25 th International Conference on
Information Technology, Computer and Telecommunication
Event Place: Tbilisi,Georgia
www.itctconf.ir
بیست و پنجمین کنفرانس بین المللی
فناوری اطلاعات، کامپیوتر و مخابرات | گرجستان
25th International Conference on Information Technology,Computer and Telecommunication
PUBLISH IN JOURNALS — INTERNATIONAL CERTIFICATION

شناسایی حملات توزیع شده منع سرویس شبکه های خودسازمان ده در محیط‌های خودرویی ابری هوشمند با استفاده از یادگیری تقویتی

نازنین صالح امین[۱]

دانشجوی دکترا، گروه کامپیوتر، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران[۱]

کامبیز مجیدزاده[۲*]

استادیار، گروه کامپیوتر، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران [۲]

چکیده

فناوری شبکه‌های خودسازمان ده شبکه های خودرویی به خصوص در زمینه جدید شبکه های خودرویی ابری به عنوان بخش کلیدی در وسایل نقلیه متصل و خودران مورد توجه واقع شده است. تحول صنعت خودرو به سمت اتوماسیون و یکپارچگی وسایل نقلیه در اکوسیستم دیجیتال، ارتباطات بی‌سیم را متحول کرده است. با این وجود، امنیت هنوز هم یک مشکل کلیدی در این چشم‌اندازهای پیشرفته فناوری به شمار می‌آید. حفاظت از یکپارچگی سیستم و حریم خصوصی داده‌ها پیش از پذیرفتن عمومی راهکارهای در شبکه های خودرویی ابری بسیار اهمیت دارد. این مطالعه به موضوع حیاتی امنیت در زمینه شبکه های خودرویی ابری توجه دارد. به طور خاص، تمرکز بر پیش‌بینی و کاهش حملات توزیع شده منع سرویس است که ممکن است عملکرد خودروهای متصل و خدمات وابسته به ابر را مختل کند. برای پردازش این مسئله، یک چارچوب طراحی نوآورانه برای مستندسازی و آنالیز جریان‌های شبکه در بستر شبکه های خودرویی ابری ارائه گردیده است. علاوه بر این، از تکنیک‌های یادگیری تقویتی برای طبقه‌بندی و تحلیل پیش‌بینی با دقت ۹۷.۳۵٪ استفاده می‌کند. معماری ذکر شده در این تحقیق قابلیت بهبود چشمگیری در راهکارهای امنیتی برای پیاده‌سازی شبکه های خودرویی ابری را ایجاد می‌کند. توانایی این امر، تضمین استفاده کاربردی را برای سیستم‌های واقعی فراهم می‌آورد و امکان پاسخ‌دهی به‌موقع به تهدیدات و نقض‌های امنیتی را میسر می‌سازد.

کلمات کلیدی: شبکه‌های خودسازمان ده، شبکه های خودرویی ابری، یادگیری تقویتی، حملات توزیع شده منع سرویس، شبیه سازی GNS۳.

مقدمه

با افزایش وابستگی به فناوری‌های اینترنتی، تهدیدات تخریبی بر فناوری‌های وب افزایش یافته و سبب قطع خدمات می‌شوند. امنیت شبکه به وزنی جدی تبدیل شده و انواع جدید حملاتی که شبکه‌ها را مختل می‌کنند، کشف شده‌اند. به ویژه، حملات توزیع شده منع سرویس، که عمدتاً با هدف غیرقابل دسترس کردن دستگاه‌ها از طریق مصرف منابع انجام می‌شود، نگرانی عمده‌ای برای کارشناسان امنیت سایبری است. حملات توزیع شده، نظیر حملات توزیع شده منع سرویس ، با فشار دادن سرورهای هدف از طریق ارسال حجم عظیمی از داده‌های ناخواسته، رشد کرده‌اند. حملات توزیع شده منع سرویس نیازمند منابع محاسباتی بالا هستند که هزینه‌ها را افزایش و شناسایی آنها را آسان‌تر می‌کند. محدودیت خدمات همچنان دغدغه‌ای برای متخصصان امنیت سایبری است. در شبکه های خودرویی ابری، مهاجمان با انبوهی از بسته‌های داده غیرضروری سرورها را به حالت سیل آسا کرده و شبکه را شلوغ می‌کنند. این پژوهش به بررسی چالش‌های حملات توزیع شده منع سرویس در این محیط می‌پردازد و محاسبات موازی برای شبیه‌سازی سناریوهای ترافیکی پیشنهاد می‌شود. گره‌های این شبکه به اشتراک‌گذاری یکپارچه اطلاعات و تقویت هوش جمعی کمک می‌کنند. این مقاله، با اتکا به[۳]GNS، شامل پنج بخش است؛ تحلیل وضعیت کنونی حملات حملات توزیع شده منع سرویس، شبیه‌سازی این حملات در شبکه های خودرویی ابری، توضیحات محاسباتی و بررسی معیارهای مختلف، نتایج و اثرات آن‌ها، و در نهایت، جمع‌بندی مشارکت‌ها و فرصت‌های تحقیقاتی آینده در امنیت و شبکه های خودرویی ابری می باشد(Das, D.et al,۲۰۲۲)(Wang, X. et al,۲۰۱۸)(De La Torre, G. et al,۲۰۲۰).

بررسی ادبیات

حملات توزیع شده منع سرویس یک چالش جدی در امنیت شبکه‌اند. روش‌های سنتی شامل جمع‌آوری ویژگی‌های ترافیک و استفاده از الگوریتم‌ها برای شناسایی حمله است. این روش‌ها متکی بر ویژگی‌های خاص حمله‌اند و ممکن است مهاجمان را قادر به فرار سازند. اینترنت با معماری ایمنی پائین‌تر به نفع هکرها عمل می‌کرد، چرا که روترهای اصلی فاقد قابلیت احراز هویت بسته‌های IP ورودی بودند و این مسأله به جعل IP و حملات توزیع شده منع سرویس انجامید. محققین گزینه‌های مختلفی چون نقشه‌های خودسازماندهی و الگوریتم‌های یادگیری ماشین برای جلوگیری از حملات توزیع شده منع سرویس بررسی کرده‌اند. با این وجود، این روش‌ها زمان محاسباتی بالایی را می‌طلبند. به تازگی، مدلی برای فیلتر خروجی انتخابی ابر ارائه شده که حملات توزیع شده منع سرویس را با تحلیل ابرداده شناسایی می‌کند.

تحلیل داده‌های بسته ماشین های مجازی به تنهایی در شناسایی حملات ناکافی است. اما شبکه‌های تعریف شده با نرم‌افزار SDN با راه‌حل‌های امنیتی مبتنی بر خود، در حال رشد هستند. این فناوری، با ترکیب تکنیک‌های آنالیز آنتروپی و یادگیری ماشین، قابلیت شناسایی مؤثرتر حملات توزیع شده منع سرویس را فراهم می‌آورد، هرچند هنوز در مراحل ابتدایی قرار دارد و به اعتبارسنجی بیشتری نیاز دارد. روش‌های دیگر مثل ردیابی IP و فیلتر کردن بسته‌ها نیز برای شناسایی حملات توزیع شده منع سرویس بررسی می‌شوند، اما محدودیت‌هایی وجود دارد. برای شناسایی حملات حملات توزیع شده منع سرویس، از روش‌هایی مانند آنالیز RTT و FPSE استفاده شده است. شبکه‌های عصبی و رمزگذارهای خودکار به‌منظور تشخیص ترافیک و حملات توزیع شده منع سرویس با دقت بالا به کار رفته‌اند. پیشرفت در یادگیری ماشین و الگوریتم‌های مختلف، چالش‌های شناسایی دقیق را باقی گذاشته است. یک پژوهش در زمینه ایمنی جاده‌ها در شرایط کم‌دید، الگوریتمی برای بهبود پروتکل AODV در شبکه های خودرویی ارائه کرده است(Singh, N.et al,۲۰۲۰)(I. Farris, T et al,۲۰۱۹)(Gaurav, A.et al,۲۰۲۲)(Gaurav, A. et al, ۲۰۲۲).

جدول۱. کارهای مرتبط

منبع	رویکرد	مزایا	معایب
(Singh, N.et al,۲۰۲۰)	چارچوب DEMD[۲]VANET-Cloud RS شامل HCAS، FACS، Twofish، ANN و فرآیندهای FT	افزایش امنیت با SHA-۳ و احراز هویت ECP در HCAS	سربار محاسباتی به علت فعالیت رمزنگاری درگیر در HCAS،که ممکن است بر کارایی سیستم اثر بذارد
(I. Farris, T et al,۲۰۱۹)	پروتکل مسیریابی AODV را در شبکه های خودرویی ابری تغییر و هنگام کاهش سرعت خودروی جلو هشدارهای لازم را به خودروها می دهد.	بهبود ایمنی جاده با اعلام هشدار راننده ها در باره کم کردن سرعت وسایل حمل و نقل، یاری در اتخاذ تصمیمات بهتر کردن و جلوگیری از حوادث در شرایط نوری ضعیف	موضوعات مرتبط با زیرساخت و به انطباق با سیستم‌ها ارتباط خودروهای فعلی
(Gaurav, A.et al,۲۰۲۲)	الگوریتم بیزی ساده، مدل مارکوف پنهان، ماشین بردار پشتیبانی که برای شناسایی حملات توزیع شده منع سرویس استفاده می شوند.	شناسایی حملات توزیع شده منع سرویس	نقص های قابل توجه در شناسایی حملات توزیع شده منع سرویس
(Gaurav, A. et al,۲۰۲۲)	انواع حملات متفاوت و موقع حملات توزیع شده منع سرویس پیشگیری انجام میشود	شناسایی حملات توزیع شده منع سرویس بر روی ماشین های مجازی	شناسایی حمله با توجه به ویژگی های حمله، تجزیه و تحلیل داده های بسته ماشین های مجازی احتمال دارد برای تشخیص حملات از اعتبار کافی برخوردار نباشند

تحقیقات برای بهبود تشخیص و جلوگیری از حملات توزیع شده منع سرویس با استفاده از شبیه‌سازی‌های GNS۳ و مدلسازی آموزش داده می‌شود.

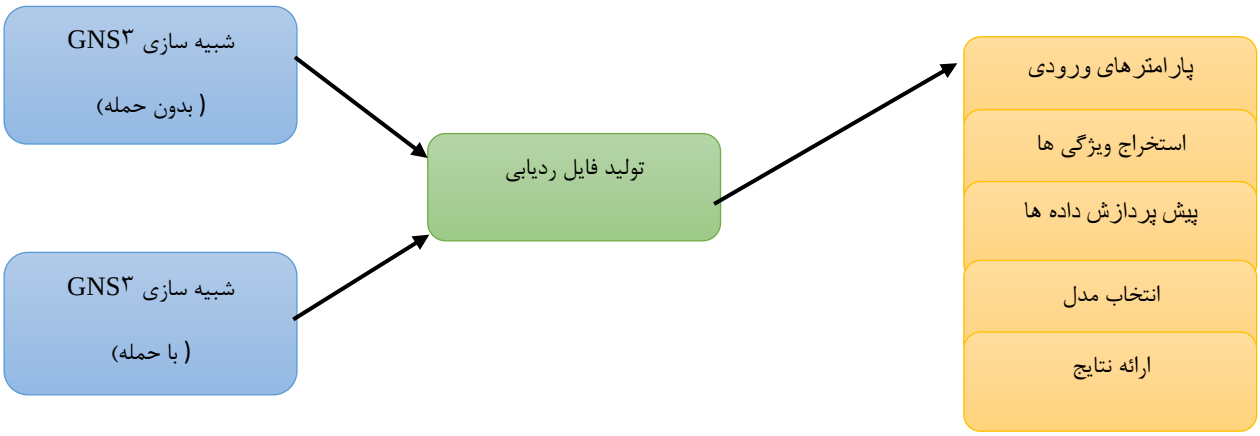
روند حملات توزیع شده منع سرویس

در اوایل حملات توزیع شده منع سرویس، هدف ایجاد ترافیک زیاد بود و وب‌سایت‌هایی مانند آمازون و یاهو مورد حمله قرار گرفتند. ابزارهای مهاجم مانند TFN و Trinoo برای این نوع حملات استفاده می‌شد. تشخیص این حملات از طریق شناسایی ناهنجاری‌ها در ترافیک شبکه انجام می‌گرفت، اما شناسایی دقیق بسته‌ها به دلیل جعل آدرس IP دشوار بود. هکرها به جمع‌آوری

رایانه‌های زامبی با طراحی کرم‌های اینترنتی روی آوردند و نمونه‌ای مانند کرم Slammer منجر به حملات توزیع شده منع سرویس وسیع شد. این حملات شامل سیل TCP SYN، TCP/UDP/ICMP و HTTP GET بودند، اما به دلیل تنوع و حجم داده‌ها، شناسایی مهاجمان توسط روش‌های موجود ناموفق شد (Alzahrani, R. J., & Alzahrani, A, ۲۰۲۱)

حملات توزیع شده منع سرویس و روش پیشنهادی

شبکه های خودرویی ابری شبکه‌ای از خودروهای متصل است که به‌طور مستقل ارتباط دارند. سه عنصر اصلی آن شامل OBU، AU و RSU بوده که OBUs نقاط شبکه را شکل می‌دهند.



شکل ۱. روش پیشنهادی

شبکه‌های خودسازمان ده به گونه‌ای طراحی شده‌اند که خودبه‌خود سازمان‌یابی کنند و خدمات خاصی ارائه دهند. شبکه های خودرویی ابری به خاطر تناوب ارسال‌ها و اندازه‌های کوتاه، در برابر حملات توزیع شده منع سرویس آسیب‌پذیر است. وسایل نقلیه می‌توانند در محدوده خود ارتباط برقرار کنند و در صورت خروج از این محدوده، اطلاعات از طریق رویکرد چند مرحله‌ای منتقل می‌شود. ساختار غیرمتمرکز گره‌ها شناسایی حملات را دشوار می‌کند.

در بخش‌های فرعی بعدی، یک روش ساختاری پیشنهاد شده است که از دو مرحله مجزا تشکیل شده است که هر دو به طور قابل‌توجهی به هدف کلی افزایش امنیت و ایمنی در شبکه‌های خودرو کمک می‌کنند. این رویکرد ماهیت پویا و چالش برانگیز محیط های خودرو را با تاکید ویژه بر ارتباطات بلادرنگ و اقدامات پیشگیرانه برای پیشگیری از تصادف در نظر می گیرد. یکی بدون حمله و دیگری با حمله، بررسی تأثیر بر نسبت تحویل بسته. در سناریو بدون حمله، وسایل نقلیه عادی با واحد کنار جاده به طور مؤثر ارتباط برقرار کرده و نرخ تحویل بسته بالایی به دست آمد. در مقابل، در سناریوی حمله، گره‌های مهاجم بسته‌ها را منحرف کرده و باعث ایجاد وضعیت حملات توزیع شده منع سرویس شدند که ارتباط را با تاخیر مواجه کرد و نرخ تحویل بسته را کاهش داد. پارامترهای مختلفی مانند IP مبدا، IP مقصد، زمان‌بندی و اندازه بسته در حین شبیه‌سازی ثبت و در فایل ردیابی ذخیره شدند.

جدول ۲. پارامترهای شبیه سازی

پارامتر	ارزش
کانال	LTE-V
انتشار رادیویی	انتشار قانون توازن
رابط شبکه	LTE-V
MAC	۳GPP
صف رابط	OFDMA
حداکثر بسته ها	۲۰۰
تعداد گره های mobile	۸
پروتکل مسیریابی	DSR
بعد X توپوگرافی	۸۰۰
بعد Y توپوگرافی	۸۰۰
زمان شبیه سازی	۱۲۰ نانو ثانیه

پیش‌بینی شامل استفاده از مدل‌های یادگیری تقویتی مانند(Gradient Boosting Machines(GBM، XGBoost، LightGBM و CatBoost برای شناسایی سناریوهای حملات توزیع شده منع سرویس و سالم است. قبل از به کارگیری مدل‌ها، مراحل پیش‌پردازش داده‌ها ضروری است که شامل مدیریت داده‌های ناقص و زائد می‌شود. در این مرحله، فیلتر کردن داده‌ها و نرمال‌سازی انجام می‌شود. هدف استخراج ویژگی، شناسایی ویژگی‌های مرتبط و حذف اطلاعات نامربوط است. در پایان، مدل‌های طبقه‌بندی بر روی داده‌های پردازش شده پیاده‌سازی و ارزیابی می‌شوند. برای مقایسه، ماتریس‌های سردرگمی رسم شده‌اند.

محاسبات و نتیجه

تمام آزمایش‌ها بر روی ویندوز انجام شده، ویژگی هایی که تأثیر عمده ای دارند نرخ تحویل بسته و انرژی هستند(Chartuni, A., & Márquez, J., ۲۰۲۱) می توان آنها را مشتق کرد

فرمول۱

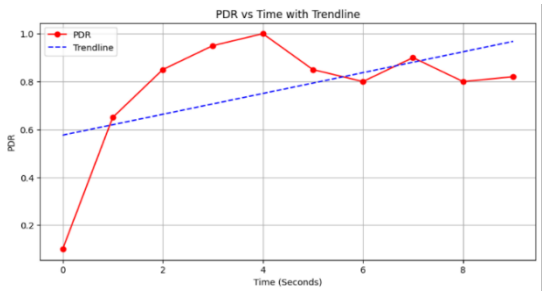
$$\text{نرخ تحویل بسته} = \frac{\text{تعداد بسته های دریافتی}}{\text{تعداد بسته های شده ارسال}}$$

فرمول۲

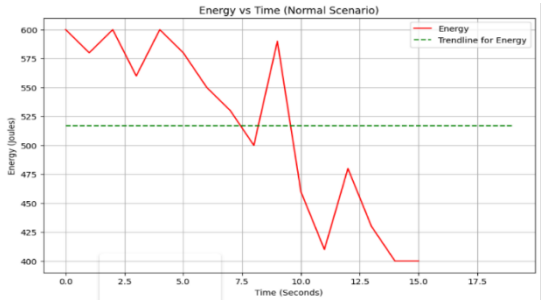
$$\text{انرژی} = \frac{\text{تعداد پرش} * \text{تعداد بسته های دریافتی} * \text{انرژی واحد به ازای هر بسته}}{\text{نرخ تحویل بسته}}$$

این مجموعه داده مشخصات متنوعی را که مدل برای آموزش استفاده کرده، شرح می‌دهد. میانگین میزان نرخ تحویل بسته در مجموعه داده ترکیبی تقریباً ۰.۸۲ است و یک الگوی بنیادی حدود ۰.۹۸ دارد. همچنین، مصرف انرژی برای داده‌های ترکیبی تقریباً

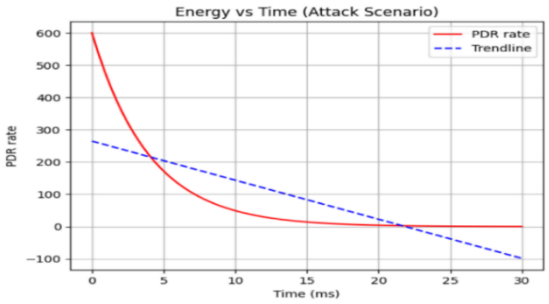
۴۰۰ است. تکنیک‌های متداول برای ارزیابی مدل‌ها به کار می‌روند. ماتریس سردرگمی در شکل ۵ و معیارهای صحت، دقت، حساسیت و F۱ در جدول ۴ نشان داده شده است. مدل XGBoost بهترین عملکرد را دارند، در حالی که مدل GBM و LightGBM پایین‌ترین امتیاز را می‌گیرند.



شکل۲. نرخ تحویل بسته در مقابل نمودار زمان (حالت حمله)



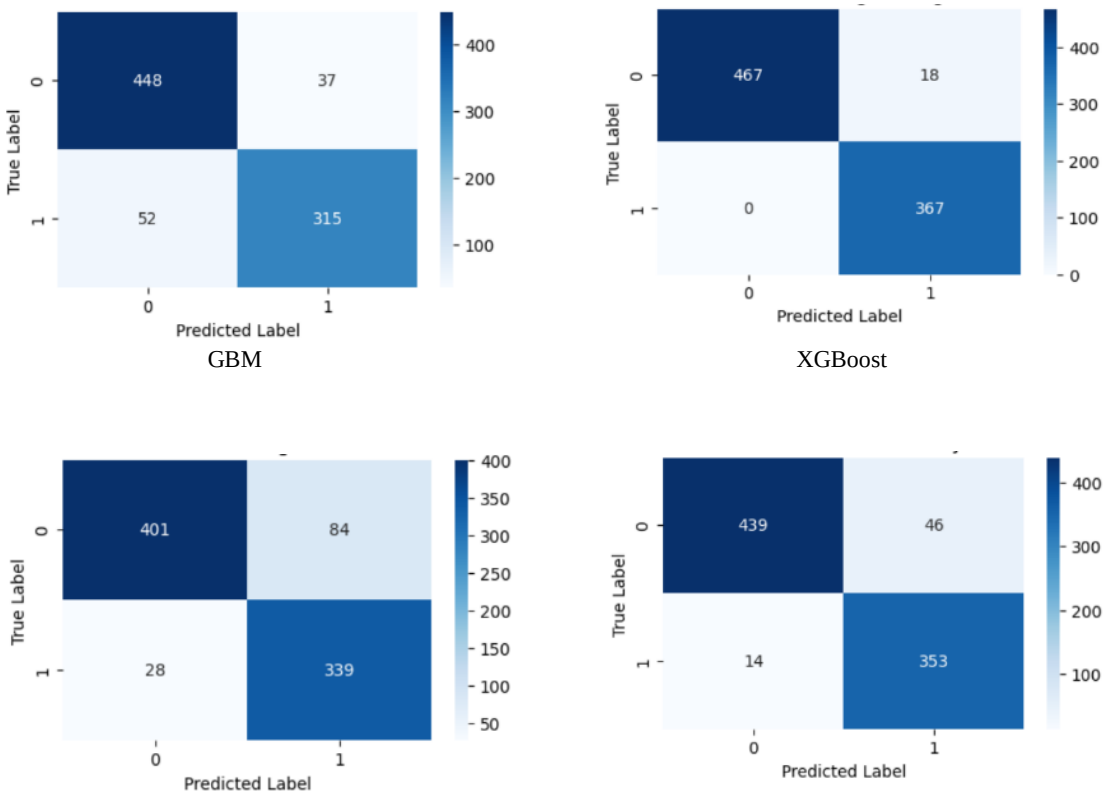
شکل۳. نمودار انرژی در مقابل زمان (حالت عادی)



شکل ۴. نمودار انرژی در مقابل زمان (حالت حمله)

جدول ۳. ویژگی های مجموعه داده

ویژگی ها	توضیحات
حملات	داده های بدست آمده از حالت عادی یا حالت حملات توزیع شده منع سرویس
IP منبع	آدرسIP منبع
IP مقصد	آدرس IP مقصد
حملات توزیع شده منع سرویس	برای حالت حملات توزیع شده منع سرویس می باشد
فاصله	برای شبیه سازی شبکه های خودرویی است
طول کل	طول بسته های ارسال شده است
نرخ تحویل بسته	$\frac{\text{تعداد بسته های دریافتی}}{\text{تعداد بسته های شده ارسال}}$



شکل ۵. ماتریس سردرگمی مدل های طبقه بندی مختلف

جدول ۴. معیارهای عملکرد

طبقه بندی مدل	امتیاز صحت	امتیاز حساسیت	امتیاز دقت	امتیاز F1
GBM	۰.۸۹۹۰	۰.۸۹۶۹	۰.۸۷۲۳	۰.۸۷۶۳
XGBoost	۰.۹۷۳۵	۰.۹۵۸۵	۱	۰.۹۷۹۳
LightGBM	۰.۸۹۹۰	۰.۸۰۹۳	۰.۹۲۹۴	۰.۸۵۱۷
CatBoost	۰.۹۲۷۵	۰.۸۸۴۲	۰.۹۶۴۱	۰.۹۲۷۲

نتایج GBM نشان دهنده ۴۴۸ پیش بینی صحیح مثبت و ۳۱۵ پیش بینی صحیح مثبت منفی، همچنین ۳۷ پیش بینی اشتباه منفی و ۵۲ پیش بینی اشتباه مثبت است. نتایج XGBoost نشان‌دهنده ۴۶۷ پیش بینی صحیح مثبت و ۳۶۷ پیش بینی صحیح مثبت منفی، همچنین ۱۸ پیش بینی اشتباه منفی و ۰ پیش بینی اشتباه مثبت است. LightGBM ۴۰۱پیش بینی صحیح مثبت و ۸۴ پیش بینی صحیح مثبت ۲۸ پیش بینی اشتباه منفی ارائه می‌دهد. CatBoost نشان‌دهنده ۴۳۹ پیش بینی صحیح مثبت و ۳۵۳ پیش بینی صحیح مثبت منفی، همچنین ۴۶ پیش بینی اشتباه منفی و ۱۴ پیش بینی اشتباه مثبت است. مدل GBM و LightGBM با صحت۰.۸۹۹۰، XGBoost برابر ۰.۹۷۳۵وCatBoost برابر۰.۹۲۷۵می باشد. مدلGBM وLightGBM دارای کمترین مقدار صحت و XGBoost بیشترین مقدار می باشد.

نتیجه گیری

می‌دهد و به ارزیابی تکنیک‌های مبتنی بر یادگیری تقویتی (Boosting) در این زمینه می‌پردازد. یکی از اجزای کلیدی آن، تحلیل آماری ویژگی‌های ترافیک شبکه، شامل وضعیت‌های عادی و حملات خصمانه است. این تحلیل، تعیین شاخص‌ها و آستانه‌ها برای شناسایی دقیق حملات توزیع شده منع سرویس را تسهیل کرده است. نتایج شبیه‌سازی ارتباط معکوس میان مصرف انرژی و نرخ تحویل بسته را نشان می‌دهد. همچنین، الگوریتم XGBoost ویژگی پیش‌بینی قابل توجهی ارائه می‌دهد.

منابع

Das, D., Sethuraman, S. C., & Satapathy, S. C. (۲۰۲۲). A decentralized open web cryptographic standard. Computers and Electrical Engineering, ۹۹, ۱۰۷۷۵۱.

Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Zhang, Y., ... & Hu, B. (۲۰۱۸). Privacy- preserving content dissemination for vehicular social networks: Challenges and solutions. IEEE Communications Surveys & Tutorials, ۲۱(۲), ۱۳۱٤-۱۳٤٥.

De La Torre, G., Rad, P., & Choo, K. K. R. (۲۰۲۰). Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems, 108*, ۱۰۹۲-۱۱۱۱.

Singh, N., Sinha, N., Liébana-Cabanillas, F.J., ۲۰۲۰. Determining factors in the adoption and recommendationof mobile wallet services in india: Analysis of the effect of innovativeness, stress to use and social influence International Journal of Information Management ٥٠, ۱۹۱–۲۰٥.

I. Farris, T. Taleb, S. Member, Y. Khettab, J. Song, S. Member, A survey on emerging SDN and NFV security mechanisms for IoT systems, IEEE Commun. Surv. Tutor. ٢١ (١) (٢٠١٩) ٨١٢–٨٣٧.

Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (٢٠٢٢). A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. Enterprise Information Systems, ١–٢٥.

Gaurav, A., Psannis, K., & Peraković, D. (٢٠٢٢). Security of cloud-based medical internet of things (miots): A survey. International Journal of Software Science and Computational Intelligence, ١٤(١), ١–١٦.

Alzahrani, R. J., & Alzahrani, A. (٢٠٢١). Security analysis of ddos attacks using machine learning algorithms in networks traffic. Electronics, ١٠(٢٣), ٢٩١٩.

Chartuni, A., & Márquez, J. (٢٠٢١). Multi-classifier of DDoS attacks in computer networks built on neural networks . Applied Sciences, ١١(٢٢), ١٠٦٠٩.

Nazanin Salehamin[1]

Department of IT and Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran[1]

Kambiz Majidzadeh[2*]

Department of IT and Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran[2]

Abstract

Vehicle ad-hoc networks (VANET) technology has attracted attention, especially in the emerging context of cloud VANET as a key component in connected and autonomous vehicles. The automotive industry's transformation towards automation and vehicle integration into the digital ecosystem has revolutionized wireless communications. However, security is still a key issue in these advanced technological landscapes. Protecting system integrity and data privacy is of utmost importance before cloud solutions in VANET are widely adopted. This study addresses the critical issue of security in the context of cloud VANET. Specifically, the focus is on predicting and mitigating DDoS attacks that may disrupt the performance of connected vehicles and cloud-dependent services. To address this issue, an innovative design framework is presented to document and analyze network flows in the cloud VANET. Furthermore, it uses reinforcement learning techniques for classification and predictive analysis with an accuracy of ۹۷,۳۵٪. The architecture outlined in this research enables significant improvements in security solutions for VANET cloud implementations. This capability ensures practical use for real systems and enables timely response to security threats and breaches.

Keywords: Ad Hoc networks, VANETs Cloud, reinforcement learning, distributed denial of service attacks, GNS۳ simulation.