دو فصلنامه علمی
فناوری اطلاعات و ارتباطات ایران

سال پانزدهم، شماره ۵۷ و۵۸ ، پاییز و زمستان ۱۴۰۲
صفحات: ۲۰ الی ۳۰

An Intrusion Detection System based on Deep Learning for CAN Bus

Fateme Asghariyan*, Mohsen Raji**

*Master student, Faculty of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran

**Associate Professor, Faculty of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran

Abstract

In recent years, with the advancement of automotive electronics and the development of modern vehicles with the help of embedded systems and portable equipment, in-vehicle networks such as the controller area network (CAN) have faced new security risks. Since the CAN bus lacks security systems such as authentication and encryption to deal with cyber-attacks, the need for an intrusion detection system to detect attacks on the CAN bus seem to be very necessary. In this paper, a deep adversarial neural network (DACNN) is proposed to detect various types of security intrusions in CAN buses. For this purpose, the DACNN method, which is an extension of the CNN method using adversarial learning, detects intrusion in three stages; In the first stage, CNN acts as a feature descriptor and the main features are extracted, and in the second stage, the discriminating classifier classifies these features and finally, the intrusion is detected using the adversarial learning. In order to show the efficiency of the proposed method, a real open source dataset was used in which the CAN network traffic on a real vehicle during message injection attacks is recorded on a real vehicle. The obtained results show that the proposed method performs better than other machine learning methods in terms of false negative rate and error rate, which is less than 0.1% for DoS and drive gear forgery attack and RPM forgery attack while this rate is less than 0.5% for fuzzy attack.

Keywords: In-vehicle network, Controller area network (CAN), Intrusion detection, Convolutional neural network (CNN), Adversarial Training

یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق برای گذرگاه CAN

فاطمه اصغریان*، محسن راجی**×

*دانشجوی کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، شیراز، ایران

** دانشیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، شیراز، ایران

تاریخ دریافت: ۱۴۰۱/۰۵/۱۹ تاریخ پذیرش: ۱۴۰۱/۰۹/۲۳

نوع مقاله: پژوهشی

چکیده

در سال‌های اخیر، با پیشرفت الکترونیک خودرو و توسعه وسایل نقلیه مدرن با کمک سیستم‌های نهفته و تجهیزات قابل حمل، شبکه‌های درون-خودرویی مانند شبکه ناحیه کنترل کننده[1] (CAN) با مخاطرات امنیتی جدیدی مواجه شده‌اند. از آنجا که گذرگاه CAN فاقد سیستم‌های امنیتی مانند تایید اعتبار و رمزگذاری برای مقابله با حملات سایبری می‌باشد، نیاز به یک سیستم تشخیص نفوذ برای شناسایی حملات به گذرگاه CAN بسیار ضرروی به نظر می‌رسد. در این مقاله، یک شبکه عصبی پیچیده متخاصم عمیق[2] (DACNN) برای تشخیص انواع نفوذهای امنیتی در گذرگاه‌های CAN پیشنهاد شده است. به این منظور، روش DACNN که گسترش یافته روش CNN با استفاده از یادگیری خصمانه است، در سه مرحله به تشخیص نفوذ می پردازد؛ در مرحله نخست، CNN به عنوان توصیفگر ویژگی ها عمل نموده و ویژگی‌های اصلی استخراج می‌شود و سپس، طبقه بندی کننده متمایزگر این ویژگی‌ها را طبقه‌بندی می کند و در نهایت، به کمک یادگیری خصمانه نفوذ تشخیص داده می شود. جهت بررسی کارآمدی روش پیشنهادی، یک مجموعه داده منبع باز واقعی مورد استفاده قرار گرفت که ترافیک شبکه CAN را بر روی یک وسیله نقلیه واقعی در حین انجام حملات تزریق پیام ضبط نموده است. نتایج به دست آمده نشان می‌دهد که روش پیشنهادی نسبت به سایر روش‌های یادگیری ماشین در نرخ منفی کاذب و میزان خطا عملکرد بهتری دارد که این میزان برای DoS و حمله جعل دنده محرک و حمله جعل RPM کمتر از ۰٫۱٪ می باشد و این میزان برای حمله فازی کمتر از ۰٫۵٪ می باشد.

واژگان کلیدی: سیستم تشخیص نفوذ، یادگیری ماشین، شبکه داخل خودرویی، شبکه ناحیه کنترل کننده (CAN)، شبکه عصبی پیچشی (CNN)، یادگیری خصمانه.

[1] Controller Area Network

[2] Deep Adversarial Convolutional Neural Network

×نویسنده مسئول: محسن راجی mraji@shirazu.ac.ir

۱. مقدمه

خودروهای ساخته شده در سال‌های گذشته به تدریج پیچیده‌تر شده‌اند و فناوری شبکه درون خودرو، ستون اصلی این تغییرات الکترونیکی است که با سرعت زیادی در حال پیشرفت هستند [1]. وسایل نقلیه امروزی شامل بسیاری از واحدهای کنترل‌کننده الکترونیکی[1] (ECU) هستند که با یکدیگر در یک شبکه درون-خودرویی ارتباط برقرار می‌کنند. شبکه ناحیه کنترل‌کننده[2] (CAN) ایجاد شده است تا یک کانال ارتباطی قابل اعتماد بین این واحدهای کنترلی برای پخش پیام‌ها فراهم کند. پروتکل‌های سریال مختلف در شبکه‌های درون-خودرویی مانندCAN، شبکه اتصال محلی[3] (LIN) و FlexRay در تبادل بلادرنگ پیام کارآمد هستند اما در برابر حملات از راه دور کاملاً آسیب پذیر خواهند بود [2]. از آنجا که پروتکل CAN از نظر طراحی فاقد مکانیسم‌های امنیتی، مانند احراز هویت و رمزگذاری، برای محافظت از ارتباطات خود در برابر حملات سایبری است، در برابر حملات امنیتی مختلف آسیب پذیر بوده و فقدان راهکارهای امنیتی در پروتکل CAN به مهاجمان این اجازه را می‌دهد تا با تزریق پیام‌های ساختگی، سیستم‌های خودرویی را کنترل کنند [3].

پیام‌های ساختگی را میتوان مستقیماً از طریق درگاه OBD-II و همچنین از طریق سیستم ارتباطات بی سیم مثل بلوتوث و WIFI تزریق کرد [4]. ارتباط محسوسی بین امنیت جاده‌ها و نقض امنیت سایبری وجود دارد، چرا که حملات مخرب می‌توانند منجر به رفتارهای غیرمنتظره‌ای شوند که باعث برخورد و ایجاد تلفات و صدمات می‌شود. به همین سبب تحقیقات درباره‌ی بهبود و ارتقای امنیت خودرو بسیار اهمیت پیدا کرده است.

راه‌های متفاوتی برای ارتقای امنیت سیستم‌های درون-خودرویی وجود دارد اما بهترین راهکار که قادر باشد در کمترین زمان ممکن تشخیص نفوذ را انجام دهد، سیستم تشخیص نفوذ (IDS) است. پیش از این، IDS مبتنی بر ناهنجاری[4] به عنوان یک رویکرد موثر برای شناسایی حملات مخرب در CAN مورد توجه قرار گرفته است [5][6]. در سال های اخیر، با اقبال محققان به روش های هوش مصنوعی و تکنیک‌های یادگیری عمیق، استفاده از این روش‌ها برای ارائه IDS بهتر نیز اوج گرفته است. استفاده از شبکه‌های عمیق پیچشی[5] (CNN) [2]، شبکه های متخاصم مولد[6] (GAN) [7]، نقشه خود سازماندهی[7] (SOM) [8]، از جمله این روش‌ها هستند. اما این روش ها، نقاط ضعف مهمی دارند؛ از جمله این که یا از داده‌های غیرواقعی استفاده می‌کنند و بنابراین نتایج آن‌ها قابل اتکا به نظر نمی‌رسد و یا این که نیاز به داده‌های بسیار زیاد دارند که ممکن است آنچنان در دسترس نباشد. بنابراین، انتظار می‌رود نتایج به دست آمده از تحقیقات پیشین در این حوزه، قابل اتکا نبوده و یا متکی به داده‌های محدود باشد و میزان خطای آن بیش از حد قابل تحمل باشد.

در این مقاله، یک IDS مبتنی بر ناهنجاری برای افزایش امنیت گذرگاه CAN در شبکه‌های درون-خودرویی ارائه می شود. برای انجام این کار، یادگیری خصمانه[8] به عنوان یک نظم دهنده در CNN معرفی شده و یک شبکه عصبی پیچشی متخاصم عمیق[9] (DACNN) برای تشخیص نفوذ های امنیتی در گذرگاه CAN و سیله نقلیه پیشنهاد می شود که با حجم بسیار کمی از داده هم سازگاری دارد. روش پیشنهادی با بهره گیری از مزیت رویکرد یادگیری خصمانه قادر است با استفاده از مجموعه محدود از حملات واقعی، داده های کارآمد بیشتری را برای آموزش بهتر IDS تولید کند. به این ترتیب، IDS پیشنهادی می تواند حملات سایبری گسترده و متنوعی مانند کاربرد انکار سرویس (DoS) و فازی و جعل را با نرخ منفی کاذب و نرخ خطای کمتر تشخیص دهد. نتایج به دست آمده نشان می‌دهد، روش پیشنهادی، با بهره بردن از حجم محدود داده ها، علاوه بر نرخ منفی کاذب و نرخ خطای کمتر به میزان دقت[10] و صحت[11] قابل قبولی هم دست می یابد.

۲. کارهای پیشین

در حوزه IDS کارهای متعددی ارائه شده است که در این بخش این کارها را در دو قسمت جداگانه بررسی می‌کنیم. در بخش اول، به کارهای مرتبطی که در سال‌های اخیر به IDS در حوزه‌های کلی‌تری مانند شبکه‌های کامپیوتری پرداخته‌اند، می‌پردازیم و سپس در قسمت دوم، به کارهایی پرداخته می‌شود که مشخصا به افزایش امنیت در ارتباطات درون-خودرویی پرداخته‌اند، اشاره می‌کنیم.

۲,۱ سیستم‌های تشخیص نفوذ جدید در شبکه‌های کامپیوتری

در دنیای امروز، امنیت شبکه یکی از مهم ترین و پر اهمیت ترین جنبه های هر شبکه‌ای می باشد که روز به روز به تعداد حملات نفوذگران به شبکه اضافه می‌شود. در صورتی که نفوذگران به شبکه دسترسی پیدا کنند می‌توانند به عنوان یک کاربر شبکه از آن شبکه استفاده کنند که این نه تنها باعث ایجاد ضررهای متعدد و جبران ناپذیر برای شبکه می شود بلکه شناسایی نفوذگران هم پس از نفوذ غیر ممکن می‌شود. به همین سبب، IDS مورد توجه محققان در

[1] Engine Control Unit
[2] Controller Area Network
[3] Local Interconnect Network
[4] Anomaly
[5] Convolutional Neural Network
[6] Generative Adversarial Networks
[7] Self-organizing map
[8] Adversarial Training
[9] Deep Adversarial Convolutional Neural Network
[10] Accuracy
[11] Precision

همه ی زمینه ها قرار گرفته اســـت. با نمایش کارآمدی روش های هوش مصـنوعی و به طور خاص یادگیری عمیق، این روش‌ها نیز به طور گسترده در زمینه تشخیص نفوذ استفاده شده‌اند.

الوم، دکتر زهانگیر و همکارش در [13] تـشخیص نفوذ شبکه برای امنیت ســـایبری با اســـتفاده از رویکردهای یادگیری عمیق بدون نظارت [1]را مطرح کردند. هوانگ و همکارانش در [14] یک مدل یادگیری عمیق بدون نظارت برای تـشخیص ناهنجاری ترافیک اولیه در شبکه را ارائه دادند. آن‌ها یک مکانیسم موثر در شناسایی ترافیک ناهنجاری یعنی D-PACK را که شامل یک شبکه عصبی پیچشی و یک مدل یادگیری عمیق بدون نظارت [2] (AE) اســـت را ارائه دادند. زوراک و همکارش در [15] تشـــخیص نفوذ مبتنی بر ناهنجاری از ویژگی‌های جریان شـــبکه با اســـتفاده از رمزگذار خودکار متنوع را بیان کردند که تمرکز آن بر روی شناسایی ترافیک شبکه غیر عادی از داده‌های مبتنی بر جریان با ا ستفاده از روش‌های یادگیری عمیق بدون نظارت با رویکرد نیمه نظارت [3] شـــده اســـت. جیابو هوانگ و همکارانش در [17] یادگیری عمیق توســـط کشـــف محله [4] را بیان کردند که یک روش یادگیری عمیق بدون نظارت به نام AND [5] اســـت. مدل AND مزایای خوشـــه بندی و یادگیری ویژگی نمونه را همزمان با کاهش معایب آن‌ها در یک فرمول اصولی ترکیب می‌کند. نجیانپینگ ژوان و همکارانش در [18] یک روش جدید یادگیری بدون نظارت برای تـشخیص عیب هو شمند یاطاقان عنا صر نورد بر اســـاس خود رمزگذار عملکردی عمیق ارائه کردند. آن ها یک مدل رمزگذارکننده خودکار کاربردی عمیق (DFAE [6]) برای اســـتخراج ویژگی از ســـیگنالهای لرزش خام طراحی کردند. توماس شـــلگل و همکارانش در [19] تشـــخیص ناهنجاری ســـریع بدون نظارت با شـــبکه های خصـــمانه تولیدی را عنوان کردند. آن ها یک رویکرد یادگیری بدون نظارت مبتنی بر یک شـــبکه خصـــمانه تولید کننده (GAN [7]) ارائه دادند که قادر به شـــناســـایی تصـــاویر غیرعادی و بخش‌های تصـویر اسـت. سـرعت تشـخیص این روش آن را به یک رویکرد عملی برای تشـــخیص ناهنجاری و غربالگری توان عملیاتی بزرگ تبدیل می‌کند. در کاری دیگر ته هان و همکارانش [21] روش DACNN را که یک چارچوب یادگیری خ صمانه در شبکه ع صبی پیچ شی برای ت شخیص هو شمند خطاهای مکانیکی ا ست، را ارائه کردند.

۲,۲ سیستم‌های تشخیص نفوذ برای ارتباطات درون-خودرویی

یک شـــبکه درون خودرو پیام‌های مهمی را منتقل می کند که برای عملکرد موثر و سایل نقلیه ضروری ا ست و به همین سبب امنیت این شبکه م سئله ی مهمی ا ست. چندین مطالعه بر روی محافظت از شبکه درون خودرو با رویکردهای مختلف متمرکز بوده اند. سونگ و همکارانش در [2] از شبکه عصبی پیچشی عمیق (DCNN [8]) برای ت شخیص نفوذ شبکه درون خودرو ا ستفاده کردند و توان ستند یک بهبود عملکرد قابل توجه نســـبت به الگوریتم های مشـــابه دیگر یادگیری ماشین داشته است.

ریاض الاســـلام و همکارش در [3] بهبود امنیت گذرگاه CAN با اختصاص شناسه‌های داوری پویا را مطرح کردند که این روش برای شناسایی حمله در سیستم گذرگاه CAN با ۱۲ شناسه داوری بدون تغییر در ساختار ا سا سی پیام CAN و سخت افزار مرتبط، امنیت داخل خودرو را افزایش می دهد. وانگ، چوندونگ و همکارانش در [5]یک سیستم ت شخیص ناهنجاری توزیع شده برای شبکه درون خودرو با اســـتفاده از حافظه زمانی ســـلســـله مراتبی [9] HTM را برای افزایش امنیت گذرگاه شـــبکه CAN وســـایل نقلیه معرفی کردند. کو سمانوس، دیمیتریوس و همکارانش در [10] یک سیستم ردیابی نفوذ جدید در برابر حملات جعلی در و سایل نقلیه الکتریکی متصل را ارائه کردند که دقت تشـــخیص را تا ۹۰ درصـــد افزایش می دهد. شنگدا لو و همکارانش در [11] یادگیری عمیق و کم عمق مکمل با تقویت، امنیت حمل و نقل عمومی را بررســـی کردند و آن را با روش‌های سنتی مقایسه کردند که نتایج نشان داد که روش آن‌ها از عملکرد بهتری برخوردار ا ست. ویتا سانتا بارلتا و همکارانش در [8] معماری کوهنن برای SOM برای تشـــخیص نفوذ در شـــبکه های ارتباطی درون خودرو را ارائه دادند که یک روش تشـــخیص نفوذ مبتنی بر فا صله با هدف شنا سایی پیام‌های حمله تزریق شده در یک گذرگاه CAN با ا ستفاده از کوهنن ا ست که ن شان می‌دهد در ت شخیص حملات به خوبی عمل می‌کند. همچنین آن‌ها کار دیگری در [9] رویکرد کوهنن بدون نظارت را هم برای ت شخیص نفوذ برای شبکه‌های ارتباطی درون-خودرویی ارائه کردند.

روش های پیشـــین تشـــخیص نفوذ مبتنی بر یادگیری عمیق برای شبکه‌های درون-خودرویی دارا نقاط ضعف عمده‌ای هستند. نیاز و اســـتفاده از حجم زیاد داده و هزینه زمانی بالا از مهم ترین نقاط ضعف کار های انجام شده ا ست همچنین عدم ا ستفاده از مجموعه

[1] Unsupervised
[2] Auto-Encoder
[3] Semi-Supervised
[4] Neighbourhood Discovery
[5] Anchor Neighbourhood Discovery
[6] Deep Functional Auto-Encoders
[7] Generative Adversarial Networks
[8] Deep Convolutional Neural Network
[9] Hierarchical Temporal Memory

داده های واقعی تهیه شده از وسایل نقلیه واقعی هم از نقاط ضعف برخی از کار هایی است که تاکنون در این زمینه انجام شده اند.

۳. پیشینه و مقدمات

در این بخش، روش های استفاده شده در روش پیشنهادی تشخیص نفوذ و شبکه ناحیه کنترل کننده ارائه می گردد. ابتدا شبکه عصبی پیچشی را که در این کار استفاده شده است را معرفی می کنیم سپس شبکه مولد متخاصم مورد استفاده را بررسی می کنیم. در ادامه به بررسی شبکه ناحیه کنترل کننده که روش پیشنهادی برای ارتقای امنیت آن است، می پردازیم.

۳,۱ شبکه عصبی عمیق

یکی از معروف‌ترین شبکه‌های عمیق به نام شبکه‌ی عصبی پیچشی است. شبکه عصبی پیچشی، (CNN) یک الگوریتم یادگیری عمیق است که ورودی را دریافت کرده و به هر یک از جنبه‌های موجود در تصویر میزان تخصیص داده و قادر به متمایزسازی آن‌ها از یکدیگر است. شبکه‌های پیچشی از فرآیندهای بیولوژیکی الهام گرفتند که الگوی اتصال بین نورون‌ها شبیه سازماندهی قشر بینایی حیوانات است که قادر است به طور موفقی وابستگی‌های زمانی و فضایی را در یک داده با استفاده از فیلترهای مرتبط ثبت کند. CNN ها نسخه های منظم پرسپترون های چندلایه هستند. پرسپترون های چندلایه معمولاً به معنای شبکه های کاملاً متصل هستند، یعنی هر نورون در یک لایه به تمام نورون های لایه بعدی متصل است. CNNها رویکرد متفاوتی نسبت به منظم‌سازی دارند: آنها از الگوی سلسله مراتبی در داده‌ها بهره می‌برند. و الگوهای با پیچیدگی فزاینده را با استفاده از الگوهای کوچکتر و ساده تری که در فیلترهای آنها نقش بسته است، جمع آوری کنید.

لایه ورودی[1]، لایه ی ورودی در واقع همان داده ی ورودی است که به شبکه ی عصبی داده خواهد شد. هیچ محاسبه ای در این لایه انجام نخواهد شد و در این لایه داده ها فقط به لایه پنهان انتقال پیدا خواهد کرد. داده ای که به عنوان ورودی به شبکه ی عصبی داده خواهد شد باید عددی باشد لایه مخفی[2]، لایه های مخفی شامل بیشتر نورون ها در شبکه ی عصبی هستند و به نوعی قلب محاسبات محسوب خواهند شد.در بلوک‌های پیچشی، برای محاسبه اندازه تعداد نورون‌های خروجی (N) از رابطه (۲) استفاده می‌شود:

$$N = \frac{W - F + 2P}{S} + 1 \qquad (۱)$$

که در آن، W اندازه تعداد نورون‌های ورودی، , (F) اندازه گام و مقدار (P) zero padding استفاده می شود.

در این لایه ها انواع محاسبات بر روی داده های ورودی انجام خواهد شد و نتیجه به لایه خروجی منتقل خواهد شد توسعه دهندگان شبکه ی عصبی بر خالف لایه ورودی و خروجی مستقیما با این لایه کار نخواهند کرد. لایه خروجی [3]، در این لایه محاسبات نهایی بر روی داده ها انجام خواهد شد و خروجی یادگرفته شده توسط شبکه عصبی تولید خواهد شد .

این روش از پیش پردازش کمتری نسبت با سایر الگوریتم های طبقه بندی استفاده می کند. شبکه CNN یاد می گیرد که فیلترها را از طریق یادگیری خودکار بهینه کرده، در حالی که در الگوریتم های سنتی این فیلترها به صورت دستی طراحی شده اند. این استقلال از دانش قبلی و مداخله انسان در استخراج ویژگی یک مزیت عمده است. این شبکه از یک عملیات ریاضی به نام پیچیدگی به جای ضرب ماتریس داخلی در یکی از لایه های خود استفاده خواهد کرد که از یک لایه ورودی، لایه های پنهان و یک لایه خروجی تشکیل شده است. لایه های پنهان شامل لایه هایی هستند که پیچشی را انجام خواهند داد. معمولاً این شامل لایه‌ای است که حاصل ضرب نقطه‌ای از هسته پیچشی را با ماتریس ورودی لایه انجام می‌دهد. نورون پیچشی داده ها را فقط برای میدان گیرنده خود پردازش می کند.

۳,۲ شبکه مولد متخاصم

شبکه های مولد متخاصم (GAN)[4] دسته ای از سیستم های یادگیر عمیق محسوب می شوند که به دسته ی مدل های مولد[5] تعلق دارند. این شبکه رویکردی با مدل‌سازی مولد با استفاده از روش‌های یادگیری عمیق مانند شبکه های عصبی پیچشی (CNN)[6] در یادگیری ماشین است که شامل اکتشاف خودکار و یادگیری قواعد یا الگوهای موجود در داده‌های ورودی می‌شود. این مدل شامل ۲ زیر مدل است که این دو زیر مدل عبارت اند از مدل مولد و مدل متمایزگر [7]است که مدل اول کار تولید نمونه های جدید را انجام می دهد و مدل دوم نمونه‌ها را به عنوان نمونه واقعی (از دامنه) یا جعلی (تولید شده) دسته‌بندی می کند. در یک معماری GAN ، متمایزگر، نمونه هایی از داده های واقعی و تولید شده را می گرفته و سعی می کند که آن ها را به بهترین وجه ممکن کلاس بندی کند و مولد که آموزش دیده تا حد ممکن متمایزگر را فریب می دهد. بهینه سازی این عملیات به صورت رابطه (۵) انجام خواهد شد که G نشان دهنده مولد و D نشان دهنده متمایز است.

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{data}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z)))] \qquad (۲)$$

که در آن، G نشان دهنده ی تابع مولد و D تابع متمایزگر است. بنابراین هدف از مولد فریب متمایزگر است، بنابراین شبکه عصبی

[1] Input layer
[2] Hidden layer
[3] Output layer
[4] Generative Adversarial Networks
[5] Generative Models
[6] Convolutional Neural Networks
[7] Discriminator Model

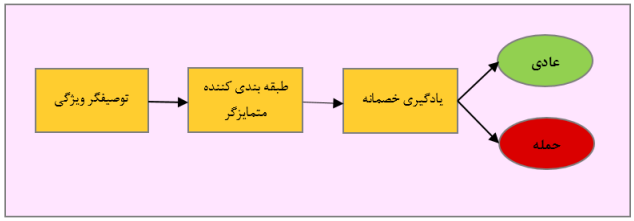
مولد آموزش دیده تا خطای کلاس بندی را به حداکثر برساند. هدف متمایزگر هم این است که داده های تولید شده جعلی را کشف کند، پس شبکه عصبی متمایزگر آموزش داده شده تا خطای کلاس بندی را به حداقل برساند. در نتیجه در هر بار تکرار، وزن شبکه مولد به منظور افزایش خطای کلاس بندی بروز می شود. این در حالی است که وزن شبکه متمایزگر برای کاهش خطای مورد نظر بروز می شود. هر دو شبکه در پی آن هستند که یکدیگر را شکست دهند به همین سبب هم هر دو بهتر و بهتر می شوند.

۳,۳ شبکه ناحیه کنترل کننده

شبکه ناحیه کنترل کننده یک گذرگاه سریال سریع است که برای ارائه یک پیوند کارآمد، قابل اعتماد و بسیار مقرون به صرفه بین سنسورها و محرک ها طراحی شده است. CAN تجهیزات الکترونیکی خودرو را متصل می کند. این اتصالات به اشتراک گذاری اطلاعات و منابع بین برنامه های کاربردی توزیع شده را تسهیل می کند. همه گره ها می توانند در هر زمانی پیام ارسال کنند، زمانی که دو گره با هم به اتوبوس د ستر سی پیدا می کنند، داوری تصمیم می گیرد که چه کسی ادامه دهد. مجموعه‌های گسترده CAN و CAN FD ما همه عملکردهای CAN و حالت‌های قدرت را با عملکرد عالی EMC، کیفیت پی شرو و یک پایه صنعتی چند منبع پوشش می‌دهند. نوآوری مخرب در این زمینه درها را به روی شبکه های خودرویی بزرگتر و انعطاف پذیرتر در آینده باز می کند. پروتکل CAN این پروتکل مجموعه ای از قوانین برای انتقال و دریافت پیام در شبکه ای از دستگاه های الکترونیکی است که تحت این قوانین تعیین شده، پیام ها از یک د ستگاه به د ستگاهی دیگر منتقل می شوند. دو نوع پروتکل وجود دارد: آدرس یا پیام. در پروتکل مبتنی بر آدرس، بسته های داده حاوی آدرس دستگاهی هستند که پیامی برای آن در نظر گرفته شده است. در پروتکل مبتنی بر پیام، هر پیام به جای یک آدرس توسط یک شناسه از پیش تعیین شده مشخص می شود. فریم CAN منتقل شده معمولاً یک پروتکل مبتنی بر پیام ا ست. پیام یک بسته داده ا ست که اطلاعات را حمل می کند. یک پیام CAN از ۰ تا ۸ بایت داده تشکیل شده است که در یک ساختار خاص (به نام فریم) سازماندهی شده اند. داده های حمل شده در هر بایت در پروتکل CANتعریف شده است. همه گره هایی که از پروتکل CAN استفاده می کنند یک فریم دریافت می کنند و بسته به شناسه گره، CAN تصمیم گیری می کند که آن را بپذیرد یا نه. اگر چندین گره پیام را همزمان ارسال کنند، گره با بیشترین اولویت دسترسی به گذرگاه را دریافت می کند. گره های با اولویت پایین باید منتظر بمانند تا گذرگاه در دسترس باشد.

۴. سیستم تشخیص نفوذ پیشنهادی

در این بخش، روش پیشنهادی مبتنی بر یادگیری عمیق خصمانه برای سیستم تشخیص نفوذ برای گذرگاه CAN در شبکه‌های درون-خودرویی ارائه می‌شود. نمای کلی این روش که از سه بخش اصلی تشکیل می‌شود، در شکل ۱ نشان داده شده است. روش که ما برای انجام این کار در نظر گرفته ایم، در سه مرحله انجام می‌شود. که ابتدا توصیفگر ویژگی قرار دارد و بعد از آن به طبقه بندی کننده متمایزگر پرداخته و در بخش سوم یادگیری خصمانه انجام می‌گردد. این سه عملکرد مختلف در قالب یک CNN که با یادگیری خصمانه ادغام شده است، ارائه می‌شود.



شکل ۱. نمای کلی از روش پیشنهادی تشخیص نفوذ برای شبکه درون-خودرویی مبتنی بر یادگیری خصمانه

۴,۱ چارچوب روش پیشنهادی

در سیستم تشخیص نفوذ پیشنهادی، از یک شبکه عصبی عمیق پیچشی که با آموزش خصمانه ادغام شده است، استفاده می‌شود. در این روش، که مبتنی بر یادگیری نظارت شده[1] است، طی سه مرحله عملیات تشخیص نفوذ انجام می‌شود؛ در مرحله اول، CNN به عنوان توصیفگر عمل نموده و سپس در در مرحله دوم، طبقه بندی کننده متمایزگر قرار دارد و در نهایت، در مرحله ی سوم به یادگیری خصمانه پرداخته می شود که برای این کار از روش GAN استفاده می شود.

در این روش، رقیب از داده‌ها یاد میگرد که این برخلاف روش‌های یادگیری عمیق رایج است. وجه تمایز دیگر روش DACNN با روش CNN در میزان استفاده این روش از مجموعه داده می‌باشد به این معنی که این روش با حجم بسیار کم داده هم سازگاری دارد.

۴-۱-۱- مرحله اول: توصیفگر ویژگی به کمک مدل CNN

در مرحله اول با استفاده از مدل CNN ، توصیفگر ویژگی انجام می‌شود به این صورت که بلوک‌های پیچشی[2] مدل CNN کار توصیفگر ویژگی را برعهده دارد. این بخش مشابه با مولد در GAN عمل می‌کند که داده‌ها را در فضای D-بعدی نگاشت می‌کند و به صورت رابطه (۱) تعریف می‌شود:

$$G_f(x;\ \theta_f): x \rightarrow R^D = G_f \qquad (۳)$$

[1] Supervised

[2] Convolutional Blocks

که در آن پارامترهای θ_f ، داده های ورودی است و G_f تابع مولد ورودی می باشد. توصیفگر ویژگی داده‌ها را می‌گیرد و توصیفگرهای ویژگی/بردارهای ویژگی را خروجی می‌دهد

در این کار، از تابع softmax استفاده می شود که خروجی آن به صورت رابطه (۳) تعریف خواهد شد:

$$O_j = \begin{bmatrix} P(y=1)|x;\theta \\ P(y=2)|x;\theta \\ \cdots \\ P(y=k)|x;\theta \end{bmatrix} = \frac{1}{\sum_{j=1}^{k} \exp(\theta^j x)} \begin{bmatrix} \exp(\theta^1 x) \\ \exp(\theta^1 x) \\ \cdots \\ \exp(\theta^k x) \end{bmatrix} \quad (۴)$$

در این k تعداد دسته ها و θ^j_x پارامترهای لایه طبقه بندی است.

۴-۱-۲- مرحله دوم: طبقه بندی متمایزگر

در مرحله دوم بر روی ویژگی‌هایی که از مرحله قبل به دست آمده است، طبقه بندی کننده متمایزگر انجام می‌شود. طبقه بندی کننده متمایزگر یاد می‌گیرند که چه ویژگی‌هایی در ورودی برای تمایز بین کلاس‌های ممکن مختلف مفید خواهد بود. از نظر ریاضی، مستقیماً احتمال خلفی P(y|x) را محاسبه می‌کند یا یک نقشه مستقیم از ورودی x به برچسب y یاد می‌گیرد. در بیشتر کارهای طبقه‌بندی، طبقه‌بندی‌کننده متمایزگر اغلب دقیق‌تر هستند. متمایزگر دو دسته از داده‌ها، داده‌های واقعی و داده‌های جعلی را مطابق با مدل GAN متمایز می کند. در این مرحله یک طبقه بندی کننده متمایزگر به عنوان حریف طراحی می‌شود، به صورت رابطه (۴) است که با پارامترهای θ_d است و هر دو زیر مجموعه داده از توصیفگر ویژگی تغذیه خواهند شد و ویژگی‌های خروجی پیشتر توسط طبقه بندی کننده متمایزگر، متمایز شده است.

$$G_d = G_d(G_f(x):\theta_d) \quad (۵)$$

که در آن، x ورودی می باشد و G نشان دهنده تابع مولد است.

۴-۱-۳- مرحله سوم: یادگیری خصمانه

در مرحله پایانی، به انجام یادگیری خصمانه بر روی خروجی‌های طبقه بندی کننده متمایزگر که مرحله دوم است و ورودی این مرحله محسوب می‌شود، پرداخته می‌شود. برای انجام این کار از مدل GAN استفاده شده است. به این صورت که این داده‌ها به عنوان مجموعه داده به مدل داده می‌شود و متناسب با آن مجموعه داده عملیات مولد[1] و متمایزگر[2] انجام شده خواهد شد.

طبقه بندی کننده‌ای که توسط لایه‌های کاملا متصل[3] بعدی در CNN ساخته شده است به صورت رابطه (۶) تعریف می‌شود:

$$G_y = G_y(G_f(x):\theta_y):R^D \rightarrow R^L \quad (۶)$$

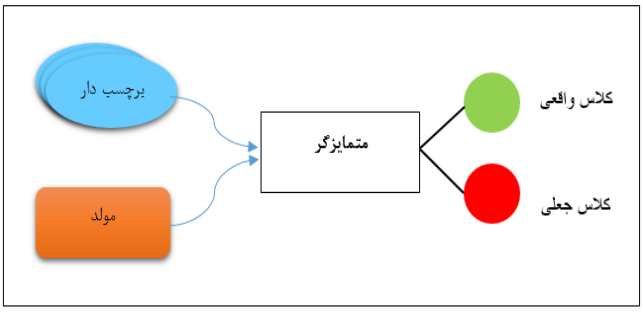
که در آن، با پارامترهای θ_y ،که در آن L تعداد دسته ها را نشان خواهد داد. از تابع softmax برای انجام این روش استفاده می‌کنیم.

در این روش میزان آنتروپی متقاطع باینر ی[4] (BCE) برای خروجی‌های به دست آمده به صورت فرمول (۷) بدست می‌آید.

$$\mathcal{L}(G_d(G_f(x_i)), d_i) = d_i \log \frac{1}{G_d(G_f(x_i))} + (1-d_i) \times \log \frac{1}{1-G_d(G_f(x_i))} \quad (۷)$$

که در آن، G تابع مولد را نشان می دهد و x_i مقدار ورودی می باشد و d_i نشان دهنده متغیر باینری برای x_i است.

در مرحله سوم که چارت این مرحله در شکل ۲ آمده است، به یادگیری خصمانه پرداخته می شود. برای انجام این کار از الگوریتم GAN استفاده شده است. این کار به صورت نظارت شده و با استفاده از برچسب‌ها کار خود را پیش می‌برد. در این مرحله ابتدا به صورت تصادفی داده‌هایی به مدل مولد داده می شود تا داده‌های جعلی تولید گردد. سپس این داده‌ها به همراه داده‌های واقعی برچسب دار به مدل متمایز داده می‌شود و بعد از سپری کردن مراحل مولد و متمایز تشخیص نفوذ انجام خواهد شد.



شکل۲. فلوچارت ساختار روش GAN

۵. بحث و نتایج

در این بخش، نتایج آزمایش‌های تجربی روش پیشنهادی تشخیص نفوذ ارائه می گردد. ابتدا مجموعه داده هایی که در این کار استفاده شده است را جهت ارزیابی روش پیشنهادی معرفی می کنیم سپس معیار های ارزیابی مورد استفاده را بررسی می کنیم. در ادامه با طرح آزمایش های مختلف به بررسی عملکرد روش پیشنهادی می پردازیم سپس نتایج بدست آمده از روش پیشنهادی را با روش های پیشین مقایسه می کنیم.

[1] Generative Model
[2] Discriminator Model
[3] fully-connected layers
[4] Binary cross entropy

۵،۱ مجموعه داده

برای انجام این تشخیص نفوذ از مجموعه داده ای استفاده کردیم که برای تهیه آن از وسیله نقلیه واقعی استفاده شده است [2]. همچنین برای ساخت این مجموعه داده از دو دستگاه سفارشی Raspberry Pi استفاده شده است که یکی برای ثبت ترافیک شبکه و دیگری برای تزریق پیام‌های ساختگی استفاده شده است. آنها از طریق پورت OBD-II واقع در زیر فرمان خودرو به شبکه داخل خودرو متصل بوده و انتقال پیام از طریق گره‌های ECU واقعی در گذرگاه CAN صورت گرفته است. از طریق پورت OBD-II، گره های سفارشی قادر به ارسال و دریافت از گره های ECU واقعی در گذرگاه CAN بودند. این مجموعه داده چهار بخش است که شامل حمله DoS و حمله فازی و حمله جعل دنده محرک و حمله جعل RPM است. هر مجموعه داده با ثبت ترافیک CAN در حین تزریق پیام های ساخته شده اشت. هرکدام از مجموعه داده‌ها حاوی 300 نفوذ تزریق پیام هستند و هر نفوذ برای 3 تا 5 ثانیه انجام می شود و هر مجموعه داده در کل 30 تا 40 دقیقه از ترافیک CAN را دارد. در حین ساخت مجموعه داده، خودرو با موتور روشن پارک شده بود. در حالت عادی ۲۶ شناسه CAN متمایز در گذرگاه CAN وجود دارد. مشخصات حملات انجام گرفته به شرح زیر است:

۱. حمله DoS[1]: تزریق پیام‌های CAN ID "0000" هر 3.0 میلی ثانیه ."0000" غالب ترین CAN ID است.

۲. حمله فازی[2] : تزریق پیامهایی با مقدار کاملاً تصادفی CAN ID و DATA هر 5.0 میلی ثانیه.

۳. حمله جعل دنده محرک و حمله جعل RPM[3] : تزریق پیام‌های مشخص CAN مربوط به / RPM اطلاعات چرخ دنده هر 1 میلی ثانیه.

Timestamp, CAN ID, DLC, DATA[0], DATA[1], DATA[2], DATA[3], DATA[4], DATA[5], DATA[6], DATA[7], Flag

۱. Timestamp: زمان (های) ثبت شده

۲. CAN ID : شناسه پیام CAN در) HEXمثلاً ۰۴۳f)

۳. DLC : تعداد بایت های داده، از ۰ تا ۸

۴. DATA[0~7] : مقدار داده (بایت)

۵. Flag : T یا R، T نشان دهنده پیام تزریق شده در حالی که R نشان دهنده پیام عادی است.

جدول 1 تعداد پیام های عادی و پیام های تزریق شده در مجموعه داده ها را نشان می دهد.

جدول ۱. مروری بر مجموعه داده

	MESSAGE	NORMAL	INGECTED
DoS Attack	3,665,771	3,078,250	587,521
Fuzzy Attack	3,838,860	3,347,013	491,847
Spoofing the drive gear	4,443,142	3,845,890	597,252
Spoofing the RPM	4,621,702	3,966,805	654,897

۵،۲ معیارهای ارزیابی

برای بررسی میزان کارآمدی سیستم پیشنهادی در تشخیص نفوذ، از دو معیار نرخ منفی کاذب و میزان خطا استفاده شده است. معیار FNR نشان می‌دهد که سیستم پیشنهادی چه میزان از حملات را شناسایی نمی کند و معیار ER نشان می دهد که احتمال خطا برای روش پیشنهادی به چه میزانی می باشد.

البته از بین این دو، معیار FNR برای تشخیص در شبکه درون خودرو از اهمیت بیشتری برخوردار است و دلیل این امر است که حتی اگر تعداد کمی از حملات شناسایی نشوند، می‌تواند باعث نقص لحظه‌ای خودرو شده و ایمنی آن را به خطر اندازد. برای محاسبه این دو معیار از روابط (۸) و (۹) استفاده می‌شود:

$$ER = \frac{FN + FN}{TP + TN + FP + FN} \qquad (۸)$$

$$FNR = \frac{FN}{FN + TP} \qquad (۹)$$

که در آن TP و TN به ترتیب مثبت واقعی و منفی واقعی (نشان دهنده تعداد پیام‌های CAN در ست به عنوان حمله و عادی) و FP و FN به ترتیب مثبت کاذب و منفی کاذب (نشان دهنده تعداد پیام‌های CAN نادرست به ترتیب حمله و عادی) هستند.

علاوه بر این، معیارهای متداول ارزیابی مدل های یادگیری عمیق شامل دقت[4]، صحت[5]، فراخوانی[6] و معیار F[7] هم برر سی شده‌اند. دقت کسری از حمله واقعی به حمله کاذب است که نشان دهنده ی درصد نمونه‌هایی است که به درستی کلاس بندی شده اند. دقت بالا مربوط به میزان FP پایین است. میزان دقت از معادله (۱۰) به دست می آید:

$$\text{Accuracy} = (TP + TF) / (TP + FP + TN + FN) \qquad (۱۰)$$

[1] DoS Attack
[2] fuzzy attack
[3] Spoofing Attack (RPM / gear)
[4] Accuracy
[5] precision
[6] Recall
[7] F1-score

صحت کسری از پیام‌های حمله‌ای است که به درستی شناسایی شده است که از طریق رابطه (۱۱) به دست می‌آید:

$$Precision = TP / (TP + FP) \quad (۱۱)$$

فراخوانی نسبت اشتباهات درست تشخیص داده شده به خطاهای واقعی که شامل خطاهای شناسایی نشده هم می‌باشد، را نشان میدهد و برای محاسبه این معیار از معادله (۱۲) کمک گرفته می شود.

$$Recall = TP / (TP + FN) \quad (۱۲)$$

نمره F1 معیار تعادلی است که در بین صحت و فراخوانی ایجاد شده است، را نشان میدهد. نکته مهم این است که از آنجا که از میانگین هارمونیک استفاده می شود، با افزایش هر دو معیار صحت و فراخوانی، این معیار نیز افزایش می یابد. این معیار با استفاده از معادله (۱۳) و با کمک گرفتن از مقادیر دقت و صحت بدست می‌آوریم:

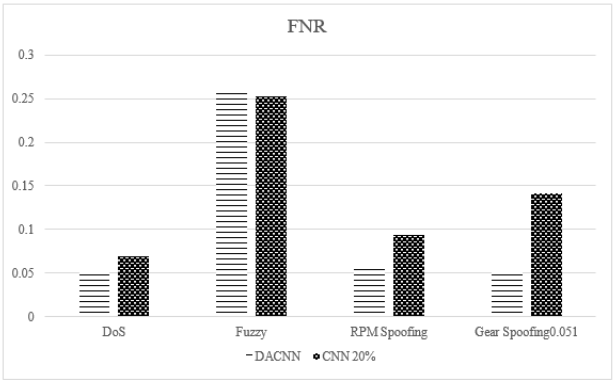
$$F1 = 2(Precision * Recall) / (Precision + Recall) \quad (۱۳)$$

به منظور بررسی میزان کارآمدی روش پیشنهادی تشخیص نفوذ مبتنی بر DACNN، آزمایش های گسترده‌ای انجام گرفته که در این بخش نتایج به دست آمده ارائه می‌گردد.

در این مجموعه آزمایش ها، ابتدا پیش پردازی بر روی مجموعه داده‌ها انجام می شود. بدین صورت که پیش از شروع کار مجموعه داده هایی را که داریم، داده هایی که دارای ویژگی خالی می باشد، حذف میکنم که میزان این داده ها در هرمجموعه داده کمتر از ۱۰٪ از میزان مجموعه داده می‌باشد به همین سبب حذف آن‌ها خللی در روند کار ایجاد نمی کند. در ادامه هر مجموعه داده ی تغییر یافته را به داده های آموزش (شامل ۸۰٪ از کل داده ها) و آزمون (۲۰٪ از کل داده‌ها) تقسیم کردیم. در آزمایش‌های صورت گرفته، مجموعه داده‌ها را به صورت جداگانه بررسی کردیم. سپس حالت دیگری را که از ادغام هر چهار نوع حمله می باشد را مورد بحث قرار دادیم.

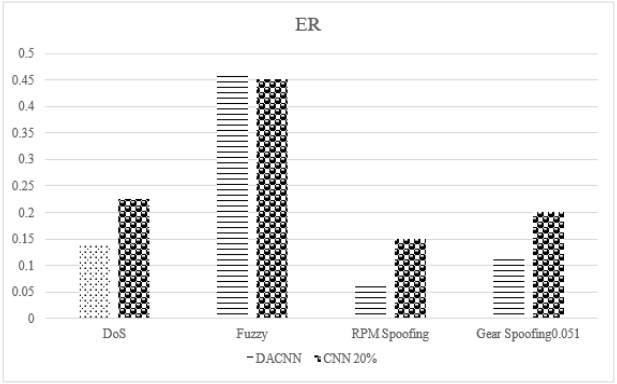
یکی از محدودیت‌های کارهای پیشین این حوزه این است که این روش ها به تعداد زیادی نمونه آموزشی نیاز دارند. بنابراین در آزمایش های انجام شده، علاوه بر این که روش پیشنهادی (DACNN) با سیستم تشخیص نفوذ مبتنی بر CNN که با تمام داده‌های آموزشی داده شده است (CNN100%) مقایسه شده است، حالتی نیز در نظر گرفته شده است که در آن CNN با ۲۰٪ از مجموعه داده آموزشی داده شود (CNN20%). به این ترتیب، می توان میزان تاثیر در دسترس بودن مجموعه داده کافی جهت رسیدن به کارآمدی در روش پیشنهادی را با روش‌های موجود بررسی نمود. قابل ذکر است که برای آموزش روش پیشنهادی هم تنها از ۲۰٪ مجموعه داده آموزشی استفاده شده است.

شکل ۳ میزان FNR را برای روش پیشنهادی و دو روش مبتنی بر CNN را برای تشخیص چهار حمله چهار حمله DoS و حمله فازی و حمله جعل دنده محرک و حمله جعل RPM نشان می دهد. همانطور که مشاهده می‌شود، میزان FNR در روش پیشنهادی کمترین مقدار را نشان می‌دهد که این میزان برای حملات DoS و حمله جعل دنده محرک و حمله جعل کمتر از ۰٫۱٪می‌باشد و این میزان برای حمله فازی کمتر از ۰٫۵٪ می‌باشد که به نظر می‌رسد که این تفاوت به دلیل پیچیدگی داده‌های این حمله در مقایسه با سایر حملات می‌باشد.



شکل۳. مقایسه FNR روش‌های تشخیص نفوذ پیشنهادی (DACNN) با روش‌های مبتنی بر CNN.

در شکل ۴ میزان ER به دست آمده برای روش پیشنهادی و دو روش مبتنی بر CNN برای تشخیص حملات مختلف نمایش داده شده است. نتایج به دست آمده نشان می‌دهد، میزان ER بدست آمده برای روش پیشنهادی با مجموعه 20% کمتر از میزان بدست آمده برای روش CNN100% است و همانطور که گفته شد میزان ER کمتر مطلوب تر است.



شکل۴. مقایسه ER روش‌های تشخیص نفوذ پیشنهادی (DACNN) با روش‌های مبتنی بر CNN.

جداول ۲ تا ۵ نتایج به دست آمده از ResNet[1] [2]، CNN100%، CNN20% و روش پیشنهادی (DACNN) را از منظر دیگر معیارها به تفکیک حملات مختلف نمایش می دهد. با توجه به نتایج به دست آمده، میتوان نتیجه گرفت که روش پیشنهادی در سایر معیارها، در هر ۴ حمله نتایج مطلوبی را دارد و به میزانی مشابه با روش CNN100% و ResNet با همان میزان مجموعه داده ۲۰٪ دست پیدا می کند.

جدول ۲. نتایج مقایسه DoS

	Accuracy	Precision	Recall	F1-score
ResNet [2]	0.887	0.713	0.887	0.787
CNN100%	0.884	0.711	0.884	0.786
CNN 20%	0.857	0.584	0.857	0.765
DACNN	0.889	0.716	0.889	0.789

جدول۳. نتایج مقایسه ی فازی

	Accuracy	Precision	Recall	F1-score
ResNet [2]	0.883	0.722	0.883	0.794
CNN100%	0.881	0.720	0.880	0.791
CNN 20%	0.913	0.754	0.913	0.823
DACNN	0.913	0.756	0.913	0.827

جدول۴. نتایج مقایسه حمله جعل دنده محرک

	Accuracy	Precision	Recall	F1-score
ResNet [2]	0.937	0.793	0.937	0.858
CNN100%	0.934	0.789	0.934	0.855
CNN 20%	0.907	0.765	0.907	0.829
DACNN	0.936	0.796	0.939	0.860

جدول ۵. نتایج مقایسه حمله جعل RPM

	Accuracy	Precision	Recall	F1-score
ResNet [2]	0.938	0.796	0.938	0.860
CNN100%	0.935	0.792	0.935	0.857
CNN 20%	0.909	0.768	0.909	0.832
DACNN	0.940	0.798	0.940	0.862

به منظور بررسی جامعیت روش پیشنهادی، عملکرد آن بر روی مجموعه داده ادغامی شامل از تمام حملات با روش های موجود مقایسه شده است. نتایج نشان می‌دهد که روش پیشنهادی برای مجموعه داده ادغامی هم در مقایسه با سایر روش‌ها بهترین عملکرد را داشته است. بر طبق این نتایج، روش پیشنهادی (DACNN) با در دسترسی به تنها ۲۰٪ از داده‌های آموزشی، به نتایجی نزدیک یا حتی بهتر از مدل CNN برای مجموعه داده کامل (CNN100%) رسیده است و از نتایج مدل CNN با ۲۰٪ از داده‌های آموزشی (CNN20%) بسیار بهتر است. به این ترتیب، می‌توان نتیجه گرفت، روش پیشنهادی می‌تواند معضل کمبود داده‌های آموزشی را به راحتی حل نموده و با تولید نمونه های بیشتر، به نتایجی بهتر از روش CNN با مجموعه داده کامل دست پیدا کند.

جدول ۶. نتایج مقایسه حالت ادغامی

	Accuracy	Precision	Recall	F1-score
CNN 20%	0.888	0.733	0.888	0.802
DACNN	0.921	0.766	0.921	0.735

۶. نتیجه گیری

در این مقاله، یک شبکه عصبی خصمانه عمیق پیچیده (DACNN) برای محافظت از گذرگاه CAN وسیله نقلیه پیشنهاد شده است که از یادگیری خصمانه به عنوان یک تنظیم کننده درگسترش روش شبکه عصبی پیچشی (CNN) استفاده می کند. برای ارزیابی DACNN پیشنهادی، از یک مجموعه داده منبع باز استفاده کردیم که ترافیک CAN را از طریق درگاه OBD-II یک وسیله نقلیه واقعی در طول حملات تزریق پیام ضبط می‌کند. این مجموعه داده شامل چهار حمله فازی و حمله DoS و جعل (RPM، Gear) است. ارزیابی روش پیشنهادی برای مجموعه داده‌های کاهش یافته (۲۰ درصد از مجموعه داده‌های هر حمله) انجام می‌شود. نتایج ارزیابی‌ها نشان می‌دهد که مدل پیشنهادی نسبت به سایر روش‌های یادگیری ماشینی در نرخ منفی کاذب و میزان خطا عملکرد قابل قبولی دارد. همچنین این روش نسبت به روش DCNN با مجموعه داده کامل از دقت خوبی برخوردار بوده و عملکرد قابل قبولی دارد.

مراجع

[1] Khan, Zadid, et al. "Long Short-Term Memory Neural Network-Based Attack Detection Model for In-Vehicle Network Security." *IEEE Sensors Letters* 4.6 (2020): 1-4.

[2] Song, Hyun Min, Jiyoung Woo, and Huy Kang Kim. "In-vehicle network intrusion detection using deep convolutional neural network." *Vehicular Communications* 21 (2020): 100198.

[3] Islam, Riadul, and Rafi Ud Daula Refat. "Improving CAN bus security by assigning dynamic arbitration IDs." *Journal of Transportation Security* 13.1 (2020): 19-31.

[4] Linxi Zhang, et al. "A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks." *Digital Object Identifier 10.1109/ACCESS.2022.3145007*

[5] Wang, Chundong, et al. "A distributed anomaly detection system for in-vehicle network using HTM." *IEEE Access* 6 (2018): 9091-9098.

[1] نتایج به دست آمده برای روش مقاله

In

[14] Hwang, Ren-Hung, et al. "An unsupervised deep learning model for early network traffic anomaly detection." *IEEE Access* 8 (2020): 30387-30399.
[15] Zavrak, Sultan, and Murat İskefiyeli. "Anomaly-based intrusion detection from network flow features using variational autoencoder." *IEEE Access* 8 (2020): 108346-108358.
[16] Merrill, Nicholas, and Azim Eskandarian. "Modified autoencoder training and scoring for robust unsupervised anomaly detection in deep learning." *IEEE Access* 8 (2020): 101824-101833.
[17] Huang, Jiabo, et al. "Unsupervised deep learning by neighbourhood discovery." *International Conference on Machine Learning*. PMLR, 2019.
[18] Aljemely, Anas H., et al. "A novel unsupervised learning method for intelligent fault diagnosis of rolling element bearings based on deep functional auto-encoder." *Journal of Mechanical Science and Technology* 34.11 (2020): 4367-4381.
[19] Schlegl, Thomas, et al. "f-AnoGAN: Fast unsupervised anomaly detection with generative adversarial networks." *Medical image analysis* 54 (2019): 30-44.
[20] CAR-HACKING DATASET, https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset
[21] T. Han, C. Liu, W. Yang, D. Jiang, "A novel adversarial learning framework in deep convolutional neural network " *intelligent diagnosis of mechanical faults, Knowledge-Based Syst. 165 (2019) 474–487.*
[6] Park, Seunghyun, and Jin-Young Choi. "Hierarchical anomaly detection model for in-vehicle networks using machine learning algorithms." *Sensors* 20.14 (2020): 3934.
[7] E. Seo, H.M. Song, H.K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network", *2018 16th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2018, pp. 1–6.*
[8] Barletta, Vita Santa, et al. "Intrusion Detection for In-Vehicle Communication Networks: An Unsupervised Kohonen SOM Approach." *Future Internet* 12.7 (2020): 119.
[9] Barletta, Vita Santa, et al. "A Kohonen SOM Architecture for Intrusion Detection on In-Vehicle Communication Networks." *Applied Sciences* 10.15 (2020): 5062.
[10] Kosmanos, Dimitrios, et al. "A novel intrusion detection system against spoofing attacks in connected electric vehicles." *Array* 5 (2020): 100013.
[11] Luo, Shengda, et al. "Complementary Deep and Shallow Learning with Boosting for Public Transportation Safety." *Sensors* 20.17 (2020): 4671.
[12] Qin, Zhi-Quan, Xing-Kong Ma, and Yong-Jun Wang. "ADSAD: An unsupervised attention-based discrete sequence anomaly detection framework for network security analysis." *Computers & Security* 99 (2020): 102070.
[13] Alom, Md Zahangir, and Tarek M. Taha. "Network intrusion detection for cyber security using unsupervised deep learning approaches." *2017 IEEE National Aerospace and Electronics Conference (NAECON)*. IEEE, 2017.