پژوهشکده علوم کامپیوتر

پروپوزال همکاری پژوهشی تک پروژه غیر مقیم

چارچوبی برای مقابله با حملات پنهان داخلی در شبکه های حمل و نقل هوشمند

A Framework to Thwart Insider Covert Attacks in Intelligent Transportation Systems

نام و نام خانوادگی متقاضی: دکتر محمد صیادحقیقی	نشانی: تهران، خیابان کارگر شمالی، تقاطع خیابان جلال آل احمد، دانشکده فنی دانشگاه تهران، دانشکده برق و کامپیوتر	نشانی پست الکترونیکی: sayad@ut.ac.ir
شمارهٔ تلفن ثابت: ۸۸۶۸۴۵۷۵	شمارهٔ تلفن همراه: ۰۹۱۲۲۰۲۷۲۵۱	

چکیده

اجزاء وسایل نقلیه هوشمند و خودران اغلب از طریق نوعی شبکه با هم ارتباط میگیرند. این غیر از شبکه خارجی است که در آن وقایع (مانند انسداد راه، تصادفات و ...) بصورت پیامهای داده گزارش میشوند. شبکه داخلی پروتکلهای مختلفی دارد که CAN bus از مشهورترین آنهاست. روی این باسها ماجولهای خودرو می نشینند که گاهی با کاربر و با دنیای بیرون (برای مثال جهت بروز رسانی firmware) تماس دارند. حمله سایبری سال ۲۰۱۵ به یک جیپ چروکی نشان داد که میتوان از راه این ماجولها به باس رسید و کنترل خودرو را بدست گرفت. برای مقابله با چنین حملات داخلی ای روشهای رمزنگارانه و امنیت شبکه کارکردی ندارند، چرا که مهاجم یک گره مشروع در شبکه است. در این پژوهش پس از بررسی حملات داخلی خودروهای هوشمند، چارچوبی برای تشخیص نفوذگر داخلی ارایه خواهد شد که سازگار با معماری باسهای مورد استفاده توسط خودروسازان باشد. چارچوب برای حداقل یک حمله پیاده سازی و شبیه سازی شده تا کارایی آن به اثبات برسد.

واژگان کلیدی:

حملات داخلی، سیستم حمل و نقل هوشمند، کشف نفوذ، امنیت سایبری

Abstract:

The components of smart and autonomous vehicles connect to each other via some sort of network. This is apart from the outside network for delivery of event messages (such as road blockade, crash, etc.). Internal network can run on different protocols, but CAN bus is the most recognized one. Over the bus, sit different vehicle modules which occasionally connect to user gadgets or outside world (e.g. to update their firmware). The 2015 cyber attack on a Jeep Cherokee showed that it is possible to access the bus via these modules and take control of the vehicle. To counter such insider attacks, cryptographic methods are useless, since the attacker is effectively a legitimate vehicle module. In this project, after studying the attacks in intelligent transportation systems, we design a framework to detect insider intruders. The proposed framework is going to be compatible with car manufacturers' current platform. The framework will be simulated and tested for at least one attack instance.

Keywords: Insider Attacks, Intelligent Transportation Systems, Intrusion Detection, Cyber Security

مقدمه

در صنعت نصل پنجم یا به عبارتی Industry 5.0 انسان و ماشین در کنار هم کار میکنند. خودروهای هوشمند و خودران شاید اولین نمونه های چنین سیستمهایی هستند. در سال ۲۰۱۵ یک جیپ مدل چروکی از راه سیستم مالتی مدیای خودرو از راه دور هک شد. این اتفاق توجه محققین را به امنیت خودروها جلب کرد. خودرو های خودران و هوشمند بخشی از اینترنت اشیا (IoT) و سیستمهای سایبری-فیزیکی (CPS) هستند. در میان کاربردهای سیستم‌های متصل به هم، سیستمهای حمل و نقل هوشمند[1] (ITS) نمونه هایی هستند که در سالهای اخیر بطور ویژه ای مورد توجه قرار گرفته اند. وسایل نقلیه هوشمند نه تنها از طریق شبکه های اقتضایی خودرویی (VANET) با یکدیگر ارتباط دارند، بلکه در داخل خود نیز اجزاء آنها از ارتباطات شبکه ای بهره می برند. حتی پیش از آنکه خودروها هوشمند شوند، صنعت خودروسازی به استفاده از شبکه داخلی برای ارتباط قطعات داخلی روی آورد. بعنوان مثال، CAN BUS یک پروتکل است که برای ارتباطات داخل خودرویی میان ماجولهای مختلف ساخته شده و هم اکنون در حال استفاده در بسیاری از خودرو هاست. این فناوری ها علاوه بر مزایای خود، چالش های امنیتی بی سابقه ای را به همراه آورده اند.

خودروهای خودران و هوشمند میتوانند از طریق برخی اجزای خود، مانند واحد مالتی مدیا، به دنیای خارج متصل شوند. این مسیر پنجره ای را برای هکرها باز می‌کند تا از راه شبکه داخلی خودرو، به اجزای داخلی آن واحد کنترل موتور (ECU) و یا حتی ماجولهای ارتباط با شبکه خودرویی دست پیدا کنند [1]. همانگونه که ذکر شد، در سال ۲۰۱۵، دو هکر در یک نمایش عمومی و سپس در کنفرانس Defcon نشان دادند که چگونه میتوان تمامی اجزاء یک خودرو جیپ مدرن را از راه دور کنترل نمود و این از برف پاک کن تا سیستم فرمان، ترمز و موتور را در بر می گرفت.

از این رو در زمینه امنیت شبکه خودروهای هوشمند و نیز وسائل نقلیه خودران، با دو مساله اصلی روبرو هستیم. نخست امنیت شبکه بین خودرویی و دوم امنیت سامانه ها و شبکه داخل خود خودروهای هوشمند. مساله امنیت شبکه بین خودرویی با کلید واژه VANET در یک دهه گذشته از منظر سرویسهای پایه امنیتی نظیر تامین محرمانگی، دست نخوردگی، احراز هویت و حتی حریم خصوصی بسیار مورد بررسی قرار گرفته است. در پروپوزال سال گذشته نیز هدف اصلی تحقیق را تشخیص داده های ارسالی غلط و جعلی در این شبکه های خودرویی بیرونی گذاشتیم. ولی بخش امنیت شبکه های داخل خودرویی (مانند امنیت CAN bus) مغفول مانده است، که مشخصاً موضوع مساله پروپوزال جاری است.

پروتکلهای ارتباطی درون خودرویی اغلب به امنیت هیچ توجهی نکرده اند و برخی بدلیل استانداردهای محدود کننده (مانند طول فریم بسیار کوتاه در CAN) قابلیت افزودن محافظ های رمزنگارانه را نیز ندارند. آلوده شدن یک یا چند ماجول خودرو که روی باس نشسته اند میتواند آثار فیزیکی بسیار خطرناکی داشته باشد و حتی جان مسافر را نیز به خطر بیاندازد. حملات پنهان دسته ای از حملات هستند که آثار آنها براحتی قابل رویت نیست اما اینگونه حملات آثار بلند مدت ملموسی را به جا میگذارند [2]. خطرناکترین نوع حمله برای خودروهای خودران و هوشمند در واقع این گونه از حملات هستند. هیچ راهی برای فلیتر کردن پیامهایی که اینگونه واحد های آلوده روی باس ارسال میکنند با روشهای تامین امنیت داده یا رمزنگاری وجود ندارد. چون در این حالت فرستنده یک عضو مشروع شبکه است. در نتیجه نیازمند روش‌هایی برای تشخیص آلودگی و

[1] Intelligent Transportation Systems

حمله سایبری و سپس مقابله با آنها هستیم. این یک چالش است که قصد داریم در این پروژه با ارایه معماری امنیتی ای سازگار با پروتکلهای موجود و سپس ابداع روشهای تحلیلی با آن به مقابله بپردازیم.

با توجه به تجارب موفق مجری در زمینه امنیت خودروهای هوشمند و نیز امنیت سامانه های سایبری-فیزیکی، و همچنین شبکه محققان همکار بین المللی وی که نتیجه تحقیقات مشترک آنها در این حوزه در بیش از ۱۸ نشریه معتبر Q1 به چاپ رسیده است، مسیر اجرای این پروژه در صورت تامین اعتبار روشن و هموار بنظر می رسد.

کارهای گذشته (پیشینه پژوهش)

سیستم های حمل و نقل هوشمند یکی از عناصر اصلی شهرهای هوشمند هستند [3]. بخش بزرگی از این شبکه حمل و نقل هوشمند را خودروهای هوشمند و خودران تشکیل میدهند که در معرض حملات سایبری هستند. حملات به این سیستمها به چند دسته تقسیم می‌شوند. ۱- حملات داخلی (شروع شده توسط وسایل نقلیه مخرب داخلی مجاز) و ۲- خارجی (راه اندازی شده توسط افراد خارجی). از منظر دیگر، حملات به دو دسته منفعل و فعال تقسیم می‌شوند [4]. حملات مخرب در این سیستمها ها می‌تواند جعل پیام، پخش مجدد پیام، خدشه به یکپارچگی، جعل هویت، ردیابی حرکت [5] و غیره باشد. اما بیشتر این موارد به حملات خارج خودرو اختصاص دارد. اجزای داخلی خودروهای هوشمند و خودران نیز میتوانند آلوده شده و خود منبع حمله شوند.

مرجع [6] چهار نوع حمله را که عملکرد خودرو را متاثر میکنند ارایه کرده است. بطور خاص، حمله به چراغ خطر، سیستم کنترل ایربگ، پنجره بالابر و مهمتر از همه، دروازه مرکزی CAN. بطور مشابه، مرجع [7] نیز تلاش نمود تعداد دیگری از حملات خودرویی را که امنیت خودرو و سرنشینانش را به مخاطره می اندازد معرفی کند. در مرجع [8]، سطوح حمله به خودروها از راه دور مطالعه شده و برای چندین خودرو، معماری شبکه داخلی و نحوه نفوذ احتمالی به آن مورد بررسی قرار گرفته است.

مولفان مرجع [9] یک مدل حمله و همچنین ارزیابی اثر آن بر روی یک سیستم کنترلی ارایه و مطالعه شده است. یکی از جنبه های این تحقیق، بررسی میزان مقاومت کنترلر در برابر حملات DoS و حملات تزریق بسته توسط دشمن بوده است. در مرجع [10]، حملات جعل روی سیستم جلوگیری از قفل ترمز (ABS) مورد بررسی قرار گرفته است. در سیستم ABS، عملگر های الکترومغناطیسی بکار میروند و در مقاله مورد بحث، سیگنالهای اندازه گیری توسط اختشاش الکترومغناطیسی تغییر داده شده و سیگنالهای مورد نظر دشمن به سنسور ها تزریق میشود. مرجع [11] نیز یک الگوریتم مقاوم جهت نظارت بر اساس روش آسایش شکل موج را پیشنهاد داد که برای منظور تشیخص حمله بکار میرود.

در مرجع [12]، نشان داده شد که چگونه در یک گروهان خودروها، حمله کنندگان سایبری به خودروها نفوذ میکنند و کنترل گروه را بدست میگیرند. مرجع [13] اثر حمله DoS را روی خودروهای متصل به هم بررسی کرده است. سپس یک روش کنترلی توسط این مقاله ارایه شده است که در گروهی از خودروهای مجهز به کنترل کروز تطبیقی که با همدیگر همکاری میکنند را در برابر حمله DoS تا حد ممکن مقاوم کند. در تحقیقات دیگری که به حملات خارجی خودرو میپردازند، منبع [14] و [15] پایداری خودروهای متصل به هم را در حضور تاخیر های شبکه مورد بررسی قرار داده است.

در یکی از مطالعات نزدیک به موضوع این پروژه، ما در [16] دو نوع حمله پنهان را به ماجول کنترل کروز تطبیقی (ACC) خودروهای هوشمند و خودران معرفی کردیم. این دو حمله از طریق تغییر جزئی شتاب خودروی دنبال کننده و یا تغییر مرجع کنترلی انجام میشوند. این حملات احتمال تصادف را در یک تعداد انبوه خودرو بطور ملموسی افزایش می دهند.

در مرجع [17]، ما یک حمله پنهان برای خودروهای خودرانی که خطوط جاده را دنبال میکنند بر اساس مفهوم یادگیری تخاصمی ارایه کردیم. در این حمله دشمن داده های خوانده شده از سنسور (یا خود سنسور) را تغییر میدهد به نحوی که انحراف از مرکز خط در مواردی بیش از حد نرمال شود. دشمن میزان این انحراف را پس از یادگیری (تقویتی) پاسخ خودرو (با استفاده از یک مدل Actor-

Critic) به مرور زمان تنظیم خواهد کرد. پس از طراحی حمله، ما یک روش کشف و جبران سازی چنین حملات داخلی ای را روی ماجول دنبال کننده خطوط ارایه کردیم.

کشف سریع نفوذ یک پارامتر مهم در حفظ ایمنی و کارایی سیستمهای همزمان[۲] میباشد. در این راستا، بسیاری از مکانزیم های کشف نفوذ برای خودروهای متصل پیشنهاد شده اند. برای مثال ما در مرجع [18] یک راه سریع تشخیص پیامهای دریافتی از سایر خودرو ها را بدون نیاز به اتکا به اشخاص ثالث مورد اعتماد ارایه کردیم. همچنین یک راهکار متمرکز برای تشخیص گرههای خرابکار در شبکه ارایه نمودیم. مرجع [19] یک الگوریتم برای تشخیص حمله تکرار پیام بر اساس راهبرد سیگنال کنترلی نویزی ارایه نمود. مراجع [20] و [21] نیز مدلهای کینماتیکی و ترکیب داده را برای توسعه یک الگوریتم تشخیص ناهنجاری بکار بردند. در [16]، یک الگوریتم تشخیص نفوذ بر اساس شبکه عصبی در این سیستمها توسعه داده شد. این الگوریتم شباهت زیادی به آنچه در [2] برای یک سیستم موتور DC به عنوان یک CPS خطی ارایه شده بود دارد. مرجع [17] یک سیستم تشخیص نفوذ بر اساس داده های GPS و نقشه های آفلاین برای سیستم دنبال کننده خودرو ارایه نمود.

همانگونه که ملاحظه شد، از کارهای ارایه شده تنها برخی به کشف نفود به ماجولهای داخلی خودرو پرداخته اند که اغلب آنها توسط ما در گذشته توسعه داده شده اند. در این تحقیق تجربه گذشته برای توسعه یک مدل جامع و یا به عبارتی یک چارچوب تشخیص نفوذ بکار گرفته خواهد شد.

دلایل انجام طرح

دلایل ضرورت اجرای این طرح بصورت فهرست وار در ذیل آمده است:

۱ -مساله ارتباط سیستم حمل و نقل با امنیت کشور. سیستمهای حمل و نقل که بخشی از آنها را خودرو ها و راهها تشکیل میدهند از جزء زیرساختهای حیاتی کشورها محسوب می شوند. با هوشمند شدن خودروها و سامانه ها و اتصال آنها به دنیای خارج، اصطلاحا سطوح حمله گسترش می یابد و امکان صدمه پذیری بوجود آمده و مخاطره افزایش می یابد. در حال حاضر خودروهای ساخت داخل ما عملا هیچ هوشمندی ای ندارند و از دنیا بسیار عقب افتاده ایم. در مورد خودروهای خودران نیز عملا هیچ کاری صورت نگرفته است. بنابراین حدس قریب به یقین آنست که بزودی با توجه به افزایش فاصله فناوری مجبوریم خودرهای هوشمند و خودران را عینا وارد کنیم و این به معنی پذیرفتن ریسکهای موجود در آنها بدون دانستن چیز زیادی در مورد میزان امنیتشان است. در گذشته، حمله به زیرساختهای حیاتی کشورها بیشتر یک فرضیه بود، اما پس از وقوع حمله استاکسنت در کشورمان اهمیت این موضوع در تمام دنیا آشکار شد. حمله سایبری به زیرساختهای تصفیه آب، شبکه توزیع برق، سیستمهای ناوبری، و ... در کشورها دیگر به حدی رخ می دهد که با یک جستجوی ساده حداقل چند خبر از این دست در سال یافت می شود. نتیجه این پژوهش میتواند راهی را ارایه کند تا بدون آنکه خللی به کارکرد خودرو وارد شود، یک ماجول بصورت اضافه شونده به خودرو متصل شده و امنیت آنرا بررسی و تامین نماید.

۲- نیاز مشارکت در تولید در زمینه خودروهای هوشمند یا خودران جهت امکان توسعه این صنعت در آینده کشور. بدیهی است که خودرو سازی سنتی ایران قادر به تولید خودروهای خودران و غیره نخواهد بود. اما میتواند در بخش خدمات ارزش افزوده (مانند شرکتهایی که برای اینترنت فایروال تولید میکنند) در این بازار حضور داشته باشد.

اهداف و محصولات طرح

طرح از نوع پژوهشی بوده و منجر به مقالات علمی و یا ثبت اختراع خواهد شد.. امکانسنجی اولیه تحقیق، انجام شده و پیشرفت ۹۰ درصدی داشته است. در حال حاضر مطمئن هستیم که این پژوهش به ثمر خواهد نشست.

[2] Real-time

برنامه و نحوه اجرای طرح

در مرحله ۱، روشهای پیشین که برای مساله تشخیص نفوذ در شبکه های درون خودرویی ارایه شده اند، بررسی میشوند.
در مرحله ۲، یک چارچوب تشخیص نفوذ برای شبکه های درون خودرویی مبتنی بر باس، ارایه میشود. برای این احتمالا کار از روشهای هوش مصنوعی نیز بهره گرفته خواهد شد.
در مرحله ۳، معماری طراحی شده در فاز ۲ برای یک حمله خاص پیاده سازی/شبیه سازی شده و مورد ارزیابی قرار خواهد گرفت.
مقالات نیز در این مرحله ارسال خواهند شد.

برنامه زمانی

مدت انجام این طرح، مطابق روال معمول پژوهشکده خواهد بود و در کمتر از ۱ سال به اتمام خواهد رسید.

شماره مرحله / فعالیت	نام مرحله/ فعالیت	درصد وزنی به کل پروژه	مدت زمان اجرا (ماه)	نمودار زمان‌بندی(ماه)											
				۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
۱	مطالعه روشهای پیشین تشخیص نفوذ برای شبکه های درون خودرویی	٪۲۰	۲												
۲	طراحی یک معماری تشخیص نفوذ برای شبکه های درون خودرویی مبتنی بر باس	٪۴۰	۵												
۳	پیاده سازی و شبیه سازی یک حمله و روش دفاع مبتنی بر معماری ارایه شده، ارزیابی مدلها و انتشار یافته های علمی	٪۴۰	۵												

همکاران طرح

همکار علمی طرح، دکتر فائزه فریور عضو هیئت علمی دانشگاه آزاد، واحد علوم و تحقیقات تهران است. سایر همکاران خارجی مانند دکتر علیرضا جلفایی از دانشگاه فلیندرز و دکتر مامون العزب از دانشگاه چارلز داروین نیز ممکن است در جریان تحقیق کمک نمایند.

ابزار مورد نیاز

کیفیت انجام پروژه و میزان واقعی بودن بستر تست و ارزیابی روشهای توسعه داده شده، به مقدار بودجه تصویب شده برای پروژه بستگی دارد. بطور ایده آل این پروژه نیاز به بستر لازم برای پیاده‌سازی عملی دارد. برای مثال باید یک خودروی واقعی مبتنی بر پروتکل CAN Bus را برای این مقصود در اختیار داشته باشیم. اما برای شبیه‌سازی و در مقیاس کوچک، با توجه به اینکه بسیاری از نرم افزارها قابل حصول بصورت آزمایشی و یا رایگان هستند، می توان در بخش پژوهشی و انتشار مقاله از آنها بهره برد.

بودجه تقریبی

میزان کار لازم برای این طرح در بخش پژوهشی حدود ۱۸ نفر ماه است که هزینه ای در حدود ۴۰۰/۰۰۰/۰۰۰ ریال برای آن پیش‌بینی شده است. اما هر گونه حمایت پژوهشگاه دانش های بنیادی کمک شایانی خواهد بود. هزینه ها به نسبت درصد وزنی در فازها توزیع می‌شوند.

مراجع

[1] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Engineering Journal*, vol. 54, no. 4. pp. 1115–1126, 2015.

[2] F. Farivar, M. S. Haghighi, S. Barchinezhad, and A. Jolfaei, "Detection and compensation of covert service-degrading intrusions in cyber physical systems through intelligent adaptive control," in *Proceedings of the IEEE International Conference on Industrial Technology*, 2019.

[3] Z. Xiong, H. Sheng, W. G. Rong, and D. E. Cooper, "Intelligent transportation systems for smart cities: A progress review," *Sci. China Inf. Sci.*, vol. 55, no. 12, pp. 2908–2914, 2012.

[4] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7. pp. 7–20, 2017.

[5] M. S. Haghighi and Z. Aziminejad, "Highly Anonymous Mobility-Tolerant Location-Based Onion Routing for VANETs," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2582–2590, 2020.

[6] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN Networks - Practical examples and selected short-term countermeasures," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008.

[7] C. Miller and C. Valasek, "Adventures in Automotive Networks and Control Units," *Tech. White Pap.*, 2013.

[8] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," *Defcon 22*, 2014.

[9] R. Van Der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (CACC)," in *IEEE Vehicular Networking Conference, VNC*, 2018.

[10] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013.

[11] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automat. Contr.*, 2013.

[12] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015.

[13] Z. A. Biron, S. Dey, and P. Pisu, "Resilient control strategy under Denial of Service in connected vehicles," in *Proceedings of the American Control Conference*, 2017.

[14] S. Oncu, J. Ploeg, N. Van De Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Network-aware analysis of string stability," *IEEE Trans. Intell. Transp. Syst.*, 2014.

[15] W. B. Qin, M. M. Gomez, and G. Orosz, "Stability analysis of connected cruise control with stochastic delays," in *Proceedings of the American Control Conference*, 2014.

[16] F. Farivar, M. S. Haghighi, A. Jolfaei, and S. Wen, "On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control," *IEEE Trans. Intell. Transp. Syst.*, 2021.

[17] F. Farivar, M. S. Haghighi, A. Jolfaei, and S. Wen, “Covert Attacks through Adversarial Learning: Study of Lane Keeping Attacks on the Safety of Autonomous Vehicles,” *IEEE/ASME Trans. Mechatronics*, 2021.
[18] I. Mirzadeh, M. S. Haghighi, and A. Jolfaei, “Filtering Malicious Messages by Trust-Aware Cognitive Routing in Vehicular Ad Hoc Networks,” *IEEE Trans. Intell. Transp. Syst.*, 2022.
[19] R. Merco, Z. A. Biron, and P. Pisu, “Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control,” in *Proceedings of the American Control Conference*, 2018.
[20] F. Alotibi and M. Abdelhakim, “Anomaly Detection for Cooperative Adaptive Cruise Control in Autonomous Vehicles Using Statistical Learning and Kinematic Model,” *IEEE Trans. Intell. Transp. Syst.*, 2021.
[21] F. Alotibi and M. Abdelhakim, “Anomaly detection in cooperative adaptive cruise control using physics laws and data fusion,” in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019, pp. 1–7.

نام و نام خانوادگی متقاضی: دکتر محمد صیادحقیقی– دانشیار دانشگاه تهران تـــاریـــخ: ۱۴۰۱/۱۱/۱۱