به نام خدا

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

تشخیص اطلاعات غلط در شبکه‌های اقتضایی خودرویی

پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر - معماری کامپیوتر

عباس میرحیدری

استاد راهنما

دکتر محمد علی منتظری

استاد مشاور

دکتر مهدی برنجکوب

اردیبهشت ماه ۱۳۹۲

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی کامپیوتر - معماری کامپیوتر آقای عباس میرحیدری

تحت عنوان

تشخیص اطلاعات غلط در شبکه‌های اقتضایی خودرویی

در تاریخ ۱۳۹۲ / ۲ / ۳۱ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان نامه	دکتر محمد علی منتظری
۲- استاد مشاور	دکتر مهدی برنجکوب
سرپرست تحصیلات تکمیلی دانشکده	دکتر مسعود عمومی

تشکر و قدردانی

پس از حمد و سپاس خداوند و قدردانی از زحمات پدر و مادرم، بر خود لازم می‌دانم از اساتید گرامی و بزرگوارم، دکتر محمد علی منتظری و دکتر مهدی برنجکوب که در روند تهیه‌ی این پایان‌نامه مرا از راهنمایی‌های ارزشمند خود بهره‌مند ساختند، نهایت تشکر و سپاس‌گذاری را به عمل آورم.

فهرست مطالب

عنوان **صفحه**

فصل سوم : پیش نیازها و مرور کارهای مرتبط

فصل چهارم : پیشنهادی برای تشخیص اطلاعات غلط در شبکه‌های VANET

فهرست شکل‌ها

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

چکیده

موفقیت و عملکرد صحیح سیستم‌های بی‌سیمی که از حسگرها برای جمع آوری اطلاعات استفاده می‌کنند، به کیفیت داده‌های جمع‌آوری شده بستگی دارد. اطلاعات غلط یکی از مهم‌ترین عوامل تأثیرگذار بر کیفیت داده‌ها می‌باشد که می‌توان آن‌ها را برخاسته از عللی نظیر خرابی حسگرها، کانال ارتباطی غیرمطمئن و یا حسگرهای به تسخیر درآورده شده دانست. شبکه‌های اقتضایی خودرویی نمونه‌ی پویایی (به علت تغییرات سریع توپولوژی) از این گونه سیستم‌ها هستند که با هدف اصلی افزایش سطح ایمنی مسافرین و جاده‌ها معرفی شده‌اند. در این شبکه‌ها، خودروها به وسایلی نظیر کامپیوتر، انواع حسگرها، سیستم موقعیت‌یاب جهانی و رابط بی‌سیم مجهز می‌شوند و اطلاعات ضروری جاده‌ها از طریق ارتباطات خودرو به خودرو و خودرو به تجهیزات کنار جاده‌ای، منتشر می‌شود. در این شرایط خودروهای بدخواه ممکن است اقدام به شایعه پراکنی و انتشار اطلاعات غلط کنند. به عنوان مثال گزارش کردن یک رخداد غیر واقعی مانند ترمز ناگهانی می‌تواند باعث اتخاذ تصمیمات نادرست و حرکات اشتباه از سوی خودروهای دریافت کننده‌ی گزارش شود که در اکثر موارد می‌تواند منجر به حوادث جبران ناپذیری بشود. بنابراین یک مسئله اساسی به منظور حفظ ایمنی در شبکه‌های اقتضایی خودرویی اینست که چگونه می‌توان به پیام‌های دریافت شده اعتماد پیدا کرد و یا به بیان دیگر چگونه می‌توان اطلاعات غلط را تشخیص داد. برای حل این مسئله معمولا از روش‌های مدیریت اعتماد استفاده می‌شود. بسیاری از روش‌های ارائه شده از مدل‌های اعتماد شهرت-محور (توزیع شده) که از شبکه‌های اقتضایی سیار گرفته شده است، استفاده کرده‌اند. اما این مدل‌ها در شبکه‌هایی که دارای توپولوژی ناپایدار هستند، عملکرد ضعیفی دارند. برخی دیگر از روش‌های ارائه شده از مدل‌های اعتماد داده-محور بهره گرفته‌اند. این مدل‌ها نیز در برابر حمله تبانی و همچنین در مناطق خلوت نتایج ضعیفی را نشان می‌دهند. بر اساس تحقیقاتی که تا کنون صورت گرفته، ارائه‌ی یک سیستم اعتماد توزیع شده‌ی محض جهت تشخیص اطلاعات غلط در شبکه‌های اقتضایی خودرویی که از استحکام کافی برخودار باشد و هنگام تغییرات سریع توپولوژی کارایی خود را از دست ندهد، تقریبا غیرعملی است. در این پایان‌نامه، یک سیستم تشخیص اطلاعات غلط برای شبکه‌های اقتضایی خودرویی پیشنهاد شده است که در آن، سابقه‌ی راستگویی خودروها در قالب یک عدد حقیقی بین ۰ و ۱ در پایگاه داده مشترک RSUها قرار داده می‌شود و هر خودرو به صورت دوره‌ای سابقه‌ی خود را از نزدیک‌ترین RSU دریافت می‌کند. هر خودرو هنگام ارسال گزارش‌هایش، شناسه خودروهای اطرافش و سابقه خود را به گزارش‌ها الحاق می‌کند. گیرنده‌ی گزارش‌ها بر اساس رده و سابقه‌ی خودروی گزارش دهنده و همچنین بر اساس درصد همسایه‌های خودروهای گزارش دهنده که گزارش او را تأیید کرده‌اند، گزارش را اعتبارسنجی می‌کنند. از آنجا که اعتماد، یک مسئله عدم قطعیت بشمار می‌رود و منطق فازی از بهترین روش‌های حل چنین مسائلی است، از استدلال فازی برای فرموله کردن شواهد و اعتبارسنجی پیام‌ها استفاده شده است. بعد از اعتبارسنجی گزارش‌ها اگر مشخص شود خودرویی گزارش غلط ارسال کرده، RSU وزن او را کاهش می‌دهد. نتایج شبیه‌سازی‌ها نشان می‌دهند که سیستم پیشنهاد شده در این پایان‌نامه جهت تشخیص اطلاعات غلط، حتی در شرایطی که سرعت خودروها و میزان تبانی در شبکه زیاد باشد دارای دقت بسیار بالایی است.

واژه‌های کلیدی: ۱- شبکه اقتضایی خودرویی ۲- رفتارهای بدخواهانه ۳- مدیریت اعتماد ۴- سیستم استدلال فازی

فصل اول
مقدمه

۱-۱- مقدمه

موفقیت و عملکرد صحیح سیستم‌های بی‌سیمی که از حسگرها برای جمع آوری اطلاعات استفاده می‌کنند، به کیفیت داده‌های جمع آوری شده بستگی دارد. داده‌های غلط یکی از مهم‌ترین عوامل تأثیرگذار بر کیفیت داده‌ها می‌باشد که می‌توان آن‌ها را برخاسته از عللی نظیر نقص فنی حسگرها، کانال ارتباطی غیرمطمئن و یا حسگرهای به تسخیر درآورده شده دانست[۱]. شبکه‌های اقتضایی خودرویی (VANET[1]) نمونه‌ی پویایی (به دلیل تغییرات سریع توپولوژی) از این گونه سیستم‌ها هستند که با هدف اصلی افزایش سطح ایمنی مسافرین و جاده‌ها معرفی شده‌اند. در این شبکه‌ها، خودروها به وسایلی نظیر کامپیوتر، انواع حسگرها، سیستم موقعیت‌یاب جهانی و رابط بی‌سیم مجهز می‌شوند و اطلاعات ضروری جاده‌ها از طریق ارتباطات خودرو به خودرو و خودرو به تجهیزات کنار جاده‌ای، منتشر می‌شود. در این شرایط خودروهای بدخواه ممکن است اقدام به شایعه پراکنی و انتشار پیام‌های غلط کنند. به عنوان مثال گزارش کردنِ یک رخداد غیر واقعی مانند ترمز ناگهانی می‌تواند باعث اتخاذ تصمیمات نادرست و حرکات اشتباه از سوی خودروهای دریافت کننده‌ی گزارش شود که در اکثر موارد می‌تواند منجر به حوادث جبران ناپذیری بشود. بنابراین یک مسئله اساسی به منظور حفظ ایمنی در شبکه‌های VANET این است که چگونه می‌توان به پیام‌های دریافت شده اعتماد پیدا کرد و یا به عبارت دیگر چگونه می‌توان اطلاعات غلطی را که برخاسته از عواملی همچون رانندگان غیردرستکار یا حسگرهای به تسخیر درآورده شده می‌باشند را شناسایی کرد.

[1] Vehicular Ad hoc NETwork

در این فصل ابتدا شبکه‌های خودرویی، کاربردها و مهم‌ترین چالش‌های آن‌ها را به اختصار معرفی می‌کنیم. سپس مسئله انتشار اطلاعات غلط در این شبکه‌ها، اهمیت تشخیص این گونه پیام‌ها و روش‌های موجود را بررسی خواهیم کرد. در آخر نیز، اهداف و ساختار ادامه‌ی این پایان‌نامه ارائه می‌شود.

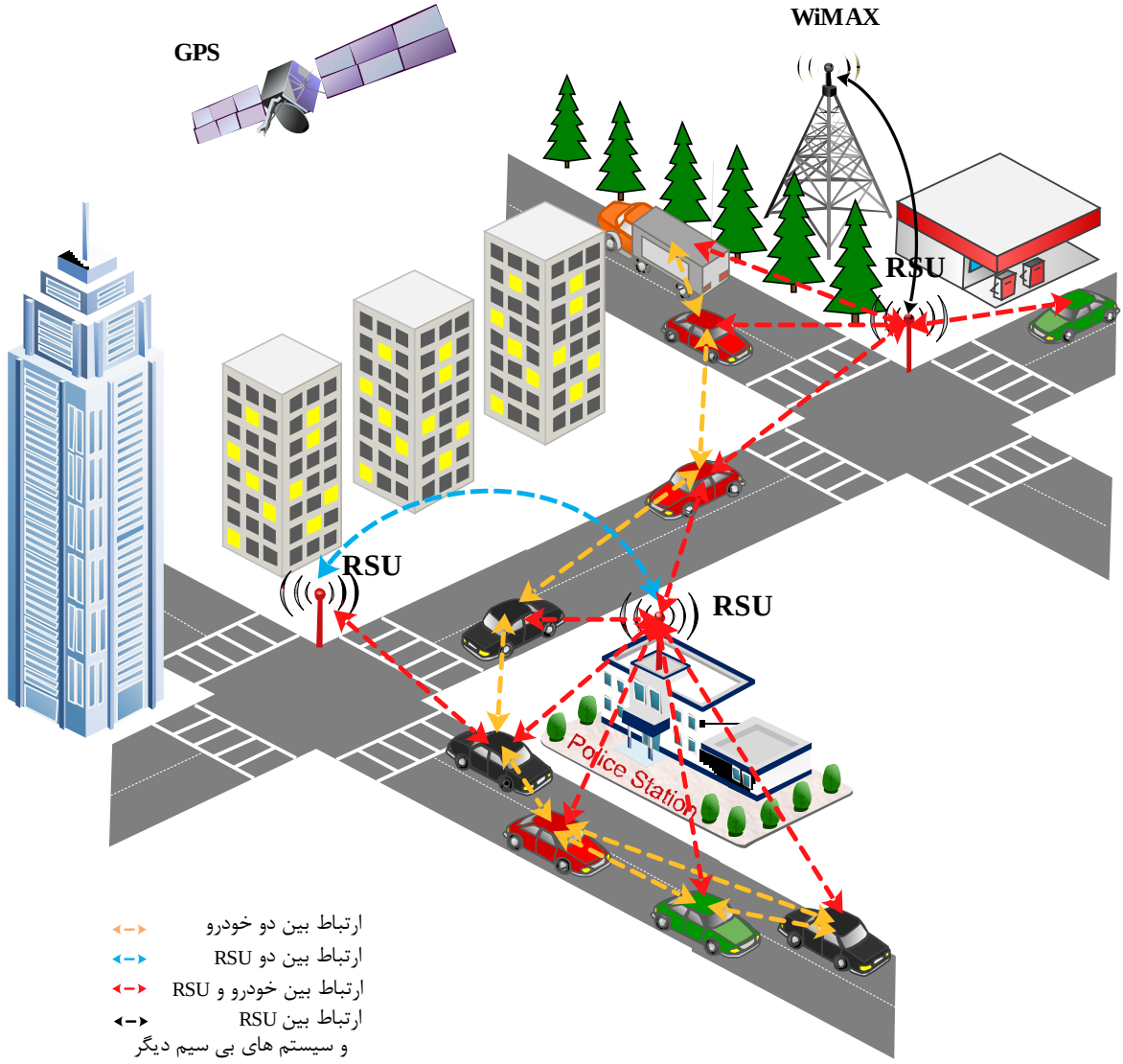
۱-۲- معرفی شبکه‌های خودرویی

براساس آمار، تصادفات رانندگی به عنوان بزرگترین عامل فوت افراد زیر ۴۰ سال، سالانه حدود ۱/۲ میلیون کشته و بیش از ۵۰ میلیون مجروح بر جای می‌گذارد[۲]. مهم‌ترین اقدام پیشگیرانه در این زمینه، تلاش برای ایجاد یک سیستم حمل ونقل هوشمند (ITS[1]) با اهدافی همچون کاهش زمان سفر، کاهش هزینه سوخت و کاهش تصادفات است. برای تحقق بخشیدن به این سیستم، گام‌های متعددی برداشته شده است که از آن جمله می‌توان به مجهز کردن خودروها به انواع سیستم‌های الکترونیک، کامپیوتر و انواع حسگرها اشاره کرد. یکی دیگر از فناوری‌های مورد نیاز در چنین سیستمی، امکان ارتباط بی‌سیم بین خودروها جهت آگاهی از اطلاعات ترافیکی است. دراین راستا، تا کنون سه نوع شبکه‌ی خودرویی مختلف شامل شبکه‌های خودرویی سلولی، شبکه‌های خودرویی اختصاصی و شبکه‌های اقتضایی خودرویی معرفی شده‌اند که در ادامه تشریح خواهند شد.

- شبکه‌های خودرویی سلولی: در این روش، خودروها بوسیله‌ی شبکه‌های سلولی اپراتورهای تلفن همراه با یکدیگر ارتباط برقرار می‌کنند و به اینترنت متصل می‌شوند. از مزیت‌های این شبکه‌ها می‌توان به استفاده از زیرساخت‌های از قبل آماده و دسترسی مداوم به اینترنت (در تمام نقاطی که خودرو تحت پوشش سیستم سلولی قرار دارد) اشاره کرد. از طرفی دیگر، وابستگی به پوشش شبکه‌های سلولی، محدودیت نرخ انتقال اطلاعات و عدم کارایی کافی در مورد کاربردهای بلادرنگ (به دلیل تأخیر ذاتی انتقال اطلاعات در سیستم‌های سلولی) را می‌توان از کاستی‌های این شبکه‌ها برشمرد.
- شبکه‌های خودرویی اختصاصی: راه اندازی این شبکه‌ها توسط شرکت‌های ثالث و با نصب تجهیزات لازم در کنار جاده‌ها و همچنین نصب رابط‌های متناسب در خودروها صورت می‌گیرد. مهم‌ترین ایراد این روش، هزینه زیاد تجهیزات و زیرساخت لازم برای برقراری چنین شبکه‌هایی می‌باشد.
- شبکه‌های اقتضایی خودرویی: شبکه‌های VANET نوع خاصی از شبکه‌های اقتضایی سیار[2] (شبکه‌های اقتضایی با گره‌های متحرک) هستند که هدف آن‌ها برقراری شبکه اقتضایی بین خودروها و تجهیزات کنار جاده‌ای (RSU[3]) می‌باشد. تمرکز ما در این پایان‌نامه بر روی این نوع از شبکه‌های خودرویی است. شکل ۱-۱ انواع ارتباط ممکن در این شبکه‌ها را نشان می‌دهد که عبارتند از: ارتباط خودرو با خودرو، ارتباط

[1] Intelligent Transportation System
[2] Mobile Ad hoc NETworks(MANETs)
[3] Road Side Unit

خودرو با RSU، ارتباط RSU با RSU و ارتباط RSU با سیستم‌های بی‌سیم دیگر نظیر وایمکس و 3G.

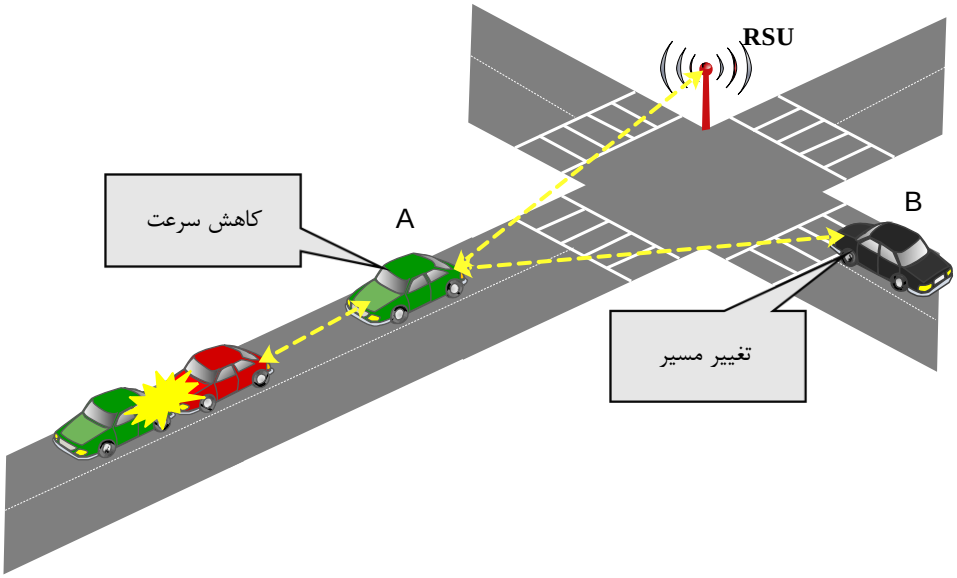


شکل ۱-۱ : معماری شبکه‌های اقتضایی خودرویی

کاربردهای شبکه‌های VANET را می‌توان به دو دسته‌ی کلی مرتبط با ایمنی[1] و غیر ایمنی[2] تقسیم کرد[۳]. اساس کاربردهای ایمنی، تبادل پیام‌هایی است که شرایط خاص و رخدادهای جاده‌ها[3] را بطوری که باعث افزایش سطح ایمنی و راحتی مسافرین شود به اطلاع می‌رسانند. به عنوان مثال، شکل ۱-۲ منتشر شدن پیام برخورد دو خودرو در شبکه را نشان می‌دهد. بر اساس این پیام، خودرو A تصمیم می‌گیرد سرعتش را کاهش دهد تا از وقوع حادثه‌ای

[1] Safety-related
[2] Non-safety
[3] Road events

دیگر جلوگیری کند. همچنین خودرو B که قصد ورود به خیابان محل تصادف را داشته، مسیر خود را عوض می‌کند تا از اتلاف وقت احتمالی خویش در آن خیابان جلوگیری کند. مثال‌هایی از کاربردهای غیر ایمنی نیز عبارتند از: پرداخت هوشمند عوارض، به اشتراک گذاری فایل‌ها، فراهم کردن اینترنت، تبلیغات تجاری و سایر خدمات رفاهی.



شکل ۱-۲ : انتشار پیام برخورد دو خودرو در VANET و تأثیر آن بر رفتار سایر رانندگان

مهم‌ترین چالش شبکه‌های اقتضایی خودرویی، امنیت آن‌ها است. با توجه به نقش این شبکه‌ها در فراهم آوردن ایمنی خودروها، نفوذ و ایجاد اختلال در چنین شبکه‌هایی می‌تواند آثار مخرب و جبران ناپذیری داشته باشد و تا زمانی که سطح امنیت این فناوری به مرتبه قابل قبولی برای صنعت تولید خودرو و رانندگان نرسد، با وجود کاربردها و مزایای زیادی که از این شبکه‌ها انتظار می‌رود، نمی‌توان آن را به صورت گسترده پیاده‌سازی کرد و مورد استفاده قرار داد.

در مبحث امنیت شبکه‌های اقتضایی خودرویی می‌توان گفت که اکثر حملات موجود در شبکه‌های اقتضایی سیار و شبکه‌های حسگر بی‌سیم[1]، شبکه‌های اقتضایی خودرویی را نیز تهدید می‌کنند[۴]. تاکنون تحقیقات زیادی درباره‌ی مقابله با تهدیدهای مرسوم شبکه‌های اقتضایی و همچنین حفظ حریم خصوصی[2] در VANET صورت پذیرفته است[۵]، در حالیکه به تهدیدهایی که تنها مربوط به شبکه‌های خودرویی هستند، به ویژه تهدیدهای علیه کاربردهای مرتبط با ایمنی، توجه کمتری شده است.

[1] Wireless Sensor Network(WSN)
[2] Privacy preservation

یکی دیگر از چالش‌های مهم شبکه‌های اقتضایی خودرویی، مسیریابی است. تحلیل پروتکل‌های مطرح ارائه شده برای شبکه‌های اقتضایی سیار نشان می‌دهد که آن‌ها در شبکه‌های اقتضایی خودرویی کارایی ضعیفی از خود نشان می‌دهند[۶]. مشکل اساسی این پروتکل‌ها در محیط‌های خودرویی، عدم ثبات مسیر انتقال بسته‌های اطلاعات به دلیل عدم ثبات توپولوژی شبکه است که منجر به از دست رفتن بسته‌ها، افزایش سربار ناشی از بازیابی مسیرها، کاهش نرخ تحویل بسته‌ها به مقصد[۱] و افزایش تأخیر انتقال می‌گردد. بنابراین وظیفه‌ی اصلی پروتکل‌های مسیریابی در شبکه‌های اقتضایی خودرویی کنترل تغییرات توپولوژی شبکه به گونه‌ای است که نیازهای کیفیت سرویس[۲] مربوط به کاربردهای مختلف، بوسیله‌ی الگوریتم مسیریابی برآورده شود. نرخ تحویل بسته‌ها به مقصد و تأخیر انتقال از جمله مهم‌ترین نیازهای کیفیت سرویس در کاربردهای مختلفِ شبکه‌های خودرویی است. مجهز بودن خودروها به سیستم‌های موقعیت یاب ماهواره‌ای نظیر GPS[۳]، وجود نوع متفاوتی از پروتکل‌های مسیریابی موسوم به پروتکل‌های مکان-محور[۴] را در شبکه‌های اقتضایی خودرویی ممکن ساخته است[۷]. این پروتکل‌ها با استفاده از اطلاعات مکانی همسایه‌های یک گره اقدام به انتخاب بهترین گره مجاور برای ارسال بسته و ادامه‌ی روند مسیریابی به سمت مقصد می‌کنند. در شبکه‌های اقتضایی خودرویی با توجه به تحرک بالای گره‌ها، پروتکل‌های مکان-محور به دلیل استفاده از اطلاعات موقعیتیِ گره‌های شبکه برای تصمیم‌گیری در مورد انتخاب بهترین مسیر، نسبت به سایر پروتکل‌های مسیریابی به کار رفته در شبکه‌های اقتضایی دیگر مانند MANET[۵]، از کارایی و مقبولیت بیشتری برخوردار هستند.

۱-۳- شرح مسئله

یکی از تفاوت‌های اصلی میان شبکه‌های اقتضایی خودرویی و شبکه‌های بی‌سیم معمولی تبادل پیام‌هایی است که با هدف فراهم شدن ایمنی بیشتر برای خودروها و مسافرین صورت می‌گیرد. در واقع، ارسال چنین پیام‌هایی در شبکه‌های VANET روی رفتار رانندگان و در نتیجه ایمنی آن‌ها تأثیر گذار است. گره‌های بدخواه[۶] می‌توانند از این شرایط سوء استفاده کنند و با ارسال پیام‌های غلط[۷] درباره‌ی رخدادهای غیر واقعی[۸]، باعث اختلال در شبکه و رفتار رانندگان بشوند. به عنوان مثال، [۸] حمله‌ای تحت عنوان تصادف هوشمندانه[۹] را معرفی کرده است. نویسنده

---

[1] Packet delivery ratio
[2] Quality of Service (QoS)
[3] Global Positioning System
[4] Position-based routing protocol
[5] Mobile Ad hoc NETwork
[6] Malicious nodes
[7] False (bogus) messages
[8] Fake (unreal) events
[9] Intelligent collision

نشان می‌دهد که یک خودروی بدخواه می‌تواند با ارسال هشدارهای غلط خاصی موجب ترمز ناگهانی سایر رانندگان و در نتیجه وقوع تصادف‌های زنجیره‌ای شود.

بطور کلی، ارسال اطلاعات، پیام‌ها یا گزارش‌های غلط در شبکه‌های خودرویی باعث گمراه شدن خودروها و حتی در برخی موارد منجر به حوادث جبران ناپذیری می‌شود. بنابراین باید مکانیزمی وجود داشته باشد که بتواند پیام‌ها یا گزارش‌های غلط را شناسایی کرده و دور بریزد. البته اگر پیام‌های غلط از جانب گره‌های غیرمجاز که عضو شبکه نیستند ارسال بشود، توسط روش‌های امنیتی مبتنی بر رمزنگاری مانند سرویس‌های احراز اصالت[۱] و یکپارچگی[۲] پیام، به راحتی تشخیص داده می‌شوند. زیرا لازمه‌ی اجرای سرویس‌های امنیتی مبتنی بر رمزنگاری در شبکه، اعطای گواهینامه‌های دیجیتالی منحصر بفرد به هر یک از گره‌های شبکه است و هر گره، تنها با در اختیار داشتن گواهینامه دیجیتالی معتبر خویش قادر خواهد بود به تبادل پیام بپردازد و سرویس‌های امنیتی را با موفقیت پشت سر بگذارد. اما در صورتیکه گره‌های مجاز شبکه مبادرت به شایعه پراکنی و ارسال پیام‌های غلط کنند، روش‌های مبتنی بر رمزنگاری راه حل خوبی برای تشخیص آن پیام‌های غلط بشمار نمی‌روند، زیرا یک کاربر مجاز شبکه که دارای گواهینامه دیجیتالی است، می‌تواند پیام‌های غلط به ظاهر معتبری تولید کند. به عنوان نمونه، می‌توان با قرار دادن یخ روی حسگر تشخیص دمای هوا یا حسگر تشخیص لغزندگی جاده، باعث تولید پیام‌های غلط شد.

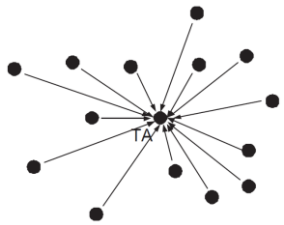
همانطور که گفته شد، سرویس‌های امنیتی مبتنی بر رمزنگاری از ورود کاربران غیر مجاز و ضربه وارد کردن آن‌ها به شبکه جلوگیری می‌کنند. اما جلوگیری یا پیشگیری از سوء استفاده‌های کاربران (موجودیت‌های) مجاز با رویکرد رمزنگاری قابل پیگیری نیست. به همین علت، برای تشخیص اینکه آیا اطلاعات گزارش شده توسط یک کاربر مجاز شبکه صحیح است یا غلط، روش‌های دیگری را باید بکار گرفت. در سال‌های اخیر، سیستم‌های مدیریت اعتماد[۳] در شبکه‌های بی‌سیم نظیر شبکه‌های اقتضایی سیار و اقتضایی خودرویی، به عنوان راه حلی مؤثر برای برخی مشکلات امنیتی نظیر تشخیص درستی پیام‌ها که توسط مکانیزم‌های معمول قابل حل نیستند، مورد استفاده قرار گرفته است. بوسیله مکانیزم‌های مدیریت اعتماد می‌توان از طریق پایش[۴] گره‌ها و معیارهایی همچون سابقه‌ی رفتار گره‌ها، میزان اعتماد به آن‌ها را تخمین زد (سطح اعتماد به هر گره معمولا با یک عدد حقیقی بین ۰ تا ۱ ارزیابی می‌شود بطوریکه عدد یک، مبین اعتماد کامل و عدد صفر عدم اعتماد را نشان می‌دهد) و بدین ترتیب میزان اطمینان از درستی اطلاعات گزارش شده، متناسب با میزان اعتماد به گره یا گره‌های گزارش دهنده‌ی آن اطلاعات ارزیابی می‌شود.

---

[1] Authentication
[2] Integrity
[3] Trust management systems
[4] Monitoring

سیستم‌های اعتماد موجود را می‌توان به سه دسته کلی تقسیم کرد که در ادامه هر کدام از آن‌ها را شرح می‌دهیم[۹].

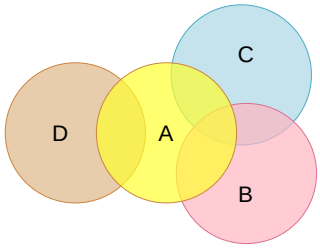
- سیستم‌ها یا مدل‌های متمرکز[۱]: فرض اکثر سیستم‌های اعتماد متمرکز این است که یک واحد TA[۲] وجود دارد که همه‌ی گره‌های شبکه می‌توانند به آن دسترسی داشته باشند (شکل ۱-۳). TA در این مدل‌ها فعالیت گره‌های شبکه را پایش می‌کند تا بتواند همواره قابلیت اعتماد به همه‌ی گره‌ها را محاسبه کند و این اطلاعات را در اختیار کسانی که به آن‌ها نیاز دارند، قرار دهد. حالت دیگر آن است که TA یک سطح اعتماد اولیه برای هر گره، در اختیار سایر گره‌ها قرار می‌دهد. سپس گره‌ها، میزان اعتماد نهایی به گره مورد نظرشان را بر اساس میزان اعتماد اولیه دریافتی از TA و اطلاعات خودشان محاسبه می‌کنند. با توجه به مقیاس شبکه می‌توان یک یا چند TA در شبکه داشته باشیم.



شکل ۱-۳: نمایش TA در مدل‌های اعتماد متمرکز

- مدل‌های مبتنی بر شهرت[۳]: این مدل‌ها از نوع توزیع شده هستند و بر خلاف مدل‌های متمرکز به هیچ زیرساختی احتیاج ندارند. فرهنگ لغت Longman، شهرت را اینگونه معنی می‌کند: نظری که مردم راجع به شخصی یا چیزی پیدا می‌کنند، بر اساس اتفاقاتی که در گذشته رخ داده است. در شبکه، هر گره شهرت گره‌های اطرافش را بر اساس اطلاعات دست اول[۴] (اطلاعاتی درباره‌ی گره‌های اطراف که بطور مستقیم و از طریق مشاهده[۵] و تجربه[۶] کسب می‌شوند) و اطلاعات دست دوم[۷] (نظر سایر گره‌ها درباره‌ی گره‌های اطراف) می‌سازد. انتظار می‌رود رفتارهای بعدی هر گره متناسب با شهرتش(شناخت قبلی از او) باشد. برای توضیح اطلاعات دست اول و دوم، شکل ۱-۴ را در نظر بگیرید:

[1] Centralized
[2] Trust Agent
[3] Reputation-based
[4] First-hand information
[5] Observation
[6] Experience
[7] Second-hand information



شکل ۱-۴: جمع آوری اطلاعات دست اول و دست دوم توسط گره‌ها

فرض کنید گره A با B ارتباط داده برقرار کرده است و بنابراین براساس تجربه، اطلاعاتی راجع به B بدست آورده است (تجربه). گره A با C و D تا کنون ارتباطی برقرار نکرده اما توسط سنسورهای خاصی، رفتار آن‌ها را زیر نظر گرفته است. مثلا برای اینکه گره A بفهمد گره C چه میزان بسته[۱] دور می‌اندازد[۲]، تعداد بسته‌های وارد شده به آن را نسبت به تعداد بسته‌های خارج شده از آن، اندازه گیری می‌کند (مشاهده).گره A نتایج تجربه‌ها و مشاهدات خود از گره‌های همسایه‌اش (گره‌هایی که در پوشش رادیویی او هستند) را در شبکه پخش[۳] می‌کند. بنابراین گره D، اطلاعاتی راجع به B و C بدست می‌آورد با اینکه همسایه او نیستند (اطلاعات دست دوم). در شبکه‌های VANET سرعت گره‌ها (خودروها) خیلی زیاد است (دریک بزرگراه ممکن است سرعت خودروها به ۱۲۰ کیلومتر در ساعت یا بیشتر نیز برسد). بنابراین توپولوژی شبکه و در واقع همسایه‌های هر خودرو مدام در حال تغییر هستند. به همین دلیل، فرصت کافی برای شناخت خودروهای همسایه و اعتماد به آنها یا داده‌های آنها بر اساس شناخت قبلی، وجود ندارد و در نتیجه به کار بردن روش‌های مبتنی بر شهرت برای شبکه‌های خودرویی کارایی لازم را ندارند.

- مدل‌های اعتماد داده-محور[۴]: این مدل‌ها نیز توزیع شده هستند و عمدتا برای تشخیص پیام‌های غلط در شبکه‌های VANET مورد استفاده قرار می‌گیرند. در سیستم‌های اعتماد مبتنی بر شهرت، براساس شناختی که از هر گره بدست می‌آید، سطح اعتماد متناسبی به آن گره اختصاص داده می‌شود و میزان اعتماد به هر پیامی، برابر با میزان اعتماد به گره یا موجودیت فرستنده‌ی آن پیام در نظر گرفته می‌شود. از این رو به آن مدل‌ها، مدل‌های موجودیت-محور نیز گفته می‌شود. در طرف مقابل، در مدل‌های داده-محور، سطح اعتماد به هر پیام، مستقل از سطح اعتماد به گره فرستنده‌اش و بر اساس پیام‌های مشابه دیگر محاسبه می‌شود. البته این ویژگی باعث می‌شود این روش‌ها در برابر حمله‌ی تبانی[۵] (چندین گره بدرفتار با همکاری یکدیگر پیام غلط مشابهی بفرستند) آسیب پذیر باشند.

---

[1] Packet
[2] Drop
[3] Broadcast
[4] Data-centric
[5] Collusion attack