند حضور یک خبره است. با توجه به موارد ذکر شده در این مقاله اقدام به استفاده از روش یادگیری عمیق با کدگذار خودکار[1] شده است. در روش پیشنهادی این پروژه ویژگی‌های استخراج شده نیاز به خبره حذف شده است و این روش کاملاً هوشمند می‌باشد و به نتایج بسیاری خوبی حاصل شده است.

[1] auto encoder

۳ معماری پیشنهادی سامانه هوشمند شناساگر

دو نمونه آزمایشگاهی سامانه هوشمند شناساگر ترافیك رمز شده VoIP اسکایپ و ابزار گریز Lantern به روش یادگیری عمیق از یك معماری مشترك بهره می‌برند. لکن در بخش تحلیل و تجزیه تحلیل بسته از یکدیگر متفاوت‌اند. لذا در این بخش معماری کلی پیشنهادی برای هر دو سامانه تحت عنوان معماری پیشنهادی سامانه شناساگر ارائه می‌گردد. این معماری بر اساس چارچوب C4ISR طراحی شده است. این چارچوب تلفیقی از معماری‌های عملیاتی، سیستمی و فناورانه است، که توسط وزارت دفاع آمریکا با هدف فراهم کردن زمینه های لازم برای تعامل‌پذیری و ارتباط بین سیستم ایجاد شده است. ماژول‌های طراحی شده در معماری پیشنهادی شامل ماژول اخذ ترافیک، ماژول پیش‌پردازش، ماژول مهندسی ویژگی‌ها، ماژول طبقه‌بند و ماژول بررسی عمیق بسته‌ها، ماژول تلفیق و ماژول خروجی می‌باشند. در شکل ۱ نمایی کلی از معماری عملیاتی، سیستمی و فناورانه به صورت توامان ارائه شده است.

ماژول اخذ ترافیک، ترافیک را از شبکه دریافت می‌نماید. ترافیک به صورت مجموعه‌ای از پکت‌ها به صورت آنلاین و آفلاین از شبکه دریافت می‌شوند. این ماژول فایل های ورودی را به صورت Pcap دریافت و به ماژول پیش‌پردازش تحویل می‌نماید و ماژول بررسی عمیق بسته‌ها ارسال می‌کند. ماژول پیش پردازش بعد از انجام عملیات پیش‌پردازش و استخراج جریان‌های (فلو) ساخته‌شده را به ماژول مهندسی ویژگی می‌فرستد. این ماژول از جریان (فلو)های دریافتی ویژگی‌های بهینه را استخراج و به ماژول طبقه‌بند تحویل می‌دهد. ماژول طبقه‌بند با استفاده از مدل هوش مصنوعی کلاسیک و یا ترکیبی تشخیص ترافیک را انجام و نتیجه نهایی تشخیص ترافیك را به ماژول خروجی سامانه تحویل داده و یا ترافیک دریافتی همزمان با ارسال به ماژول پیش‌پردازش می‌تواند به صورت انتخابی به ماژول تحلیل ترافیک تحویل داده شود و نتایج تشخیص و شناسایی از هر دو ماژول تحلیل ترافیک و ماژول طبقه‌بند دریافت و بعد از انجام تلفیق نتایج و تلفیق در ماژول تلفیق و تصمیم‌گیری، نتیجه نهایی به ماژول خروجی تحویل داده شود. در ماژول خروجی برچسب نهایی زده می‌شود و اعمال سیاست لازم در نظر گرفته شود. در شکل ۱، بخش‌های زرد رنگ نشان‌دهنده وظایف و فرآیندهای هر ماژول، بخش‌های سبز رنگ فناوری‌ها و ابزارهای مورد استفاده در هر ماژول هستند و فلش‌های آبی رنگ ترتیب و روند انجام وظایف می‌باشند.

فرآیندها و وظایف بخش‌ها در این معماری عبارتند از:

(۱) ماژول اخذ ترافیک، ترافیک شبکه را به دو صورت آنلاین و آفلاین از شبکه دریافت می‌نماید. امکان اخذ ترافیك توسط ابزارهای WIRESHARK و TCPDUMP و به صورت فایل‌های Pcap فراهم می‌شود و خروجی ماژول اخذ ترافیک به ماژول‌های پیش‌پردازش و ماژول بررسی عمیق بسته‌ها به صورت همزمان ارسال می‌گردد.

شکل ۱. معماری سیستمی سامانه پیشنهادی تشخیص ترافیک ابزار گریز

(۲) ماژول پیش‌پردازش، پس از انجام فرآیندهای تعریف شده نظیر نرمال‌سازی، سفیدسازی و حذف نویز و استخراج جریان از فایل‌های Pcap، جریان‌های استخراج شده را به ماژول مهندسی ویژگی بهینه ارسال می‌نماید.

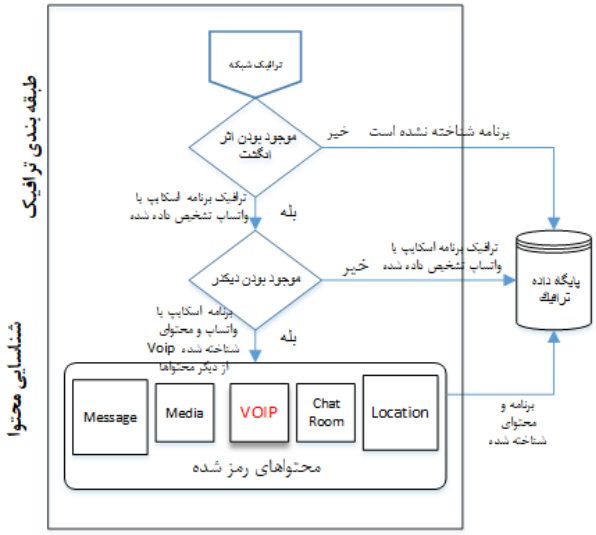
(۳) در ماژول مهندسی ویژگی‌های بهینه، استخراج ویژگی‌های بهینه توسط ابزارها و فناوری‌های Netmate، CICFLowMeter و FlowCalc انجام می‌شود. نتیجه این ویژگی‌های بهینه به ماژول طبقه‌بند و بررسی عمیق بسته‌ها ارسال می‌گردد.

(۴) در ماژول طبقه‌بند، مدل هوش مصنوعی توسط ابزارهای نظیر Weka، Scikit Learn و TensorFlow اعمال می‌گردد و نتیجه این شناسایی ترافیک رمز به ماژول خروجی ارسال می‌شود.

(۵) در ماژول تحلیل ترافیک برای شناساگر Lantern، از الگوی‌های رفتاری ابزارهای گریز که در کتابخانه امضا موجود است، استفاده شده و نتیجه اعلام می‌گردد. این ماژول دارای دیتابیس نگهداری و بروزرسانی الگوهای رفتاری است. همچنین شناسایی برنامه و پروتکل مربوطه در واحد تجزیه تحلیل بسته و تشخیص ترافیک رمز VOIP برنامه Skype مطابق شکل ۲ صورت خواهد گرفت.

(۶) در ماژول تلفیق نتایج حاصله در ماژول طبقه‌بند و ماژول تحلیل ترافیک را مقایسه و در صورت یکسان بودن نتایج، نتیجه را به ماژول خروجی ارسال می‌گردد و در صورت یکسان نبودن با ارسال پیامی درخواست انجام مجدد طبقه‌بندی ترافیک با الگوریتم‌های دیگر (استفاده از طبقه‌بند دوم با الگوریتم متفاوت) را به ماژول طبقه‌بند ترافیک ارسال می‌نماید و بعد از دریافت نتیجه، رای‌گیری بر اساس دو طبقه‌بندی با الگوریتم‌های متفاوت و نتیجه تحلیل ترافیک انجام و نتیجه نهایی به ماژول خروجی ارسال می‌گردد.

(۷) در ماژول خروجی برچسب‌گذاری ترافیک ابزار گریز و ترافیک



شکل ۲. روند پیشنهای شناسایی برنامه و پروتکل در واحد تجزیه تحلیل بسته سامانه پیشنهادی ترافیک رمز VoIP

رمز VOIP برنامه Skype در مقیاس با ترافیک عادی مشخص می‌گردد تا اعمال سیاست لازم بر روی ترافیک انجام گیرد.

لازم به ذکر است به دلیل خواناتر شدن شکل ۱ این موارد فقط در مورد ترافیک ابزار گریز در خروجی نشان داده شده است و شمای کلی مربوط به عملیات جداسازی ترافیک رمز VoIP اسکایپ در شکل ۲ تصویر گردیده است.

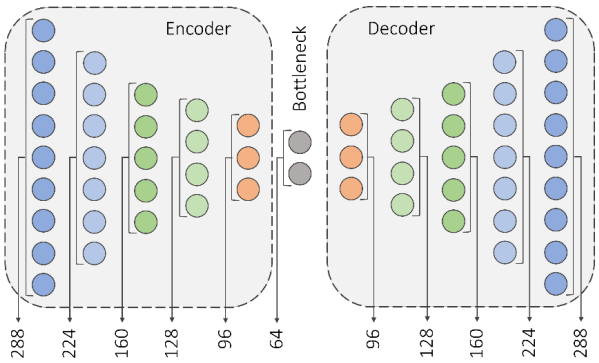
۴ شیوه‌ی پیاده‌سازی سامانه‌های تشخیص ترافیک رمز VoIP اسکایپ و ابزار گریز Lantern

۱.۴ مشخصات شبکه‌ی کدگذار خودکار پیشنهادی

توصیف شبکه‌ی کدگذار خودکار پیشنهادی پیاده شده را می‌توان در قالب ویژگی‌های زیر تشریح نمود:

تعداد لایه‌های پنهان: یکی از موارد بسیار پر اهمیت در انتخاب یک شبکه، تعیین تعداد لایه‌های پنهان می‌باشد. علت اصلی این امر آن است که کم بودن یا زیاد بودن تعداد این لایه‌ها، نقش مؤثری در کم‌برازش [1] یا بیش‌برازش [2] شناساگر خواهد داشت. چرا که در صورت کم بودن تعداد لایه‌ها، درجه آزادی مدل بسیار کمتر از درجه آزادی واقعی انتخاب شده و در نتیجه با وجود عملکرد خوب مدل بر روی دادگان آموزش، عملکرد آن بر روی دادگان آزمایش با خطای بسیاری مواجه خواهد شد. در نقطه مقابل، زیاد بودن تعداد این لایه‌ها نیز ممکن است پیچیدگی مدل را از پیچیدگی مسئله‌ی طبقه‌بندی بیشتر نموده و یا به عبارت دیگر، درجه آزادی مدل را از درجه آزادی واقعی بیشتر گرداند. در نتیجه مدل جزئیات غیرضروری بسیاری را از داده آموزش فراگرفته و قدرت خود را در مواجهه با داده جدید از دست می‌دهد.

[1] underfitting [2] overfitting



شکل ۳. فرایند نمایی از شبکه‌ی کدگذار خودکار پیشنهادی پیاده‌شده در سامانه و تعداد دقیق نورون‌های موجود در هر لایه از آن

با توجه به نکات ذکر شده و بر مبنای بررسی‌های عملی بر روی مجموعه دادگان ورودی، تعداد لایه‌های شبکه در هر کدام از بخش‌های کدگذاری و کدگشایی برابر با پنج عدد در نظر گرفته شده و یک لایه نیز به عنوان لایه پنهان میانی لحاظ گردید. همچنین ساختار کدگشا نیز قرینه‌ی ساختار کدگذار انتخاب گردید.

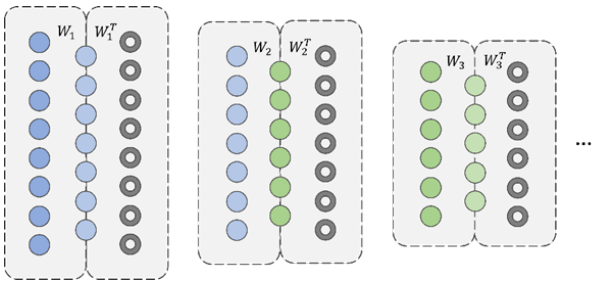
تعداد نورون‌های موجود در هر لایه: اهمیت انتخاب تعداد نورون‌های موجود در هر لایه، کاملاً مشابه با موارد ذکر شده برای تعداد لایه‌های پنهان می‌باشد. چراکه افزایش تعداد این نورون‌ها امکان بیش‌برازش و کاهش تعداد آن‌ها امکان کم‌برازش را افزایش خواهد داد. با این وجود در انتخاب تعداد نورون‌ها، جلوگیری از کاهش ناگهانی تعداد نورون‌ها از یک لایه به لایه دیگر و تلاش برای کاهش ملایم این تعداد به صورت نسبتاً خطی، همراه با مضرب ۳۲ در نظر گرفتن تعداد نورون‌ها در هر لایه (به منظور کمک به عملکرد سخت‌افزار پیاده‌سازی) مورد نظر بوده است. به همین دلیل، تعداد نورون‌های هر لایه به ترتیب ۲۸۸، ۲۲۴، ۱۶۰، ۱۲۸، ۹۶ و ۶۴ لحاظ گردید. بنابراین کاهش تعداد نورون‌ها در انتقال از دو لایه اول ۶۴ عدد، و این کاهش در انتقال از لایه‌های بعدی به میزان ۳۲ عدد در نظر گرفته شد. ساختار پیشنهادی در شکل ۳ قابل مشاهده خواهد بود.

شیوه‌ی استفاده از وزن‌ها: همان گونه که اشاره گردید، معماری بخش کدگشایی مدل پیاده‌شده قرینه‌ی بخش کدگذاری آن در نظر گرفته شد. در چنین شرایطی می‌توان وزن‌های لایه‌های کدگشایی را ترانهاده‌ی وزن‌های کدگذار در لایه‌های متناظر در نظر گرفت. این مسئله در شبکه‌های کدگذار خودکار ، مطابق با شکل ۴ می‌باشد. این کار با کاهش تعداد وزن‌ها مدل را سبک‌تر نموده و از بیش‌برازش شبکه جلوگیری می‌نماید. بنابراین در شبکه‌ی پیاده‌شده نیز این ویژگی مورد استفاده قرار خواهد گرفت.

۲.۴ مشخصات شبکه عصبی پیچشی عمیق پیشنهادی

با توجه به انجام فرایند استخراج ویژگی در شبکه کدگذار خودکار، عمیق‌تر نمودن شبکه‌های عصبی پیچشی عمیق[1] و پیچیده‌تر نمودن آن، علاوه بر بالا بردن هزینه‌ی زمانی و سخت‌افزاری سامانه نهایی، احتمال بروز

[1]Deep Convolutional Neural Network (DCNN)



شکل ۴. شیوه‌ی استفاده از ترانهاده‌ی وزن‌های لایه‌های کدگذاری در لایه‌های کدگشایی شبکه کدگذار خودکار

شکل ۵. معماری نهایی سامانه پیاده‌سازی شده همراه با نمایی از معماری شبکه‌ی پیچشی پیاده شده، همراه با لایه‌های تمام متصل انتهایی (سمت راست)

بیش‌برازش در سامانه را نیز افزایش خواهد داد. به همین منظور، در این بخش از سامانه به دو لایه پیچشی و دو لایه ادغام[2] با ساختاری ساده، همراه با یک لایه‌ی تمام متصل دارای ۶۴ نورون و یک لایه تمام متصل دارای دو عدد نورون (به منظور انجام فرایند طبقه‌بندی دودویی) اکتفا خواهد شد. همچنین با توجه به برداری (تک‌بعدی) بودن ویژگی‌های استخراج شده از شبکه کدگذار خودکار ، از لایه‌های پیچشی یک‌بعدی به جای پیچشی دوبعدی استفاده می‌گردد.

فیلتر در نظر گرفته شده برای لایه پیچشی نخست، یک فیلتر ۱ در ۳ با عمق ۸ می‌باشد. خروجی این لایه، به یک لایه ادغام با روش حداکثر تجمع و گام ۲ اعمال می‌گردد. فیلتر لایه پیچشی دوم نیز یک فیلتر ۱ در ۳ با عمق ۱۶ خواهد بود. خروجی این لایه نیز به یک لایه ادغام با روش حداکثر تجمع[3] و گام ۲ اعمال می‌گردد. در نهایت خروجی لایه ادغام، مسطح شده و به یک لایه‌ی تمام متصل با تعداد ۶۴ نورون وارد می‌گردد. در لایه‌ی انتهایی شبکه نیز، لایه ۶۴ نورونی به یک لایه‌ی تمام متصل با تعداد ۲ نورون متصل می‌شود که این لایه، وظیفه‌ی طبقه‌بندی دادگان را بر عهده خواهد داشت. نمایی از معماری شرح داده شده، در سمت راست شکل ۵ قابل مشاهده می‌باشد.

۳.۴ شیوه‌ی یکپارچه‌سازی ماژول‌ها و ساختار نهایی سامانه‌ها

همان گونه پیش از این بیان گردید، سامانه‌ها را می‌توان به دو بخش کلی شبکه‌ی کدگذار خودکار و شبکه‌های عصبی پیچشی عمیق همراه با لایه‌های تمام متصل انتهایی تقسیم‌بندی نمود. اگر چه این دو بخش در مرحله‌ی آموزش سامانه‌ها به صورت فازبندی‌شده آموزش می‌بینند، ولی در نهایت، سامانه‌ی نهایی یک سامانه‌ی یکپارچه متشکل از هر دو

[2]pooling layer [3]MAX-pooling

شبکه خواهد بود. شیوه‌ی یکپارچه‌سازی نیز بدین صورت است که پس از آموزش دیدن شبکه کدگذار خودکار، تمامی لایه‌های مربوط به کدگشایی از انتهای شبکه برداشته شده و لایه‌های کدگذار همراه با لایه‌ی پنهان میانی (لایه استخراج ویژگی) باقی خواهد ماند. سپس، لایه‌ی پنهان میانی به شبکه‌ی پیچشی طراحی شده متصل می‌گردد. بدین ترتیب، سامانه‌ها فرایند استخراج ویژگی و طبقه‌بندی را به صورت یکپارچه انجام خواهد داد. معماری مفهومی سامانه در شکل ۵ نمایش داده شده است.

۵ نتایج ارزیابی عملکردی پیاده‌سازی دو نمونه آزمایشگاهی سامانه هوشمند شناساگر ترافیک رمز شده، بهبود و رفع اشکالات احتمالی

در فاز سوم پروژه متدولوژی و روال‌های ارزیابی دو سامانه به صورت جعبه سفید و سیاه ارائه گردید. با توجه به اینکه تست‌های جعبه سفید در صورتی که عملکرد سامانه از حدی پایین‌تر باشد جهت اشکال‌زدایی پیشنهاد می‌شود و چون خوشبختانه سامانه‌ها عملکرد مناسبی داشتند نیازی به اشکال‌زدایی و انجام تست‌های جعبه سفید نبود. بر این اساس، عملکرد دو سامانه مبتنی بر آزمون‌های جعبه سیاه ارزیابی شده است. شایان ذکر است که چون دو نمونه آزمایشگاهی بدون برون سپاری و به صورت داخلی توسط تیم پروژه در پژوهشگاه ارتباطات و فناوری اطلاعات توسعه داده شده است، تنها به انجام بخشی از آزمون‌های جعبه سیاه در حد تأیید عملکرد نمونه آزمایشگاهی اکتفا شده است. به منظور شفاف شدن مسئله ارزیابی عملکردی دو سامانه شناساگر ترافیک رمزی VoIP اسکایپ و ابزار گریز Lantern ابتدا مشخصات مجموعه داده و فرآیند آماده‌سازی داده‌های ترافیکی جهت توسعه و ارزیابی ارائه می‌شود و سپس نتایج آزمون‌های عملکردی برای هر سامانه به طور مجزا گزارش می‌شود.

۱.۵ مشخصات مجموعه داده و فرآیند آماده‌سازی جهت توسعه و ارزیابی سامانه‌های پیشنهادی

مجموعه دادگان مورد استفاده جهت آموزش و آزمایش مدل هوش مصنوعی سامانه‌های شناساگر ترافیک رمزی و ابزار گریز، متشکل از ۷۶۲ عدد فایل pcap استخراج شده در آزمایشگاه می‌باشد. در این مجموعه دادگان، بسته‌های داده از نظر نوع ترافیک، برنامه کاربردی تولید کننده بسته داده، نوع ابزار گریز استفاده شده، سیستم‌عامل و ارائه‌دهنده سرویس اینترنت برچسب‌زنی شده‌اند. برای جمع‌آوری دادگان از دو سیستم کلاینت و سرور استفاده شده است که سرور دارای سیستم عامل فدورا است ولی از کلاینت های متنوعی برای جمع‌آوری داده به صورت متنوع و جامع استفاده شده است. مشخصات این سیستم ها در جدول ۱ درج شده است. جزئیات برچسب‌های موجود در مجموعه دادگان، در جدول ۲ قابل مشاهده است.

در مجموعه دادگان یاد شده، برچسب فایل‌های pcap در قالب یک فایل csv با نام data log ارائه گردیده است. تعداد سطرهای این فایل برابر با تعداد فایل‌های pcap و ستون‌های آن نشان‌دهنده‌ی نام فایل،

جدول ۱. مشخصات سیستم‌های جمع آوری دادگان

سیستم	مشخصات
سرور	Processor: Intel(R), Core(TM) i7-6700K CPU @4 GHz 4 GHz, Installed memory (RAM): 32/0 GB, System type: 64bit oprating system, X64-based processor, Disk Capacity: 1.0 TB, OS Name: fedora 33(Work station), OS type: 64-bit, Gname version: 3.38.1
کلاینت ۱ (ویندوزی)	Memory: 8.00 GiB, Processor: Intel(R), Core(TM) i5-2400s CPU @2.5 GHz 2.5 GHz, Disk Capacity 1.0 TB, OS Name: Windows 7 or windows 10, OS type: 64-bit
کلاینت ۲ (لینوکسی)	Memory: 7.8 GiB, Processor: Intel(R), Core(TM) i5-2400s CPU @2.5 GHz* 4, Disk Capacity: 1.0 TB, OS Name: fedora 33 (Work station), OS type: 64-bit, Gname version: 3.38.1
کلاینت ۳ (گوشی آیفون)	Software: 15.3.1, Model name: iphone13 pro max
کلاینت ۴ (گوشی اندروید)	Android version: 8.1.0, Model name: j7Pro

جدول ۲. جزئیات برچسب‌های موجود در مجموعه دادگان

مشخصات بسته داده	برچسب‌های موجود
نوع ترافیک	Web Browse, Insta Browse, Watch Video, Video Call, Voice Call, Send Email, Text Chat, Text Message, Torrent DL, File DL, No Task
برنامه کاربردی	Chrome, Firefox, You tube, Skype, Zoom, Instagram, WhatsApp, qBittorrent
نوع ابزار گریز	Lantern, Hotspot Shield, Ultra Surf, None
سیستم‌عامل	Win10, Win7, Fedora, Android, IOS
ارائه‌دهنده سرویس اینترنت	FibreTCI, MCI, ITRC

A	B	C	D	E	F	G
1634132064.pcap	WatchVideo	Instagram	None	Fedroa	FibreTCI	2021-10-13 17:04:24 +0330
1634132112.pcap	WatchVideo	Instagram	None	Fedroa	FibreTCI	2021-10-13 17:05:12 +0330
1634132178.pcap	WatchVideo	Instagram	None	Fedroa	FibreTCI	2021-10-13 17:06:18 +0330
1634132271.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:07:51 +0330
1634132328.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:08:48 +0330
1634132400.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:10:00 +0330
1634132448.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:10:48 +0330
1634132523.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:12:03 +0330
1634132774.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:16:14 +0330
1634132833.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:17:13 +0330
1634133322.pcap	WatchVideo	Instagram	Lentern	Fedroa	FibreTCI	2021-10-13 17:25:22 +0330
1634134854.pcap	TextChat	Skype	None	Win7	FibreTCI	2021-10-13 17:50:54 +0330
1634134945.pcap	TextChat	Skype	None	Win7	FibreTCI	2021-10-13 17:52:25 +0330
1634135037.pcap	TextChat	Skype	None	Win7	FibreTCI	2021-10-13 17:53:57 +0330

شکل ۶. نمونه‌ای از محتویات فایل data log

مشخصات فایل (متناسب با جدول فوق) و تاریخ ذخیره‌سازی فایل می‌باشد. نمونه‌ای از سطرها و ستون‌های این فایل در شکل ۶ نشان داده شده است.

علاوه بر فایل data log، فایل csv دیگری با نام discard نیز همراه با

مجموعه دادگان ارائه گردیده است که فایل‌های pcapای است که در آن‌ها فرد گردآورنده، از صحت و درستی شرایط موجود جهت جمع‌آوری داده اطمینان نداشته و بسته‌های ذخیره شده را نامعتبر می‌داند. بنابراین لازم است در راستای جلوگیری از ایجاد اختلال در فرایند آموزش مدل، این دادگان تفکیک شده و حذف گردند. با توجه به نکات ذکر شده، جداسازی فایل‌های موجود در discard، به طور خودکار و توسط یک کد نوشته شده به زبان پایتون صورت پذیرفت. در نتیجه تعداد فایل‌های pcap مورد استفاده جهت آموزش شبکه به ۷۰۶ عدد تقلیل یافت.

در ادامه‌ی این بخش، شیوه‌ی جداسازی دادگان مربوط به ابزار گریز Lantern و غیر از آن، و همچنین دادگان مربوط به ترافیک رمز شده VoIP اسکایپ و غیر از آن؛ همراه با چگونگی پردازش دادگان یاد شده جهت آماده‌سازی ورودی مورد نیاز برای آموزش مدل، شرح داده خواهد شد.

۱.۱.۵ مجموعه دادگان مورد استفاده جهت شناسایی ترافیک رمز شده ابزار گریز Lantern

همان گونه که اشاره گردید، مجموعه دادگان تهیه‌شده از طیف گسترده‌ای از کاربردها تشکیل شده است. با این وجود، با توجه به هدف طبقه‌بندی، یعنی شناسایی ترافیک ابزار گریز Lantern از سایر ترافیک‌ها لازم است مجموعه دادگان به دو طبقه‌ی کلی تقسیم‌بندی گردد. به گونه‌ای که بسته‌های دارای برچسب Lantern در یک طبقه و مجموع سایر بسته‌ها در طبقه‌ای دیگر قرار گیرند. نکته‌ی قابل توجه، قرارگیری بسته‌های مربوط به سایر ابزار گریزها در طبقه‌ی دوم می‌باشد. به گونه‌ای که طبقه‌ی دوم، هر دو حالت ترافیک رمز شده عادی و ترافیک رمز شده عبوری از سایر ابزار گریزها را نیز شامل می‌گردد.

جهت دست‌یابی به تقسیم‌بندی یاد شده، یک کد به زبان پایتون تهیه گردید. در این کد، ابتدا فایل data log خوانده شده و مشخصات آن در قالب یک دیکشنری ذخیره می‌گردد. سپس، فایل‌های pcap نام برده شده در فایل data log توسط پکیج dpkt بازگشایی شده و بسته‌های موجود در آن‌ها استخراج می‌گردد. شیوه‌ی دقیق این کار در بخش بعدی شرح داده خواهد شد. در حین استخراج بسته‌ها، تمامی بسته‌های به دست آمده از هر فایل pcap با توجه به مشخصات آن فایل در دیکشنری، با یکی از دو برچسب Lantern یا Non-Lantern برچسب‌زنی شده و به مجموعه دادگان نهایی افزوده می‌گردند. با تکمیل این فرایند، مجموعه دادگان مورد نظر تشکیل خواهد شد. لازم به ذکر است که در مراحل فوق، pcapهای مشخص‌شده در فایل discard از سایر pcapها تفکیک شده و هیچ کدام از بسته‌های موجود در آن‌ها مورد استفاده قرار نخواهند گرفت.

پس از تشکیل مجموعه دادگان، لازم است داده‌ها یک مرتبه مخلوط [1] گردند. علاوه بر آن، لازم است بخشی از مجموعه دادگان مخلوط شده به آموزش، بخشی دیگر به اعتبارسنجی و بخشی دیگر به آزمایش اختصاص داده شوند. هر دو فرایند یاد شده توسط تابع train_test_split از کتابخانه sklearn صورت می‌پذیرد.

[1] shuffle

جدول ۳. تعداد بسته‌های داده مورد استفاده جهت پیاده‌سازی

نوع ترافیک	تعداد بسته‌های آموزش	تعداد بسته‌های اعتبارسنجی	تعداد بسته‌های آزمایش	تعداد کل بسته‌ها
Lantern	۲۶۹۹۹۸	۵۸۰۰۵	۵۷۹۱۲	۳۸۵۹۱۵
Non-Lantern	۱۴۷۵۷۳۴	۳۱۶۰۸۰	۳۱۶۱۷۴	۲۱۰۷۹۸۸

جدول ۴. تعداد بسته‌های داده مورد استفاده جهت پیاده‌سازی

نوع ترافیک	تعداد بسته‌های آموزش	تعداد بسته‌های اعتبارسنجی	تعداد بسته‌های آزمایش	تعداد کل بسته‌ها
Skype VoIP	۵۷۲۲۳	۱۲۱۵۸	۱۲۲۵۵	۸۱۶۳۶
Non- Skype VoIP	۱۶۸۸۵۰۹	۳۶۱۹۲۷	۳۶۱۸۳۱	۲۴۱۲۲۶۷

با توجه به وضعیت مرسوم در آموزش مدل‌های یادگیری، در این پیاده‌سازی ٪۷۰ از بسته‌ها به دادگان آموزش، ٪۱۵ از آن‌ها به دادگان اعتبارسنجی و ٪۱۵ باقی‌مانده نیز به دادگان آزمایش تخصیص یافت. بدین ترتیب، تعداد بسته‌های داده در هر کدام از حالات یاد شده به صورت جدول ۳ خواهد بود.

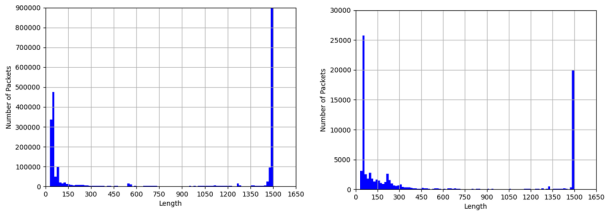
۲.۱.۵ مجموعه دادگان مورد استفاده جهت شناسایی ترافیک رمز شده VoIP اسکایپ

روند تشکیل مجموعه دادگان مورد استفاده جهت شناسایی ترافیک VoIP اسکایپ مشابه با مجموعه دادگان ترافیک Lantern می‌باشد. با این تفاوت که برخلاف دادگان Lantern که در آن‌ها فایل‌های دارای برچسب Lantern به طبقه Lantern و سایر فایل‌ها به طبقه Non-Lantern اختصاص داده شدند؛ در تهیه این دادگان فایل‌های دارای هر دو برچسب نوع ترافیک Voice Call و برنامه کاربردی Skype به عنوان دادگان Skype-VoIP و سایر فایل‌ها به عنوان دادگان Non-Skype-VoIP در نظر گرفته خواهند شد. لازم به ذکر است که با توجه به محدودیت تعداد بسته‌های مربوط به Skype-VoIP در مجموعه دادگان ارائه‌شده، ممکن است سامانه‌ی شناساگر با چالش مواجه گردیده و امکان دست‌یابی به عملکردی مشابه با سامانه‌ی قبل را نداشته باشد.

همانند سامانه‌ی شناساگر ترافیک ابزار گریز Lantern، در پیاده‌سازی این سامانه نیز ٪۷۰ از بسته‌ها به دادگان آموزش، ٪۱۵ از آن‌ها به دادگان اعتبارسنجی و ٪۱۵ باقی‌مانده نیز به دادگان آزمایش تخصیص یافت. بدین ترتیب، تعداد بسته‌های داده در هر کدام از حالات یاد شده به صورت جدول ۴ خواهد بود.

۳.۱.۵ فرایند آماده‌سازی ورودی‌های سامانه شناساگر

شیوه‌ی استخراج ورودی در سامانه‌ی شناساگر ترافیک VoIP اسکایپ کاملاً مشابه با سامانه‌ی شناساگر ترافیک Lantern می‌باشد. به همین دلیل، ابتدا لازم است که هیستوگرام طول لایه پروتکل اینترنت برای



شکل ۷. هیستوگرام طول لایه پروتکل اینترنت در بسته‌های داده مربوط به Skype-VoIP (سمت چپ) و بسته‌های داده مربوط به Non-Skype-VoIP (سمت راست)

بسته‌های داده‌ی هر دو مجموعه Skype-VoIP و Non-Skype-VoIP استخراج گردد. این هیستوگرام‌ها در شکل ۷ قابل مشاهده خواهند بود.

همان گونه که مشاهده می‌گردد، انتخاب پیشین، یعنی استخراج ۳۰۰ بایت ابتدایی از لایه پروتکل اینترنت همچنان معتبر می‌باشد. به همین دلیل، سرآیند لایه پروتکل اینترنت همراه با ۳۰۰ بایت ابتدایی این لایه به عنوان ورودی سامانه در نظر گرفته خواهد شد. همچنین بسته‌های مربوط به پروتکل تفکیک آدرس (ARP) نیز مانند گذشته حذف شده و از قرار گرفتن آن‌ها در مجموعه داده‌گان جلوگیری می‌گردد.

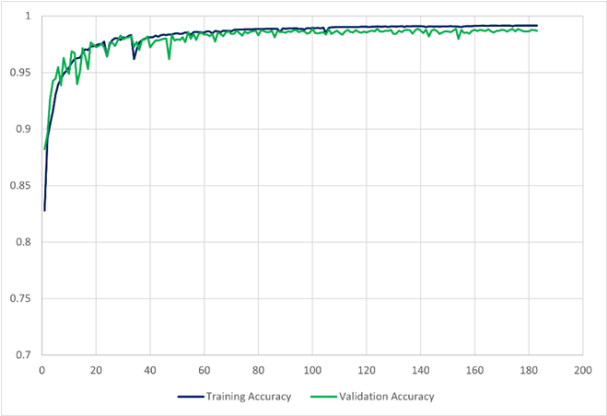
۶ نتایج پیاده‌سازی سامانه‌های پیشنهادی

در این بخش، نتایج حاصل از سامانه‌های پیاده‌سازی شده مورد بررسی قرار خواهد گرفت. ابتدا تجهیزات نرم‌افزاری مورد نیاز از جمله کتابخانه‌های به کار گرفته شده جهت پیاده‌سازی بیان گردیده و سپس تجهیزات سخت‌افزاری استفاده شده جهت انجام فرایند آموزش مدل نیز معرفی خواهد شد. پس از آن، نمودارهای روند یادگیری برای هر دو سامانه‌ی شناساگر ترافیک ابزار گریز Lantern و شناساگر ترافیک رمز شده VoIP اسکایپ همراه با صحت عملکرد و ماتریس سرگشتگی مربوط به هر کدام ارائه می‌گردد. در نهایت، نتایج ارزیابی عملکرد سامانه از طریق آزمون‌های ارزیابی ارائه گردیده و نقاط قوت و ضعف سامانه بیان خواهد شد.

۱.۶ تجهیزات نرم‌افزاری و سخت‌افزاری مورداستفاده جهت پیاده‌سازی سامانه پیشنهادی

به طور کلی، پیاده‌سازی سامانه از طریق کدهای نوشته‌شده به زبان برنامه‌نویسی Python و با استفاده از کتابخانه‌های موجود برای آن انجام شده است.

از نظر تجهیزات سخت‌افزاری، آموزش سامانه را می‌توان بر روی هر دو پردازنده CPU و GPU انجام داد. البته تفاوت اصلی در استفاده از این دو پردازنده، سرعت آموزش دیدن مدل خواهد بود. چرا که با توجه به ظرفیت بالای موجود جهت موازی‌سازی بخش‌های مختلف محاسبات صورت پذیرفته در روند آموزش مدل، قدرت عملکرد سخت‌افزار GPU در انجام این پردازش‌های موازی منجر به افزایش سرعت آموزش مدل نسبت به سخت‌افزار CPU می‌گردد.



شکل ۸. نمودار روند یادگیری فاز دوم پروژه از آموزش سامانه پیشنهادی شناساگر ترافیک رمز شده ابزار گریز Lantern

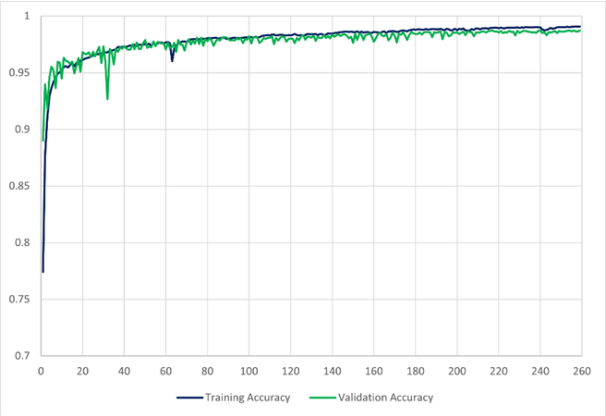
همچنین، از بستر Google Colab جهت آموزش مدل استفاده گردیده است، زیرا امکان استفاده‌ی رایگان از سخت‌افزارهای پردازشی CPU، GPU و TPU فراهم گردیده است. همچنین امکان اتصال فضای ابری Google Drive به این بستر نیز، قابلیت استفاده از مجموعه داده‌گان شخصی جهت آموزش مدل را تسهیل نموده است. با وجود امکان انتخاب نوع سخت‌افزار پردازشی در این بستر، امکان تعیین و شناسایی مدل دقیق سخت‌افزار مورد استفاده امکان‌پذیر نخواهد بود. به همین جهت، از بیان مدل دقیق سخت‌افزار مورد استفاده در این پیاده‌سازی صرف‌نظر می‌گردد.

۱.۱.۶ خروجی روند آموزش و ارزیابی سامانه پیشنهادی شناساگر ترافیک ابزار گریز Lantern

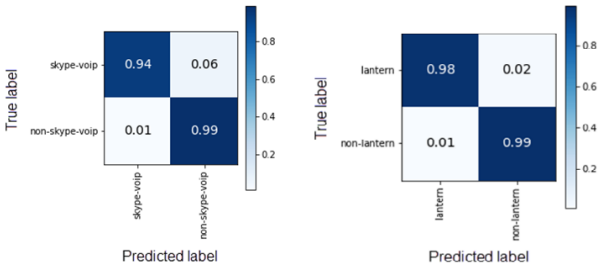
نمودار روند یادگیری فاز دوم پروژه از آموزش سامانه شناساگر ترافیک رمز شده ابزار گریز Lantern مطابق با شکل ۸ می‌باشد. همان گونه که در این نمودار قابل مشاهده است، توقف فرایند یادگیری مدل پیش از وقوع بیش‌برازش صورت پذیرفته است. همچنین در طول آموزش، صحت عملکرد سامانه بر روی داده‌گان اعتبارسنجی، به طرز مطلوبی رشد صحت عملکرد سامانه بر روی داده‌گان آموزش را دنبال نموده است. پس از تکمیل آموزش سامانه به کمک داده‌گان آموزش، صحت عملکرد آن بر روی داده‌گان آزمایش مورد بررسی قرار گرفت. صحت به دست آمده بر روی این داده‌گان ۹۸٫۸۹٪ گزارش گردید.

۲.۱.۶ خروجی روند آموزش و ارزیابی سامانه شناساگر ترافیک سامانه‌ی شناساگر ترافیک رمز شده VoIP اسکایپ

بخش نمودار روند یادگیری فاز دوم پروژه از آموزش سامانه شناساگر ترافیک رمز شده VoIP اسکایپ مطابق با شکل ۹ می‌باشد. همان گونه که در نمودار قابل مشاهده است، در این سامانه نیز توقف فرایند یادگیری مدل پیش از وقوع بیش‌برازش صورت پذیرفته و صحت عملکرد بر روی داده‌گان اعتبارسنجی، صحت عملکرد بر روی داده‌گان آموزش را دنبال نموده است.



شکل ۹. نمودار روند یادگیری فاز دوم پروژه از آموزش سامانه پیشنهادی شناساگر ترافیک رمز شده VoIP اسکایپ



شکل ۱۰. ماتریس سرگشتگی ناشی از اعمال دادگان آزمایش به سامانه پیشنهادی شناساگر ترافیک رمز شده VoIP (سمت راست) و سامانه پیشنهادی شناساگر ترافیک رمز شده ابزار گریز Lantern (سمت چپ)

با تکمیل آموزش سامانه، صحت عملکرد آن بر روی دادگان آزمایش نیز مورد بررسی قرار گرفت و مقدار ٪۹۸٫۷۳ برای آن گزارش گردید. ماتریس سرگشتی متناظر نیز در شکل ۱۰ نمایش داده شده است.

۷ نتایج آزمون‌های ارزیابی عملکردی سامانه پیشنهادی

در این بخش، عملکرد دو سامانه‌ی پیاده‌سازی شده به کمک برخی از آزمون‌های جعبه سیاه مورد بررسی قرار می‌گیرد. در این آزمون‌ها، سامانه همانند یک جعبه سیاه در نظر گرفته شده و بر مبنای خروجی‌های حاصل از آن ارزیابی می‌گردد. در همین راستا، به منظور ارزیابی عملکردی سامانه‌ها، آزمون‌های زیر مطابق دستورالعمل ارائه شده در فاز سوم پروژه انجام شدند:

- آزمون دقت (Precision)
- آزمون حساسیت (Sensitivity) و بازیابی (Recall)
- آزمون تشخیص‌پذیری (Specificity)
- آزمون F-measure [۴]
- آزمون ضریب همبستگی متیوس (MCC [۱])
- آزمون کاپا

در ادامه، نتایج آزمون‌های فوق برای هر دو سامانه شناساگر ارائه

[1] Matthews Correlation Coefficient

جدول ۵. نتایج آزمون‌های ارزیابی سامانه شناساگر ترافیک رمز شده ابزار گریز Lantern و سامانه شناساگر ترافیک رمز شده VoIP اسکایپ

نام آزمون	نتیجه آزمون Lantern	نتیجه آزمون VoIP-Skype
Accuracy	۰٫۹۸۸۹	۰٫۹۸۷۳
Precision	۰٫۹۵۱۹	۰٫۷۴۰۷
Sensitivity (Recall)	۰٫۹۷۷۶	۰٫۹۴۰۰
F1-measure	۰٫۹۶۴۶	۰٫۸۲۸۵
Specificity	۰٫۹۹۱۰	۰٫۹۸۸۹
MCC	۰٫۹۵۸۱	۰٫۸۲۸۳
Kappa	۰٫۹۵۸۰	۰٫۸۲۲۰

خواهد شد. نتایج آزمون‌های ارزیابی سامانه شناساگر ترافیک رمز شده ابزار گریز Lantern و سامانه شناساگر ترافیک رمز شده VoIP اسکایپ در جدول ۵ ارائه گردیده است. همان گونه که در جدول ۵ مشاهده می‌گردد، سامانه‌های پیاده شده در تمامی آزمون‌ها نتایج قابل قبول و مطلوبی به دست آورده است که این مسئله، قدرت عملکرد این سامانه را نشان خواهد داد. علت اصلی پایین بودن آزمون دقت در سامانه شناساگر ترافیک رمز شده VoIP اسکایپ را می‌توان درصد بالای عدم توازن مجموعه دادگان مورد استفاده جهت آزمایش سامانه دانست. رابطه‌ی دقت به صورت زیر تعریف می‌گردد.

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP})$$

در این رابطه، تعداد دادگانی از کلاس منفی که به اشتباه عضوی از کلاس مثبت در نظر گرفته شده‌اند، تاثیر بسیاری بر روی مخرج کسر خواهد داشت. حال اگر در مجموعه دادگان مورد استفاده جهت آزمایش تعداد دادگان کلاس منفی بسیار بیشتر از تعداد دادگان کلاس مثبت باشد، درصد اندکی خطا در دادگان کلاس منفی (به دلیل قابل توجه بودن تعداد این داده‌های خطادار نسبت به تعداد کل دادگان کلاس مثبت) مخرج کسر را به میزان تاثیرگذاری افزایش داده و آزمون دقت را با چالش مواجه می‌نماید. به منظور بررسی صحت این ادعا، آزمون‌های دقت، F-measure، ضریب همبستگی متیوس و کاپا برای دادگان آزمایش نسبتاً متوازن دارای ۱۲۲۵۵ عدد داده‌ی مربوط به ترافیک رمز شده VoIP اسکایپ و ۶۱۸۳۱ عدد داده‌ی مربوط به ترافیک غیر از آن در خصوص مواردی که درصد ارزیابی کمتر از ۰٫۹ داشته اند تکرار گردید. آزمون‌های یاد شده در شرایط جدید نتایج قابل قبول‌تری نسبت به گذشته کسب نموده‌اند که در ستون مربوط به داده‌های متوازن آورده شده در جدول ۵ این امر مشهود است.

۸ نتیجه‌گیری

با دانش کسب شده از مراحل قبلی و شناخت نیازمندی‌های فنی و عملیاتی مورد نظر، سکوی آزمایشگاهی جهت توسعه و ارزیابی سامانه هوشمند شناساگر ترافیک رمز شده VoIP اسکایپ و ابزارگریز Lantern در

پژوهشگاه ارتباطات و فناوری اطلاعات ایجاد گردید[۱]. در این آزمایشگاه چند اقدام کلیدی به شرح زیر انجام شد:

- اخذ ترافیک رمزی، ابزار گریز و نرمال برچسب‌دار
- پیاده‌سازی ماژول‌های دو نمونه آزمایشگاهی سامانه‌های هوشمند شناساگر ترافیک رمزی و ابزار گریز مبتنی بر شبکه‌های یادگیری عمیق
- آموزش و اعتبارسنجی دو نمونه آزمایشگاهی سامانه‌های هوشمند شناساگر ترافیک رمزی VoIP اسکایپ و ابزار گریز Lantern
- ارزیابی عملکردی دو نمونه آزمایشگاهی سامانه مبتنی بر متدولوژی جعبه سیاه و اشکال‌زدایی
- استخراج ویژگی‌های بهینه خودکار و هوشمند با استفاده از فناوری یادگیری ماشین
- دست‌یابی به نتایج با دقت بالا

دقت شناسایی ترافیک در هر دو بخش شناسایی ترافیک لنترن و اسکایپ بسیار مورد توجه و قابل مقایسه با نتایج حاصل شده با روش‌های یادگیری ماشین می‌باشد. به عنوان نمونه نتیجه تشخیص ترافیک ابزار گریز (TOR) [۳] ۹۳/۷ و نتیجه شناسایی ترافیک اسکایپ [۱۴] ۹۱/۶۱ مشاهده شده است و در این مقاله نتیجه شناسایی ترافیک لنترن ۹۸/۸۹ و ترافیک اسکایپ ۹۸/۷۳ است.

در این مقاله جهت استفاده و بهره‌برداری متخصصین در این حوزه، روال تولید مجموعه داده از حیث نحوه توسعه سیستم‌های روتر و کلاینت و مشخصات مجموعه داده اخذ شده تشریح گردید. در گام بعدی فرآیند پیاده‌سازی سامانه‌های هوشمند تشخیص ترافیک رمزی و ابزار گریز به تفصیل ارائه شد و در ضمن در این مقاله از روش یادگیری عمیق با کدگذاری خودکار استفاده شده است که هوشمندسازی روش در مرحله استخراج ویژگی‌های بهینه نیز به همراه داشته است. سپس نحوه آموزش و اعتبارسنجی مدل هوش مصنوعی این سامانه‌ها مورد بحث قرار گرفت. در نهایت دو نمونه آزمایشگاهی مطابق با روال‌های تست جعبه سیاه استخراج شده در مرحله سوم مورد ارزیابی قرار گرفتند.

مراجع

[1] Fonyi, Shane. Overview of 5g security and vulnerabilities. *The Cyber Defense Review*, 5(1):117–134, 2020.

[2] Akpakwu, Godfrey Anuga, Silva, Bruno J., Hancke, Gerhard P., and Abu-Mahfouz, Adnan M. A survey on 5g networks for the internet of things: Communication technologies and challenges. *IEEE Access*, 6:3619–3647, 2018.

[3] Aminuddin, Mohamad Amar Irsyad Mohd, Zaaba, Zarul Fitri, Singh, Manmeet Kaur Mahinderjit, and Singh, Darshan Singh Mahinder. A survey on tor encrypted traffic monitoring. *International Journal of Advanced Computer Science and Applications*, 9(8), 2018.

[4] Powers, David MW. Evaluation: from precision, recall and f-measure to roc, informedness, markedness and correlation. *arXiv preprint arXiv:2010.16061*, 2020.

[5] Srivastava, Nitish, Hinton, Geoffrey, Krizhevsky, Alex, Sutskever, Ilya, and Salakhutdinov, Ruslan. Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*, 15(1):1929–1958, 2014.

[6] Buduma, N. Fundamentals of deep learning: Designing next-generation machine intelligence algorithms.-sebastopol, ca, usa: O'reilly media. 2017.

[7] Duchi, John, Hazan, Elad, and Singer, Yoram. Adaptive subgradient methods for online learning and stochastic optimization. *Journal of machine learning research*, 12(7), 2011.

[8] Zeiler, Matthew D. Adadelta: an adaptive learning rate method. *arXiv preprint arXiv:1212.5701*, 2012.

[9] Kingma, Diederik P and Ba, Jimmy. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.

[10] Ioffe, Sergey and Szegedy, Christian. Batch normalization: Accelerating deep network training by reducing internal covariate shift. in *International conference on machine learning*, pp. 448–456. pmlr, 2015.

[11] He, Kaiming, Zhang, Xiangyu, Ren, Shaoqing, and Sun, Jian. Deep residual learning for image recognition. in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770–778, 2016.

[12] Chicco, Davide, Tötsch, Niklas, and Jurman, Giuseppe. The matthews correlation coefficient (mcc) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData mining*, 14(1):1–22, 2021.

[13] McHugh, Mary L. Interrater reliability: the kappa statistic. *Biochemia medica*, 22(3):276–282, 2012.

[14] Seddigh, Nabil, Nandy, Biswajit, Bennett, Don, Ren, Yonglin, Dolgikh, Serge, Zeidler, Colin, Knoetze, Juhandre, and Muthyala, Naveen Sai. A framework & system

[۱] این پروژه تحت عنوان «نحوه شناسایی مشخصه‌های یک ترافیک خاص رمزنگاری‌شده و اعمال سیاست» بر روی آن با کد ۶۳۰۹۹۰۱۱۰ و با مجری‌گری آقای دکتر محمود سعیدی در آبان سال ۱۴۰۰ با موفقیت کامل در پژوهشکده امنیت پژوهشگاه فناوری اطلاعات و ارتباطات اجرا گردیده است.

for classification of encrypted network traffic using machine learning. in *2019 15th International Conference on Network and Service Management (CNSM)*, pp. 1–5. IEEE, 2019.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 1 (pp. 33–43)
https://monadi.isc.org.ir

Presented at the ISCISC 2022 in University of Giulan, Rasht, Iran

Designing and Implementing two Laboratory Samples of the Intelligent System for Detecting Encrypted VoIP Skype Traffic and the Lantern Escape Tool using Deep Learning Method★

Mahmoud saeidi *, Nasrin Taaj and Azadeh Bamdad Moghaddam

Information and Technology Research Communication Institute (ITRC), Tehran, Iran

ARTICLE INFO.

Keywords:
the proposed architecture of the intelligent system for identifying cryptographic traffic and evasive tools
deep learning
proposed automatic coding network
deep convolutional neural networks
evaluation of system performance tests

dor: 20.1001.1.24763047.1401.11.2.4.3

Type: research paper

ABSTRACT

The proposed method for implementing cryptographic traffic detector systems and evasive tools in this article is a method based on deep learning, which due to the importance of optimal and automatic extraction of features from the input data set, an automatic encoder network has been used in the feature extraction phase. Then, the output of the middle hidden layer of this network is applied to a deep convolutional neural network. Deep convolutional neural networks can play an effective role in improving the performance of the system by taking into account the spatial connections between features. Finally, the output of deep convolutional neural network is also applied to two fully connected layers in order to perform the classification process. So that the number of neurons in the second fully connected layer will be equal to the expected number of layers of the system. In the first part of this article, the specifications of the proposed systems for the implementation of cryptographic traffic detectors and evasion tools will be mentioned in terms of operational architecture and features. Then, the characteristics of the networks used in the implementation of the system, and the method of their integration to form the final identifier system are briefly stated. After that, the training stage of the system and its implementation method will be introduced and at the end, how to adjust the parameters of the model and the mechanisms used to improve the overall performance of the system and the results of its performance evaluation will be presented.

© 2022 ISC

★ The ISCISC 2022 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: msaeidi40@itrc.ac.ir (Mahmoud saeidi), n_taj@itrc.ac.ir (Nasrin Taaj), azadehbamdad@itrc.ac.ir (Azadeh Bamdad Moghaddam)
© 2022 ISC. All rights reserved.