باسمه تعالی

علیرضا نودهی

گزارش کار پروژه

ابتدا به شرح مسئله میپردازیم

خودروهای متصل و خودمختار (CAVs) انتظار دارند ایمنی جاده و کارایی سیستم حمل و نقل را به طور چشمگیری بهبود بخشند. با این حال، CAV ها می توانند در برابر حملات در سطوح مختلف آسیب پذیر باشند، به عنوان مثال، حملات به شبکه های داخل خودرو و شبکه های بین خودرویی. این حملات مخرب نه تنها منجر به از بین رفتن محرمانه بودن و حریم خصوصی کاربر می شود، بلکه منجر به عواقب جدی تری مانند آسیب بدنی و از دست دادن جان می شود. سیستم تشخیص نفوذ (IDS) یکی از مؤثرترین راه‌ها برای نظارت بر عملیات وسایل نقلیه و شبکه‌ها، شناسایی انواع مختلف حملات و ارائه اطلاعات ضروری برای کاهش و اصلاح اثرات حملات است. برای اطمینان از ایمنی CAVها، تشخیص دقیق حملات مختلف به موقع بسیار مهم است. IDS مبتنی بر یادگیری ماشین (ML) میتواند این مشکل را حل کند که برای شبکه‌های درون خودرویی و بین خودرویی است.

وسایل نقلیه متصل و خودمختار (CAVs) که دارای انواع حسگرها، ارتباطات بی‌سیم و محاسبات داخلی هستند، وسایل نقلیه را قادر می‌سازند تا محیط را درک کنند، با محیط اطراف خود ارتباط برقرار کنند و برخی یا کامل عملکردهای رانندگی را کنترل کنند. یک خودروی پیشرفته مدرن دارای بیش از ۱۰۰ سنسور با قدرت محاسباتی است و به طور مداوم از طریق رابط های مختلف به اینترنت و سایر وسایل نقلیه یا سرورها متصل است.

چنین سرویس‌های متصل و برنامه‌های تلفن همراه به معنای افزایش سطوح حمله است که راه را برای مهاجمان هموار می‌کند تا به صورت غیرفعال یا فعال به شبکه دسترسی پیدا کنند.

حملات غیرفعال در پس‌زمینه رخ می‌دهد، مانند استراق سمع یا جمع‌آوری داده‌ها از طریق ضربه زدن به اتصال ارتباطی. در یک حمله فعال، حریف در واقع بر عملیات شبکه مورد حمله تأثیر می گذارد. از جمله تهدیدات فعال در یک محیط خودروی متصل می توان به DoS، تزریق اطلاعات نادرست، جعل، حملات Sybil و غیره اشاره کرد. بنابراین، داشتن یک معماری کاملاً تعریف‌شده و سازگار - هم در داخل وسیله نقلیه و هم در فضای ابری - برای تولیدکنندگان تجهیزات اصلی (OEM) و سایر شرکت‌کنندگان بخش تحرک برای

تضمین امنیت این اکوسیستم‌های پیچیده‌تر بسیار مهم است . ارتباط در یک وسیله نقلیه متصل می تواند در دو بخش اتفاق بیفتد: شبکه درون وسیله نقلیه یا داخل خودرو، و شبکه بین خودرو .شبکه ارتباطی درون خودرو از حسگرهای زیادی تشکیل شده است که از طریق گذرگاه شبکه کنترل کننده منطقه (CAN)با یکدیگر در ارتباط هستند. این مسیرهای ارتباطی به دلیل ساخت آنها، که به منظور کاهش کابل کشی در خودرو بود، به حملات حساس هستند.

Can Bus یک استاندارد ارتباطی در وسیله نقلیه است که برای تسهیل ارتباط بین واحدهای کنترل الکترونیکی مختلف (ECU) یا همان سنسور ها در وسایل نقلیه مدرن طراحی شده است. در دهه ۱۹۸۰ توسط بوش توسعه یافت و به یک استاندارد در الکترونیک خودرو تبدیل شد.

پروتکل CAN Bus یک پروتکل مبتنی بر پیام است، به این معنی که داده ها به شکل پیام هایی منتقل می شوند که به تمام دستگاه های متصل در شبکه پخش می شوند. هر ECU (به عنوان مثال، واحد کنترل موتور، واحد کنترل انتقال، واحد کنترل کیسه هوا) می تواند پیام ارسال و دریافت کند، اما هر پیام با یک شناسه منحصر به فرد برچسب گذاری می شود که اولویت آن را دیکته می کند.

این پروتکل برای ارتباطات بلادرنگ طراحی شده است و تضمین می کند که سیستم های حیاتی مانند ترمز و مدیریت موتور می توانند قابل اعتماد و سریع عمل کنند.همچنین CAN Bus به دلیل تحمل خطا و قابلیت اطمینان آن شناخته شده است. حتی اگر بخشی از شبکه آسیب دیده یا از کار بیفتد، می تواند به کار خود ادامه دهد.

Can bus از یک سیستم دو سیم (CAN_H و CAN_L) استفاده می کند که سیگنال دیفرانسیل را ارائه می دهد که به کاهش نویز و بهبود قابلیت اطمینان ارتباط کمک می کند.

داده های استاندارد CAN شامل موارد زیر است: CAN ID (۱۲۸ بیت) - SOF (شروع قاب) (۱ بیت)، شناسه پایه (۱۱ بیت)، درخواست از راه دور جایگزین (SRR) (۱ بیت)، بیت پسوند شناسه (IDE) (۱ بیت)، شناسه توسعه یافته (۱۸ بیت)، درخواست انتقال از راه دور (RTR) (۱ بیت)، بیت های رزرو شده (۲ بیت)، کد طول داده (DLC) (۴ بیت)، داده (۶۴ بیت)، بررسی افزونگی چرخه ای (CRC) (۱۶ بیت)، ACK (۲ بیت) و EOF (۷ بیت). در گذرگاه CAN، شکاف‌های بین پیام‌های متوالی فضای بین فریم (IFS) نامیده

می‌شود که حداقل سه بیت متوالی دارند.

	Arbitration		Control			Data	CRC		ACK		
SOF	ID	RTR	IDE	RBO	DLC	DAT A	CRC	CRC DeL	ACK	ACK DeL	EOF

یک IDS در یک استراتژی امنیتی، مهاجم، موقعیت مهاجم، زمان حمله، مکان، نوع فعالیت نفوذ، لایه‌ای که حمله در آن رخ داده و گره‌های متاثر از حمله را شناسایی می‌کند. بنابراین IDS را می‌توان به عنوان یک سیستم سخت‌افزاری و/یا نرم‌افزاری تعریف کرد که برای شناسایی ترکیبی از فعالیت‌هایی که به منظور تهدید محرمانگی، یکپارچگی یا در دسترس بودن منبع طراحی شده‌اند، تعریف می‌شود.

IDS در حوزه خودرو بر تشخیص در دروازه‌های مرکزی، سنسورها و CAN bus و واحد OBD تمرکز دارد. مزایای رویکردهای مبتنی بر ML شامل ظرفیت آن‌ها برای ساخت مدل‌های صریح و ضمنی از الگوهای بررسی‌شده است که به‌طور منظم برای افزایش عملکرد تشخیص بر اساس یافته‌های قبلی به روز می‌شوند.

شبکه درون خودرو: تهدیدات امنیتی و IDS

- حمله جعل CAN bus

از آنجایی که پروتکل CAN رویه‌های احراز هویت و رمزگذاری را ارائه نمی‌کند، می‌توان از یک گره در معرض خطر به گذرگاه CAN ضربه زد و پیام‌های جعلی را با یک شناسه موجود در شبکه ارسال کرد. با انجام این کار، یک مهاجم با ایجاد پیام‌های نامعتبر به وسیله نقلیه، عملکردی را در خودرو مختل می‌کند. با اجرای احراز هویت گره و رمزگذاری پیام می توان از حمله جعل جلوگیری کرد. با این حال، بار محاسباتی بر روی ECU ها وارد می کند.

-حمله CAN bus Fuzzing

ECU ها برای عملکرد موثر به ارتباطات CAN bus متکی هستند، اما از آنجایی که پیام های CAN bus فاقد احراز هویت هستند، ECU ها نمی توانند اعتبار منبع پیام را تأیید کنند.در این نوع حمله، هدف یک مهاجم بررسی اتفاقاتی است که در ECU ها اتفاق می افتد و در عین حال هدف حمله را نیز ردیابی می کند. به عنوان مثال، اگر مهاجم به دنبال تغییر

سرعت وسیله نقلیه باشد، ارتباط بین ECU مورد نظر و CAN bus و همچنین تغییر در سرعت وسیله نقلیه در هنگام حمله را کنترل می کند. علاوه بر این، گذرگاه CAN را می توان به عنوان یک جعبه سیاه توسط مهاجم در نظر گرفت، که در آن شناسه CAN و مقادیر payload به طور تصادفی، بدون اطلاع قبلی از شناسه های CAN واقعی در سیستم، تولید می شوند. این شامل انتقال فریم های CAN به طور تصادفی برای ایجاد اختلال در عملکرد خودرو است. برای جلوگیری از وقوع تجزیه و تحلیل داده ها، رمزگذاری و احراز هویت مورد نیاز است، که دومی تضمین می کند که در وهله اول فقط ECU های معتبر فریم های CAN را ارسال می کنند.

-حمله جعل فریم CAN bus

حملات جعل فریم زمانی اتفاق می‌افتد که مقادیر اشتباهی به پیام‌های موجود در بار CAN Bus اضافه شود .این حمله بار دیگر نتیجه عدم احراز هویت و رمزگذاری در معماری CAN bus است. مکانیسم‌های احراز هویت به کاربران اجازه می‌دهد تا قبل از اقدام بر روی منبع داده‌ها برای مقابله با این نوع حمله، احراز هویت کنند. به منظور شناسایی این حمله، یک سیستم باید ثبات شناسه CAN و بار داده را در مدتی ارزیابی کند.

-حمله تزریق CAN bus

بدون رمزگذاری و احراز هویت، هر گره می تواند به گذرگاه متصل شود و گذرگاه را برای داوری و فیلدهای داده منتقل شده نظارت کند. همچنین، هنگامی که یک گره مخرب به گذرگاه CAN دسترسی پیدا می کند، این امکان برای آن وجود دارد که داده های هدفمند یا انبوه را منتقل کند، که امکان تغییرات در فرکانس و تغییر فریم های گذرگاه CAN را فراهم می کند. این می تواند باعث ایجاد رویدادهای تقلبی شود و باعث شود که بخش هایی از وسیله نقلیه به دلخواه عمل کنند. روش های احراز هویت و حفاظت از یکپارچگی می تواند این حمله را متوقف کند.

- حمله CAN bus DoS

ECU های متصل به گذرگاه CAN برای دسترسی به کانال بر اساس اولویت CAN ID رقابت می کنند. فیلد داوری توسط گره های CAN Bus برای تعیین اولویت پیام و اینکه کدام گره مجاز است از گذرگاه برای انتقال اطلاعات استفاده کند استفاده می شود. بنابراین، با استفاده از بالاترین شناسه انتساب ممکن می توان یک حمله برای اشغال گذرگاه و جلوگیری از استفاده سایر گره ها از آن راه اندازی کرد. با دانستن نرخ انتقال شناسه پیام

CAN موجود در ECU، می‌توان با افزایش فرکانس پیام‌های تزریق شده، یک حمله DoS را آغاز کرد.

حال که با مسئله و تهدیدات آن آشنا شدیم وقت آن است که راه حلی برای حل این مشکل ارائه کنیم.

ما میتوانیم برای حل مشکل از یادگیری تحت نظارت (supervised) یا از یادگیری بدون نظارت(unsupervised) بهره بجوییم.

یادگیری تحت نظارت شامل آموزش یک مدل بر روی یک مجموعه داده برچسب‌گذاری شده است. در این رویکرد، هر نمونه آموزشی با برچسب یا خروجی مربوطه همراه است. هدف یادگیری یک نقشه برداری از ورودی ها به خروجی ها است تا مدل بتواند برچسب ها را برای داده های دیده نشده پیش بینی کند.

در این نوع یادگیری، مدل با جفت ورودی-خروجی ارائه می شود و می آموزد که خروجی را بر اساس ویژگی های ورودی پیش بینی کند. اما دریادگیری بدون نظارت مجموعه داده بدون برچسب های صریح است. مدل سعی می کند الگوها، ساختارها یا روابط را در داده ها شناسایی کند. مدل ، داده های ورودی را تجزیه و تحلیل می کند و الگوها یا گروه بندی های ذاتی را در آن کشف می کند.

از مزایای یادگیری بدون نظارت میتوان به عدم نیاز به داده‌های برچسب دار اشاره کرد که پیدا کردن برسب و ساخت آن می تواند گران و زمان بر باشد. این باعث می شود زمانی که برچسب ها کمیاب یا در دسترس نیستند مفید باشد.

تشخیص ناهنجاری نیر یکی دیگر از مزیت های روش‌های بدون نظارت، به‌ویژه روش‌های خوشه‌بندی و مبتنی بر چگالی است که برای تشخیص ناهنجاری مناسب هستند، زیرا می‌توانند نقاط داده‌ای را شناسایی کنند که به خوبی با اکثر داده‌ها مطابقت ندارند. همچنین

مقیاس پذیری بالای بسیاری از الگوریتم های یادگیری بدون نظارت می توانند نسبت به همتایان تحت نظارت خود نسبت به مجموعه داده های بزرگ مقیاس پذیرتر باشند، به ویژه زمانی که برچسب گذاری مجموعه داده های بزرگ غیرعملی باشد.

برای ارائه روش کارآمد برای حل مشکلات امنیتی در can bus به دلیل محدودیت هایی نظیر پهنای کم باند ارتباطی، عدم نیاز به برچسب و همچنین سرعت بالا ، قابلیت تشخیص

حملات روز صفر و سازگاری با داده های جدید باعث می‌شود از یادگیری بدون نظارت بهره ببریم.

جنگل ایزوله برای تشخیص ناهنجاری

وقتی صحبت از تشخیص ناهنجاری در یادگیری بدون نظارت می شود، الگوریتم جنگل جداسازی برجسته می شود.

Isolation Forest یا به اختصار iForest ی ک الگوریتم برا ی تشخیص ناهنجاری داده است که در سال ۲۰۰۸ توسعه یافت. Isolation Forest با استفاده از درختان باینری ناهنجاری ها را تشخیص می دهد .این الگوریتم دارای پیچیدگی زمانی خطی و نیاز به حافظهپه کم است که با داده های با حجم بالا به خوبی کار می کند.در اصل، الگوریتم برای تشخیص ناهنجاری ها بر ویژگی های ناهنجاری ها، یعنی کم و متفاوت بودن تکیه دارد. هیچ تخمین چگالی در الگوریتم انجام نشده است. این الگوریتم با الگوریتمهای درخت تصمیم (design tree) متفاوت است زیرا فقط از اندازه گیری طول مسیر یا تقریب برای ایجاد امتیاز ناهنجاری استفاده می شود، هیچ گره و برگ آماری در توزیع کلاس یا مقدار هدف مورد نیاز نیست.

Isolation Forest بسیار سریع است زیرا فضای داده را به طور تصادفی با استفاده از ویژگی انتخاب شده تصادفی و نقطه تقسیم تصادفی انتخاب شده، تقسیم می کند. امتیاز ناهنجاری به طور معکوس با طول مسیر مرتبط است زیرا ناهنجاری ها برای جداسازی به تقسیم های کمتری نیاز دارند، به دلیل این که آنها معمولا کم تعداد و متفاوت هستند .اکثر رویکردهای مبتنی بر مدل موجود برای تشخیص ناهنجاری، نمایه ای از نمونه های عادی را می سازند، سپس نمونه هایی را که با نمایه عادی تطابق ندارند به عنوان ناهنجاری شناسایی می کنند. استفاده از این روش جداسازی، iForestرا قادر می سازد تا از نمونه گیری فرعی تا حدی استفاده کند که در روش های موجود امکانپذیر نیست .اکثر رویکردهای مبتنی بر مدل موجود برا ی تشخیص ناهنجاری، نمایه ای از نمونه های عادی را می سازند، سپس نمونه هایی را که با نمایه عادی مطابقت ندارند به عنوان ناهنجاری شناسایی می کنند را جدا می کند.

برای نمونه گیری و اجرای الگوریتم و حل مسئله از مجموعه داده‌های تشخیص نفوذ، مانند مجموعه داده‌های تشخیص نفوذ خودرو (ML350)، کمک می‌گیریم.

این داده ها با استفاده از CL2000 از مرسدس ML350 جمع آوری شد. از آنجایی که شناسه‌های CAN و بایت‌های داده در قالب اعشاری بودند، از پیش پردازش برای تبدیل داده‌ها به نمایش‌های عددی با اعمال نرمال‌سازی و پرچم‌های رمزگذاری استفاده شد. نمونه داده های مجموعه داده از ۴ شناسه CAN مختلف جمع آوری شده است. حملات در مجموعه داده از حملات DoS و فازی جمع آوری شده است. مجموعه داده شامل ۳۳۴٬۵۱۹ نمونه داده عادی و ۳۹۶٬۰۰۰ نمونه داده حمله است.

پس از اجرای Isolation Forest بر روی کل داده ها با استفاده از معیار f1 دقت را تعیین میکنیم.

کمیت مدل های طبقه بندی را می توان با عبارات زیر استنتاج کرد:

مثبت واقعی (TP) - تعداد داده های عادی درست پیش بینی شده اند.

منفی واقعی (TN) - تعداد داده های حمله ای که به درستی پیش بینی شده اند.

مثبت کاذب (FP) - تعداد داده های عادی که به اشتباه به عنوان حمله پیش بینی شده اند..

منفی کاذب (FN) - تعداد داده های حمله ای که به اشتباه به عنوان داده های عادی پیش بینی شده اند.

بر اساس عبارات مورد بحث در بالا، چندین معیار ارزیابی برای ارزیابی مدل در نظر گرفته شده است.

۱) accuracy : نسبت داده هایی است که به درستی پیش بینی شده اند به کل مجموعه داده آزمون. دقت بالاتر یعنی مدل بهتر است. دقت معیار خوبی برای مجموعه داده آزمایشی است که شامل کلاس های متعادلی است. دقت را می توان به صورت زیر تعریف کرد:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

۲)Precision : دقت نسبت داده هایی است که حمله به درستی پیش بینی شده است به تعداد کل داده های حمله پیش بینی شده. هرچه دقت بالاتر باشد، مدل بهتر است. دقت را می توان به صورت تعریف کرد

$$Precision = \frac{TP}{TP + FP}$$

امتیاز F1 :امتیاز F1 میانگین هارمونیک دقت و یادآوری است. هرچه امتیاز F1 بالاتر باشد، مدل بهتر است F1-Score .را می توان به صورت زیر تعریف کرد :

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

تمامی مقادیر بالا بین ۰ و ۱ هستند.

درنهایت با بررسی نتایج مختلف آزمون ها و خطاهای گوناگون و پیداکردن طول مناسب برای درخت نتایج زیر به دست آمد :

Precision = 0.9993555581301049

Accuracy = 0.8839307824983816

F1 score = 0.8732252676334371