بهبود امنیّت پلاتون در شبکه‌های خودرویی

تیمور درزاده[1]، نیک‌محمد بلوچزهی[2*]، احمد بختیاری‌شهری[3]
[1]دانشجوی ارشد دانشکده مهندسی برق و کامپیوتر، دانشگاه سیستان و بلوچستان
[2و3] استادیار دانشکده مهندسی برق و کامپیوتر ، دانشگاه سیستان و بلوچستان

چکیده

با رشد روزافزون خودروها و افزایش شبکه‌های حمل‌ونقل و به‌تبع آن نیاز به یک سامانه امن‌تر و کارآمدتر، به شبکه‌های خودرویی توجه شده است. در همین راستا برای مدیریت بهینه و ساده‌تر سامانه‌های حمل‌ونقل، دسته‌بندی خودروها به پلاتون پیشنهاد شده است. هرچند شبکه‌های خودرویی و پروتکل ارتباطی استاندارد IEEE 802.11p ابزار کلیدی برای توسعهٔ برنامه‌های کاربردی پلاتون هستند، اما همکاری بین خودروها در این پروتکل بر اساس یک ساختار ارتباطی قابل‌اعتماد نیست؛ و ظهور ناگهانی یک حملهٔ مخرّب می‌تواند باعث به‌خطرافتادن صحّت جریان ترافیک داده‌ها شود. هرچند برای مقابله با مشکلات مطرح‌شده الگوریتم رأی‌گیری پیشنهاد شده بود، به دلیل نیاز خودروها به دریافت اطّلاعات از دست‌کم دو خودرو جهت رأی‌گیری، در اغلب توپولوژی‌ها کارایی لازم را نداشت؛ و سبب کاهش اثر حملهٔ دست‌کاری برای خودروی قربانی نشده بود. در این پژوهش جهت رفع مشکلات الگوریتم رأی‌گیری، راه‌کار مناسبی با استفاده از تغییرات فاصلهٔ هر خودرو نسبت به خودروی رهبر و همچنین، بهترین سرعت خودروی مخرّب نسبت به سرعت رهبر پیشنهاد شده است. شبیه‌سازی راه‌کار پیشنهادی نشان می‌دهد که این پژوهش نسبت به حملات دست‌کاری در زمان ۰/۴۳ ثانیه و نسبت‌به حملات جعل پیام در زمان ۰/۴۸ ثانیه واکنش نشان می‌دهد. همچنین، مشکلات الگوریتم رأی‌گیری را برطرف کرده است.

واژگان کلیدی: پلاتون، شبکه‌های خودرویی، امنیت.

Improve the security of the platoon in vehicular networking

Teymoor Dorzadeh[1], Nik-Mohammad Balouchzahi[*2], Ahmad Bakhtiyari Shahri[3]
Author: Faculty of Electrical and Computer Engineering,
University of Sistan and Baluchestan, Zahedan, Iran[1]
Assistant Professor, Faculty of Electrical and Computer Engineering,
University of Sistan and Baluchestan, Zahedan, Iran[2,3]

Abstract

The growth of vehicles and the increase in urban traffic have been led to the need for safe, secure and efficient Intelligent Transportation Systems (ITS). Improving the efficiency of ITS needs an efficient communication system. To this end, vehicular networks have been considered as a communication infrastructure in ITS. One of the mechanisms to manage vehicles in ITS is to categorize vehicles into platoon. Platoon is proposed as a way to increase road capacity, improve safety, minimize travel time, increase fuel efficiency, reduce environmental impact, lower-traffic jams and facilitate driving. To create a platoon through autonomous cooperative driving, vehicles must be able to communicate wirelessly, which is possible through vehicular networks. Wireless communications in vehicular networks suffer from three major problems, which are: limited range of radiofrequency, high data transmission over the wireless network, as well as security problems. Using omni-directional antennas and utilizing DSRC channels in the lower layers are the base solutions to overcome these issues but,

* نویسندهٔ عهده‌دار مکاتبات
* Corresponding author

• تاریخ ارسال مقاله: ۱۳۹۹/۹/۴ • تاریخ پذیرش: ۱۴۰۰/۹/۲۹ • تاریخ انتشار: ۱۴۰۲/۰۵/۲۰ • نوع مطالعه: پژوهشی

Omnidirectional antennas spread the vulnerability to all nodes within the signal propagation range and congestion challenges in the DSRC channel intensify the collision of packets. Such issues decrease the platoon's stability and security. Recent studies on vehicular networks security have focused on presenting solutions to reduce vulnerabilities at the level of communications. However, while the security of communications has been extensively explored in previous work, the security of platoons has recently been considered by researchers. In vehicular networks, an attack can pose a threat to the security and privacy of the platoon, so the security of the platoon has received a great deal of attention.

To improve the security of the platoon, the SP-VLC solution is proposed. This method uses asymmetric encryption and the transmission of information through Visible Light Communications (VLC) to overcome security challenges .In intra-platoon attacks, the attacker is a member of the platoon and has access to all keys and encrypted information, so this solution is not effective against platoon's internal attacks .Moreover, the SP-VLC solution uses only the data flow topology of predecessor-following to transfer data. Another solution which fixes internal attack problem of SP-VLC solution is voting method. But this solution does not work well for the "predecessor-following" information flow topology because vehicles in the voting process need to receive information from at least two vehicles, while in the mentioned topology, vehicles receive information only from the vehicle in front. Therefore, the voting solution does not have the required efficiency in "predecessor-following" topology.
To overcome the challenges of the voting method, a new solution has been proposed that takes advantage of changes in the distance of each vehicle from the leader vehicle and the best speed of the malicious vehicle compared to the leader speed before the attack. Also, in order to evaluate the efficiency of the proposed solution, evaluation in Bidirectional-leader (BDL) and Predecessor-leader following (PLF) topologies has been performed as a representative of other information flow topologies. The performance of the proposed solution has been evaluated using OMNeT ++, SUMO, and PLEXE tools. To measure the efficiency of the proposed method, the parameters of position error, speed error and control effort have been used. The simulation of the proposed solution shows that this study responds to spoofing attack in 0.43 seconds and to message falsification attack in 0.48 seconds.

Keywords: platoon, vehicular networking and security

۱- مقدمه

امروزه با رشد روزافزون خودروها و افزایش سیستم‌های حمل‌ونقل در کشور، نیاز به یک سیستم حمل‌ونقل امن‌تر و کارآمدتر وجود دارد. لازمهٔ بهبود بهره‌وری و کارایی سیستم‌های حمل‌ونقل، وجود یک بستر ارتباطی کاراست. برای این منظور، شبکه‌های خودرویی به‌عنوان یکی از زیرساخت‌های ارتباطی سیستم‌های حمل‌ونقل هوشمند[۱] مورد توجه واقع شده‌اند.

از طرفی، با توجّه به‌این‌که مدیریّت سیستم‌های حمل‌ونقل یکی از مهم‌ترین عوامل در تعیین میزان مرگ و میر جاده‌ای و تولید گازهای گلخانه‌ای است، و با افزایش جمعیت و درآمد، تعداد خودروها در حال افزایش است، کنترل و مدیریّت سیستم‌های حمل‌ونقل به یک مسئلهٔ چالش‌برانگیز تبدیل شده است. بنابراین ارائهٔ یک راه‌کار مناسب جهت رفع چالش‌های حوزهٔ حمل‌ونقل از اهمیت ویژه‌ای برخوردار است. به‌علاوه، به نظر می‌رسد با فناوری‌های پیشرفته می‌توان راه‌حل‌های مطمئن و کم‌هزینه‌ای برای این حوزه پیشنهاد داد. تلاش‌های زیادی جهت بهبود کارایی سیستم‌های حمل‌ونقل، با هدف کاهش میزان آلودگی، بهره‌وری از سوخت، بهبود ایمنی، کاهش تصادفات، تسهیل رانندگی و کاهش استرس برای مسافران صورت گرفته است. سیستم‌های حمل‌ونقلی که از رانندگی مشارکتی (پلاتون[۲]) برای مدیریّت بهینه و ساده‌تر استفاده می‌کنند، نمونه‌ای از این تلاش‌ها هستند[1] . شکل (۱) پلاتونی از خودروهای متصل‌شده تحت ارتباطات کوتاه‌برد اختصاصی[۳] را نشان می‌دهد.

برای ایجاد پلاتون از طریق رانندگی مشارکتی خودکار[۴]، خودروها باید با یکدیگر ارتباط برقرار کنند و این امر از طریق شبکه‌های خودرویی امکان‌پذیر است[2] . چنین ارتباطاتی از سه مشکل عمده رنج می‌برند که عبارتند از: کمبود محدودهٔ فرکانس‌های رادیویی[۵]، ترافیک داده‌های بی-سیم که به‌سرعت در حال افزایش است، بر روی طیف فرکانس‌های رادیویی فشار ایجاد می‌کند. همچنین، مشکلات امنیّتی از دیگر موارد مطرح در این نوع ارتباطات

[۱] Intelligent Transportation Systems (ITS)

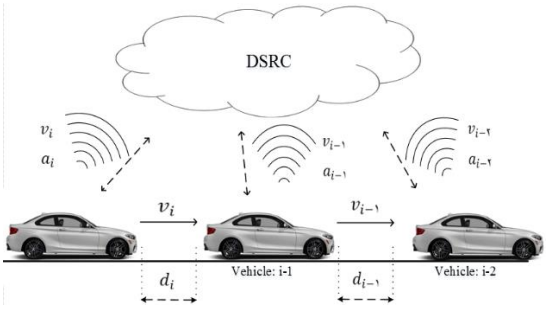
[۲] platoon

[۳] Dedicated Short-range Communications (DSRC)

[۴] Driving an autonomous cooperative

[۵] Radio-frequency (RF)

است که استفاده از آنتن‌های همه‌جهته باعث می‌شود آسیب‌پذیری این ارتباطات به تمام گره‌های فعال در محدودهٔ انتشار سرایت کند. ازدحام در کانال ارتباطات کوتاه‌برد اختصاصی باعث تشدید برخورد[1] بسته می‌شود. چنین مشکلاتی منشأ تضعیف پایداری پلاتون و کاهش ایمنی آن می‌شوند[3, 4] .



(شکل ۱): پلاتونی از خودروهای متصل شده تحت ارتباطات کوتاه برد اختصاصی

Fig1. platoon of connected vehicles under Dedicated short-range Communications

مطالعات پیشین در مورد آسیب‌پذیری‌های امنیّتی شبکه‌های خودرویی توجّه خود را بر طبقه‌بندی دقیق حملات مخرّب و راه‌حل‌هایی برای کاهش آن‌ها در سطح ارتباطات بین خودرویی متمرکز کرده‌اند[5] . با این وجود، درحالی‌که امنیّت در سطح ارتباطات در کارهای قبلی به - طور گسترده بررسی شده است، امنیّت کنترل‌کننده‌ها با توجّه به نقش کلیدی آن‌ها در مدیریّت پلاتون، به‌تازگی به‌عنوان یک المان ویژه به‌منظور افزایش سطح حفاظت از عملکرد طبیعی پلاتون، مورد توجه قرار گرفته است. از آن-جا که در شبکه‌های خودرویی یک حملهٔ سایبری می‌تواند منجر به مفهومی خطرناک برای امنیّت و حفظ حریم خصوصی برای خودروهای پلاتون شود، امنیّت یک نقطهٔ مهم در کنترل‌کننده‌های پلاتون است.

برای تأمین امنیّت در پلاتون، راه‌کار SP-VLC برای مقابله با حملات پیشنهاد داده شده است. این راه‌کار در مقابل حملات داخلی از کارایی لازم برخوردار نیست، زیرا برای مقابله با حملات از کلید مخفی با استفاده از رمزنگاری نامتقارن و انتقال اطّلاعات از طریق ارتباطات نور مرئی استفاده کرده است، که در حملات داخلی کاربر مخرّب عضوی از پلاتون است و به تمام کلیدهای مخفی و اطّلاعات رمزشده دسترسی دارد. همچنین، راه‌کار SP-VLC برای انتقال اطّلاعات فقط از توپولوژی جریان اطّلاعات هر خوردو با خودرو جلویی خودش استفاده کرده است[4] . همچنین، راه‌کار رأی‌گیری در سطح کنترل‌کننده‌ها پیشنهاد شده است، که مشکلات راه‌کار SP-VLC را برطرف کرده است. ولی راه‌کار رأی‌گیری برای توپولوژی جریان اطّلاعات «هر خودرو فقط با خودروی جلو» کارایی لازم را ندارد. علت این امر در نیاز خودروها جهت انجام رأی‌گیری به دریافت اطّلاعات از دست‌کم دو خودرو نهفته است، که در توپولوژی یادشده خودروها اطّلاعات را فقط از خودرو جلویی دریافت می‌کنند. همچنین، در راه‌کار رأی‌گیری، خودرویی که در معرض حملهٔ مستقیم دست‌کاری قرار گرفته است، اثر حمله برایش کاهش داده نشده است. بنابراین، راه‌کار رأی‌گیری از کارایی لازم برخوردار نیست[6] . در این مقاله جهت رفع مشکلات راه‌کار رأی‌گیری، راه‌کار مناسبی با استفاده از تغییرات فاصلهٔ هر خودرو نسبت به خودروی رهبر و بهترین سرعت خودروی مخرّب نسبت به سرعت رهبر قبل از حمله پیشنهاد شده است.

در ادامه، این مقاله به شرح زیر است:

در بخش دوم، کارهای پیشین ارائه می‌شود. در بخش سوم، پس از معرفی الگو سیستم و توپولوژی‌های جریان اطّلاعات مورد استفاده در پلاتون و راه‌کار پیشنهادی بیان شده است. در بخش چهارم، پس از معرّفی محیط شبیه‌سازی به توصیف سناریو و حملات در نظر گرفته‌شده در شبکه پرداخته شده است. سپس، نتایج شبیه‌سازی برای ارزیابی و تجزیه و تحلیل راه‌کار پیشنهادی در مقابل حملات مخرّب ارائه داده می‌شود. در بخش پنجم، نتیجه‌گیری و در آخر پیشنهادها و محدودیت‌های روش پیشنهادی مطرح می-شوند.

۲- پیشینهٔ پژوهش

ادبیّات مربوط به حملات سایبری به شبکه‌های خودرویی گسترده و متنوع است. در این بخش نخست، به حملات مخرّب در پلاتون پرداخته می‌شود. سپس به اقدامات متقابل در برابر حملات مخرّب در جهت تأمین امنیّت پلاتون خودرویی پرداخته می‌شود.

۲-۱-حملات مخرّب در شبکه‌های خودرویی

حملات لایهٔ کاربردی بر عملکرد درست رانندگی مشارکتی با تغییر پیام‌های ردوبدل‌شده بین خودروها برای دستیابی و حفظ حرکت مشترک تأثیر می‌گذارند. به‌طور ویژه، در یک حملهٔ دست‌کاری[1]، گره مخرّب با توجه به همسایگی ایجادشده از طریق توپولوژی استفاده‌شده در سناریو، اقدام به تغییر شاخص‌های حرکتی از قبیل شتاب و سرعت خودروی هدف می‌کند[5, 6] . درحالی‌که در یک حملهٔ

[1] Collison

جعل پیام[۲]، گره مخرّب داخلی یا خارجی برای پلاتون، شروع به گوش دادن به پیام‌های بی‌سیم ردوبدل‌شده بین خودروها کرده و پس از دریافت هر پیام، محتوای پیام را تغییر می‌دهد و در نهایت پیام‌های مخرّب را در همان لحظه دوباره پخش می‌کند. تغییر مقدار زمینهٔ پیام‌ها، بر روی اجرای راهبرد کنترل‌کننده پلاتون می‌تواند اثرات متفاوتی داشته باشد. به‌عنوان مثال، تغییر در زمینهٔ موقعیّت یک خودرو منجر به افزایش یا کاهش فاصلهٔ بین خودروها و در بدترین حالت موجب برخورد می‌شود[7] . گره مخرّب در حملات بازپخش[۳]، شروع به گوش دادن به پیام‌های بی‌سیم ارسال‌شده بین خودروها می‌کند، امّا پس از ذخیرهٔ محتوای پیام، سعی می‌کند که پیام را دوباره در زمانی دیگر ارسال کند؛ که در این حالت اثر حمله می‌تواند بسیار خطرناک باشد[3, 4, 8] . اگر یک خودرو داخلی مخرّب هویت چندین خودرو را جعل کند، پلاتون در معرض حملهٔ سیبیل[۴] است. در این حالت هویّت‌های دروغین این توهّم را ایجاد می‌کنند که خودروهای اضافی در طول جاده وجود دارند و بنابراین، می‌توانند از آن در طرّاحی هر نوع حمله‌ای در سیستم استفاده کنند[9] . پژوهش‌ها نشان داده است که رمزنگاری کلید عمومی ابزاری برای مقابله با این نوع حملات است[5] .

در حملهٔ انکار سرویس[۵]، یک گره مخرّب با استفاده از باتهای خودروها، ظرفیت ارتباطات یک خودرو یا گروهی از خودروها را تحت فشار قرار می‌دهد و با ارسال بیش از حد، خودروها را در تبادل اطّلاعات لازم برای رانندگی مشارکتی ناتوان می‌کند[10 ,6] . حملات انکار سرویس، حملاتی بسیار خطرناک تلقی می‌شوند، زیرا بر روی الگوریتم کنترل‌کننده‌ها به‌درستی اجرا شده و سبب ناپایداری جریان ترافیک و در موارد شدیدتر باعث تصادف می‌شوند. در حملهٔ انتقال‌های انفجاری[۶]، گره مخرّب سعی می‌کند جریان ترافیک داده را دست‌کاری کند تا فقط برخی از بیکن‌ها با توزیع نرخ کاهش تصادفی پراکنده شوند[6] ؛ و در یک حملهٔ استراق سمع [۷]گره مخرّب اطّلاعات ارزشمندی را در مورد خودروهای پلاتون استخراج و از آن‌ها برای منافع خود استفاده می‌کند. در حملهٔ پارازیت[۸]، گره مخرّب یک وقفهٔ زمانی که یک اختلال در ارتباط عمدی بین اعضای پلاتون است، ایجاد می‌کند. علاوه‌بر این، حمله بدافزار[۹] باعث اختلال جدی در عملیات شبکه‌های خودرویی می‌شود. این حمله به‌طور معمول توسط گره‌های مخرّب داخلی و در زمان به‌روزرسانی‌های نرم‌افزاری سنسورهای داخلی خودروها و واحدهای کنار جاده‌ای انجام می‌شود[4, 9] . در حملهٔ سیاه‌چاله[۱۰] یک خودرو مخرّب اعلام می‌کند که کوتاه‌ترین مسیر برای به دست آوردن داده‌ها را دارد و سپس خودروهای دیگر را مسیریابی و هدایت می‌کند. بنابراین، گره مخرّب قادر به جدا کردن بستهٔ داده یا حفظ آن است. هنگامی‌که مسیر جعلی با موفقیّت برقرار شد، خودرو مخرّب می‌تواند بسته را رها، یا به جلو هدایت کند. راه‌حل‌های موجود برای مقابله با این حمله، طراحی پروتکل‌هایی است که بیش از یک مسیر برای مقصد در نظر می‌گیرند؛ هرچند پردازش و بار اضافه‌ای را به شبکه تحمیل می‌کنند[11] . حمله کرم چاله[۱۱] یک حملهٔ سیاه‌چالهٔ شدید است که در آن دو یا چند خودرو مخرّب تونلی را برای انتقال بسته‌های داده از انتهای شبکه به سمت خودرو مخرّب در انتهای دیگر ایجاد می‌کنند. با این روش، بسته‌ها در شبکه پخش شده و خودروهای مخرّب کنترل چندین اتصال یا پیوند کوتاه شبکه را بر عهده می‌گیرند. یکی از شناخته‌شده‌ترین رویکردها برای جلوگیری از حملات کرم چاله، دستهٔ سه‌تایی بسته است[5] . حملهٔ خطرناک دیگر، که به بیزانس[۱۲] معروف است[12] ، با ایجاد حلقه‌های مسیریابی و سپس هدایت بسته‌های داده از طریق مسیرهای غیربهینه، یک خودرو یا گروهی از خودروها را به خطر می‌اندازد؛ و سبب تخریب یا اختلال در خدمات مسیریابی می‌شود [12]. برای مقابله با این حمله، پروتکل مسیریابی منبع قوی[۱۳] معرفی شده است. یکی از ویژگی‌های این پروتکل امکان ارسال بسته‌ها به مقصد مربوط، حتی در شرایط خصمانهٔ حمله بیزانس است[13] .

حملات مخرّب می‌توانند در سطح سیستم نیز اتفاق بیفتند. این نوع از حملات با دست‌کاری سخت افزار یا نرم افزار خودرو انجام می‌شوند که می‌توانند توسط مخرّب

[۱] Spoofing
[۲] Message Falsification
[۳] Replay
[۴] Sybil
[۵] Denial of Service
[۶] Burst Transmission
[۷] Eavesdropping
[۸] Jamming
[۹] Malware
[۱۰] Black Hole
[۱۱] Wormhole
[۱۲] Byzantine
[۱۳] Robust Source Routing

خودی در سطح تولید و یا توسط مخرّب خارجی در یک خودرو بدون نظارت (به‌عنوان مثال با جایگزینی یا تغییر سنسورهای خاص خودرو) انجام شوند. در همهٔ این موارد، اگر سخت‌افزار یا نرم‌افزار سنسورهای داخلی استفاده شود یا معیوب باشد، اطّلاعات ورودی به سیستم دقیق نیستند، حتی اگر کانال ارتباطی ایمن، یا یک معماری به‌روز در شبکه‌های خودرویی پیاده‌سازی شده باشد. این بی‌دقّتی می‌تواند بر عملکرد پروتکل‌های سطح بالا تأثیر جدی بگذارد. از این رو نباید خطر دست‌کاری را نادیده گرفت. یکی از محبوب‌ترین روش‌ها برای مقابله با این نوع حملات استفاده از سنسورهای ضد دست‌کاری[1] است [11]. مطالعات نشان داده است در میان حملات سطح سیستم، حملات توهّم[2] می‌تواند خطرناک‌تر از دیگر حملات باشند. زیرا گره مخرّب به‌طور هدفمند، سنسورهای خودرو را فریب داده تا سنسورها اطّلاعات نادرستی تولید کنند. این امر باعث می‌شود پیام‌های هشدار نادرست در مورد ترافیک به همسایگان ارسال شوند. از این رو، نفوذ اطّلاعات از یک سنسور کلابردار که یک گره مخرّب داخلی است، می‌تواند موقعیّت، سرعت و جهت‌گیری خودروهای دیگر را تغییر داده و بدین ترتیب باعث بروز حادثه شود[14] .

۲-۲- اقدامات متقابل برای حملات مخرّب در پلاتون

در سال ۲۰۱۸، سیهان اوکار و همکاران [4] یک پروتکل امنیّتی ترکیبی را مبتنی بر IEEE 802.11p و VLC[3] به اسم SP-VLC با هدف اطمینان از پایداری پلاتون و ایجاد مانورهای پلاتون تحت تزریق بسته‌های داده، گوش دادن به کانال، حملات پارازیت و حملات به مانورهای پلاتون پیشنهاد کردند. این پروتکل، از VLC برای کلید مخفی و تبادل اطّلاعات با بهره‌گیری از جهت‌گیری و نفوذناپذیری نور برای مقابله با حملات استفاده می‌کند، با این وجود استفادهٔ تنها از VLC در پلاتون خودرویی، می‌تواند پایداری پلاتون را از بین ببرد. زیرا در هنگام مواجهه با اثرات محیطی مانند مه، از بین رفتن خط دید در یک جاده انحنادار، و افزایش فاصله بین‌خودرویی، خودروها توانایی دسترسی به همدیگر توسط VLC را نخواهند داشت. بنابراین، IEEE 802.11p همچنین، در انتقال‌های پلاتون استفاده شده است تا قابلیت اطمینان بهتر را فراهم کند. در سال ۲۰۱۸، *پتریلو* و همکاران [6] پایداری پلاتون و ردیابی رهبر را در مقابل حملات لایهٔ کاربردی (از قبیل دستکاری و جعل پیام) و حملات لایهٔ شبکه (از قبیل انکار سرویس و انتقال‌های انفجاری) با توپولوژی‌های مختلف جریان اطّلاعات بررسی و ارزیابی کردند. برای مقابله با این نوع حملات، استفاده از سازوکار رأی‌گیری را پیشنهاد کردند. در این سازوکار، پلاتون قادر خواهد بود تا در برابر یک رفتار مخرّب، پایداری خود را حفظ کرده، سرعت رهبر را به‌درستی ردیابی کند. در سال ۲۰۱۸، جهانشاهی و همکاران [15] یک مشاهده‌گر حالت لغزشی سازگار برای یک رشته مجهّز به کنترل کروز سازگار مشارکتی از خودروها، تحت یک کلاس از حملات مؤثّر بر شبکهٔ ارتباطی V2V پیشنهاد دادند. هر خودرو به یک مشاهده‌گر حالت لغزشی سازگار مجهز شده است که موقعیّت طولی، سرعت و شتاب خودرو جلویی را تخمین می‌زند. چنین مشاهده‌گری این امکان را فراهم می‌کند تا حملاتی را که می‌خواهند داده‌های منتقل‌شده توسط خودرو قبلی را تغییر دهند، شناسایی کند.

در سال ۲۰۱۸، *بوئیرا* و همکاران [16] طرح اثبات موقعیّت مکانی را برای کاهش حملات جعل موقعیّت پیشنهاد دادند. طرح موقعیّت مکانی با کمک سازوکارهای رمزنگاری برای مقابله با تأثیر مخالف تحرک بالا در سرویس‌های موقعیّت به خودروها این امکان را می‌دهد تا حملات جعل موقعیّت را با سربار کم و کارایی مناسب تشخیص دهند. در سال ۲۰۱۸، *موسوی‌نژاد* و همکاران [17] برای تشخیص حملات سایبر به سیستم‌های کنترل شبکهٔ خودرویی مبتنی بر پلاتون، الگوریتمی با استفاده از روش‌های فیلتر عضویت در مجموعه بیضی شامل دو مجموعه بیضوی پیش‌بینی و بیضوی تخمین که از طریق به‌روزرسانی مجموعهٔ بیضوی پیش‌بینی با داده‌های اندازه‌گیری محاسبه می‌شود، پیشنهاد دادند. برای شناسایی حملات اگر هیچ تقاطعی بین مجموعه بیضی پیش‌بینی و مجموعهٔ تخمین‌زده‌شده توسط خروجی اندازه‌گیری قبلی وجود نداشته باشد، سیگنال کنترل‌کننده با حملات به خطر افتاده است. در سال ۲۰۱۸، *مرکو* و همکاران [18] در مورد تشخیص حملهٔ بازپخش در یک سیستم خودرویی متصل تحت کنترل کروز، یک الگوریتم تشخیص غیرمتمرکز بر اساس روش سیگنال کنترل نوفه[4] و cross-correlator پیشنهاد دادند.

خلاصه‌ای از کارها و مطالعات بررسی‌شده در این بخش در مورد اقدامات متقابل برای حملات مخرّب در پلاتون خودرویی در جدول (۱) بیان شده است.

[1] tamper-proof

[2] illusion

[3] Visible Light Communication (VLC)

[4] Noisy

(جدول ۱): بررسی مطالعات گذشته

Table1: Review of Previous Studies

راه‌کار	هدف	حملات								روش حل
		سایبر	جعل پیام	جعل هویت	پارازیت	دست‌کاری	انکار سرویس	انتقال‌های انفجاری	بازپخش	
[4]	اطمینان از پایداری و ایجاد مانورهای امن	✗	✓	✓	✓	✗	✗	✗	✓	الگوریتم ترکیبی IEEE 802.11p و VLC
[6]	پایداری و ردیابی سرعت رهبر	✗	✓	✗	✓	✓	✓	✓	✗	الگوریتم رأی‌گیری
[15]	تشخیص و تخمین حملات	✓	✗	✗	✗	✗	✗	✗	✗	مشاهده‌گر حالت لغزشی سازگار
[16]	کاهش حملات	✗	✓	✗	✗	✗	✗	✗	✗	طرح اثبات موقعیّت $Vouch$
[17]	تخمین حملات	✓	✗	✗	✗	✗	✗	✗	✗	فیلتر عضویت در مجموعهٔ بیضوی
[18]	تشخیص حملات	✗	✗	✗	✗	✗	✗	✗	✓	الگوریتم تشخیص غیرمتمرکز بر اساس روش سیگنال کنترل نوفه و cross-correlator

۳ – راه‌کار پیشنهادی برای بهبود امنیّت پلاتون

۳-۱- الگوی سیستم

یک پلاتون شامل مجموعه‌ای از $N+1$ خودرو که از ۰ تا N شماره‌گذاری شده‌اند، در نظر گرفته می‌شود و در آن خودرو شماره صفر رهبر فرض می‌شود. در این مقاله فرض بر این است که پلاتون شکل گرفته است. کلیهٔ خودروها در یک خط مستقیم و با شروع از فاصله‌های متفاوت از همدیگر و بر اساس سیاست فاصلهٔ لحاظ‌شده در پلاتون، حرکت می‌کنند. همچنین، ترتیب تردّد خودروها تغییر نمی‌کند و تمامی خودروها دارای خواص فیزیکی، مکانیکی و قابلیت‌های ارتباطی یکسانی هستند. احتمال آسیب‌پذیری تمامی خودروها در برابر حملات وجود دارد که ممکن است منجر به بروز رفتارهای غیر عادی شود [6].

همچنین، در این مقاله فرض می‌شود که هر خودرو درون پلاتون به GPS[۱] و سنسورهای محلی ساخته‌شده مانند: انکودر (ارائه اطّلاعات سرعت طولی) و واحد اندازه‌گیری درونی[۲] (ارائه اطّلاعات شتاب طولی) مجهز است. علاوه‌بر آن مجهز به سخت‌افزار ارتباطی جهت استفاده در محیط‌های با تحرک بالا (IEEE 802.11p) جهت اشتراک‌گذاری اطّلاعات محلی با همسایگان و دریافت سیگنال‌های مرجع از گره رهبر است [19].

[۱] Global Positioning System

[۲] Inertial Measurement Unit (IMU)

۳-۲- توپولوژی‌های جریان اطّلاعات[۱] مورد استفاده در پلاتون

توپولوژهای جریان اطّلاعات مشخص می‌کند که هر خودرو مجاز به دریافت اطّلاعات از کدام خودروهای درون مجموعهٔ پلاتون است. خودروهای درون پلاتون با دریافت جریان‌های اطّلاعاتی از دیگر خودروهای درون پلاتون، اطّلاعات تحرک را به‌روزرسانی می‌کنند که تأثیر مستقیمی بر رفتار جریان پلاتون می‌گذارند. توپولوژهای جریان اطّلاعاتی که در یک پلاتون استفاده می‌شوند، از توزیع تصادفی خاصی پیروی نمی‌کنند. همچنین، وجود بستر ارتباطی بین گره‌های درون پلاتون (در برد هم بودن گره‌ها)، الزامی در دریافت اطّلاعات توسط گره‌ها ایجاد نمی‌کند، بلکه توپولوژی جریان اطّلاعات مشخص‌کنندهٔ چگونگی تبادل اطّلاعات است [20, 21].

از رایج‌ترین توپولوژی‌های جریان اطّلاعات موردتوجه در پلاتون می‌توان به توپولوژی‌های زیر اشاره کرد:

- ارتباط هر خودرو فقط با خودرو جلویی[۲]
- ارتباط هر خودرو با خودرو جلویی و خودرو رهبر[۳]
- ارتباط هر خودرو با خودرو جلویی و عقبی (دو طرفه)[۴]
- ارتباط هر خودرو با خودرو جلویی و عقبی (دو طرفه) و رهبر[۵]
- ارتباط هر خودرو با دو تا از خودروهای جلویی[۶]
- ارتباط هر خودرو با دو خودروی جلویی و رهبر[۷]

که در [20, 21] جزئیّات توپولوژی‌های جریان اطّلاعات برای خودروهای پلاتون مشابه شکل (۲) نشان داده شده است.

۳-۳- راه‌کار پیشنهادی برای مقابله با رفتارهای مخرّب

مطالعات پیشین در مورد آسیب‌پذیری‌های امنیّتی شبکه‌های خودرویی توجّه خود را بر دسته‌بندی دقیق حملات مخرّب و راه‌حل‌هایی برای کاهش آن‌ها در سطح ارتباطات بین خودرویی تمرکز کرده‌اند [5]. با این وجود، در حالی که امنیّت در سطح ارتباطات در کارهای قبلی به‌طورگسترده بررسی شده است، به امنیّت کنترل‌کننده‌ها با توجه به نقش کلیدی آن‌ها در مدیریّت پلاتون، به‌تازگی به‌عنوان یک المان ویژه به‌منظور افزایش سطح حفاظت از عملکرد طبیعی پلاتون، توجّه شده است.

برای طراحی کنترل‌کننده‌ها، اطّلاعات می‌تواند بر اساس توپولوژی‌های جریان اطّلاعات مختلف جریان یابند. اگرچه تمام خودروها در امتداد یک خط حرکت می‌کنند (تشکیل پلاتون)، توپولوژی‌های جریان اطّلاعات مختلف ممکن است در فضای سایبر فیزیکی به وجود آیند. عملکرد کنترل‌کننده‌ها به انعطاف‌پذیری توپولوژی‌های جریان اطّلاعات بستگی دارد، یعنی توانایی کنترل‌کننده‌ها برای مقابله با حملات ارتباط نزدیکی با انواع توپولوژی جریان اطّلاعات. در [6] پتریلو و همکارانش مانور پایداری پلاتون در مقابل حملات لایه کاربردی (از قبیل دست‌کاری و جعل پیام) و حملات لایهٔ شبکه (از قبیل انکار خدمات و انتقال‌های انفجاری) را در حضور توپولوژی‌های مختلف جریان اطّلاعات مورد بررسی و ارزیابی کردند. برای مقابله با این نوع حملات در راه‌کار پیشنهادشده از سازوکار رأی‌گیری استفاده شده است که در این صورت پلاتون قادر خواهد بود در برابر یک رفتار مخرّب، پایداری خود را حفظ کند. با وجود عملکرد مناسب سازوکار رأی‌گیری در اغلب توپولوژی‌ها، این راه‌کار برای توپولوژی جریان اطّلاعات «هر خودرو فقط با خودرو جلو» از کارایی لازم برخوردار نیست. علت این امر در نیاز خودروها جهت انجام رأی‌گیری به دریافت اطّلاعات از دست‌کم دو خودرو نهفته است که در توپولوژی ذکرشده خودروها اطّلاعات را فقط از خودرو جلویی دریافت می‌کنند. همچنین، در راه‌کار ارائه‌شده خودرویی که در معرض حمله دست‌کاری قرار گرفته شده باشد، اثر حمله برای آن کاهش داده نشده است، بنابراین، سازوکار رأی‌گیری از کارایی لازم برخوردار نیست. در این مقاله جهت رفع مشکل توپولوژی هرخودرو فقط با خودرو جلویی در مقابل حملات لایهٔ کاربردی و خودرویی که در معرض حمله مستقیم دست‌کاری قرار گرفته، راه‌کار مناسبی پیشنهاد شده است. همچنین، جهت بررسی صحت راه‌کار پیشنهادی، ارزیابی در توپولوژی BDL نیز به‌عنوان نماینده‌ای از دیگر توپولوژی‌های جریان اطّلاعات، انجام شده است.

جهت ارائهٔ الگوریتم پیشنهادشده در این مقاله به‌منظور تثبیت پایداری پلاتون تحت توپولوژی‌های مختلف جریان اطّلاعات، ساختار ارتباطی شبکه با یک گراف جهت‌دار که هر خودرو در آن یک گره از گراف فرض شده است، الگو می‌شود. برای این منظور، یک شبکه از N خودرو به‌عنوان یک گراف جهت‌دار $G = (V.E.A)$ که توسّط مجموعه‌ای از گره‌ها $V = \{1.\cdots.N\}$ و مجموعه‌ای از لبه‌ها

[۱] Information Flow Topologies (IFT)

[۲] Predecessor Following (PF)

[۳] Predecessor-leader following (PLF)

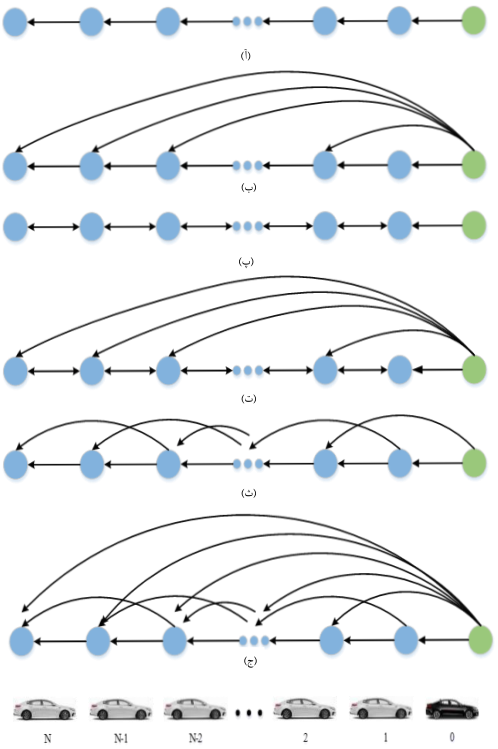
[۴] Bidirectional (BD)

[۵] Bidirectional-leader (BDL)

[۶] Two-predecessors following (TPF)

[۷] Two-predecessor-leader following (TPLF)

$E \subseteq V \times V$ تشکیل شده است، فرض می‌شود. توپولوژی گراف به یک ماتریس مجاورتی با عناصر غیرمنفی به‌صورت $A = [a_{i.j}]_{N\times N}$ نمایش داده می‌شود. در ادامه، چنانچه پیوند ارتباطی جهت ارسال اطّلاعات از خودرو j به خودرو i وجود داشته باشد، $a_{i.j} = 1$ و در غیر این‌صورت $a_{i.j} = 0$ فرض می‌شود. علاوه‌بر این، $a_{i.i} = 0$ است. حضور لبه $(i.j) \in E$ به این معنی است که خودرو i می‌تواند اطّلاعات را از خودرو j به‌دست آورد و لزوماً برعکس آن صادق نیست.



(شکل ۲): نمونه توپولوژی‌های ارتباطی پلاتون:
(آ): PF ؛ (ب): PLF ؛ (پ): BD ؛ (ت): BDL ؛ (ث): TPF ؛ (ج): TPLF ؛ [20, 21]

Fig2. Examples of Platoon communication topologies: (a): PF; (b): PLF; (c): BD; (d): BDL; (e): TPF; (f): TPLF[20, 21]

در بقیهٔ مقاله N خودرو با یک عامل رهبر به‌عنوان پلاتون در نظر گرفته می‌شوند، و از گراف جهت‌دار پیشرفته G_{N+1} برای الگوسازی توپولوژی شبکهٔ پلاتون به‌دست‌آمده استفاده می‌شود [6].

باتوجه‌به‌این‌که خودروها در یک محیط ارتباطی بی-سیم غیرایده‌ال حرکت می‌کنند، اطّلاعات می‌تواند توسط هر خودرو با تأخیرهای متفاوت زمانی دریافت شود، مقدار تأخیرهای متغیّر زمان بستگی به شرایط واقعی شبکه از قبیل ازدحام دارد [22, 23]. از این‌رو در واقعیّت اختلالات ارتباطی ناشی از تأخیر اجتناب‌ناپذیر است، بنابراین، ورودی کنترل‌کننده که بر اساس اطّلاعات قدیمی محاسبه می‌شود، تحت تأثیر تأخیرهای متغیّر زمان قرار می‌گیرد [24].

هدف از کنترل پلاتون تنظیم سرعت و فاصلهٔ نسبی هر خودرو با خودروهای مجاور و خودرو رهبر با توجه به توپولوژی جریان اطّلاعات در حضور گره‌های مخرّب است [6, 25]. از این‌رو، یک پلاتون از مجموعه‌ای شامل N خودرو به همراه خودرو رهبر به‌عنوان گره مرجع تشکیل می‌شود.

پویایی خودرو iام می‌تواند به‌عنوان عامل درونی در پلاتون به صورت زیر توصیف شود $(i = 1, \cdots, N)$ [6]:

$$\dot{r}_i(t) = v_i(t)$$
$$\dot{v}_i(t) = \frac{1}{M_i} u_i(t) \qquad (۱)$$

که r_i بر حسب متر و v_i بر حسب متر بر ثانیه موقعیّت مطلق خودرو iام (با توجه به چارچوب مرجع مشخص) و سرعت خودرو iام هستند؛ M_i جرم خودرو iام است و نیروی محرّکه u_i ورودی کنترل را نشان می‌دهد، که به‌طور مناسب برای دستیابی به هدف کنترل انتخاب می-شود.

به‌طور مشابه پویایی خودرو رهبر به صورت زیر است:

$$\dot{r}_0(t) = v_0$$
$$\dot{v}_0 = 0 \qquad (۲)$$

متغیّرهای حالت رهبر r_0 و v_0 هستند. با توجه به رابطه‌های (۱) و (۲) ، مسألهٔ حفظ یک سیاست فاصله بین خودرویی مطلوب و یک سرعت ثابت مشترک (همان‌طورکه توسط رهبر تحمیل شده است) می‌توانند به‌عنوان روابط زیر بازنویسی شوند:

$$r_i(t) \leftarrow \frac{1}{\Delta_i}\left\{\sum_{j=0}^{i} \alpha_{ij}\cdot\left(r_j(t) - s_{ij}\right) + \sum_{j=i+1}^{N} \alpha_{ij}\cdot\left(r_j(t) + s_{ij}\right)\right\}$$
$$v_i(t) \leftarrow v_0 \qquad (۳)$$

که s_{ij} فاصله بین خودروهای i و j است؛ با توجه به [6] فاصلهٔ مطلوب s_{ij} به صورت $s_{ij} = h_{ij}v_0 + s_{ij}^{st}$ بیان می‌شود، جایی که h_{ij} زمان پیشروی و s_{ij}^{st} فاصلهٔ بین خودرو i و j در حالت توقّف است؛ a_{ij} (برای $i = 1, \cdots, N$ و $j = 0, \cdots, N$) الگوهایی از توپولوژی‌های جریان اطّلاعاتی پلاتون از حضور یا عدم حضور یک پیوند ارتباطی بین خودروهای i و j است. در ادامه نیز چنین فرض می‌شود که $a_{0j} = 0$ به‌ازای تمام مقادیر $j = 0, \cdots, N$ است؛ زیرا رهبر داده‌ها را از هیچ خودروی دیگری در نظر نمی‌گیرد. $\Delta_i = \sum_{j=0}^{N} a_{ij}$ درجه خودرو i یعنی تعداد خودروهایی که با خودرو i یک پیوند ارتباطی ایجاد کرده‌اند.

مسئلهٔ حفظ یک سیاست فاصله بین خودرویی

مطلوب و یک سرعت ثابت مشترک که در رابطهٔ (۳) آمده‌اند، با استفاده از دو رابطهٔ زیر حل می‌شوند:

$$u_i(t) = -b[v_i(t) - v_0] - \frac{1}{\Delta_i}\sum_{j=0}^{N} k_{ij} * a_{ij} * y_{ij}(t)$$
$$v_i(t) = AvgSpeed \qquad (۴)$$
$$y_{ij}(t) = \left[r_i(t) - r_j\left(t - \tau_{ij}(t)\right) - s_{ij} - \text{که} \right.$$
$$\left. \tau_{ij}(t)v_0\right]$$

فاصله بین خودرویی واقعی بین خودروi و خودروj است ؛ K_{ij} و b از متغیّرهای کنترلی هستند که باید به‌طور احتمالی تنظیم شوند تا بتوانند رفتار متقابل بین خودروهای همسایه را تنظیم کنند؛ $\tau_{ij}(t)$ تأخیرهای متغیّر زمانی هستند که بر روی خودروiام زمانی که اطّلاعات از همسایه jام منتقل می‌شود، تأثیر می‌گذارند. تأخیرهای $\tau_{ij}(t)$ محدود شده است [26, 27, 28] و قابل تشخیص از طریق مهر زمان‌سنج در اطّلاعات منتقل شده است [26, 29]. r_i موقعیّت خودرو i و r_j موقعیّت خودروهای ارتباطی با خودروi طبق توپولوژی جریان اطّلاعات هستند. علاوه‌بر این $AvgSpeed$ میانگین سرعت خودروهای ارتباطی با خودروi است و به صورت زیر بیان می‌شود:

$$AvgSpeed = \frac{1}{\Delta_i} * \{\sum_{j=0.Malicious\ [j]\neq 1}^{N} a_{ij} * v_j(t) + \sum_{j=0.Malicious[j]=1}^{N} a_{ij} * BestSpeed[j]\} \qquad (۵)$$

که $BestSpeed$ آرایه‌ای به اندازهٔ تعداد خودروها است، و در آن بهترین سرعت هر خودرو ذخیره می‌شود، مقدار اولیهٔ آن برای تمام خودروها ۱۰۰ متر بر ثانیه است و برای به‌روزرسانی آن هر بار اختلاف سرعت واقعی خودروj با v_0 را به دست آورده و با اختلاف بهترین سرعت پیشین خودروj($BestSpeed[j]$) با v_0 مقایسه می‌شود. اگر اختلاف سرعت واقعی با v_0 کمتر باشد، (یعنی سرعت واقعی به سرعت v_0 نزدیک‌تر باشد)، آن را به‌عنوان $BestSpeed$ در نظر می‌گیرد.

علاوه بر این، $Malicious$ آرایه‌ای برای شناسایی خودروهای مخرّب به اندازهٔ تعداد خودروها است که مقدار اولیهٔ آن برای تمام خودروها صفر است و هرگاه خودرویی مخرّب باشد، مقدار خانهٔ مربوط به آن خودرو در آرایه $Malicious$ یک می‌شود، یعنی آن خودرو به‌عنوان مخرّب شناسایی می‌شود.

برای شناسایی حملات از روابط زیر استفاده می‌شود:

$$d_{i0}(t) = [r_0(t) - r_i(t)]$$
$$d_{i0}^{st} = i * (s_{i,i-1}^{st} + l) \qquad (۶)$$

که d_{i0} فاصلهٔ واقعی بین خودروi و خودرو رهبر است؛ r_0 و r_i موقعیّت واقعی خودرو رهبر و خودروi هستند؛ d_{i0}^{st} فاصلهٔ بین خودروiام و رهبر در حالت توقّف است، $s_{i,i-1}^{st}$ فاصلهٔ بین خودرو i و $i-1$ در حالت توقّف است؛ و همچنین، l طول خودرو است. اگر اختلاف بین d_{i0} و d_{i0}^{st} بیشتر از آستانهٔ δ_1 باشد، یک حمله امنیّتی در کانال ارتباطی رخ داده است. برای شناسایی خودرو مخرّب سرعت هر خودرویی که بر اساس توپولوژی جریان اطّلاعات پیوند ارتباطی با خودروi دارد، اختلافش با v_0 به دست می‌آید، و اگر اختلاف سرعت هرکدام از آن‌ها بیشتر از آستانه δ_2 باشد، آن خودرو به‌عنوان مخرّب شناسایی می‌شود. اگر هیچ‌کدام از خودروهای ارتباطی مخرّب نباشند، اختلاف سرعت خودروi با سرعت v_0 به دست می‌آید. اگر مقدار اختلاف از آستانه δ_2 بیشتر باشد، خودروi تحت حملهٔ مستقیم قرار گرفته است. بر این اساس آرایهٔ $Malicious$ به‌روزرسانی می‌شود. در آخر اگر خودرو مخرّبی وجود داشته باشد، یا خود خودروi تحت حملهٔ مستقیم قرار گرفته باشد، از میانگین سرعت خودروهای ارتباطی با خودروi برای به‌روزرسانی سرعتش استفاده می‌شود، درغیراین‌صورت از سرعت واقعی خود خودروi و میانگین فاصلهٔ واقعی خودروهای ارتباطی با خودروi استفاده می‌شود. این روش برای همه خودروهای موجود در پلاتون به‌جز رهبر در هر مرحله تکرار می‌شود.

یک مرور کلی از راه‌کار پیشنهادی در شکل (۳) گزارش شده است. توجه داشته باشید که اطّلاعات دریافت‌شده توسط خودرو رهبر و تمام اطّلاعات منتقل‌شده توسط دیگر خودروها در داخل پلاتون می‌توانند به خطر بیفتند.

۴- نتایج ارزیابی و شبیه‌سازی راه‌کار پیشنهادی

در این بخش راه‌کار پیشنهادی با استفاده از ابزارهای OMNeT++، SUMO و PLEXE ارزیابی شده است. جهت اندازه‌گیری کارایی روش ارائه‌شده، از شاخص‌های خطای موقعیّت، خطای سرعت و تغییرات شتاب استفاده شده است. در ادامه، سناریوی شبکه و ترافیک تشریح شده و بعد از آن سناریوهای حمله توضیح داده خواهند شد. در نهایت، سناریوهای مختلف حمله به کمک ابزارهای شبیه‌سازی ارزیابی می‌شوند.

۴-۱- محیط شبیه‌سازی

به‌منظور ارزیابی ایمنی و امنیّت سیستم کنترل کروز سازگار مشارکتی، از پلتفرم PLEXE[30] تحت ابزار شبیه-

سازی OMNeT++ استفاده شده است. پلتفرم PLEXE یک افزونهٔ منبع باز است که به‌طور گسترده با افزودن قابلیت‌ها و کنترل‌های پلاتون در چارچوب رابط Veins توسعه داده شده است [31]. رابط Veins، امکان تعامل شبیه‌ساز شبکهٔ OMNeT++[32] و شبیه‌ساز ترافیک جاده SUMO[33] را فراهم می‌کند. پلتفرم PLEXE با ایجاد یک گره شبکه در شبیه‌ساز OMNeT++ به‌ازای هر خودرو که در SUMO تحرّک دارد، امکان تعامل را بر بستری مشابه رابط Veins فراهم می‌کند. این پلتفرم یک سیستم ارتباطی خودرویی مبتنی بر پروتکل IEEE 802.11p و یک الگوی تحرک واقع-گرایانه مبتنی بر SUMO را ایجاد می‌کند. هنگامی‌که یک خودرو حرکت می‌کند، پلتفرم PLEXE امکان دست‌یابی به اطلاعات حرکتی موجود SUMO را در OMNeT++ به کمک رابط Veins فراهم می‌کند. شبیه‌سازی رفتار گره‌های شبکه در ابزار شبیه‌سازی OMNeT++ و به کمک پروتکل-های موجود صورت می‌پذیرد، در حالی که SUMO تحرک گره‌ها و رفتار حرکتی آن‌ها در محیط جاده را شبیه‌سازی می‌کند. شکل (۴) نمای کلی چارچوب شبیه‌سازی به کمک ابزارهای ذکرشده را در این مقاله نشان می‌دهد.

جهت فراهم نمودن تحرّک خودروها، در پلتفرم PLEXE رده‌ای به نام BaseApp طرّاحی شده است که داده‌های مرتبط با پلاتون را از بسته‌های دریافت‌شده از لایهٔ شبکه یا پیوند داده استخراج می‌کند و اگر چنین داده‌هایی از خودرو رهبر یا خودرو پیرو باشند، داده‌های استفاده‌شده در کنترل کروز سازگار مشارکتی را از طریق رابط TraCI به‌روز می‌کند. ردهٔ SimplePlatooningApp با ارث‌بری از ردهٔ BaseApp سبب توسعهٔ رفتارهای خودرو در مجموعهٔ پلاتون می‌شود. ردهٔ BaseApp در ابزار موجود بوده است، که در این مقاله توسعه داده شده است.

Input Data: $v_0, r_j(t)$ and $\tau_{ij}(t)$ $(\forall\, j = 0,1,\cdots,N)$
Result: The Platoon Control
Declarations:

$$y_{ij}(t) = \left[r_i(t) - r_j\left(t - \tau_{ij}(t)\right) - s_{ij} - \tau_{ij}(t)v_0\right]; d_{i0}(t) = [r_0(t) - r_i(t)];$$

Initialization:

$$d_{i0}^{st} = i * \left(\, s_{i,i-1}^{st} + l\,\right);\ s_{ij} = h_{ij}v_0 + s_{ij}^{st}; \Delta_i = \sum_{j=0}^{N} a_{ij};\ \delta_1 = 3;\ \delta_2 = 0.01;$$

$$BestSpeed[j] = 100\ and\ Malicious[j]\ = 0\ for(\forall j = 0,1,\cdots,N);$$

for $j = 0$ ***to*** N ***do***
  if $a_{ij} == 1$ && $|v_j(t) - v_0| < |BestSpeed[j] - v_0|$ ***then*** $BestSpeed[j] = v_j(t)$;
if *All vehicles achieve the optimum distance policy and fixed speed common* ***then***
  if $|d_{i0} - d_{i0}^{st}| > \delta_1$ ***then***
    $flag = false$;
    for $j = 0$ ***to*** N ***do***
      if $a_{ij} == 1$ && $|v_j(t) - v_0| > \delta_2$ ***then***
        $Malicious\ [j] = 1$;
        $flag = true$;
      end
    end
    if $|v_i(t) - v_0| > \delta_2$ && $!flag$ ***then*** $Malicious\ [i] = 1$;
  end
end

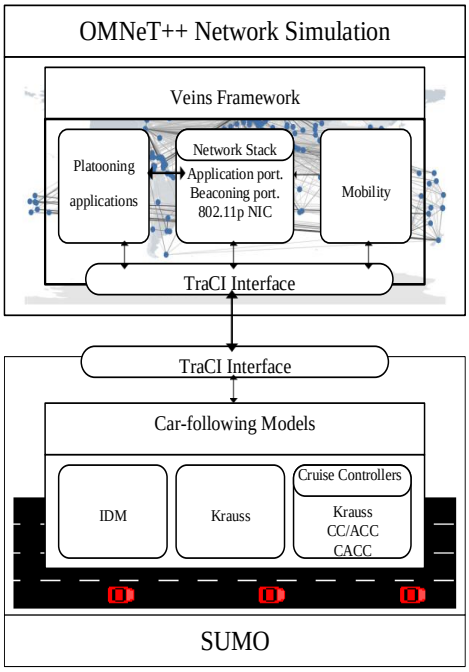
$$AvgSpeed = \frac{1}{\Delta_i} * \left\{ \sum_{j=0, Malicious\ [j] \neq 1}^{N} a_{ij} * v_j(t) \quad + \sum_{j=0, Malicious[j]=1}^{N} a_{ij} * BestSpeed[j] \right\};$$

if $\exists\exists_j: Malicious[j] = 1$ ***then*** $v_i(t) = AvgSpeed$;
else

$$u_i(t) = -b[v_i(t) - v_0] - \frac{1}{\Delta_i}\sum_{j=0}^{N} k_{ij} * a_{ij} * y_{ij}(t);$$

(شکل ۳): شبه‌رمز راه‌کار پیشنهادی برای خودروiام

Fig3. pseudo-code Suggested solution for the ith vehicle



(شکل ۴): ساختار نمادین شبیه‌سازی [30]

Fig4. Schematic structure of the simulator [30]

۴-۲- سناریوی شبکه و ترافیک

برای نشان‌دادن اثربخشی راه‌کار پیشنهادی جهت استفاده در رانندگی مبتنی بر کنترل کروز سازگار مشارکتی در حضور حملات مخرّب، یک آزادراه به‌طول ۱۰ کیلومتر حاوی یک پلاتون با هفت خودرو به‌علاوهٔ رهبر در نظر گرفته شده است که از طریق پروتکل پیوند دادهٔ IEEE 802.11p با هم در ارتباط هستند و در طول آزادراه و در یک خط(لاین) حرکت می‌کنند. برای نشان دادن کارایی راه‌کار پیشنهادی ارائه‌شده، از پلتفرم PLEXE استفاده می‌شود. مهم‌ترین مانورهای مورداستفاده در پلاتون عبارتند از مانور پایداری پلاتون و مانور ردیابی رهبر. در این مقاله بر روی مانور پایداری پلاتون تمرکز شده است که پلاتون باید دارای توانایی شروع با شرایط اولیهٔ مختلف بوده و بتواند رفتار رهبر را تقلید کند و به سیاست‌های فاصلهٔ مطلوب و سرعت ثابت مشترک برسد [6].

شاخص‌های مربوط به شبیه‌سازهای شبکه و ترافیک مورداستفاده در این مقاله به‌ترتیب در جداول (۲) و (۳) آورده شده‌اند.

۴-۳- شرح حملات و سناریوهای موردارزیابی

۴-۳-۱- حملهٔ دست‌کاری

در حملهٔ دست‌کاری، گره مخرّب با توجه به همسایگی ایجادشده از طریق توپولوژی جریان اطّلاعات مورداستفاده در سناریو، اقدام به تغییر شاخص‌های حرکتی از قبیل شتاب و سرعت خودروی هدف می‌کند. این نوع حمله باعث به خطر افتادن پایداری پلاتون و در بدترین حالت ممکن است باعث برخورد بین خودروهای پلاتون شود [5, 6].

در سناریوی شبیه‌سازی‌شده، فرض می‌شود که یک گره مخرّب داخلی کنترل خودرو سوم را به دست می‌گیرد و یک آفست ثابت به مقدار شتاب فعلی آن در لحظهٔ معین t اضافه می‌کند. یعنی خودرو سوم شروع به حرکت با شتاب نادرست می‌کند، از این رو حرکت همهٔ خودروهای همسایه مختل می‌شود.

جدول ۲: شاخص‌های شبیه‌سازی شبکه

Table2: Parameters of Network Simulation

شاخص	مقدار	واحد
الگو PHY/MAC	IEEE 802.11p/1609.4 single channel (CCH)	----------
فرکانس	5.89	GHz
نرخ بیت	6	$Mbit/s$
اندازهٔ بسته	200	bit
قدرت سیگنال	20	dbm
فرکانس بیکن	10	Hz

جدول ۳: شاخص‌های شبیه‌سازی ترافیک

Table3: Parameters of Traffic Simulation

شاخص	مقدار	واحد
طول بزرگراه	10	km
تعداد لاین‌ها	4(دوطرفه)	------
سرعت خودروها	27.78	m/s
سایز پلاتون	8	خودرو
حداکثر شتاب خودروهای پلاتون	3.5	m/s^2
جرم خودروهای پلاتون	1460	kg
طول هر خودرو در پلاتون	4	m
زمان پیشروی $h_{i,i-1}$	0.8	s
متغیّرهای کنترلی k_{ij}	$k_{10}=460, k_{i0}=80 (i=2,\cdots,N)$ $k_{i,i-1}=860, k_{i,i+1}=860$ درغیر این صورت $k_{ij}=0$	$1/s^2$
متغیّر کنترلی b	1800	$1/s$
فاصله در حالت توقّف s_{ij}^{st} بین دو خودرویی متوالی i و j	15	m
زمان شبیه‌سازی	200	s

۴-۳-۲- حملهٔ جعل پیام

در حملهٔ جعل پیام، یک گره مخرّب شروع به گوش دادن به پیام‌های ردوبدل‌شده بین خودروها بر روی بستر ارتباطی

بی‌سیم و پس از دریافت هر پیام، محتوای آن را جعل می‌کند. سرانجام، پیام‌های مخرّب تغییریافته را در همان لحظه دوباره پخش می‌کند. این نوع حمله در بدترین حالت باعث تصادف می‌شود [3].

در این سناریو فرض می‌شود که گره مخرّب چهارمین خودرو در پلاتون است. این خودرو زمینهٔ موقعیّت خودش را با افزودن مقدار پنج متر به‌عنوان آفست به موقعیّت فعلی خود تغییر می‌دهد؛ سپس، اطّلاعات دست‌کاری‌شده و نادرست را به خودروهای همسایه ارسال می‌کند.

۴-۴- نتایج شبیه‌سازی

۴-۴-۱-وضعیت پلاتون بدون حملات

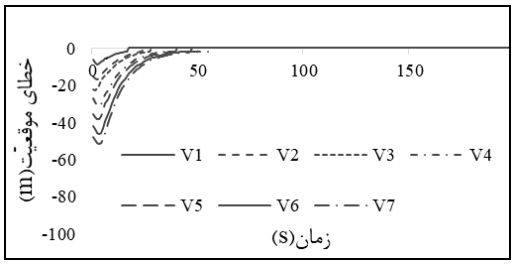
برای درک بهتر و ارزیابی تأثیر حملات مخرّب و اثربخشی راه‌کار پیشنهادی در مقابله با حملات دست‌کاری و جعل پیام، نخست، توانایی راه‌کار پیشنهادی در شرایط مطلوب نشان داده می‌شود؛ یعنی هنگامی‌که هیچ گره مخرّبی حضور ندارد. همان‌طورکه در شکل (۵) نشان داده شده است، همهٔ خودروها با شروع از فاصله‌های متفاوت از سیاست فاصلهٔ لحاظ‌شده در پلاتون، به سمت موقعیّت‌های مطلوب حرکت کرده و بعد از گذشت حدود ۶۰ ثانیه فواصل بین خودرویی به فاصلهٔ مطلوب و سرعت خودروها به سرعت رهبر همگرا می‌شوند. نتایجِ نشان‌داده‌شده در شکل (۵) مربوط به توپولوژی جریان اطّلاعات PF است.

پایداری پلاتون تحت توپولوژی PF در حالت بدون حمله در شکل (۵) نشان داده شده است. نمودار خطای موقعیّت در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به‌صورت $r_i(t) - r_0(t) + h_{i0}v_0 + s_{i0}^{st}$ به‌ازای تمام $i = 1, \cdots, N$ محاسبه شده است. نمودار خطای سرعت در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به‌صورت $v_i(t) - v_0$ به‌ازای تمام $i = 1, \cdots, N$ محاسبه شده است. تغییرات شتاب در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به‌صورت $\alpha_i(t)$ به‌ازای تمام $i = 0, \cdots, N$ محاسبه شده است.

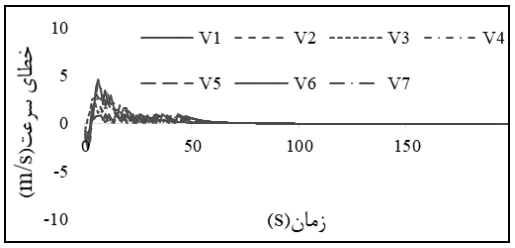
۴-۴-۲- حملهٔ دست‌کاری

سناریوی درنظرگرفته‌شده به این صورت است که در این حمله، پایداری پلاتون تحت توپولوژی جریان اطّلاعات PF ارزیابی شده است. به این منظور، در زمان $t = 70$ ثانیه، یک گره مخرّب داخلی کنترل خودرو سوم را به دست می‌گیرد و با تنظیم نادرست شتاب آن اطّلاعات جعلی را تزریق می‌کند.

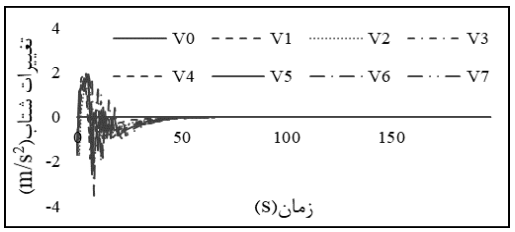
حملهٔ دست‌کاری با مقدار آفست‌ها و δ_1های متفاوت انجام شده است، که نتایج در جدول (۴)، جدول (۵)، جدول (۶)، جدول (۷)، جدول (۸)، شکل (۶) و شکل (۷) آورده شده است.



(آ)



(ب)



(پ)

(شکل ۵): پایداری پلاتون تحت توپولوژی PF در حالت بدون حمله: (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

Fig5. Stability of Platoon under the PF topology in the without attack state: (a): position error; (b): speed error; (c): control effort

(جدول ۴): حملهٔ دست‌کاری با آفست یک

Table4: Spoofing Attack with Offset One

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	1.637410122011
5	2.837302108112

(جدول۵): حملهٔ دست‌کاری با آفست دو

Table5: Spoofing Attack with Offset Two

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	0.83740278597
5	1.337410125304

)جدول ۶): حملهٔ دست‌کاری با آفست سه

Table6: Spoofing Attack with Offset Three

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	0.567402787779
5	0.897410133421

(جدول ۷): حملهٔ دست‌کاری با آفست چهار

Table7: Spoofing Attack with Offset Four

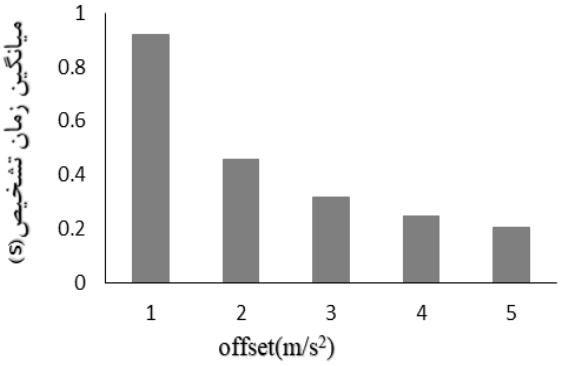
$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	0.43740278878
5	0.687410137913

(جدول ۸): حملهٔ دست‌کاری با آفست پنج

Table8: Spoofing Attack with Offset Five

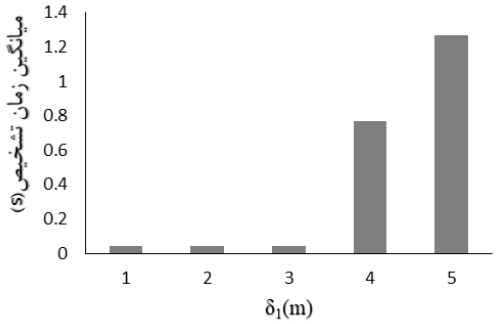
$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	0.35741019189
5	0.55739878213

در حمله دست‌کاری مقدار آفست بر حسب متر بر مجذور ثانیه است، به مقدار شتاب خودرویی که در معرض حمله قرار گرفته، اضافه می‌شود. و مقدار δ_1 بر حسب متر است، که اگر اختلاف فاصلهٔ هر خودرو نسبت به رهبر بیشتر از آن باشد، آن خودرو به‌عنوان مخرّب شناسایی می‌شود. همان‌طورکه در جداول ۴ تا ۸ و شکل‌های ۶ و ۷ مشاهده می‌شود. در حملهٔ دست‌کاری هرچه مقدار δ_1 بیشتر باشد، میانگین زمان تشخیص حمله بیشتر خواهد شد. زیرا هرچه δ_1 بیشتر باشد، زمان بیشتری می‌خواهد تا به فاصلهٔ مدنظر برای تشخیص حمله برسد. ولی هرچه δ_1 کمتر باشد، زمان کمتری می‌خواهد تا به فاصلهٔ مدنظر برای تشخیص حمله برسد. همچنین، در این حمله هر چه مقدار آفست بیشتر باشد، میانگین زمان تشخیص حمله کمتر خواهد شد. زیرا مقدار آفست به شتاب خودرویی که در معرض حمله قرار گرفته است، اضافه می‌شود، و باعث می‌شود که خودرو مخرّب زودتر به فاصلهٔ مدنظر برای تشخیص حمله برسد. ولی اگر این مقدار کمتر باشد، زمان بیشتری می‌خواهد تا به فاصلهٔ مدنظر برای تشخیص حمله برسد.



(شکل ۶): میانگین زمان تشخیص حمله با آفست‌های متفاوت هنگام حملهٔ دست‌کاری

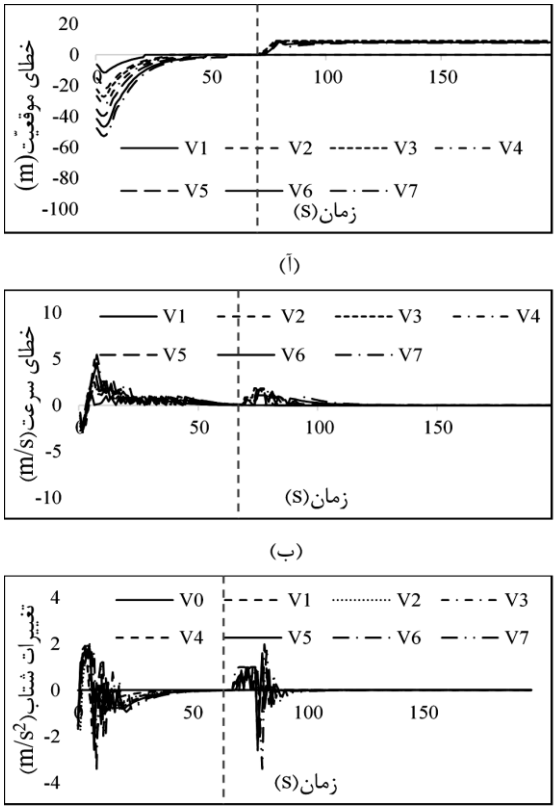
Fig6. Average attack detection time with different offsets during spoofing attack



(شکل ۷): میانگین زمان تشخیص حمله با δ_1های متفاوت هنگام حمله دست‌کاری

Fig7. Average attack detection time with different $\delta_1$during spoofing attack

که در ادامه نتایج شبیه‌سازی برای حملهٔ دست‌کاری با مقدار آفست سه و $\delta_1 = 3$ آورده شده است.

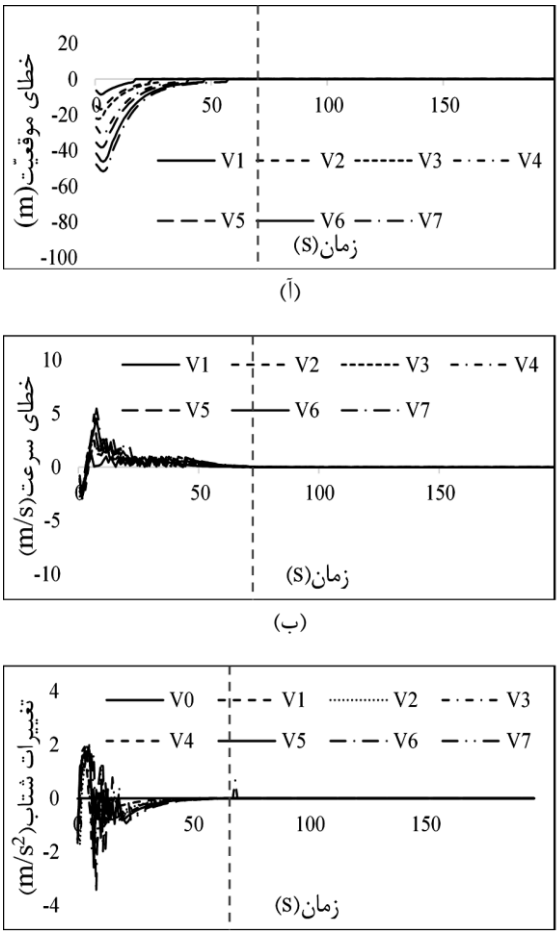


(شکل ۸): اثر حمله دست‌کاری بدون الگوریتم پیشنهادی (حمله مخرّب در زمان $t = 70$ ثانیه شروع می‌شود؛ که با خط عمودی خاکستری نشان داده شده است). پایداری پلاتون تحت توپولوژی **PF**: (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

Fig8. Effect of spoofing attack without the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the PF topology: (a): position error; (b): speed error; (c): control effort

برای بررسی اثر حمله دست‌کاری و آشکارسازی بهتر توانایی راه‌کار پیشنهادی در خنثی کردن حمله، رفتار پلاتون در حالتی که الگوریتم پیشنهادی غیرفعّال باشد،

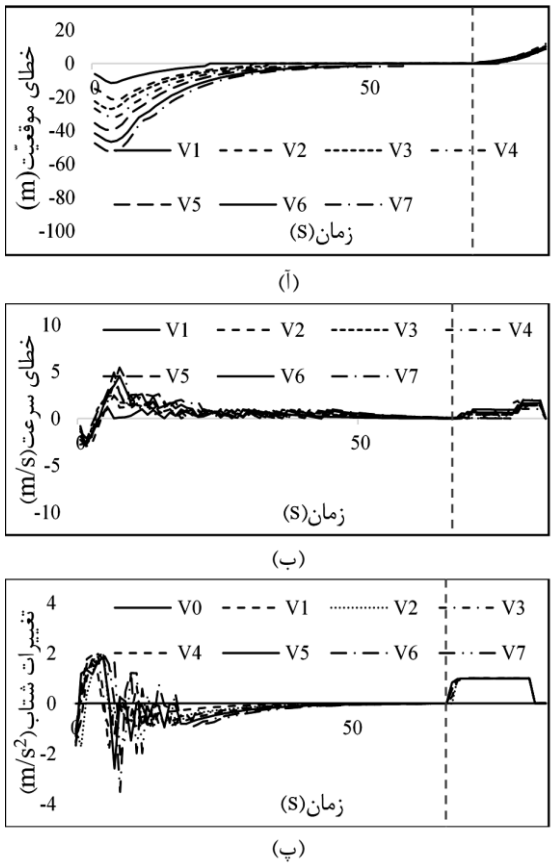
نشان داده شده است. در این حالت، خودروها به همهٔ اطّلاعات دریافتی اعتماد دارند ($Malicious_i = 0$ به اعضای تمام خودروها). نتایج حاصل‌شده در شکل (۸) نشان می‌دهد که چگونه حملهٔ دست‌کاری به‌شدت بر سیاست فاصله بین خودرویی تأثیر می‌گذارد (خطای موقعیّت خودروهای ۳-۴-۵-۶-۷ همان‌طورکه در شکل (۸) (آ) مشخص شده است به صفر همگرا نمی‌شوند؛ درحالی‌که پس از گذر به‌طور تقریبی ۳۰ ثانیه نیازهای شتاب و سرعت بازیابی می‌شوند. شکل (۸) (ب) و (پ) را مشاهده کنید).



(شکل ۹): اثر حمله دست‌کاری با الگوریتم پیشنهادی (حمله مخرّب در زمان $t = 70$ ثانیه شروع می شود. که با خط عمودی خاکستری نشان داده شده است). پایداری پلاتون تحت توپولوژی PF: (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

Fig9. Effect of spoofing attack with the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the PF topology: (a): position error; (b): speed error; (c): control effort

پایداری پلاتون تحت توپولوژی PF در حالت حملهٔ دست‌کاری بدون الگوریتم پیشنهادی در شکل(۸) نشان داده شده است. نمودار خطای موقعیّت در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به صورت $r_i(t) - r_0(t) + h_{i0}v_0 + s_{i0}^{st}$ به‌ازای تمام $i = 1, \cdots, N$ محاسبه شده است. نمودار خطای سرعت در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به‌صورت $v_i(t) - v_0$ به‌ازای تمام $i = 1, \cdots, N$ محاسبه شده است. تغییرات شتاب در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به صورت $\alpha_i(t)$ به‌ازای تمام $i = 0, \cdots, N$ محاسبه شده است.

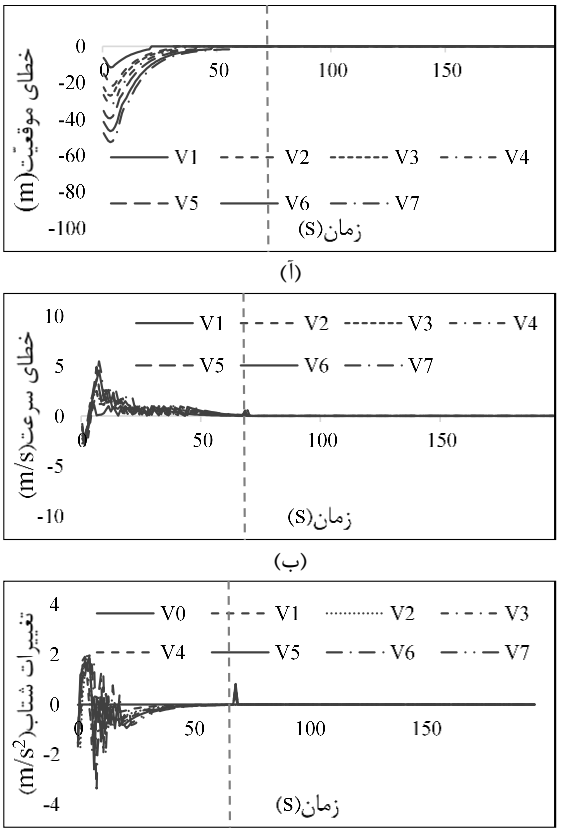


(شکل ۱۰): اثر حملهٔ دست‌کاری بدون الگوریتم پیشنهادی (حمله مخرّب در زمان $t = 70$ ثانیه شروع می شود؛ که با خط عمودی خاکستری مشخص شده است). پایداری پلاتون تحت توپولوژی BDL (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

Fig10. Effect of spoofing attack without the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the BDL topology: (a): position error; (b): speed error; (c): control effort

هنگام فعال کردن الگوریتم پیشنهادی خودروهای ۴-۵-۶-۷ می‌توانند اطّلاعات جعل‌شده را از خودرو ۳ همان‌طورکه در شکل (۹) نشان داده شده است، شناسایی کنند و از این رو، آن‌ها به سیاست فاصلهٔ مطلوب می‌رسند (خطاهای موقعیّت به صفر همگرا می‌شود به شکل(۹) قسمت (آ) مراجعه کنید). همان‌طورکه در شکل (۹) مشاهده می‌کنید، حتی اثر گره مخرّب برای خودرو ۳ که در معرض حملهٔ مستقیم به سیگنال شتاب خود قرار دارد،

کاهش داده شود. با استفاده از این الگوریتم، اجتناب از برخورد با بهبود قابل توجهی مواجه می‌شود. پایداری پلاتون تحت توپولوژی PF در حالت حملهٔ دست‌کاری با الگوریتم پیشنهادی در شکل (۹) نشان داده شده است.



(شکل ۱۱): اثر حملهٔ دست‌کاری با الگوریتم پیشنهادی (حمله مخرّب در زمان $t = 70$ ثانیه شروع می شود. که با خط عمودی خاکستری مشخص شده است). پایداری پلاتون تحت توپولوژی BDL (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

Fig11. Effect of spoofing attack with the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the BDL topology: (a): position error; (b): speed error; (c): control effort

برای ارزیابی دقیق‌تر کارایی راه‌کار پیشنهادی، در بدترین حالت نیز ارزیابی شده است که در آن، همهٔ خودروها در معرض حمله دست‌کاری بر روی سیگنال شتاب قرار می‌گیرند. نتایج در غیاب الگوریتم پیشنهادی بر روی توپولوژی BDL نشان می‌دهد که پلاتون پس از ۱۵ ثانیه از آغاز حمله همان‌طورکه در شکل (۱۰) مشاهده می‌کنید، باعث برخورد خودروهای درون پلاتون می‌شود.

در مقابل با به‌کاربردن الگوریتم پیشنهادی، می‌توان اثرات مخرّب را به طور نسبتاً کامل کاهش داد. در واقع، همه خودروها اکنون قادر به جلوگیری از برخورد هستند، همان‌طورکه در شکل (۱۱) قسمت (آ) نشان داده شده است. خودروها مشخّصات سرعت و شتاب رهبر را ردیابی می‌کنند (نتایج را در شکل(۱۱) قسمت‌های (ب) و (پ) مشاهده کنید). توجه داشته باشید که این مثال با هدف نشان دادن عملکرد به‌نسبت خوب راه‌کار پیشنهادی در بدترین حالت گزارش شده است.

۴-۴-۳-حملهٔ جعل پیام

سناریوی درنظرگرفته‌شده به این صورت است که در آن، پایداری پلاتون تحت توپولوژی جریان اطّلاعات PF ارزیابی شده است. برای این منظور در $t = 70$ ثانیه، خودرو چهارم از پلاتون زمینهٔ موقعیّت پیام‌های ارسال‌شده را جعل می‌کند. تمام خودروهای دیگر اطّلاعات جعلی را می‌پذیرند و سپس آن‌ها را برای اعمال کنترل طولی به کار می‌برند. این حمله با مقدار آفست‌ها و δ_1های متفاوت انجام‌شده است، که نتایج در جدول (۹)، جدول (۱۰)، جدول (۱۱)، جدول (۱۲)، جدول (۱۳)، شکل (۱۲) و شکل (۱۳) آورده شده است.

(جدول ۹): حمله جعل پیام با آفست سه

Table9: Message Falsification Attack with Offset Three

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	------
5	------

(جدول ۱۰): حملهٔ جعل پیام با آفست چهار

Table10: Message Falsification Attack with Offset Four

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	1.137403704827
5	------

(جدول ۱۱): حملهٔ جعل پیام با آفست پنج

Table11: Message Falsification Attack with Offset five

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	1.137403704827
5	1.537399562256

(جدول ۱۲): حملهٔ جعل پیام با آفست شش

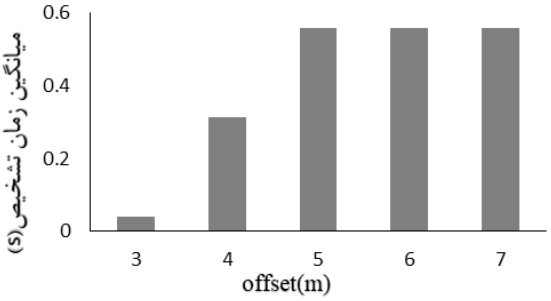
Table12: Message Falsification Attack with Offset Six

$\delta_1\ (m)$	زمان تشخیص حملات (s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	1.137403704827
5	1.537399562256

(جدول ۱۳): حملهٔ جعل پیام با آفست هفت

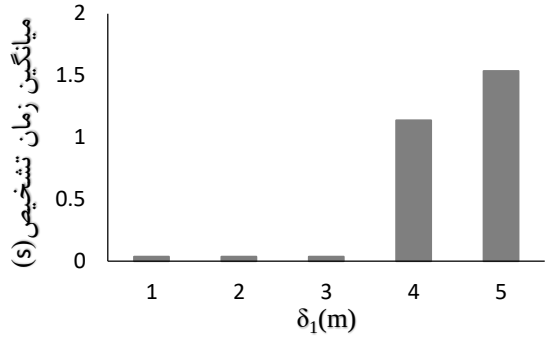
Table13: Message Falsification Attack with Offset Seven

δ_1 (m)	زمان تشخیص حملات(s)
1	0.037401104609
2	0.037401104609
3	0.037401104638
4	1.137403704827
5	1.537399562256



(شکل ۱۲): میانگین زمان تشخیص حمله با آفست‌های متفاوت هنگام حملهٔ جعل پیام

Fig12. Average attack detection time with different offsets during message falsification attack

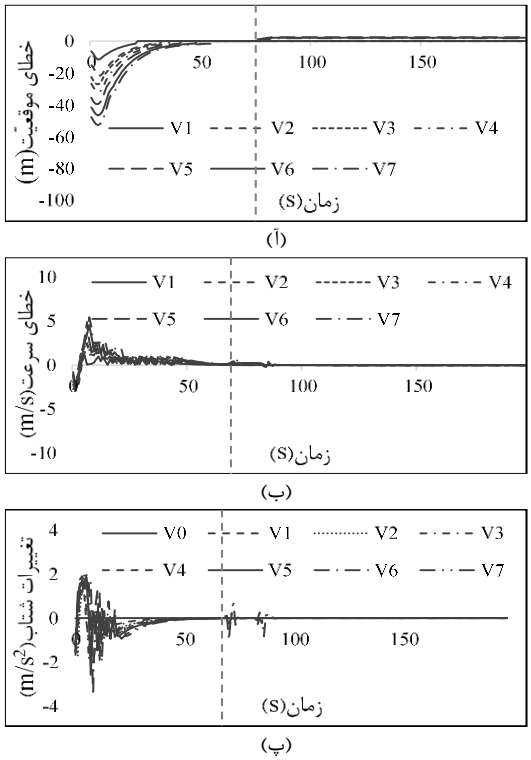


(شکل ۱۳): میانگین زمان تشخیص حمله با δ_1های متفاوت هنگام حملهٔ جعل پیام

Fig13. Average attack detection time with different $\delta_1$during message falsification attack

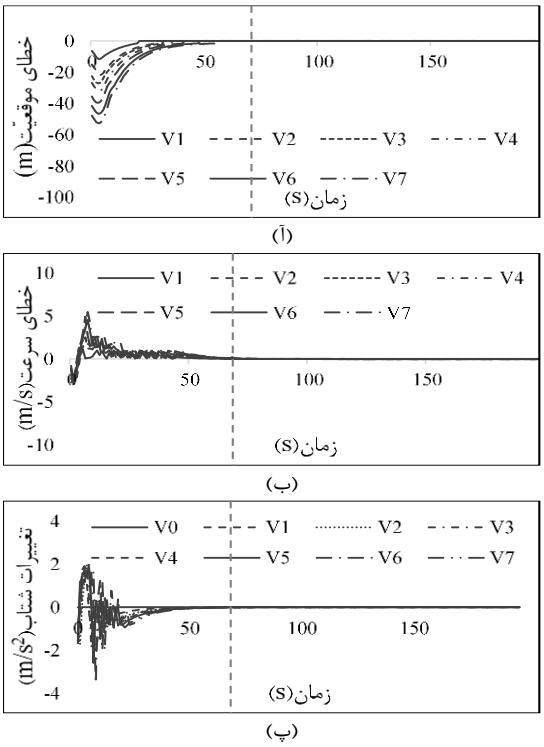
در حملهٔ جعل پیام مقدار آفست بر حسب متر است، که خودرو مخرّب به موقعیّت فعلی خود اضافه کرده و آن را برای خودروهای همسایه، طبق توپولوژی جریان اطّلاعات ارسال می‌کند. و مقدار δ_1 بر حسب متر است، که اگر اختلاف فاصلهٔ هر خودرو نسبت به رهبر بیشتر از آن باشد، حمله شناسایی می‌شود. همان طورکه در جداول ۹ تا ۱۳ مشاهده شد، هنگامی‌که مقدار آفست کمتر از مقدار δ_1 باشد، حمله قابل تشخیص نیست. ولی هنگامی‌که مقدار آفست بزرگ‌تر یا مساوی δ_1 باشد، حمله قابل تشخیص است. همان‌طورکه در شکل ۱۲ مشاهده شد. در حملهٔ جعل پیام در حالتی که مقدار آفست کوچک‌تر مساوی δ_1 است، هر چه مقدار آفست بیشتر باشد، میانگین زمان تشخیص حمله بیشتر می‌شود. ولی هنگامی‌که مقدار آفست بیشتر از δ_1 باشد، میانگین زمان تشخیص حمله برابر با میانگین زمان تشخیص حمله در حالتی که مقدار آفست با δ_1 مساوی است، می‌شود. همچنین، در این حمله هر چه مقدار δ_1 بیشتر باشد، میانگین زمان تشخیص حمله بیشتر خواهد شد. زیرا هر چه δ_1 بیشتر باشد، زمان بیشتری می‌خواهد تا به فاصلهٔ مدنّظر برای تشخیص حمله برسد. ولی هرچه δ_1 کمتر باشد، زمان کمتری می‌خواهد تا به فاصلهٔ مدنظر برای تشخیص حمله برسد.

که در ادامه نتایج شبیه‌سازی برای حملهٔ جعل پیام با مقدار آفست ۵ و $\delta_1 = 3$ آورده شده است. نخست، در نظر بگیرید که الگوریتم پیشنهادی فعال نیست، در شکل (۱۴) در مورد توپولوژی PF نشان می‌دهد که خطاهای موقعیّت خودروهای ۵-۶-۷ به صفر همگرا نمی‌شود و از این رو پایداری پلاتون تضمین نمی‌شود. توجه داشته باشید همان‌طور که انتظار می‌رود، جعل موقعیّت به‌طور عمده بر فاصله بین خودرویی تأثیر می‌گذارد (اثرات روی خطاهای سرعت و شتاب ناچیز است؛ همان‌طورکه در شکل (۱۴) (ب) و (پ) نشان داده شده است).



(شکل ۱۴): اثر حمله جعل پیام بدون الگوریتم پیشنهادی(حمله مخرّب در زمان $t = 70$ ثانیه شروع می شود. که با خط عمودی خاکستری مشخص شده است). پایداری پلاتون تحت توپولوژی PF: (آ): خطای موقعیّت (ب): در خطای سرعت (پ): تغییرات شتاب

Fig14. Effect of message falsification attack without the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the PF topology: (a): position error; (b): speed error; (c): control effort



(شکل ۱۵): اثر حمله جعل پیام با الگوریتم پیشنهادی (حملهٔ مخرّب در زمان $t = 70$ ثانیه شروع می شود. که با خط عمودی خاکستری مشخص شده است). پایداری پلاتون تحت توپولوژی PF: (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

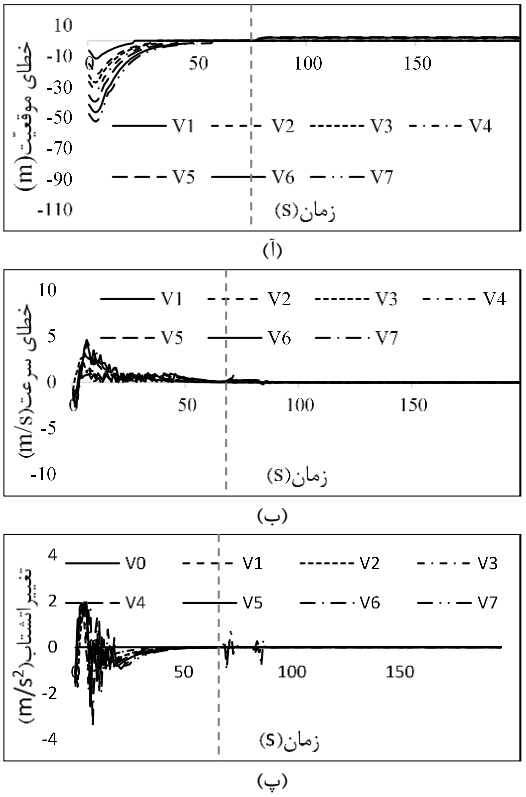
Fig15. Effect of message falsification attack with the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the PF topology: (a): position error; (b): speed error; (c): control effort

پایداری پلاتون تحت توپولوژی PF در حالت حمله جعل پیام بدون الگوریتم پیشنهادی در شکل(۱۴) نشان داده شده است. نمودار خطای موقعیّت در بازه زمانی ۰ تا ۲۰۰ ثانیه و به صورت $r_i(t) - r_0(t) + h_{i0}v_0 + s_{i0}^{st}$ به‌ازای تمام $i = 1, \cdots, N$ محاسبه شده است. نمودار خطای سرعت در بازهٔ زمانی ۰ تا ۲۰۰ ثانیه و به‌صورت $v_i(t) - v_0$ به‌ازای تمام $i = 1, \cdots, N$ محاسبه شده است.

تغییرات شتاب در بازه زمانی ۰ تا ۲۰۰ ثانیه و به‌صورت $\alpha_i(t)$ به‌ازای تمام $i = 0, \cdots, N$ محاسبه شده است.

شکل (۱۵) نتایج به‌دست‌آمده در سناریوی حملهٔ جعل پیام را با تفاوت قابل‌توجهی با به‌کاربردن الگوریتم پیشنهادی به‌عنوان یک اقدام متقابل برای تشخیص رفتار مخرّب نشان می‌دهد. توجه داشته باشید که متفاوت از نتایج قبلی اکنون خودرو ۵ قادر است پیام جعلی ارسال‌شده توسط خودرو ۴ را شناسایی و از اطّلاعات ذخیره‌شده از پیش برای رانندگی مشارکتی استفاده کند. در نتیجه، خودروهای ۶-۷ اطّلاعات گمراه‌کننده را دریافت نمی‌کنند و هدف پایداری پلاتون هنوز حفظ می‌شود.

همچنین، استفاده از الگوریتم پیشنهادی، عملکردی مشابه برای توپولوژی جریان اطّلاعات BDL در پی دارد که نتایج آن در شکل‌های ۱۶ و ۱۷ آورده شده است.

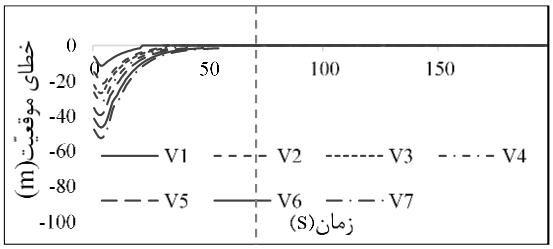


(شکل ۱۶): اثر حملهٔ جعل پیام بدون الگوریتم پیشنهادی (حمله مخرّب در زمان $t = 70$ ثانیه شروع می شود. که با خط عمودی خاکستری مشخص شده است). پایداری پلاتون تحت توپولوژی BDL: (آ): خطای موقعیّت (ب): خطای سرعت (پ): تغییرات شتاب

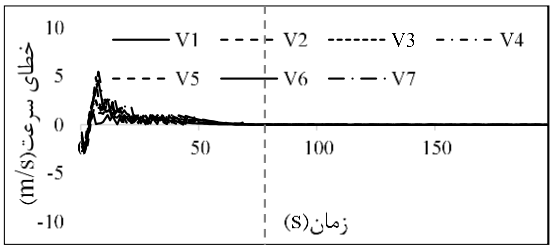
Fig15. Effect of message falsification attack without the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the BDL topology: (a): position error; (b): speed error; (c): control effort

۵- مقایسه با کارهای پیشین

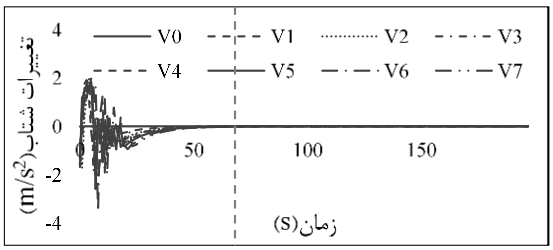
در اینجا عملکرد راه‌کار پیشنهادی با کار آقای آلبرتو پتریلو [6] بحث می‌شود. در [6] از روش رای‌گیری برای مقابله با حملات در حضور توپولوژی‌های مختلف جریان اطّلاعات بررسی و ارزیابی شده است. با و جود عملکرد مناسب سازوکار رأی‌گیری در بیشتر توپولوژی‌ها این راه‌کار برای توپولوژی جریان اطّلاعات «هر خودرو فقط با خودرو جلو» از کارایی لازم برخوردار نیست. علّت این امر در نیاز خودروها برای انجام رأی‌گیری به دریافت اطّلاعات از دست‌کم دو خودرو نهفته است که در توپولوژی ذکرشده خودروها اطّلاعات را فقط از خودرو جلویی دریافت می‌کنند.



(آ)



(ب)



(پ)

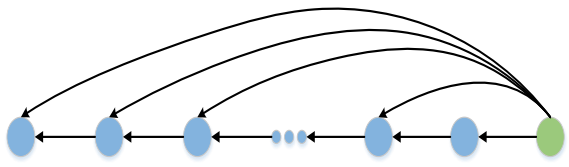
(شکل ۱۷): اثر حملهٔ جعل پیام با الگوریتم پیشنهادی (حمله ثانیه شروع می شود. که با خط عمودی $t = 70$ مخرّب در زمان خاکستری مشخص شده است). پایداری پلاتون تحت توپولوژی BDL: (آ): خطای موقعیّت (ب): خطای سرعت

(پ): تغییرات شتاب

Fig15. Effect of message falsification attack with the proposed algorithm (attack begins at time t =70[s] as highlighted by the vertical gray dash line). Stability of Platoon under the BDL topology: (a): position error; (b): speed error; (c): control effort

باتوجّه‌به ارزیابی سناریوهای حملات دست‌کاری و جعل پیام در حضور توپولوژی PF و نتایج شبیه‌سازی که در بخش‌های قبل ارائه شده است، راه‌کار پیشنهادی این مقاله در مقابل حملات دست‌کاری و جعل پیام در حضور توپولوژی‌های مختلف جریان اطّلاعات (از قبیل PF و BDL) عملکرد مناسبی داشته است.

در ادامه، راه‌کار پیشنهادی با روش رأی‌گیری در [6] تحت حمله دست‌کاری در حضور توپولوژی جریان اطّلاعات PLF که در شکل (۱۸) نشان داده شده، مقایسه شده‌اند.



(شکل ۱۸): توپولوژی جریان اطّلاعات PLF

Fig16. Information flow topology PLF

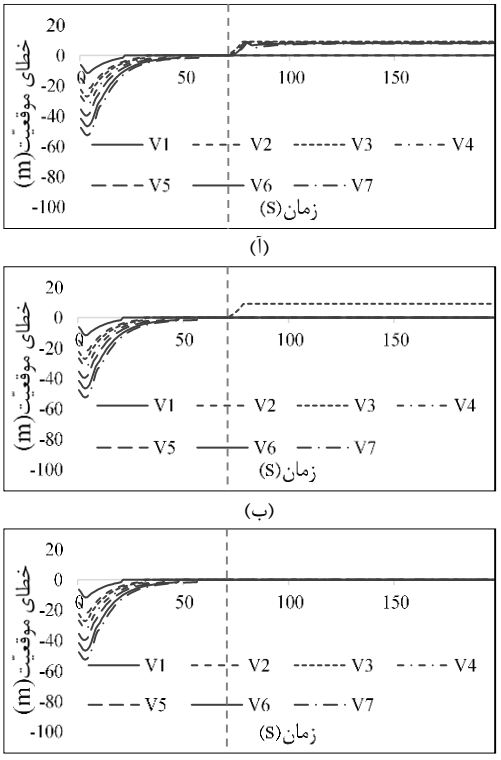
پایداری پلاتون در حالت حملهٔ دست‌کاری تحت توپولوژی PLF در روش رأی‌گیری در [6] و راه‌کار پیشنهادی این مقاله در شکل (۱۹)، شکل (۲۰) و شکل (۲۱) با هم مقایسه شده‌اند. از این مقایسه نتیجه گرفته می‌شود که راه‌کار پیشنهادی برای خودرویی که در معرض حمله مستقیم دست‌کاری سیگنال شتاب قرار گرفته است، اثر حمله برای خطای موقعیّت، خطای سرعت و تغییرات شتاب کاهش داده شده است در صورتی که روش رأی‌گیری اثر آن را کاهش نداده است.

به‌دلیل این که الگوریتم رای‌گیری، خودرویی را که اطّلاعات جعلی یا دست‌کاری‌شده به خودروهای ارتباطی تحت توپولوژی جریان اطّلاعات فرستاده است، به‌عنوان خودرو مخرّب شناسایی می‌کند، قادر به تشخیص خودرویی که در معرض حملهٔ دست‌کاری قرار گرفته باشد نیست، پس، در نتیجه قادر به کاهش دادن اثر حمله دست‌کاری بر روی خودرویی مدنظر نیست. ولی در راهکار پیشنهادی این مقاله بر اساس مقایسهٔ فاصله هر خودرو با خودرو رهبر حمله تشخیص داده می‌شود. اگر حمله توسط خودروهای ارتباطی با خودروی مدنظر صورت گرفته باشد، آن‌ها را بر اساس مقایسهٔ اختلاف سرعتشان با مقدار سرعت ثابت مشترک، و اگر از آستانه تعیین‌شده بیشتر باشد، به‌عنوان خودرو مخرّب شناسایی می‌کند. همچنین، اگر خودرو، در معرض حملهٔ دست‌کاری قرار داشته باشد، اختلاف سرعت خود خودرو با سرعت ثابت مشترک v_0 را به دست می‌آورد. اگر این مقدار بیشتر از آستانهٔ تعیین‌شده باشد، حملهٔ دست‌کاری بر روی خودرو مدنظر را شناسایی می‌کند و اثر آن را کاهش می‌دهد.

علاوه‌بر این راه‌کار پیشنهادی در مقایسه با کار آقای سیهان اوکار [4] بحث و بررسی شده است. در [4] از روش SP-VLC برای مقابله با حملات استفاده شده است. با وجود عملکرد مناسب در مقابل حملات خارجی، این روش در مقابل حملات داخلی از کارایی لازم برخوردار نیست؛ زیرا برای مقابله با حملات از کلید مخفی با استفاده از رمزنگاری نامتقارن و انتقال اطّلاعات از طریق ارتباطات نور مرئی استفاده کرده است. همچنین، در روش SP-VLC برای انتقال اطّلاعات فقط از توپولوژی جریان اطّلاعات PF استفاده شده است. درصورتی‌که راه‌کار پیشنهادی این مقاله در مقابل حملات داخلی از کارایی لازم برخوردار است و همچنین، برای انتقال اطّلاعات از توپولوژی‌های جریان اطّلاعات بیشتری استفاده کرده است.

۶- نتیجه‌گیری

در این مقاله به مشکل رانندگی مشارکتی برای خودروهای پلاتون در حضور آسیب‌پذیری‌های امنیّتی در شبکه‌های خودرویی پرداخته شده است. برای جلوگیری از پیامدهای خطرناک و برای ایمنی، نخست باید اثرات ناشی از حملات مخرّب شناسایی و سپس اقدامات متقابل برای کاهش اثر آن‌ها در نظر گرفته شود. بر اساس مطالعه حملات دست-کاری و جعل پیام، در این مقاله یک راه‌کار پیشنهاد و بررسی و ارزیابی شده است. تجزیه و تحلیلی که با شبیه‌ساز PLEXE انجام شده است، استحکام راه‌کار پیشنهادی در برابر آسیب‌پذیری‌ها و واکنش‌پذیری خوب در واکنش به حملات مخرّب را نشان می‌دهد.

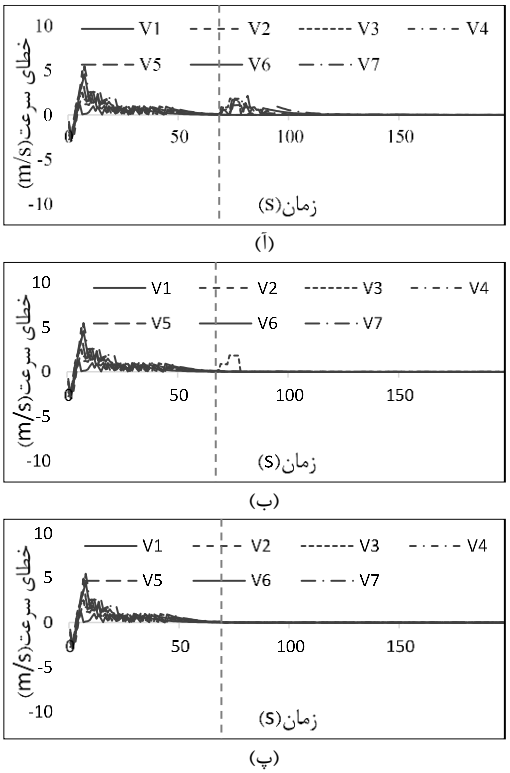


(شکل ۱۹): مقایسهٔ خطای موقعیّت تحت دو راه‌کار رای‌گیری و پیشنهادی (آ): بدون الگوریتم (ب): رای‌گیری (پ): پیشنهادی

Fig17. Comparison of position error under two voting and proposed strategies (a): without algorithm (b): voting (c): proposed

راه‌کار پیشنهادی با روش رأی‌گیری موجود در ادبیات مقایسه شده است، با وجود عملکرد مناسب در سازوکار رأی‌گیری بیشتر توپولوژی‌ها، این راه‌کار برای توپولوژی جریان اطّلاعات «هر خودرو فقط با خودرو جلو» از کارایی لازم برخوردار نیست و همچنین، در راه‌کار ارائه‌شده اثر حملهٔ دست‌کاری سیگنال شتاب بر روی خودرویی که صورت گرفته، کاهش داده نشده است. همان‌طورکه در نتایج شبیه‌سازی نشان داده شده است، راه-کار پیشنهادی برای توپولوژی جریان اطّلاعات «هر خودرو فقط با خودرو جلو»، و اثر حملهٔ دست‌کاری سیگنال شتاب را بر روی خودرویی که صورت گرفته، کاهش داده است.

علاوه‌بر این راه‌کار پیشنهادی با روش SP-VLC مقایسه شده است. با وجود عملکرد مناسب روش SP-VLC برای مقابله با حملات خارجی این روش در مقابل حملات داخلی از کارایی لازم برخوردار نیست. همچنین، روش SP-VLC برای انتقال اطّلاعات فقط از توپولوژی جریان اطّلاعات PF استفاده شده است. درصورتی‌که سرانجام



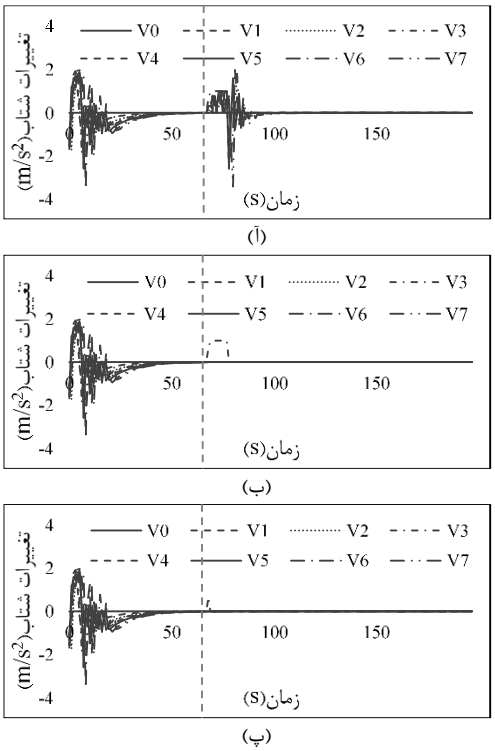
(شکل ۲۰): مقایسهٔ خطای سرعت تحت دو راه‌کار رأی‌گیری و پیشنهادی (آ): بدون الگوریتم (ب): رای‌گیری (پ): پیشنهادی

Fig18. Comparison of speed error under two voting and proposed strategies (a): without algorithm (b): voting (c): proposed

راه‌کار پیشنهادی این مقاله در مقابل حملات داخلی از کارایی لازم برخوردار است. و همچنین، برای انتقال اطّلاعات از توپولوژی‌های جریان اطّلاعات بیشتری استفاده کرده است.

۷- پیشنهادها

در این مقاله، خودروهای پلاتون همگن فرض شده است. در واقعیّت، یک پلاتون می‌تواند از خودروهای ناهمگن تشکیل شده باشد. در نتیجه، الگوریتم پیشنهادی این مقاله ممکن است برای یک پلاتون ناهمگن از کارایی لازم برخودار نباشد. همچنین هنگام حملات، همه خودروهای پلاتون باید بتوانند به‌طور صحیح سرعت متغیّر رهبر را در زمان‌های مختلف ردیابی کنند. قصد بر این است تا با در نظر گرفتن دو حالت مطرح‌شده راه‌کار این مقاله در آینده گسترش داده شود.



(شکل ۲۱): مقایسه تغییرات شتاب تحت دو راه‌کار رای‌گیری و پیشنهادی (آ): بدون الگوریتم (ب): رای‌گیری (پ): پیشنهادی

Fig19. Comparison of control effort under two voting and proposed strategies (a): without algorithm (b): voting (c): proposed

8- Refrence ۸- مراجع

[1] E. Coelingh and S. Solyom, "All aboard the robotic road train," Ieee Spectrum, vol. 49, no. 11, pp. 34-39, 2012.

[2] A. K. Saha and D. B. Johnson, "Modeling Mobility for Vehicular Ad Hoc Networks," Proceedings of the 1st ACM International Workshop on Vehicular Ad hoc Networks , 2004, pp. 91-92.

[3] Ucar, Seyhan, Ergen, Sinem Coleri and Ozkasap, Oznur, "Security vulnerabilities of IEEE802.11 p and visible light communication based platoon," in 2016 IEEE Vehicular Networking Conference (VNC), 2016.

[4] Ucar, Seyhan, Ergen, Sinem Coleri and Ozkasap, Oznur, "IEEE 802.11 p and visible light hybrid communication based secure autonomous platoon," IEEE Transactions on Vehicular Technology, vol. 67, no. 9, pp. 8667-8681, 2018.

[5] M. S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in International Conference on Signal Processing and Communication Systems, 2012.

[6] A. Petrillo, A. Pescapé and S. Santini, "A collaborative approach for improving the security of vehicular scenarios: The case of platooning," Computer Communications, vol. 122, pp. 59-75, 2018.

[7] DeBruhl, Bruce, Weerakkody, Sean, Sinopoli, Bruno and Tague, Patrick, "Is your commute driving you crazy? a study of misbehavior in vehicular platoons," in Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2015.

[8] Kim, Yeongkwun and Kim, Injoo, "Security issues in vehicular networks," in The International Conference on Information Networking 2013 (ICOIN), 2013.

[9] A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET, CRC press, 2016.

[10] Garip, Mevlut Turker, Gursoy, Mehmet Emre, Reiher, Peter and Gerla, Mario, "Congestion attacks to autonomous cars using vehicular botnets," in NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA, 2015.

[11] Engoulou, Richard Gilles, Bellaïche, Martine, Pierre, Samuel and Quintero, Alejandro, "VANET security surveys," Computer Communications, vol. 44, pp. 1-13, 2014.

[12] Alcaraz, Cristina, Lopez, Javier and Wolthusen, Stephen, "OCPP protocol: Security threats and challenges," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2452-2459, 2017.

[13] Crepeau, Claude, Davis, Carlton R and Maheswaran, Muthucumaru, "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.

[14] Hasrouny, Hamssa, Samhat, Abed Ellatif, Bassil, Carole and Laouiti, Anis, "VANet security challenges and solutions: A survey," Vehicular Communications, vol. 7, pp. 7-20, 2017.

[15] Jahanshahi, Niloofar and Ferrari, Riccardo MG, "Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach," IFAC-PapersOnLine, vol. 21, no. 23, pp. 212-217, 2018.

[16] Boeira, Felipe, Asplund, Mikael and Barcellos, Marinho P, "Mitigating position falsification attacks in vehicular platooning," in 2018 IEEE Vehicular Networking Conference (VNC), 2018.

[17] Mousavinejad, Eman, Yang, Fuwen, Han,

topologies," Transportation Research Part C: Emerging Technologies, pp. 360-383, 2017.
[27] A. Botta, A. Pescape and G. Ventre, "Quality of service statistics over heterogeneous networks: Analysis and applications," European Journal of Operational Research, vol. 191, no. 3, pp. 1075-1088, 2008.
[28] R. P. Karrer, I. Matyasovszki, A. Botta and A. Pescape, "MagNets - experiences from deploying a joint research-operational next-generation wireless access network testbed," in 2007 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities, Lake Buena Vista, FL, USA, 2007.
[29] G. Chen and F. L. Lewis, "Leader-following control for multiple inertial agents," International Journal of Robust and Nonlinear Control, vol. 21, no. 8, pp. 925-942, 2011.
[30] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler and R. L. Cigno, "PLEXE: A Platooning Extension for Veins," 2014 IEEE Vehicular Networking Conference (VNC), 2014, pp. 53-60.
[31] C. Sommer, "Veins," 2006. [Online]. Available: https://veins.car2x.org/. [Accessed 2020].
[32] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in SIMUTools 2008 - 1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems, Belgium, 2008.

تیمور درزاده کارشناس ارشد مهندسی کامپیوتر از دانشگاه سیستان و بلوچستان است. زمینه‌های پژوهشی وی شبکه‌های کامپیوتری و امنیّت در شبکه‌های خودرویی است.
نشانی رایانامهٔ ایشان عبارت است از:
Teymoor_drzfb@pgs.usb.ac.ir

نیک‌محمد بلوچزهی دانش‌آموختهٔ کارشناسی مهندسی کامپیوتر از دانشگاه یزد در سال ۱۳۸۰ و ارشد و دکتری مهندسی کامپیوتر از دانشگاه علم و صنعت ایران به‌ترتیب در سال‌های ۸۲ و ۹۴ است. وی هم اکنون استادیار گروه مهندسی فناوری اطّلاعات، دانشکدهٔ مهندسی برق و

Qing-Long, Qiu, Quanwei and Vlacic, Ljubo, "Cyber attack detection in platoon-based vehicular networked control systems," in 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE), 2018.
[18] Merco, Roberto, Biron, Zoleikha Abdollahi and Pisu, Pierluigi, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in 2018 Annual American Control Conference (ACC), 2018.
[19] Santini, Stefania, Salvi, Alessandro, Valente, Antonio Saverio, Pescapé, Antonio, Segata, Michele and Cigno, Renato Lo, "A consensus-based approach for platooning with intervehicular communications and its validation in realistic scenarios," IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 1985-1999, 2016.
[20] Yang, Zheng, Shengbo, Eben Li, Jianqiang, Wang, Dongpu, Cao and Keqiang, Li, "Stability and Scalability of Homogeneous Vehicular Platoon: Study on the Influence of Information Flow Topologies," IEEE Transactions on Intelligent Transportation Systems , vol. 17, no. 1, pp. 14 - 26, 2016.
[21] S. E. Li, Y. Zheng, K. Li and J. Wang, "An Overview of Vehicular Platoon Control under the Four-Component," in 2015 IEEE Intelligent Vehicles Symposium (IV), Seoul, South Korea, 2015.
[22] Yang, Zheng, Shengbo, Eben Li, Jianqiang, Wang, Le, Yi Wang and Keqiang, Li, "Influence of information flow topology on closed-loop stability of vehicle platoon with rigid formation," in International IEEE Conference on Intelligent Transportation Systems (ITSC), 2014.
[23] Yongcan, Cao, Wenwu, Yu, Wei, Ren and Guanrong, Chen, "An Overview of Recent Progress in the Study of Distributed Multi-Agent Coordination," IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 427 - 438, 2013.
[24] Jean-Pierre, Richard, "Time-delay systems:an overview of some recent advances and open problems," Automatica, 2003.
[25] D, Swaroop and J.K, Hedrick, "String stability of interconnected systems," IEEE Transactions on Automatic Control, vol. 41, no. 3, pp. 349 - 357, 1996.
[26] A. Salvi, S. Santini and A. S. Valente, "Design, analysis and performance evaluation of a third order distributed protocol for platooning in the presence of timevarying delays and switching

کامپیوتر دانشگاه سیستان و بلوچستان است. زمینهٔ پژوهشی موردعلاقهٔ ایشان شبکه‌های بی‌سیم، شبکه‌های خودرویی، محاسبات ابری خودرویی، محاسبات مهی خودرویی، شبکه‌های نرم‌افزارمحور و سامانه‌های کارایی بالاست.

نشانی رایانامهٔ ایشان عبارت است از:

balouchzahi@ece.usb.ac.ir

احمد بختیاری‌شهری دکترای خود را در رشتهٔ علوم کامپیوتر در سال ۱۳۹۳ دریافت کرده است. ایشان هم‌اکنون استادیار گروه مهندسی فناوری اطّلاعات، دانشکده برق و کامپیوتر دانشگاه سیستان و بلوچستان است. نام‌برده تاکنون بیش از پنج مقالهٔ علمی در مجلات و کنفرانس‌های معتبر داخلی و خارجی به چاپ رسانده است. زمینه‌های پژوهشی وی رمزنگاری، امنیّت شبکه، شبکه‌های کامپیوتری و فناوری اطّلاعات است.

نشانی رایانامهٔ ایشان عبارت است از:

bakhtiyari@ece.usb.ac