Encyclopedia of Digital Transformation
Vol. 2; No. 4; PP. 1-18
winter 2021
DOI: 10.22034/dtj.2023.394376.1087

MehrAlborz University

DoS Attack Detection in the loV Using Convolutional Neural Network

Zahra Janfada[1], Seyed Amin Hosseini Seno[2]

Abstract

The Internet of Vehicles (IoV) is an emerging concept in Intelligent Transportation Systems (ITS) that aims to improve pedestrian and driver safety and traffic monitoring, But the IoV is vulnerable to various attacks. Therefore, security in the IoV is a serious issue because it directly affects the lives of the users. One of the most important attacks in the IoV is the Denial of Service (DoS) attack, which prevents access to the services of IoV and most importantly causes traffic and road accidents and the safety of users. endangers Therefore, a solution based on deep learning is proposed to detect DoS attacks in the IoV. The proposed model consists of a 10-layer convolutional neural network that can effectively detect different types of denial of service attacks. The performance of the proposed model is evaluated with real and new VDoS-LRS dataset. Experimental results show that the proposed intrusion detection system has reached a 100% accuracy rate.

Keywords: *Entrepreneurial Marketing Ecosystem, Online Sales, Insurance Industry*.

---

1. M.Sc. Student, Department Computer Engineering, Ferdowsi University, Mashhad, Iran.

2. Assistant Professor, Department Computer Engineering, Ferdowsi University, Mashhad, Iran.

Submitted: 2023-04-24
Accepted: 2023-11-12
Corresponding Author: Seyed Amin Hosseini Seno
Email: hosseini@um.ac.ir

دانشنامهٔ تحول دیجیتال

دانشگاه مهرالبرز
دورهٔ ۲، شمارهٔ ۴
زمستان ۱۴۰۰
صص. ۱- ۱۸

Encyclopedia of Digital Transformation
DOI: 10.22034/dtj.2023.394376.1087

تشخیص حمله انکار سرویس در اینترنت وسایل نقلیه با استفاده از شبکه عصبی کانولشن

زهرا جانفدا[۱]، سیدامین حسینی سنو[۲]

چکیده

اینترنت وسایل نقلیه (IoV) مفهومی نوظهور در سیستم‌های حمل‌ونقل هوشمند (ITS) است که هدف بهبود ایمنی عابران پیاده و رانندگان و نظارت بر ترافیک را دنبال می‌کند؛ اما ارتباطات اینترنت وسایل نقلیه در برابر حملات مختلف آسیب‌پذیر هستند؛ بنابراین امنیت در اینترنت وسایل نقلیه یک مسئله جدی است؛ زیرا مستقیماً بر زندگی کاربران آن تأثیر می‌گذارد. یکی از مهم‌ترین حملات در این محیط، حمله انکار سرویس (DoS) است که از دسترسی به سرویس‌های اینترنت وسایل نقلیه جلوگیری می‌کند و از همه مهم‌تر باعث ترافیک و تصادفات جاده‌ای می‌شود و ایمنی کاربران را به خطر می‌اندازد؛ بنابراین، یک راه‌حل مبتنی بر یادگیری عمیق برای شناسایی حملات انکار سرویس در محیط اینترنت وسایل نقلیه پیشنهاد شده است. مدل پیشنهادی از شبکه عصبی کانولوشن ۱۰ لایه تشکیل شده است که می‌تواند انواع مختلف حملات انکار سرویس را به طور مؤثر تشخیص دهد. عملکرد مدل پیشنهادی با مجموعه داده واقعی و جدید VDoS-LRS ارزیابی شده است. نتایج تجربی نشان می‌دهد که سیستم تشخیص نفوذ پیشنهادی به نرخ صحت ۱۰۰٪ رسیده است.

کلمات کلیدی: *اینترنت وسایل نقلیه، حمله انکار سرویس، سیستم تشخیص نفوذ، شبکه عصبی کانولوشن.*

---

۱. دانشجو کارشناسی ارشد گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد، ایران.

۲. استادیار گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد، ایران.

تاریخ دریافت مقاله: ۱۴۰۲/۰۲/۰۴
تاریخ پذیرش نهایی مقاله: ۱۴۰۲/۰۸/۲۱
نویسندهٔ مسئول مقاله: سید امین حسینی سنو
Email: hosseini@um.ac.ir

مقدمه

هر روز بر تعداد وسایل نقلیه در جاده‌ها افزوده می‌شود؛ بنابراین نیاز به سیستم‌های حمل‌ونقل هوشمند (ITS)[1]مدام در حال افزایش است. افزایش تعداد وسایل نقلیه در جاده‌ها می‌تواند منجر به افزایش تصادفات و ترافیک طولانی‌مدت شود (آدیکاری و همکاران[2]، ۲۰۲۰). برای حل این مشکلات به یک سیستم مدیریتی خوب نیاز است. یکی از راه‌حل‌های ارائه شده توسط محققان، اینترنت وسایل نقلیه (IoV) است که در مقایسه با شبکه‌های اقتضایی خودرو (VANET) از مقیاس‌پذیری بالاتری برخوردار هستند و شبکه عظیمی از خدمات را برای شهرهای بزرگ فراهم می‌کند؛ بنابراین اینترنت وسایل نقلیه یکی از فعال‌ترین زمینه‌های تحقیقاتی در سیستم‌های حمل‌ونقل هوشمند محسوب می‌شود که ترکیبی از شبکه‌های اقتضایی خودرو و اینترنت اشیاء (IoT)[3]است (شارما و کاوشیک[4]، ۲۰۱۹)

بنابراین اینترنت وسایل نقلیه شبکه‌ای از وسایل نقلیه مجهز به سنسورها، نرم‌افزارها و فناوری‌هایی هستند که هدف اتصال و تبادل داده‌ها را دنبال می‌کنند. در واقع یک هدف مهم اینترنت وسایل نقلیه این است که وسایل نقلیه بتوانند در زمان واقعی با رانندگان، عابران پیاده، سایر وسایل نقلیه و زیرساخت‌های کنار جاده‌ای ارتباط برقرار کنند (احمد[5]، ۲۰۲۳).

در چارچوب اهداف اینترنت اشیاء، بسیاری از این اشیاء مانند وسایل نقلیه متصل، اتومبیل‌هایی هستند که می‌توانند به صورت بی‌سیم با انواع مختلف دستگاه‌های متصل به اینترنت، دستگاه‌های موجود در ماشین یا خارج از ماشین ارتباط و تعامل برقرار کنند. این امر منجر به یک نوع خاص از اینترنت اشیاء به نام اینترنت وسایل نقلیه می‌شود که دستیابی به مدیریت یکپارچه در حمل‌ونقل هوشمند و سایر کاربردهای شهرهای هوشمند را فراهم می‌کند (رانی و شارما[6]، ۲۰۲۳). با توجه به استفاده از فناوری‌های پیشرفته ارتباطات در اینترنت وسایل نقلیه، این محیط در مقابله با مسائل مختلف ترافیکی و رانندگی سودمند است و منجر به ایمنی مسافران می‌شود و تجربه رانندگی را راحت می‌کند. ارتباط بین خودرویی، ارتباط درون خودرویی و اینترنت موبایل وسایل نقلیه، سه مؤلفه اصلی ارتباطی اینترنت وسایل نقلیه هستند (عباسی و همکاران[7]، ۲۰۲۱).

به دلیل باز بودن و خود سازمان‌دهی محیط اینترنت وسایل نقلیه، مهاجمان مخرب زیادی می‌توانند وارد این محیط شوند؛ زیرا برای ارتباطات کارآمد در اینترنت وسایل نقلیه، از انواع مختلف فناوری‌های بی‌سیم استفاده می‌شود (صمد و همکاران[8] ، ۲۰۱۸). الف) ارتباطات وسایل نقلیه (DSRC / CALM)، ب) ارتباطات تلفن (LTE، WiMax و ماهواره) و ج) ارتباطات استاتیک برد کوتاه (Zigbee، بلوتوث و Wi-Fi). از طرفی در اکثر کاربردهای اینترنت وسایل نقلیه مربوط به ایمنی، پیام‌ها پخش می‌شوند و باید در مدت زمان کوتاهی تحویل داده شوند و پیام ارسالی نیز باید ایمن و رمزگذاری شود تا هیچ‌گونه اطلاعات شخصی در مورد کاربر را فاش نکند؛ بنابراین با در نظرگرفتن مکانیزم‌های امنیتی نباید به این مهاجمان اجازه دهیم تا باعث تأخیر در ارسال پیام‌های زمان واقعی شوند.

از طرفی ادغام سنسورها با وسایل نقلیه، وضعیت کاملی از اینترنت وسایل نقلیه را تشکیل می‌دهد که پس از آن مسئول هرگونه اثر مخرب بر روی شبکه است. هرگونه داده خارجی از سنسورهای دشمن مربوط به محیط سیستم ترمز، تشخیص دود، سیستم هشداردهنده و وضعیت جاده می‌تواند کاملاً شبکه را گمراه کند و یک وضعیت ناخوشایند به وجود آورد. دسته دیگری از حمله باز از طریق رایانش ابری اتفاق می‌افتد. مهاجمان ابری می‌توانند یک حمله مداوم Dos[9] انجام دهند و به کاربران واقعی با نقض دسترسی آن‌ها به این فناوری، آسیب برسانند (کریمتات و همکاران[10]، ۲۰۲۰)؛ بنابراین امنیت یکی از مهم‌ترین چالش‌ها

1. Intelligent Transportation System
2. Adhikary et al.
3. Internet of Objects
4. Sharma & Kaushik
5. Ahmed
6. Rani & Sharma
7. Abbasi et al.
8. Samad et al.
9. Denial-Of-Service
10. Kirimtat et al.

برای پیاده‌سازی اینترنت وسایل نقلیه است؛ زیرا پیام‌های حیاتی در این محیط به صورت بلادرنگ به اشتراک گذاشته می‌شوند. تحویل بلادرنگ این پیام‌ها می‌تواند بر زندگی کاربران تأثیر بگذارد. قبل از استقرار اینترنت وسایل نقلیه برای استفاده عمومی، الزامات امنیتی مانند احراز هویت، در دسترس بودن، یکپارچگی و محرمانگی باید رعایت شود (کلارستقی و همکاران[1]، ۲۰۱۹). الزام در دسترس بودن بسیار مهم است؛ زیرا پیام‌های بلادرنگ در اینترنت وسایل نقلیه ردوبدل می‌شوند. اگر در دسترس بودن پیام‌ها به خطر بیفتد، می‌تواند منجر به یک وضعیت بسیار بحرانی مانند از دست دادن جان کاربران شود.

حمله انکار سرویس (DoS) یک حمله جدی است که می‌تواند شبکه خودرویی را از بین ببرد. در واقع، هدف اصلی هر نوع حمله انکار سرویس این است که خدمات شبکه برای کاربران مورد نظر در دسترس نباشد (کومار و دوتا[2]، ۲۰۱۸). حملات انکار سرویس می‌توانند موجب هرج‌ومرج و نارضایتی کاربران شوند و جان انسان‌ها را به خطر بیندازند. هم‌چنین وقوع حملات انکار سرویس در یک بازه زمانی کوتاه، شناسایی آن‌ها را پیچیده‌تر می‌کند؛ بنابراین یافتن راه‌حلی دقیق برای شناسایی انواع حملات انکار سرویس یکی از اقدامات لازم برای نجات جان کاربران، ارتقاء سطح امنیت اینترنت وسایل نقلیه، حفظ کیفیت خدمات و جلب رضایت کاربران است (ورما و همکاران[3]، ۲۰۲۱).

حمله DoS در اینترنت وسایل نقلیه می‌تواند به سه روش مختلف اتفاق افتد (آدیکاری و همکاران، ۲۰۲۰):

الف) مسدود کردن کانال‌های ارتباطی که در آن دسترسی کاربران به شبکه با مسدود کردن کانال ارتباطی محدود می‌شود. پارازیت کانال با ارسال سیگنال با فرکانس بالا بین گره‌های موجود در یک دامنه یا بین گره‌ها و RSU[4] انجام می‌شود.

ب) بار اضافه شبکه که در آن مهاجم، ترافیک جعلی را به گره‌های دیگر یا RSU های شبکه ارسال می‌کند و گره‌های دیگر را مشغول می‌کند و آن‌ها را از انجام کارهای اساسی بازمی‌دارد و در نهایت عملکرد شبکه کاهش پیدا می‌کند.

ج) از بین بردن بسته در این حالت، مهاجم با drop کردن بسته‌ها، اطلاعات را برای سایر گره‌ها غیرقابل‌دسترس می‌کند.

با توسعه مداوم فناوری یادگیری عمیق در سال‌های اخیر، استفاده از فناوری یادگیری عمیق در تشخیص نفوذ، بیشتر و بیشتر می‌شود (احمد و همکاران، ۲۰۲۱). یادگیری عمیق، زیرمجموعه‌ای از یادگیری ماشین است که به شبکه عصبی عمیق مربوط می‌شود و یکی از داغ‌ترین مسائل روز محسوب می‌شود. در اصل در یادگیری عمیق مدلی ساخته و آموزش داده می‌شود و در نهایت مدل ذخیره شده همانند یک پایگاه داده خواهیم داشت که با سرعت بسیار بالا می‌تواند پاسخگوی تست و آزمایش مورد نظر باشد. هم‌چنین الگوریتم‌های یادگیری عمیق نسبت به الگوریتم‌های کم‌عمق (SNN) از میزان صحت و دقت بالاتری برخوردار هستند؛ بنابراین رویکرد یادگیری عمیق برای تشخیص حملات در اینترنت وسایل نقلیه از جدیدترین موضوعات در این زمینه محسوب می‌شود که به نتایج بسیار خوبی دست یافته است.

شبکه‌های عصبی کانولوشن (CNN[5]) ، از رایج‌ترین مدل‌های یادگیری عمیق محسوب می‌شود که برای پردازش داده‌های حجیم و ماتریسی بسیار مورد استفاده قرار می‌گیرند (احمد و همکاران، ۲۰۲۱). شبکه‌های عصبی کانولوشن هم‌چنین یک الگوریتم یادگیری عمیق متمایز کننده است که برای به حداقل رساندن تعداد ورودی‌های داده مورد نیاز برای شبکه عصبی مصنوعی قدیمی (ANN) با استفاده از نمایش معادل، تعامل پراکنده و اشتراک پارامترها، طراحی شده است؛ بنابراین شبکه‌های عصبی کانولوشن مقیاس‌پذیرتر می‌شود و به زمان کمتری برای آموزش نیاز دارد.

در این مقاله، ما یک مدل یادگیری عمیق برای تشخیص حمله انکار سرویس در اینترنت وسایل نقلیه با استفاده از مجموعه داده جدید (راحل و همکاران[6]، ۲۰۲۰) VDoS-LRS ارائه می‌کنیم. همچنین انواع مختلف حملات انکار سرویس را ارزیابی می‌کنیم و زمان تشخیص را برای داشتن یک مدل بلادرنگ در نظر می‌گیریم.

1. Kelarestaghi et al.
2. Kumar & Dutta
3. Verma et al.
4. Road Side Unit
5. Convolutional Neural Network
6. Rahal et al.

این پژوهش دارای نوآوری‌های زیر است:

۱) یک سیستم تشخیص نفوذ مبتنی بر شبکه عصبی کانولوشن برای تشخیص حمله انکار سرویس در اینترنت وسایل نقلیه پیشنهاد می‌شود. سیستم تشخیص نفوذ پیشنهادی می‌تواند انواع مختلف حملات انکار سرویس از جمله سیلاب UDP، سیلاب SYN و Slowloris را شناسایی کند.

۲) دو مدل مختلف شبکه عصبی کانولوشن برای تشخیص حمله انکار سرویس در اینترنت وسایل نقلیه مقایسه می‌شود تا با انتخاب تعداد مناسب لایه‌ها به بهترین نرخ تشخیص و زمان تشخیص بلادرنگ برسیم.

۳) روش پیشنهادی بر روی مجموعه داده واقعی و جدید VDoS-LRS که داده‌های شبکه واقعی را در سه محیط بزرگراه، شهری و روستایی نشان می‌دهد، ارزیابی می‌شود. برخی از سیستم‌های تشخیص نفوذ ارائه شده از مجموعه داده‌های غیرخودرویی یا بسیار قدیمی استفاده می‌کنند که باعث ارزیابی نادرست می‌شود.

پیشینهٔ پژوهش

استفاده از IDS های مبتنی بر یادگیری ماشین در بسیاری از کارهای موجود در زمینه تشخیص حملات در اینترنت وسایل نقلیه دیده می‌شود. در پژوهش (سای و همکاران[1]، ۲۰۲۰)، به کمک ماشین بردار پشتیبانی به تشخیص حملات سیل DDoS مبتنی بر UDP در اینترنت وسایل نقلیه پرداخته شده است. این سیستم پیشنهادی با ارائه یک الگوریتم سبک‌وزن و کاهش ویژگی‌ها از ۲۹ به ۴، محدودیت منابع OBU را در نظر گرفته است. در واقع به منظور کاهش ویژگی‌ها، الگوریتم کارآمد انتخاب ویژگی مبتنی بر هم‌بستگی برای آموزش SVM استفاده می‌شود. با این حال، استفاده از تابع هسته بهینه در SVM که برای جداسازی داده‌ها زمانی که به صورت خطی قابل تفکیک نیستند، استفاده می‌شود، یک چالش برای دستیابی به سرعت دسته‌بندی مورد نظر است (دادی و عابد[2]، ۲۰۲۰).

(کادام و کرووی[3]، ۲۰۲۱) از دسته‌بندی مبتنی بر KNN برای شناسایی حمله DDoS در شبکه‌های خودرویی استفاده کرده‌اند؛ اگرچه استفاده از KNN ساده است؛ اما تعیین مقدار بهینه k و شناسایی گره‌های از دست رفته، زمان‌بر و پرهزینه است.

در برخی مطالعات (بانگی و همکاران[4]، ۲۰۲۱)، (زنگ و همکاران[5]، ۲۰۲۱) RF برای تشخیص ناهنجاری و نفوذ در محیط اینترنت وسایل نقلیه پیشنهاد شده است و نشان داده‌اند که RF بهتر از KNN، شبکه عصبی مصنوعی (ANN) و SVM در تشخیص DDoS در شبکه‌های اینترنت وسایل نقلیه عمل می‌کند؛ زیرا به ویژگی‌های ورودی کمتری نیاز دارد. در نتیجه به محاسبات سنگین برای انتخاب ویژگی در IDS بلادرنگ نیاز ندارد.

(دی آنجلو و همکاران[6]، ۲۰۲۰) مناسب بودن خوشه‌بندی k-mean را برای تشخیص ناهنجاری در شبکه‌های اینترنت وسایل نقلیه با محاسبه شباهت ویژگی نشان می‌دهد. در واقع یک رویکرد مبتنی بر داده برای تشخیص ناهنجاری‌ها در گذرگاه CAN ارائه می‌شود که رفتار پیام‌های عبوری از گذرگاه را یاد می‌گیرد و سپس پیام‌ها را دسته‌بندی می‌کند و در نهایت در صورت کاربردهای مخرب، هشدار می‌دهد. این سیستم پیشنهادی قادر به تشخیص انواع حملات DoS است و نشان داده است که k-means بهتر از KNN و SVM در تشخیص حملات عمل می‌کند؛ اما معیارهای ارزیابی دقت، فرخوانی و معیار F را به منظور تشخیص کارآمدتر بررسی نکرده است.

یادگیری عمیق از بهترین رویکردها برای محافظت از اینترنت وسایل نقلیه است؛ زیرا دقت بالایی در تشخیص حملات شناخته شده دارد.

---

1. Sai et al.
2. Dadi & Abid
3. Kadam & Krovi
4. Bangui et al.
5. Zeng et al.
6. D’Angelo et al.

(ژانگ و همکاران[1]، ۲۰۱۹) و (اشرف و همکاران[2]، ۲۰۲۰) یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق برای سیستم‌های حمل‌ونقل هوشمند پیشنهاد دادند که به صحت کلی ۹۹٪ و ۹۸٪ به ترتیب برای مجموعه داده‌های car hacking و UNSWNB-15، رسیده است.

(اله و همکاران، ۲۰۲۲) یک مدل یادگیری عمیق ترکیبی به منظور بهبود صحت تشخیص حمله سایبری در اینترنت وسایل نقلیه پیشنهاد دادند. همچنین (علادی و همکاران[3]، ۲۰۲۱) یک سیستم تشخیص نفوذ مبتنی بر شبکه عصبی عمیق (DNN) برای شبکه‌های خودرویی پیشنهاد دادند. این سیستم تشخیص نفوذ پیشنهادی با استقرار در واحدهای کنار جاده‌ای (RSUs) و دریافت تمام داده‌های همه پخشی وسایل نقلیه و دسته‌بندی آن‌ها به ترافیک مخرب و عادی، تشخیص ناهنجاری را انجام می‌دهد. این سیستم به صحت بالای ۹۸٪ دست یافته است.

برخی از محققان از شبکه عصبی کانولوشن برای شناسایی حملات در اینترنت وسایل نقلیه استفاده کردند. (نی و همکاران[4]، ۲۰۲۰) یک سیستم تشخیص نفوذ مبتنی بر داده با چارچوب شبکه عصبی کانولوشن ارائه دادند که رفتارهای واحد کنار جاده‌ای در اینترنت وسایل نقلیه را در برابر حملات مختلف تجزیه‌وتحلیل می‌کند. سیستم تشخیص نفوذ پیشنهادی، محدودیت منابع واحدهای داخلی (OBU) وسایل نقلیه را در نظر گرفته است و داده‌های شبکه را از واحدهای کنار جاده‌ای جمع‌آوری می‌کند. در نهایت، صحت معماری عمیق پیشنهادی در مقایسه با شبکه‌های عصبی کم‌عمق، SVM و PCA به ۹۷/۶۰٪ رسیده است.

همچنین (احمد و همکاران، ۲۰۲۱) یک سیستم تشخیص نفوذ برای محافظت از درگاه CAN وسایل نقلیه در برابر حملات DoS و Fuzzy ارائه کردند. معماری VGG استفاده شده و سیستم یادگیری عمیق ارائه شده به طور قابل توجهی نرخ مثبت کاذب (FPR) را در مقایسه با تکنیک‌های یادگیری ماشین قدیمی کاهش می‌دهد. صحت کلی این سیستم به ۹۶٪ با نرخ مثبت کاذب ۰/۶٪ رسیده است.

(زنگ و همکاران، ۲۰۱۹) یک چارچوب DeepVCM برای تشخیص ترافیک مخرب در واحدهای داخلی وسایل نقلیه پیشنهاد دادند که از شبکه عصبی کانولوشن و LSTM تشکیل‌شده است. عملکرد این مدل با دقت، فراخوانی و معیار F1 ارزیابی شده است؛ اما معیار صحت مورد بررسی قرار نگرفته است؛ اگرچه سیستم‌های تشخیص نفوذ پیشنهادی در اینترنت وسایل نقلیه دقت بالایی دارند؛ اما هنوز جای زیادی برای بهبود عملکرد وجود دارد. هم‌چنین، شناسایی مؤثر انواع مختلف حمله انکار سرویس از نیازهای اساسی اینترنت وسایل نقلیه محسوب می‌شود تا از اثرات مخرب این حمله جلوگیری شود، در حالی که اکثر سیستم‌های تشخیص نفوذ پیشنهادی به آن توجه نکردند. به منظور ارائه یک سیستم تشخیص نفوذ مؤثر و کارا، در نظر گرفتن تمام معیارهای ارزیابی و استفاده از مجموعه داده واقعی، ضروری هست؛ بنابراین، مدل پیشنهادی به تشخیص دقیق انواع حمله انکار سرویس در اینترنت وسایل نقلیه با استفاده از مجموعه داده VDoS-LRS می‌پردازد.

1. Zhang et al.
2. Ashraf et al.
3. Alladi et al.
4. Nie et al.

جدول ۱: مقایسه سیستم‌های تشخیص نفوذ موجود مبتنی بر یادگیری کم‌عمق در IoV

مقاله	سال	تکنیک استفاده شده	مجموعه داده	هدف	معیارهای ارزیابی	محدودیت‌ها
نی و همکاران	۲۰۲۰	شبکه عصبی کانولوشن (CNN)	(ایجاد یک بستر آزمایشی برای شبیه‌سازی صحنه IoV)	طراحی یک سیستم تشخیص نفوذ مبتنی بر داده با تجزیه‌وتحلیل رفتارهای RSU، در برابر حملات مختلفی که منجر به نوسانات نامنظم جریان ترافیک می‌شود.	صحت، دقت، فراخوانی، معیار F و هشدار غلط ۱	- عدم استفاده از مجموعه داده عمومی. - ارزیابی روش پیشنهادی صرفاً با چهار مهاجم، یک RSU و بیست OBU.
اشرف و همکاران	۲۰۲۰	شبکه عصبی بازگشتی LSTM	Car Hack و UNSWN-B15	ارائه یک سیستم تشخیص نفوذ برای سیستم حمل‌ونقل هوشمند (ITS)، به ویژه برای کشف فعالیت‌های مشکوک شبکه داخل وسیله نقلیه (IVN)، ارتباطات V2V و V2I	صحت، دقت، فراخوانی و معیار F	- زمان پاسخ بالا. - نیاز به بررسی انواع بیشتر حملات. - عدم فیلتر کردن ویژگی‌ها. - عدم تشخیص چند کلاسه.
علادی و همکاران	۲۰۲۱	شبکه عصبی عمیق (DNN)	VeReMi Extension	ارائه یک سیستم تشخیص نفوذ مبتنی بر DNN که با استقرار در RSU ها و دریافت داده‌های همه پخشی وسایل نقلیه، تشخیص ناهنجاری را انجام می‌دهد.	صحت، دقت، فراخوانی و معیار F	- عدم بررسی نرخ مثبت کاذب، نرخ منفی کاذب و زمان پاسخ. - بار محاسباتی زیاد بر روی RSU ها ممکن است موجب اختلال در عملکرد آن در IoV شود.

1. False Alarm

جدول ۱: مقایسه سیستم‌های تشخیص نفوذ موجود مبتنی بر یادگیری کم‌عمق در IoV

مقاله	سال	تکنیک استفاده شده	مجموعه داده	هدف	معیارهای ارزیابی	محدودیت‌ها
علادی و همکاران	۲۰۲۱	LSTM انباشته شده و CNN-LSTM	VeReMi Extension	شناسایی وسایل نقلیه بدرفتار قبل از درخواست ارتباط از واحد داخلی (OBU) وسایل نقلیه، با کمک واحدهای کنار جاده‌ای	صحت، دقت، فراخوانی و معیار F	- تأخیر در ارتباطات V2V به دلیل استفاده ازRSU - نامناسب برای کاربردهای حساس به تأخیر به دلیل استفاده از محاسبات لبه‌ای

روش پژوهش

راهکار پیشنهادی

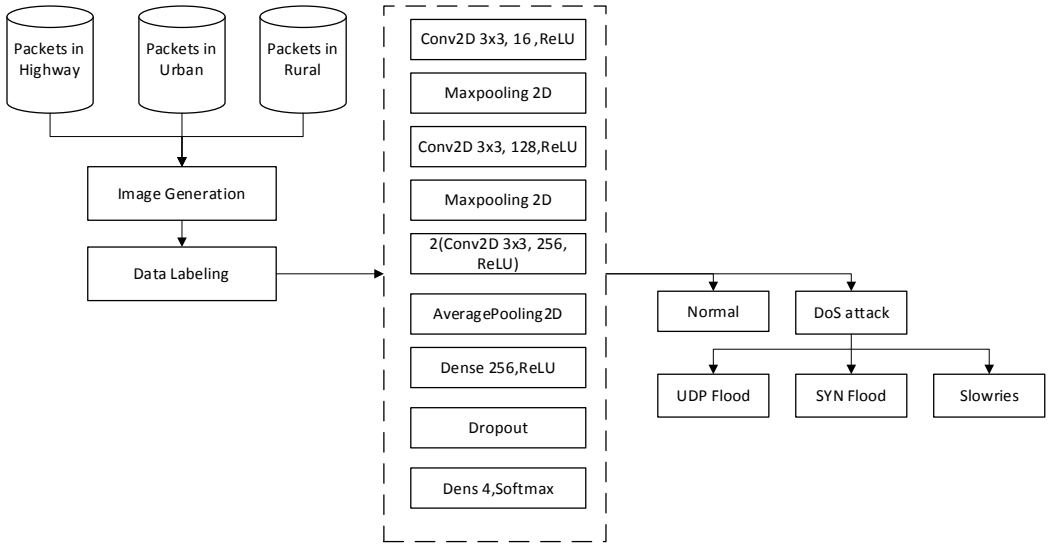
هدف این پژوهش، توسعه یک سیستم تشخیص نفوذ است که بتواند انواع مختلف حملات انکار سرویس از جمله سیلاب SYN، سیلاب UDP و Slowloris را در سه محیط بزرگراه، شهری و روستایی شبکه اینترنت وسایل نقلیه شناسایی کند. حمله سیلاب SYN با ارسال درخواست‌های زیاد SYN به وسیله نقلیه قربانی، از فرآیند دست دادن سه‌گانه TCP سوءاستفاده می‌کند تا منابع وسیله نقلیه را تمام کند و آن را برای ارتباط با سایر گره‌ها غیرقابل دسترس کند. حمله سیلاب UDP تعداد زیادی بسته UDP را به پورت‌های یک سرور می‌فرستد و می‌تواند با پاسخ دادن به بسته‌های ارسالی، سرور را مشغول نگه دارد؛ بنابراین، برای تعداد زیادی از بسته‌های UDP، وسیله نقلیه قربانی مجبور به ارسال بسته‌های ICMP زیادی می‌شود و در نهایت برای سایر کاربران از دسترس خارج می‌شود (گایو و همکاران[1]، ۲۰۱۹). Slowloris یک حمله انکار سرویس لایه کاربرد است که در آن تعداد زیادی درخواست HTTP به سرور ارسال می‌شود. داده‌ها به آرامی و به صورت دوره‌ای به سرور ارسال می‌شود؛ بنابراین سرور را مشغول می‌کند و از کار می‌اندازد.

شکل ۱ معماری این چارچوب را نشان می‌دهد. بسته‌ها در سه محیط اینترنت وسایل نقلیه به تصاویر تبدیل می‌شوند و پس از برچسب‌گذاری، توسط مدل پیشنهادی ما مبتنی بر شبکه عصبی کانولوشن آموزش داده می‌شوند تا بسته‌ها در اینترنت وسایل نقلیه به عادی و مخرب دسته‌بندی شوند.

پیش‌پردازش داده‌ها

برای توسعه سیستم تشخیص نفوذ پیشنهادی برای اینترنت وسایل نقلیه، از مجموعه داده VDoS-LRS (راحل و همکاران، ۲۰۲۰) استفاده شده است که شامل سه نوع اصلی حمله انکار سرویس: سیلاب SYN، سیلاب UDP و Slowloris است. این مجموعه داده مختص اینترنت وسایل نقلیه است و سه محیط شهری، بزرگراه و روستایی را در نظر گرفته است؛ زیرا هر سه محیط دارای ویژگی‌های متمایزی از جمله پوشش شبکه و سرعت وسیله نقلیه هستند.

1. Gao et al.



شکل ۱: چارچوب سیستم تشخیص نفوذ پیشنهادی مبتنی بر شبکه عصبی‌کانولوشن.

مجموعه داده VDoS-LRS دارای ۷۹ ویژگی و ۷۴۷۶۹۴ رکورد در محیط بزرگراه، ۲۶۱۸۹۱ رکورد در محیط شهری و ۶۴۶۴۲۶ رکورد در محیط روستایی است. همچنین این مجموعه داده ویژگی‌های شبکه را بر اساس پنج دسته مختلف، زمان، بایت‌ها، بسته‌ها، رفتار و جریان در نظر گرفته است. ویژگی‌های مبتنی بر رفتار (مانند: duration) برای ارزیابی گره بر اساس اقدامات قبل از رفتار آن استفاده می‌شود. به عنوان مثال، اگر یک اتصال برای مدت طولانی طول بکشد، این رفتار ممکن است رفتار یک حمله DoS باشد. ویژگی‌های مبتنی بر بایت‌ها و بسته‌ها (مانند: total_f/b_Packets، Init_Win_bytes_forward/backward، f/b_AvgBytesPerBulk، total/min/max/mean/std_f/b_Pktl، f/b_PktsPerSecond و ...) برای شمارش تعداد بایت‌ها یا بسته‌های مبادله شده، استفاده می‌شود. ویژگی‌های مبتنی بر بایت و بسته، امکان تشخیص افزایش ترافیک زیاد و غیرعادی که نشانه حمله DoS است را فراهم می‌کند. علاوه بر این، زمان صرف شده بین انتقال بسته‌ها در یک حمله DoS خیلی کوتاه است؛ به همین دلیل، ویژگی‌های مبتنی بر زمان (مانند: Min/mean/max/std_active، total/min/max/mean/std_f/b_iat، Min/mean/max/std_idle و ...) می‌تواند نشان‌دهنده حملات DoS باشد. ویژگی‌های جریان داده (مانند: Flow_Pkts/Byts_PerSecond، min/max_flowpktl، Min/max/mean/std_flowiat، Sflow_f/b_Packet و ...) به جای تمرکز بر روی بسته‌ها، روی جریانی از بسته‌ها با فضای ذخیره‌سازی کمتر کار می‌کنند.

این مجموعه داده، پورت و آدرس IP مبدأ و مقصد را در نظر نگرفته است؛ زیرا مهاجم‌ها می‌توانند به راحتی آن‌ها را تغییر دهند. همچنین ممکن است مدل، دسته‌بندی را گمراه کند و از تجزیه‌وتحلیل دقیق بقیه ویژگی‌ها جلوگیری کند.

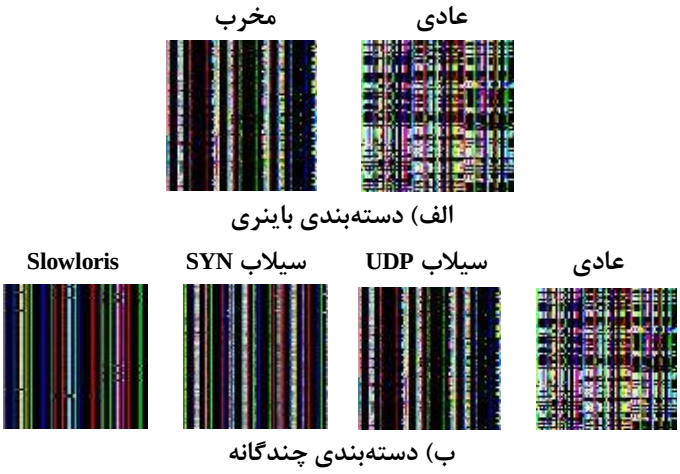
برای پیش‌پردازش بسته‌ها در سه محیط اینترنت وسایل نقلیه از Dropna برای تمیز کردن داده‌ها استفاده کردیم. از طرفی با توجه به کم بودن نمونه‌های کلاس حمله Slowloris و کلاس عادی، با مشکل داده‌های نامتعادل روبرو شدیم که منجر به پیش‌بینی نادرست می‌شود (دو و همکاران[1]، ۲۰۲۱)؛ بنابراین، برای داشتن داده‌های متعادل، از نمونه‌گیری بیش از حد تصادفی استفاده کردیم که نمونه‌های کلاس را بدون از دست دادن اطلاعات تکرار می‌کند.

سپس داده‌ها را به فرم‌های تصویر تبدیل کردیم؛ زیرا مدل‌های شبکه عصبی کانولوشن عملکرد بهتری روی تصاویر دارند (یانگ و شامی[2]، ۲۰۲۲). هر تصویر یک تصویر مربع رنگی با سه کانال قرمز، آبی و سبز است. مجموعه داده VDoS-LRS دارای ۷۹ ویژگی است؛ بنابراین هر بسته به تصویری به شکل ۳*۷۹*۷۹ تبدیل می‌شود. برای دسته‌بندی باینری، اگر همه

1. Du et al.
2. Yang & Shami

نمونه‌های یک تصویر، مخرب باشند، آن تصویر به عنوان مخرب برچسب‌گذاری می‌شود. از طرف دیگر، تصاویر با نمونه‌های معمولی با عنوان عادی برچسب‌گذاری می‌شوند. برای نسخه دسته‌بندی چندگانه چارچوب ما، تصویر با بیشترین نمونه از هر نوع حمله انکار سرویس به عنوان همان نوع حمله برچسب‌گذاری می‌شود.

پس از پیش‌پردازش داده‌ها، تصاویر آماده آموزش، توسط مدل پیشنهادی ما مبتنی بر شبکه عصبی کانولوشن هستند. نمونه‌های هر کلاس در محیط بزرگراه در شکل ۲ نشان داده شده است. همان‌طور که شکل ۲ قابل مشاهده است، نمونه‌های عادی و نمونه‌های مخرب دارای الگوهای ویژگی متفاوت هستند، در حالی که انواع مختلف حمله انکار سرویس دارای الگوهای ویژگی مشابه هستند که این مسئله تشخیص دقیق انواع مختلف حمله انکار سرویس را دشوار می‌کند.



شکل ۲: نمونه تصاویر هر کلاس در محیط بزرگراه: الف) دسته‌بندی باینری، ب) دسته‌بندی چندگانه.

تجزیه‌وتحلیل یافته‌ها

مدل پیشنهادی مبتنی بر شبکه عصبی کانولوشن

شبکه عصبی کانولوشن زیرگروهی از شبکه‌های عصبی است که عمدتاً برای دسته‌بندی تصاویر استفاده می‌شود (سونگ و همکاران[1]، ۲۰۲۰). شبکه عصبی کانولوشن به طور خودکار ویژگی‌های مهم را بدون نظارت انسانی تشخیص می‌دهد و لایه‌های کانولوشنی آن بدون از دست دادن اطلاعات، ابعاد بالای تصاویر را کاهش می‌دهد. همچنین لایه‌های ادغام آن تعداد پارامترهای یادگیری را کاهش می‌دهد و از بیش برازش جلوگیری می‌کند.

پس از آموزش مدل‌های مختلف شبکه عصبی کانولوشن بر روی مجموعه داده VDoS-LRS، دو مدل شبکه عصبی کانولوشن با بهترین عملکرد انتخاب می‌شوند. مدل ۱ و مدل ۲، مدل‌های منتخبی هستند که با تعداد لایه‌های مناسب و چیدمان صحیح آن‌ها طراحی شده‌اند. این دو مدل ساختار مشابهی دارند، با این تفاوت که مدل ۲ دارای لایه‌های کانولوشن بیشتری است که در جدول ۲ توضیح داده شده است. جدول ۲ ساختار این دو مدل را توضیح می‌دهد. تعداد نورون‌ها در هر لایه در پرانتز نشان داده شده است.

در هر دو مدل ۱ و ۲، فعال‌ساز واحد خطی اصلاح شده (ReLU) و لایه حداکثر ادغام پس از لایه‌های کانولوشن استفاده می‌شود. لایه کانولوشن، تصویر را برای یک ویژگی خاص فیلتر می‌کند و فعال‌ساز واحد خطی اصلاح شده، آن ویژگی را در تصویر فیلتر شده تشخیص می‌دهد. در نهایت، لایه حداکثر ادغام تصویر را متراکم می‌کند تا ویژگی‌ها را افزایش دهد؛ بنابراین، استفاده از واحد خطی اصلاح شده به جلوگیری از رشد نمایی در محاسبات مورد نیاز برای راه‌اندازی شبکه عصبی

1. Song et al.

کمک می‌کند (راغو و همکاران[1]، ۲۰۱۷). همچنین استفاده از لایه ادغام میانگین جهانی و لایه حذفی به جلوگیری از بیش برازش مدل پیشنهادی ما کمک می‌کنند.

در نهایت، از تابع softmax برای دسته‌بندی چندگانه به منظور برگرداندن احتمال‌های هر کلاس استفاده می‌شود که کلاس هدف بیشترین احتمال را دارد. سپس، آنتروپی متقاطع طبقه‌ای (categorical crossentropy) به عنوان تابع ضرر برای محاسبه تفاوت بین توزیع‌های احتمال استفاده می‌شود. از آنجایی که ما بیش از دو کلاس داریم، تابع ضرر آنتروپی متقاطع طبقه‌ای بهترین انتخاب است. همچنین از آدام به عنوان بهینه‌ساز برای کاهش تابع ضرر و ارائه دقیق‌ترین نتایج ممکن استفاده کردیم؛ زیرا این بهینه‌ساز بسیار سریع است (لی و همکاران[2]، ۲۰۲۱).

جدول ۲: چیدمان لایه‌ها در دو مدل ارائه شده

لایه‌ها	مدل ۱	مدل ۲
لایه ۱	Conv(16)	Conv(16)
لایه ۲	Maxpooling	Maxpooling
لایه ۳	Conv(256)	Conv(128)
لایه ۴	Averagepooling	Maxpooling
لایه ۵	Dense(256)	Conv(256)
لایه ۶	Dropout	Conv(256)
لایه ۷	Dense(4)	Averagepooling
لایه ۸	-	Dense(256)
لایه ۹	-	Dropout
لایه ۱۰	-	Dense(4)

مدل ۱ و ۲ بر روی مجموعه داده آموزشی با تعداد تکرار لازم و یکسان آموزش داده می‌شوند. از بین این دو مدل، مدل ۲ انتخاب می‌شود؛ زیرا نتایج بهتری در دسته‌بندی انواع مختلف حمله انکار سرویس به دست می‌آورد. شرح کامل ارزیابی این دو مدل در ادامه آورده شده است. بهترین مدل پیشنهادی (مدل ۲) یک شبکه عصبی کانولوشن منحصربه‌فرد ۱۰ لایه است که دارای توپولوژی لایه زیر است: لایه کانولوشن، لایه حداکثر ادغام، لایه کانولوشن، لایه حداکثر ادغام، لایه کانولوشن، لایه کانولوشن، لایه ادغام میانگین جهانی، لایه متراکم، لایه حذفی و در نهایت لایه متراکم. داشتن چندین لایه کانولوشن که در امتداد عمق مدل قرار گرفته‌اند، به مدل اجازه می‌دهد تا ویژگی‌های سطح بالا (نه فقط لبه‌ها و گوشه‌ها) را از تصاویر ورودی استخراج کنند. همچنین با استفاده از دو لایه کانولوشن متوالی می‌توانیم نمایش بهتری از تصویر، بدون از دست دادن سریع تمام اطلاعات مکانی داشته باشیم.

ارزیابی مدل پیشنهادی

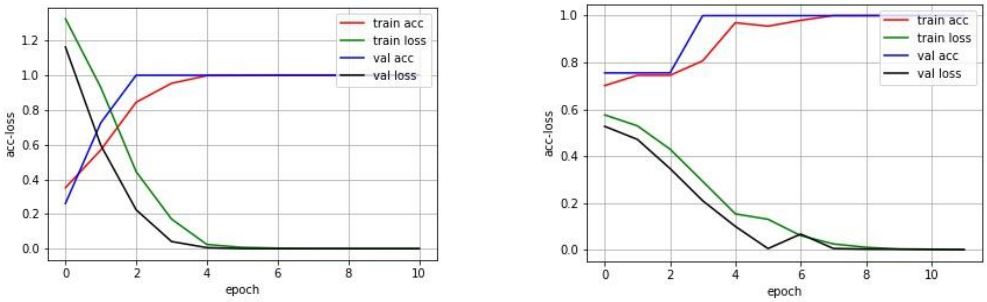
سیستم تشخیص نفوذ مبتنی بر شبکه عصبی کانولوشن پیشنهادی بر روی مجموعه داده VDoS-LRS (راحل و همکاران، ۲۰۲۰) ارزیابی شده است. این مجموعه داده، جدید و مربوط به سال ۲۰۲۰ است. در این بخش، مدل شبکه عصبی کانولوشن پیشنهادی خود را از طریق دو سناریو ارزیابی می‌کنیم: دسته‌بندی باینری برای دسته‌بندی بسته‌ها به ترافیک عادی و مخرب و دسته‌بندی چندگانه برای دسته‌بندی انواع مختلف حمله انکار سرویس (سیلاب SYN، سیلاب UDP و Slowloris). ما از

1. Raghu et al.
2. Li et al.

٪۱۰۰ مجموعه داده VDoS-LRS برای آزمایش‌های خود استفاده کردیم. ۷۵ درصد آن برای آموزش و ۲۵ درصد آن برای تست استفاده شده است.

ما آزمایش‌های خود را با استفاده از کتابخانه‌های Keras و Scikit-learn در پایتون انجام دادیم. در آزمایش‌ها، از بستر Google colab برای آموزش سریع‌تر مدل استفاده شده است؛ زیرا دارای GPU قدرتمند (Tesla K80) و پردازنده Intel Xeon با دو هسته ۲/۲۰ گیگاهرتز است.

معیارهای ارزیابی، از جمله صحت، دقت، فراخوانی، معیار F1، نرخ مثبت کاذب و نرخ منفی کاذب (FNR) برای ارزیابی عملکرد استفاده شده‌اند تا ارزیابی کاملی از سیستم تشخیص نفوذ پیشنهادی داشته باشیم (پاورز[1]، ۲۰۲۰). علاوه بر این، برای ارزیابی کارآمد مدل پیشنهادی، زمان تست هر بسته نیز در نظر گرفته شده و مقایسه می‌شود. در آزمایش‌های ما، تعداد دوره‌ها برابر با ۲۰ در نظر گرفته شده است؛ زیرا دوره‌های بسیار زیاد می‌تواند منجر به بیش برازش مجموعه داده آموزشی شود. همچنین، مقدار صبر (patience) برابر ۸ برای توقف زودهنگام (Early stopping) انتخاب شده است تا اگر در طول ۸ دوره، بهبود عملکرد مدل در مجموعه داده اعتبارسنجی مشاهده نشود، آموزش را متوقف تا از بیش برازش جلوگیری کند. همچنین به منظور افزایش سرعت آموزش، اندازه دسته را برابر ۱۲۸ در نظر گرفتیم؛ زیرا دسته‌های بزرگ‌تر مراحل جستجوی کمتری را برای حل بهینه انجام می‌دهند.



الف) دسته‌بندی باینری **ب) دسته‌بندی چندگانه**

شکل ۳: نمودارهای صحت و ضرر به دوره در مدل (۲) برای محیط شهری.

جداول ۳ تا ۵ نتایج دسته‌بندی این دو مدل را در سه محیط (بزرگراه، شهری و روستایی) شرح می‌دهند. همان‌طور که نتایج نشان می‌دهد، مدل پیشنهادی ما انواع مختلف حملات انکار سرویس را در هر سه محیط به طور مؤثر تشخیص می‌دهد. مدل ۲ لایه‌های کانولوشنی بیشتری نسبت به مدل ۱ دارد که باعث می‌شود ویژگی‌های سطح پایین بیشتری را یاد بگیرد و در دسته‌بندی چندگانه به نتایج بهتری دست پیدا کند؛ اما زمان تشخیص حملات را افزایش می‌دهد. همچنین نتایج مختلف در سه محیط نشان می‌دهند که هر محیط با ویژگی‌های منحصربه‌فرد خود مانند تراکم شبکه و سرعت وسایل نقلیه بر نتایج تشخیص حمله تأثیر می‌گذارد.

با ملاحظه مقادیر معیارهای ارزیابی به دست آمده، مشاهده می‌کنیم که مدل پیشنهادی در تمام معیارهای ارزیابی از جمله صحت، دقت، فراخوانی و معیار F بیشترین مقدار را دارد. این عملکرد خوب، نشان‌دهنده انتخاب تعداد مناسب لایه‌ها و چیدمان درست آن‌ها در مدل پیشنهادی است. در واقع هر چه داده‌های نرمال به درستی در کلاس نرمال و داده‌های هر نوع کلاس حمله انکار سرویس (سیلاب SYN، سیلاب UDP و Slowloris) به درستی در کلاس همان نوع حمله شناسایی شوند، مقدار دقت و فراخوانی بالاتری خواهیم داشت؛ بنابراین این مدل پیشنهادی بالاترین کارایی در تشخیص ترافیک مخرب در شبکه‌های خودرویی را خواهد داشت.

1. Powers

همان‌طور که در شکل ۳ نشان داده شده است، مدل پیشنهادی دارای صحت آموزشی ۱۰۰٪ و صحت اعتبارسنجی ۱۰۰٪ است. نمودارهای آبی و قرمز به ترتیب صحت اعتبارسنجی و آموزش و نمودارهای مشکی و سبز به ترتیب تابع ضرر اعتبارسنجی و آموزش را نشان می‌دهند. فاصله بین نمودارهای اعتبارسنجی و دقت آموزش در دوره‌های پایانی، بیش برازش را نشان می‌دهد؛ اگر فاصله بیشتر باشد، بیش برازش بیشتر است؛ اما همان‌طور که شکل ۳ نشان می‌دهد، ما کمترین بیش برازش را داریم.
همان‌طور که نمودارها در شکل ۳ نشان می‌دهد، تابع زیان مدل پیشنهادی ما در هر سه محیط بزرگراه، شهری و روستا با شیب کاهشی خوبی به کمترین مقدار رسیده است. این نشان‌دهنده رسیدن به نرخ یادگیری بهینه هست؛ زیرا هر چه نرخ یادگیری کوچک‌تر انتخاب شود، امکان بهبود تابع زیان بیشتر خواهد بود. از طرفی هرچه نرخ یادگیری بزرگ‌تر انتخاب شود، ممکن است با نوسان نمودار تابع زیان و مشکل بیش برازش روبرو شویم؛ بنابراین از مقدار کم تابع زیان و عدم نوسان آن نتیجه می‌گیریم که بهترین نرخ یادگیری برای این مدل پیشنهادی انتخاب شده است. همچنین از دلایلی که می‌توان برای شیب کاهشی خوب و بدون نوسان نمودار تابع زیان مدل پیشنهادی نام برد، استفاده درست لایه‌های حذف تصادفی در بین لایه‌های Dense است.

جدول ۳: ارزیابی و مقایسه عملکرد مدل‌ها در محیط بزرگراه

	روش	کلاس	دقت	فراخوانی	معیار F	میانگین مثبت کاذب	میانگین منفی کاذب	میانگین صحت	زمان تست هر بسته (ثانیه)
دسته‌بندی چندکلاسه	مدل ۱	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰۰۵۶	۰/۰۰۱۴۱	۰/۹۹۹۱۳	۰/۰۵۴۷۸
		حمله سیلاب UDP	۱/۰۰	۰/۹۹۴۳۵	۰/۹۹۷۱۷				
		حمله سیلاب SYN	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله Slowloris	۰/۹۹۲۵۷	۱/۰۰	۰/۹۹۶۲۷				
	مدل ۲	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۸۲۴
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله Slowloris	۱/۰۰	۱/۰۰	۱/۰۰				
	(راحل و همکاران ، ۲۰۲۰)	عادی	۰/۹۹۹۸۸	۰/۹۹۹۹۲	۰/۹۹۹۹۰	۰/۰۰۰۰۳	۰/۰۰۰۲۵	۰/۹۹۹۹۸	-
		حمله سیلاب UDP	۰/۹۹۹۹۹	۰/۹۹۹۹۹	۰/۹۹۹۹۹				
		حمله سیلاب SYN	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله Slowloris	۰/۹۹۹۰۵	۰/۹۹۹۰۵	۰/۹۹۹۰۵				
دسته‌بندی باینری	مدل ۱	عادی	۱/۰۰	۰/۹۶۳۴۱	۰/۹۸۱۳۷	۰/۰۱۸۲۹	۰/۰۱۸۲۹	۰/۹۹۷۱۳	۰/۰۵۴۲۰
		مخرب	۰/۹۹۶۹۰	۱/۰۰	۰/۹۹۸۴۵				
	مدل ۲	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۶۰۲۲
		مخرب	۱/۰۰	۱/۰۰	۱/۰۰				
		عادی	۰/۹۹۹۸۸	۰/۹۹۹۹۲	۰/۹۹۹۹۰	۰/۰۰۰۰۴	۰/۰۰۰۰۴	۰/۹۹۹۸۸	-

	(راحل و همکاران ۲۰۲۰،	مخرب	۰/۹۹۹۹۹	۰/۹۹۹۹۹	۰/۹۹۹۹۹				

همچنین همان‌طور که نمودارها در شکل ۳ نشان می‌دهد، مرحله‌به‌مرحله یادگیری بهتر شده و با کمترین تکرار، روند نزولی تابع زیان کامل می‌شود. از آنجایی تابع زیان داده‌های آموزشی به تابع زیان داده‌های اعتبارسنجی نزدیک است، می‌توان نتیجه گرفت بیش برازش به خوبی کنترل شده است. مدل شبکه عصبی کانولوشن پیشنهادی ما نه تنها روی داده‌های آموزشی خوب جواب داده؛ بلکه در مورد داده‌های آزمایشی بسیار خوب عمل می‌کند؛ به عبارت دیگر، بالا بودن مقادیر معیارهای ارزیابی در مدل پیشنهادی و کاهش بسیار خوب تابع زیان، نشان‌دهنده عملکرد بسیار عالی راهکار پیشنهادی ما است.

اکثر مقالاتی که به تشخیص حملات در اینترنت وسایل نقلیه پرداختند، حملات مخرب انکار سرویس را در نظر نگرفتند یا مقالاتی که به تشخیص حمله DoS پرداختند، انواع این حمله را در نظر نگرفتند. برخی مقالات برخی معیارهای ارزیابی ذکر شده را به منظور ارزیابی راهکار پیشنهادی خود بررسی نکردند که یکی از دلایل آن می‌تواند پایین بودن آن معیار باشد. به طور مثال، مقاله (زنگ و همکاران، ۲۰۱۹) در ارزیابی روش پیشنهادی خود به منظور تشخیص حمله DoS در IoV، معیار صحت را بررسی نکرده است.

جدول ۴: ارزیابی و مقایسه عملکرد مدل‌ها در محیط شهری

	روش	کلاس	دقت	فراخوانی	معیار F	میانگین مثبت کاذب	میانگین منفی کاذب	میانگین صحت	زمان تست هر بسته (ثانیه)
دسته‌بندی چندکلاسه	مدل ۱	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۱۳۹
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله Slowloris	۱/۰۰	۱/۰۰	۱/۰۰				
	مدل ۲	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۲۳۲
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله Slowloris	۱/۰۰	۱/۰۰	۱/۰۰				
	(راحل و همکاران، ۲۰۲۰)	عادی	۰/۹۹۹۸۹	۰/۹۹۹۶۹	۰/۹۹۹۷۹	۰/۰۰۰۰۸	۰/۰۰۰۰۸	۰/۹۹۹۹۷	-
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۰/۹۹۹۹۸	۰/۹۹۹۹۸	۰/۹۹۹۹۸				

	حمله Slowloris	۰/۹۹۲۷۵	۱/۰۰	۰/۹۹۶۳۶				
دسته‌بندی باینری	مدل ۱	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۰۵۶
		مخرب	۱/۰۰	۱/۰۰	۱/۰۰				
	مدل ۲	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۰۵۷
		مخرب	۱/۰۰	۱/۰۰	۱/۰۰				
	(راحل و همکاران، ۲۰۲۰)	عادی	۱/۰۰	۰/۹۹۹۸۴	۰/۹۹۹۹۴	۰/۰۰۰۰۵	۰/۰۰۰۰۵	۰/۹۹۹۹۹	-
		مخرب	۰/۹۹۹۹۹	۱/۰۰	۰/۹۹۹۹۹				

همچنین از آن جایی که حمله DoS به طور ناگهانی اتفاق می‌افتد و در دسترس بودن شبکه IoV را به خطر می‌اندازد؛ لازم است که به منظور تشخیص به موقع این حمله، زمان پاسخ روش پیشنهادی را محاسبه کنیم تا مطمئن شویم روش پیشنهادی در کمترین زمان، این حمله را تشخیص می‌دهد و شبکه IoV را از خطر بزرگ این حمله نجات می‌دهد؛ اما اکثر مقالات این معیار مهم را بررسی نکردند.

برای محافظت از اینترنت وسایل نقلیه در برابر حملات با استفاده از تکنیک‌های یادگیری ماشین، تحقیقات زیادی انجام شده است؛ اما از مجموعه داده‌های مختص شبکه خودرویی استفاده نکردند. اکثر آن‌ها از مجموعه داده‌های NSL-KDD، KDD99 و UNSW-NB15 که فاقد داده‌های شبکه خودرویی هستند، استفاده کردند که باعث ارزیابی نادرست مدل پیشنهادی می‌شود. از سوی دیگر، برخی از تحقیقات از داده‌های شبیه‌سازی‌شده استفاده کردند در حالی که پارامترهای شبیه‌سازی، محیط واقعی را منعکس نمی‌کنند؛ بنابراین، ما یک ارزیابی صحیح از مدل پیشنهادی خود داشتیم؛ زیرا مجموعه داده VDoS-LRS، یک مجموعه داده جدید، واقعی و مختص اینترنت وسایل نقلیه است.

جدول ۵: ارزیابی و مقایسه عملکرد مدل‌ها در محیط روستایی

	روش	کلاس	دقت	فراخوانی	معیار F	میانگین مثبت کاذب	میانگین منفی کاذب	میانگین صحت	زمان تست هر بسته (ثانیه)
دسته‌بندی چند کلاسه	مدل ۱	عادی	۰/۹۹۳۲۰	۱/۰۰	۰/۹۹۶۵۹	۰/۰۰۰۴۴	۰/۰۰۱۴۲	۰/۹۹۹۲۹	۰/۰۵۶۲۵
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۱/۰۰	۰/۹۹۴۲۹	۰/۹۹۷۱۳				
		حمله Slowloris	۱/۰۰	۱/۰۰	۱/۰۰				
	مدل ۲	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۶۹۶
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله Slowloris	۱/۰۰	۱/۰۰	۱/۰۰				

	(راحل و همکاران، ۲۰۲۰)	عادی	۰/۹۹۹۵۹	۰/۹۹۹۸۹	۰/۹۹۹۷۴	۰,۰۰۰۰۴	۰,۰۰۰۳۷	۰,۹۹۹۹۸	–
		حمله سیلاب UDP	۱/۰۰	۱/۰۰	۱/۰۰				
		حمله سیلاب SYN	۱/۰۰	۰/۹۹۹۹۹	۰/۹۹۹۹۹				
		حمله Slowloris	۰/۹۹۹۵۴	۰/۹۹۸۶۲	۰/۹۹۹۰۸				
دسته‌بندی باینری	مدل ۱	عادی	۰/۹۲۳۰۸	۱/۰۰	۰/۹۶	۰/۰۰۵۱۴	۰/۰۰۵۱۴	۰/۹۹۰۸۳	۰/۰۵۶۱۰
		مخرب	۱/۰۰	۰/۹۸۹۷۰	۰/۹۹۴۸۲				
	مدل ۲	عادی	۱/۰۰	۱/۰۰	۱/۰۰	۰/۰۰	۰/۰۰	۱/۰۰	۰/۰۵۷۵۳
		مخرب	۱/۰۰	۱/۰۰	۱/۰۰				
	(راحل و همکاران، ۲۰۲۰)	عادی	۰/۹۹۹۸۹	۰/۹۹۹۶۹	۰/۹۹۹۷۹	۰/۰۰۰۱۵	۰/۰۰۰۱۵	۰/۹۹۹۹۸	–
		مخرب	۰/۹۹۹۹۸	۰/۹۹۹۹۹	۰/۹۹۹۹۹				

(راحل و همکاران، ۲۰۲۰) با استفاده از الگوریتم درخت تصمیم (DT) به صحت ۹۹/۹۹٪ دست یافتند؛ اما زمان تشخیص را برای تشخیص بلادرنگ حملات مخرب انکار سرویس در نظر نگرفتند. همچنین، نتایج نشان می‌دهد که مدل‌های شبکه عصبی کانولوشن از سایر الگوریتم‌های یادگیری ماشین قدیمی در هر سه محیط بهتر عمل می‌کنند.

نتیجه‌گیری

اینترنت وسایل نقلیه در مقایسه با شبکه‌های اقتضایی خودرو، مقیاس‌پذیرتر است و شبکه بزرگ‌تری را برای شهرهای بزرگ فراهم می‌کند؛ اما امنیت و حریم خصوصی از چالش‌های اساسی این محیط محسوب می‌شوند؛ زیرا حملات مختلفی ممکن است در اینترنت وسایل نقلیه رخ دهد و باعث نارضایتی کاربر و ناکارآمدی شبکه شود. یکی از مهم‌ترین حملات، حمله انکار سرویس است که در دسترس بودن شبکه را به خطر می‌اندازد و موجب تصادفات جاده‌ای و از دست دادن جان کاربران می‌شود. سیستم‌های تشخیص نفوذ موجود نمی‌توانند انواع مختلف حملات انکار سرویس را به طور مؤثر شناسایی کنند؛ بنابراین برای محافظت از اینترنت وسایل نقلیه در برابر حملات انکار سرویس، ما یک چارچوب تشخیص نفوذ مبتنی بر شبکه عصبی کانولوشن را پیشنهاد دادیم. سیستم تشخیص نفوذ پیشنهادی ما شامل یک شبکه عصبی کانولوشن ۱۰ لایه است که سه نوع حمله انکار سرویس: سیلاب UDP، سیلاب SYN و Slowloris را در سه محیط (بزرگراه، شهری و روستایی) شناسایی می‌کند. این چارچوب هم دسته‌بند باینری و هم دسته‌بند چندگانه است. سیستم تشخیص نفوذ پیشنهادی ما بر روی مجموعه داده VDoS-LRS ارزیابی شده است؛ زیرا استفاده از مجموعه داده‌های واقعی مختص اینترنت وسایل نقلیه چالشی برای ارزیابی صحیح است. همچنین، تمام معیارهای ارزیابی برای ارزیابی کامل این سیستم استفاده شده است. نتایج تجربی نشان می‌دهد که سیستم تشخیص نفوذ پیشنهادی ما می‌تواند به طور مؤثر انواع مختلف حملات انکار سرویس را با نرخ صحت ۱۰۰٪ نسبت به چارچوب موجود شناسایی کند. در کارهای آینده، سیستم تشخیص نفوذ پیشنهادی خود را برای شناسایی سایر حملات در محیط اینترنت وسایل نقلیه گسترش خواهیم داد.

منابع

Abbasi, S, et al. (2021). Internet of Vehicles: Architecture, services, and applications. International Journal of Communication Systems. 34(10): p. e4793.

Adhikary, K, et al. (2020). Hybrid algorithm to detect DDoS attacks in VANETs. Wireless Personal Communications. 114(4): p. 3613-3634.

Adhikary, K, et al. (2020). Evaluating the Impact of DDoS Attacks in Vehicular Ad-Hoc Networks. International Journal of Security and Privacy in Pervasive Computing (IJSPPC). 12(4): p. 1-18.

Ahmed, M.K. (2023). CoVANET: A VANET application for detecting and tracking COVID-19 cases in real-time. in AIP Conference Proceedings. AIP Publishing LLC.
Ahmed, I, et al. (2021). Deep Learning-based Intrusion Detection System for Internet of Vehicles. IEEE Consumer Electronics Magazine.
Alladi, T, et al. (2021). DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs. IEEE Transactions on Vehicular Technology. 70(11): p. 12013-12023.
Alladi, T, et al. (2021). Securing the internet of vehicles: A deep learning-based classification framework. IEEE networking letters. 3(2): p. 94-97.
Ashraf, J, et al. (2020). Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems. 22(7): p. 4507-4518.
Bangui, H, et al. (2021). A hybrid data-driven model for intrusion detection in VANET. Procedia Computer Science. 184: p. 516-523.
Dadi, S, Abid, M. (2022). Enhanced intrusion detection system based on autoencoder network and support vector machine. in Networking, Intelligent Systems and Security: Proceedings of NISS 2021. Springer.
D'Angelo, G, Castiglione, A, Palmieri, F. (2020). A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet of Things Journal. 8(16): p. 12518-12527.
Du, G, et al. (2021). Towards graph-based class-imbalance learning for hospital readmission. Expert Systems with Applications. 176: p. 114791.
Gao, Y, et al. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. IEEE Access. 7: p. 154560-154571.
Kadam, N, Krovi, R.S. (2021). Machine learning approach of hybrid KSVN algorithm to detect DDoS attack in VANET. International Journal of Advanced Computer Science and Applications. 12(7).
Kelarestaghi, K.B, et al. (2019). Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures. arXiv preprint arXiv:1903.01541.
Kirimtat, A, et al. (2020). Future trends and current state of smart city concepts: A survey. IEEE access. 8:p. 86448-86467.
Kumar, S, Dutta, K. (2018). Trust based intrusion detection technique to detect selfish nodes in mobile ad hoc networks. Wireless Personal Communications. 101(4): p. 2029-2052.
Li, W, Wang, G.G, and Gandomi, A.H. (2021). A survey of learning-based intelligent optimization algorithms. Archives of Computational Methods in Engineering. 28(5): p. 3781-3799.
Nie, L, et al. (2020). Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering. 7(4): p. 2219-2230.
Powers, D.M. (2020). Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. arXiv preprint arXiv:2010.16061.
Powers, D.M. (2020). Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. arXiv preprint arXiv:2010.16061.
Rani, P, and Sharma, R. (2023). Intelligent transportation system for internet of vehicles based vehicular networks for smart cities. Computers and Electrical Engineering. 105: p. 108543.
Rahal, R, Amara Korba, A, and Ghoualmi-Zine, N. (2020). Towards the development of realistic dos dataset for intelligent transportation systems. Wireless Personal Communications. 115(2): p. 1415-1444.
Raghu, M, et al. (2017). On the expressive power of deep neural networks. in international conference on machine learning. PMLR.
Sai, K.M, et al. (2020). A lightweight Anomaly based DDoS flood attack detection for Internet of vehicles.
Sharma, S, Kaushik, B. (2019). A survey on internet of vehicles: Applications, security issues & solutions. Vehicular Communications. 20: p. 100182.
Samad, A, et al. (2018). Internet of vehicles (IoV) requirements, attacks and countermeasures. in Proceedings of 12th INDIACom; INDIACom-2018; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi.
Sherazi, H.H.R, et al. (2019). DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. Sustainable Computing: Informatics and Systems. 23: p. 13-20.
Song, H.M, Woo, J, Kim, H.K. (2020). In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications. p. 100198.
Shu, J, et al. (2020). Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach. IEEE Transactions on Intelligent Transportation Systems, 2020. 22(7): p. 4519-4530.

Ullah, S, et al. (2022). HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. Sensors. 22(4): p. 1340.

Verma, A, et al. (2021). The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions. Applied Sciences. 11(10): p. 4682.

Yang, L, Shami, A. (2022). A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles. arXiv preprint arXiv:2201.11812.

Zang, M, Yan, Y. (2021). Machine learning-based intrusion detection system for big data analytics in VANET. in 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring). 2021. IEEE.

Zhang, J, et al. (2019). Intrusion detection system using deep learning for in-vehicle security. Ad Hoc Networks. 95: p. 101974.

Zeng, Y, et al. (2019). Deepvcm: a deep learning based intrusion detection method in vanet. in 2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing, (HPSC) and IEEE intl conference on intelligent data and security (IDS). IEEE.