Archive of SID

ارائه مکانیزم انگیزشی برای مشارکت خودروها در رایانش ابری خودرویی با حفظ حریم خصوصی

مهین نادری‌پور[۱]، توسکا درگاهی[۲]، احمدخونساری[۳]

[۱]دانشکده مهندسی برق و کامپیوتر، پردیس دانشکده‌های فنی، دانشگاه تهران، m.naderipoor@ut.ac.ir

[۲]دانشکده مهندسی الکترونیک، دانشگاه رم تر ورگاتا، tooska.dargahi@uniroma2.it

[۳]دانشکده مهندسی برق و کامپیوتر، پردیس دانشکده‌های فنی، دانشگاه تهران، ak@ipm.ir

چکیده

خودروهای پیشرفته و گران‌قیمت، تجهیزات و حسگرهایی دارند که در اکثر اوقات بلااستفاده باقی مانده‌اند. فراهم کردن شرایطی که خودروها بتوانند منابع مازاد خود را در اختیار دیگران قرار دهند یکی از انگیزه‌های شکل‌گیری ابرخودرویی بوده است. در ابرخودرویی همانند رایانش ابری، خودروها می‌توانند درخواست‌هایی همچون انجام محاسبات، دریافت اطلاعات و غیره را به ابرخودرویی داده و سرویس مدنظر خود را دریافت کنند. اکثر سرویس‌هایی که ابرخودرویی ارائه می‌دهد به عنوان سرویس‌های ارزش افزوده شناخته می‌شوند و خودروها می‌بایست به ازای دریافت آن‌ها هزینه پرداخت کنند. پرداخت هزینه سرویس‌ها به صورت بین خودرویی مساله چالش برانگیزی است چراکه هر دو موجودیت سرویس‌دهنده و سرویس‌گیرنده متحرک هستند. همچنین مساله مربوط به حفظ حریم خصوصی سرویس‌دهنده و سرویس‌گیرنده نیز چالش‌هایی را به همراه دارد. در این مقاله به منظور پرداخت هزینه سرویس‌ها و به تبع آن تشویق خودروها به شرکت در ابرخودرویی، از مکانیزم انگیزشی مبتنی بر توکن بهره گرفته شده است. مجازی بودن ماهیت توکن، آن را مستعد سوء استفاده‌های بسیاری می‌کند. اگر ساختار مناسبی برای ایجاد و پرداخت توکن وجود نداشته باشد، استفاده از توکن می‌تواند منجر به نقض حریم خصوصی سرویس‌گیرنده همچون ردیابی سرویس‌گیرنده توسط سایر خودروها یا مرجع صادرکننده توکن گردد. به‌علاوه مسایلی مانند استفاده چندباره توکن به صورت غیرقانونی نیز یکی از مهم‌ترین چالش‌ها است. به همین دلیل در ادامه راهکاری برای پرداخت هزینه سرویس‌ها به صورت بین خودرویی با حفظ حریم خصوصی ارائه شده است به نحوی که از استفاده مجدد توکن جلوگیری می‌کند. در نهایت راهکار پیشنهادی از نقطه نظر امنیت، حریم خصوصی، سربار ارتباطی، بارکاری، مقیاس‌پذیری و استفاده مجدد توکن مورد ارزیابی قرار گرفته است.

واژه‌های کلیدی

حریم خصوصی، رایانش ابری خودرویی، رایانش ابری، شبکه‌های موردی بین خودرویی، تشخیص استفاده مجدد

۱- مقدمه

با قرار داشتن در عصر ارتباطات، دورانی در حال تجربه شدن است که در آن فن‌آوری‌های موجود در تعامل با یکدیگر موجب ابداع فن‌آوری‌های نوین شده‌اند. رایانش ابری خودرویی[1] نمونه‌ای از این فن‌آوری‌ها و حاصل تلفیق فن‌آوری رایانش‌ابری[2] با شبکه‌های موردی بین‌خودرویی[3] بوده است. رایانش ابری خودرویی (ابرخودرویی) به شبکه‌ای از خودروها گفته می‌شود که منابع محاسباتی، ذخیره‌سازی، ارتباطی و حسگری خود را به صورت سازماندهی شده و پویا به کاربران مجاز تخصیص می‌دهند [۱].

ابرخودرویی بستری را فراهم می‌کند تا با استفاده از آن به رخدادهایی که نمی‌توان از قبل سرمایه‌هایی را برای پاسخ‌دهی به آن‌ها در نظر گرفت، پاسخ سریع و به‌هنگام داد. با توجه به ماهیت ابرخودرویی، چالش‌های زیادی در این حوزه مطرح شده است. مدیریت منابع، کیفیت داده، احراز اصالت خودروهای با تحرک بالا، قابلیت اعتماد، قابلیت گمنامی، حفظ حریم خصوصی کاربران و مالکین خودروها، خودخواهی خودروها در مشارکت و غیره نمونه‌ای از این چالش‌ها هستند [۲]-[۴]. برای مقابله با چالش مربوط به امنیت و حریم خصوصی در این حوزه، از تکنیک مجازی‌سازی و تکنیک‌های گمنام‌سازی مانند نام‌مستعار و رمزنگاری داده‌های حساس استفاده شده است. یکی‌دیگر از مسایلی که در ابرخودرویی چالش‌برانگیز است مساله عدم مشارکت خودروها است. درواقع با توجه به اختیاری بودن مشارکت خودروها، ممکن است برخی خودروها تمایلی به شرکت در ابرخودرویی نشان ندهند. به همین دلیل می‌بایست راهکارهایی برای تشویق خودروها به شرکت در ابرخودرویی ارایه کرد.

[1] Vehicular cloud computing

[2] Cloud computing

[3] Vehicular ad-hoc network

www.SID.ir

Archive of SID

در حوزه‌های مختلف برای مقابله با مساله عدم همکاری اعضای شبکه مکانیزم‌های انگیزشی بسیاری ارائه شده است [۵]، [۶]. این مکانیزم‌های انگیزشی به دو دسته مبتنی بر اعتبار و مبتنی بر شهرت تقسیم‌بندی شده‌اند. در روش مبتنی بر اعتبار(توکن)، گره‌ها می‌بایست برای استفاده از منابع شبکه، هزینه آن منابع را پرداخت کنند. در حالی که روش مبتنی بر شهرت، یک رویکرد کنترلی برای شناسایی گره‌های بدرفتار ارائه می‌کند. در این روش، گره‌ها ترافیک همسایگانشان را نظارت کرده و مشارکت آن‌ها در شبکه را ذخیره می‌کنند. در صورتی که سهم مشارکت آن‌ها در شبکه کم باشد آن‌ها را ایزوله کرده و با آن‌ها تعامل برقرار نمی‌کنند. کیهو لیم[1]و همکاران در مقاله [۷] برای اولین بار یک معماری انگیزشی مبتنی بر توکن برای مقابله با عدم همکاری خودروها در ابرخودرویی ارائه دادند. در این معماری که برگرفته از چارچوب معماری VuC[2] است [۸]، وظیفه کنترل تراکنش‌ها بر عهده موجودیت‌های تعریف شده در ابر سنتی قرار دارد. در معماری VuC، خودروها به‌واسطه واحدهای کنارجاده‌ای[3] به ابرسنتی متصل شده و از آن سرویس دریافت می‌کنند و یا وظیفه‌ای را در قالب سرویس برای ابرخودرویی انجام می‌دهند.

در این مقاله برای تشویق خودروها به شرکت در ابرخودرویی از مکانیزم انگیزشی مبتنی بر توکن استفاده شده است. با توجه به این‌که در ابرخودرویی برخی خودروها به‌عنوان سرویس‌دهنده و برخی به‌عنوان سرویس‌گیرنده (کارگزار[4]) عمل می‌کنند. هر خودرو سرویس‌دهنده می‌تواند به ازای ارائه سرویس به دیگران از آن‌ها توکن دریافت می‌کند. توکن، پول الکترونیکی است و ماهیت فیزیکی ندارد. مجازی بودن ماهیت توکن، آن را مستعد سوء استفاده‌های بسیاری می‌کند. اگر ساختار مناسبی برای ایجاد و پرداخت توکن وجود نداشته باشد، مرجع صادرکننده و یا سایر خودروها می‌توانند خودرو سرویس‌گیرنده را شناسایی کرده، مکان فیزیکی، الگوی حرکتی و الگوی دسترسی وی به داده‌های شبکه خودرویی را تشخیص دهند. به این ترتیب، استفاده از توکن می‌تواند منجر به نقض حریم خصوصی سرویس‌گیرنده گردد و یا مسایلی مانند استفاده چندباره توکن به صورت غیرقانونی پدید آید.

به منظور کاهش بارکاری سرور، کاهش تاخیر در پرداخت‌های الکترونیکی بین خودروها و افزایش گمنامی از پرداخت به صورت برون‌خط[5] استفاده شده است. در پرداخت به صورت برون‌خط وظیفه کنترل تراکنش‌ها به خودروها سپرده می‌شود. با توجه به پویایی بسیار بالای شبکه خودرویی، انتخاب شاهد از بین خودروها مساله چالش برانگیزی است. به همین دلیل با محدود کردن اعتبار توکن به یک ابرخودرویی، به دنبال تسهیل روند انتخاب شاهد و افزایش امکان تشخیص استفاده مجدد توکن هستیم. در نهایت راهکار پیشنهادی از نقطه نظر امنیت، حریم خصوصی، سربار ارتباطی، بارکاری، مقیاس‌پذیری و استفاده مجدد توکن مورد ارزیابی قرار گرفته است.

۲- مدل و فرضیات شبکه

جهت اجرای طرح پیشنهادی، ویژگی‌هایی برای شبکه، واحدهای کنارجاده‌ای و خودروها در نظر گرفته شده است. در مورد محیط شبکه، مشابه با آنچه در مقاله [۹] ارائه شده است فرض بر این است که شبکه خودرویی متشکل از زیرشبکه‌هایی است که با یکدیگر وجه اشتراکی ندارند. هر زیرشبکه به عنوان یک سلول شناخته شده و یک منطقه جغرافیایی را پوشش می‌دهد. این دیدگاه مشابه با شبکه تلفنی سلولی است. سلولی در نظر گرفتن محیط، مزایایی را به همراه دارد که عبارتند از محلی‌شدن ارتباطات، مقیاس‌پذیری و سفارشی‌سازی امنیت و حریم خصوصی. تعیین اندازه سلول وابسته به فاکتورهایی همچون بازه ارتباطی DSRC[6](بین ۳۰۰ تا ۱۰۰۰ متر)، میزان نیاز به ارتباط با سایر خودروهای درون سلول و غیره است.

در میانه هر سلول، یک واحد کنار جاده‌ای مستقر شده است که وظیفه نظارت بر کل سلول را برعهده دارد. درون هر واحد کنار جاده‌ای یک سرور به عنوان یک موجودیت قابل اعتماد[7] تعبیه شده است. این سرور وظیفه تخصیص نام مستعار[8]، صدور مجوز[9]و کلید ابرخودرویی، تخصیص و بازخریدکردن توکن‌ها در شبکه را بر عهده دارد. در این‌جا فرض بر این است که سرور سلول مورد سوء استفاده قرار نمی‌گیرد.

هر خودرو ، مجهز به یک واحد درون خودرو به نام OBU [10]، یک سیستم موقعیت‌یاب جهانی[11] و یک فرستنده/گیرنده بی‌سیم سازگار با فن‌آوری DSRC، سه دسته منبع محاسباتی، ذخیره‌سازی و حسگری است. واحد درون خودرویی علاوه بر وظیفه برقراری ارتباط با سایر خودروها/زیرساخت، وظیفه نگهداری کلید عمومی/خصوصی خودرو، نام‌های مستعار خودرو، اطلاعات مالی خودرو و سایر اطلاعات محرمانه مربوط به خودرو را نیز برعهده دارد. خودروها در این‌جا به عنوان موجودیت‌هایی خودخواه[12]، کنجکاو[13] و حساس به حریم خصوصی[14] و منطقی[15] در نظر گرفته می‌شوند. خودخواه بودن یعنی خودروها همواره تمایل به استفاده از منابع دیگران دارند اما خودشان منبعی را برای استفاده دیگران به اشتراک

[1] Kiho Lim
[2] Vehicles using clouds
[3] Road Side Unit
[4] Broker
[5] Offline

[6] Dedicated Short Range Communications
[7] Trusted
[8] pseudonyms
[9] Digital Certificate
[10] On Board Unit
[11] GPS
[12] Selfish
[13] Curious
[14] Privacy sensitive
[15] rational

www.SID.ir

Archive of SID

نمی‌گذارند. کنجکاو و حساس بودن نسبت به حریم خصوصی یعنی کاربران تمایلی به افشا اطلاعات خود ندارند اما همواره علاقه‌مند هستند تا در مورد دیگران کسب اطلاعات کنند. منطقی بودن یعنی خودروها تنها در صورتی که به نفع‌شان باشد، اقدام به بدرفتاری می‌کنند.

در شبکه خودرویی، مرکز کنترل و پایش به عنوان یک موجودیت قابل اعتماد در شبکه، وظیفه ثبت خودروها و نظارت بر سرورهای شبکه را بر عهده دارد. هر خودرو و واحد کنارجاده‌ای هنگام ورود به شبکه یک کلید عمومی/خصوصی از مرکز کنترل و پایش دریافت می‌کنند تا در مواقع لزوم با استفاده از آن ارتباط امنی را با یکدیگر برقرارکنند. مرکز کنترل و پایش برای هر خودرو یک اکانت در پایگاه داده خود ایجاد کرده و دو نوع اعتبار مالی و شهرت برای وی در نظر می‌گیرد.

برای تشکیل ابرخودرویی، سرویس‌گیرنده نیازمند دریافت مجوز از سرور سلول است تا با استفاده از آن اعتبار خود را در شبکه تایید کند. همچنین سرویس گیرنده برای برقراری ارتباط با اعضا ابر نیازمند کلیدی است که به آن کلید ابر گفته می‌شود. این کلید به همراه مجوز به خودرو سرویس گیرنده داده می‌شود. با توجه به معماری‌های متفاوتی که برای ابرخودرویی در مقالات مختلف ارائه شده است[۸]،[۳] معماری VC[1] به عنوان معماری مبنا در این مقاله مورد استفاده قرار گرفته است. در این معماری خودروها منابع خود را با یکدیگر به اشتراک گذاشته و ابرخودرویی را در حین حرکت و یا در حالت ایستا شکل می‌دهند.

۳- مدل تهدید

تهدیدهای مختلف در حوزه امنیت و حریم خصوصی در مدل مورد نظر عبارتند از: شناسایی خودروها از طریق برقراری ارتباط میان شناسه اصلی خودرو و نام مستعار آن و یا بین دو نام مستعار، استراق سمع منفعل با نصب یک دستگاه گیرنده قوی در بخشی از شبکه، افشا اطلاعات[2]، انکار[3]، فریب دادن دیگران با جعل هویت[4].

۴- راهکار پیشنهادی

۴-۱- ساختار مورد استفاده برای نام‌های مستعار

در روش پیشنهادی، هر نام مستعار مشابه با ساختار آدرس‌های آیپی، از دو بخش شناسه سلول (معادل با نام شبکه در ساختار آدرس‌های آیپی) و شناسه خودرو (معادل با نام هاست در ساختار آدرس‌های آیپی) تشکیل شده است. بخش اول نام مستعار، شناسه سلول است که به صورت منحصر به فرد برای هر سلول توسط مرکز کنترل و پایش تعیین شده است. بخش دوم یک عدد تصادفی است که به عنوان شناسه منحصر به فرد خودرو در آن سلول محسوب می‌شود. این شناسه توسط سرور سلول برای هر خودرویی که درون آن سلول باشد و نیاز به ارتباط با سایر اعضای آن سلول داشته باشد تولید و نگهداری می‌شود. در واقع در این‌جا سرور سلول مشابه با سرور DHCP در شبکه عمل می‌کند. این نام مستعار نشان‌دهنده این است که خودرو درون این سلول حضور دارد و این ساختار برای نام‌های مستعار به مسیریابی بسته‌ها در شبکه خودرویی کمک می‌کند.

نام‌های مستعار می‌بایست مدت اعتبار مشخصی داشته باشند تا مهاجمان نتوانند از آن‌ها سوء استفاده کنند. به همین منظور برای نام‌های مستعار برچسب زمانی(TS)[5] در نظر گرفته می‌شود. در صورتی که زمان تعیین شده در برچسب زمانی به صفر برسد، نام مستعار اعتبار خود را از دست می‌دهد و خودرو می‌بایست مجددا درخواست دریافت نام مستعار دهد. علاوه بر برچسب زمانی، درصورتی که خودرو از سلول خارج شود، نام مستعار وی منقضی می‌گردد و خودرو نمی‌تواند از آن نام در سلول‌های دیگر استفاده کند. هر خودرو در صورتی که نیاز به برقراری ارتباط با سایر خودروهای درون سلول داشته باشد، قبل از برقراری ارتباط می‌بایست به سرور سلول درخواست دریافت نام مستعار بدهد. مراحل درخواست و دریافت نام مستعار در سه مرحله به صورت زیر انجام می‌شود.

۱. خودرو درخواست دهنده، پیغام خود مبنی بر دریافت نام مستعار را با کلیدعمومی سرور سلول رمز کرده و برای وی ارسال می‌کند.
۲. سرور به محض دریافت پیغام، با کلید خصوصی خود آن را رمزگشایی کرده و بعد از بررسی اصالت خودرو، در صورتی که شرایط دریافت نام مستعار را داشته باشد (یکی از شرایط، حضور فیزیکی داشتن در سلول است) یک نام مستعار برای خودرو تولید کرده و به وی ارسال می‌کند.
۳. خودرو بعد از دریافت پیغام و بازگشایی آن به نام مستعار خود دست می یابد. از این پس تا زمانی که نام مستعار خودرو اعتبار داشته باشد، خودرو از آن نام برای دریافت سرویس و برقراری ارتباط با سایر خودروهای درون سلول استفاده می‌کند.

۴-۲- نحوه تشکیل و سرویس‌دهی ابرخودرویی

در این پژوهش، روند تشکیل ابرخودرویی به صورت زیر است.

هر خودرو در صورتی که درخواستی برای انجام داشته باشد، اقدام به تشکیل ابر می‌کند. برای این منظور در ابتدا درخواست دریافت مجوز به همراه تعداد توکن مورد نیاز خود را به سرور سلول ارسال می‌کند. سرور سلول با دریافت این درخواست، از مرکز کنترل و پایش در مورد اعتبار مالی و شهرت خودرو پرس و جو کرده و با توجه به اطلاعات دریافتی، جدولی را برای هر خودرو در پایگاه داده خود ایجاد می‌کند. در صورتی که اعتبار شهرت و مالی خودرو از حد آستانه تعیین شده کمتر باشد، سرور مجوز تشکیل ابر را برای وی صادر نمی‌کند. در غیر این صورت مجوز برای خودرو صادر شده و به همراه کلید ابر به وی ابلاغ می‌گردد (گام ۱ در شکل ۱). خودرو با استفاده از مجوز، خود را به سایر خودروهای درون سلول معرفی

[1] Vehicular Cloud
[2] Information Disclosure
[3] Repudiation
[4] Spoofing of user identity
[5] Time Stamp

www.SID.ir

Archive of SID

می‌کند و با استفاده از کلید ابر با اعضا شرکت کننده در ابرخودرویی ارتباط برقرار می‌کند.

در صورتی که به علت کمبود اعتبار، برای خودرو مجوز صادر نگردد، علت عدم صدور مجوز به وی اطلاع داده می‌شود. اگر علت عدم صدور مجوز کمبود اعتبار شهرت خودرو باشد در این صورت خودرو می‌بایست با شرکت در سایر ابرهای خودرویی ایجاد شده و انجام درست کارهایی که به وی محول شده اعتبار شهرت خود را افزایش دهد تا بتواند در صورت نیاز به تشکیل ابر، مجوز دریافت کند. نکته‌ای که در اینجا وجود دارد این است که این اعتبار در صورت بروز تخلف به صورت تصاعدی (نسبت تصاعد ۲) کاهش و در صورت انجام درست کارهای محول شده به خودرو به صورت عددی (نسبت عددی ۱) افزایش می‌یابد. تصاعدی بودن کاهش اعتبار و عددی بودن افزایش اعتبار انگیزه‌ای برای تخلف کمتر است چراکه جبران آن سخت و زمان‌بر است. اگر علت عدم صدور مجوز کمبود اعتبار مالی خودرو باشد در این صورت خودرو ممکن است درخواست افزایش اعتبار را به مرکز کنترل و پایش اعلام کند و مجددا بعد از افزایش اعتبار اقدام به دریافت مجوز نماید و یا ممکن است در ابرهای خودرویی دیگر شرکت کرده و توکن دریافت کند و با استفاده از توکن‌های دریافتی اعتبار مالی خود را افزایش دهد.

بعد از دریافت مجوز، خودرو نیاز به دریافت توکن از سرور دارد تا با استفاده از آن پرداخت‌های خود را انجام دهد (گام ۲ در شکل ۱). نحوه درخواست و دریافت توکن در بخش ۴-۳ به تفصیل بیان شده است. خودرو سرویس‌گیرنده با استفاده از مجوز دریافتی از سرور سلول، اقدام به اجرای فرایند تشکیل ابرخودرویی می‌کند [۱۰]. فرایند تشکیل ابرخودرویی از چندین فاز به شرح زیر تشکیل شده است (گام ۳ در شکل ۱):

فاز کشف منابع[1]: خودروی سرویس‌گیرنده در قالب کارگزار پیغام REQ را به همراه مجوز خود در شبکه منتشر می‌کند و از سایر خودروها دعوت می‌کند تا در فرایند شکل‌گیری ابر شرکت کنند. هر خودرویی که تمایل به شرکت در ابرخودرویی داشته باشد منابعی که در اختیار دارد را در قالب پیغام REPs به کارگزار اعلام می‌کند.

فاز شکل‌گیری ابر[2]: کارگزار با دریافت پیغام‌های REPs از جانب داوطلبان، آن خودروهایی را انتخاب می‌کند که الگوی حرکتی مشابه‌ای با وی داشته باشند یعنی سرعت و جهت حرکت آن‌ها تا حدی مشابه بوده و فاصله آن‌ها از هم کم باشد. کارگزار این مساله را می‌تواند با محاسبه موقعیت مکانی خودروها در دو بازه زمانی متفاوت به دست آورد. هدف کارگزار به انجام رساندن کار با صرف حداقل منابع است به همین دلیل، منابع همه خودروهای داوطلب را به کار نمی‌گیرد و تنها به مقدار مورد نیاز از منابع استفاده می‌کند. با این کار به سایر خودروها نیز اجازه می‌دهد در صورت نیاز ابری را تشکیل داده و از منابع موجود استفاده کنند.

[1] Cloud resource discovery

[2] Cloud formation

فاز پرداخت[3]: کارگزار قبل از استفاده از منابع خودروهایی که اعلام آمادگی کرده‌اند می‌بایست هزینه اجاره منابع آن‌ها را پرداخت کند و در صورتی که پرداخت با موفقیت انجام شود خودرو متقاضی، منبع خود را برای مدت مشخص و تعیین شده در اختیار ابر قرار می‌دهد. روند پرداخت در بخش ۴-۴ به تفصیل بیان شده است.

فاز تخصیص منابع و جمع‌آوری نتایج[4] : کارگزار، کار خود را به تعداد واحدهای کاری مشخص شده شکسته و هر واحدکاری را برای انجام به یک خودرو تخصیص می‌دهد. سپس جدولی آماده کرده و در آن جدول ثبت می‌کند که هر کار به چه خودرویی تخصیص داده شده است.

فاز انتشار محتوی[5]: کارگزار بعد از جمع‌آوری نتایج از اعضا و تجمیع آن‌ها، محتوی به‌دست آمده را در صورت نیاز در شبکه منتشر می‌کند.

فاز نگهداری[6]: در ابرخودرویی، هریک از اعضا که قصد خروج از ابر را داشته باشند درخواست خروج خود را به کارگزار می‌دهند. کارگزار به ازای هر خودروی خروجی، خودرویی دیگری را از بین خودروهایی که در فاز کشف منابع اعلام آمادگی کرده بودند به عنوان جایگزین خودروی خارج شده انتخاب می‌کند تا کار مربوط به خودروی خروجی را انجام دهد. البته با توجه به تحرک بالای خودروها، کارگزار، قبل از انتخاب خودرو جایگزین می‌بایست در مورد حضور خودرو در آن بخش از شبکه مطمئن شود. در نهایت کارگزار، کار را به خودرو انتخابی تخصیص داده و جدول خود را به روز می‌کند. در صورتی که خودرویی ناگهانی از ابر خارج شود (به علت تغییر سلول و یا خراب شدن) اگر بعد از مدت زمان مشخصی هیچ پیغامی از وی دریافت نشود کارگزار آن خودرو را به عنوان خودروی خروجی درنظر می‌گیرد.

فاز آزادسازی ابر[7]: هنگامی که کارگزار بخواهد ابرخودرویی را متلاشی کند در این صورت ابتدا یک پیغام آزادسازی منابع به همه اعضا ارسال کرده سپس لیست اعضا را حذف می‌کند. از این پس خودروها آزاد هستند تا در هر ابرخودرویی دیگری شرکت کنند.

۴-۳- ساختار توکن و نحوه دریافت آن

در این مقاله، به منظور حفظ گمنامی و حریم خصوصی متقاضیان توکن، از امضای کور [۱۱] برای ایجاد توکن استفاده می‌گردد. به این ترتیب خودروهای متقاضی توکن به توکنی دست می‌یابند که هیچ نشانی از هویت آن‌ها را در برندارد. در نتیجه این خودروها به راحتی و بدون نگرانی از افشا هویت‌شان می‌توانند آن توکن را در شبکه خرج کنند. فرایند امضای کور در حالت کلی به این صورت است که خودرو متقاضی توکن، به تعداد مورد نیاز، عدد تصادفی (m) تولید کرده و بعد از انجام عملیات کوری بر روی

[3] payment

[4] Task assignment and result collection

[5] Content publishing and sharing

[6] Cloud maintenance

[7] Cloud release

www.SID.ir

Archive of SID

آن‌ها، حاصل را برای سرور سلول ارسال می‌کند. سرور سلول بعد از تایید درخواست خودرو، با استفاده از کلید خصوصی خود، تک تک مقادیر کور شده را امضا کرده و نتیجه (σ^*_m) را به خودرو برمی‌گرداند. خودرو با استفاده از فاکتور کور، پیغام را رمزگشایی کرده و حاصل $<m , \sigma_m>$ را به عنوان توکن خود در نظر می‌گیرد. در این حالت اگر سرور سلول و یا هر موجودیت دیگری توکن را دریافت کند، از روی آن توکن نمی‌تواند مالک آن را تعیین کند اما می‌تواند توکن را اعتبارسنجی کند چراکه امضای سرور سلول بر روی آن وجود دارد. به این ترتیب حریم خصوصی دارنده توکن حفظ می‌شود. جزییات بیشتر این روش را می‌توان در مقالات [۱۲]، [۱۱] مطالعه کرد. دقت کنید که اگر توکن با نام مستعار خودرو امضا شده باشد در این صورت، سرور سلول می‌تواند تمام فعالیت‌های آن خودرو را تحت کنترل داشته باشد. این مساله ممکن است مخالف با علاقه‌مندی خودروها باشد و حریم خصوصی آن‌ها را نقض کند.

۴-۴- پرداخت

به منظور انجام عمل پرداخت در محیط خودرویی می‌بایست شاهد یا شاهدانی وجود داشته باشند تا در مورد صحت پرداخت اظهار نظر کنند تا به این ترتیب از سوء استفاده توکن و استفاده چندباره آن توسط یک فرد جلوگیری شود. با توجه به پویایی محیط، تحرک بالا و الگوی حرکتی خاص خودروها در شبکه خودرویی انتخاب شاهدانی از بین خودروها برای کنترل تراکنش‌ها مساله چالش برانگیزی است. به همین دلیل اولین راهکاری که به ذهن می‌رسد، انتخاب سرور سلول به عنوان شاهد تراکنش‌ها است. انتخاب سرور سلول به عنوان شاهد تراکنش‌ها به خاطر ماهیت متمرکز بودن آن مشکلاتی از قبیل نقطه شکست، افزایش بارکاری، کاهش راندمان و غیره را به همراه دارد به همین دلیل می‌بایست به دنبال راهکارهایی بود تا بتوان از خودروها به عنوان شاهدان تراکنش‌ها استفاده کرد. در ادامه با توجه به فرضیاتی که برای ساختار توکن و نوع مجوز ابرخودرویی در نظر گرفته شده است، راهکاری برای این منظور پیشنهاد شده است.

فرضیات:

در این رویکرد، مجوز تشکیل ابری که به خودرو کارگزار داده می‌شود یکبار مصرف است و کارگزار تنها یکبار با استفاده از این مجوز می‌تواند اقدام به تشکیل ابر نماید. این مجوز با کلید سرور سلول امضا شده است در نتیجه برای همه اعضا سلول معتبر است. مجوزهای تشکیل ابر، مدت اعتبار مشخصی دارند و در صورت اتمام مدت اعتبارشان به هیچ عنوان نمی‌توان با استفاده از آن‌ها اقدام به تشکیل ابر کرد. از طرفی سرور سلول توکن‌هایی را که برای کارگزار صادر می‌کند ابتدا با کلید ابر و سپس با کلید سرور سلول امضا می‌کند (ترتیب امضا توکن مانع از تخلف کارگزار می‌گردد). به این ترتیب توکن‌ها تنها درون همان سلول و همان ابرخودرویی قابل استفاده و معتبر هستند.

نحوه پرداخت:

در این روش، هر خودرویی که عضو ابر است به عنوان شاهدی برای توکن محسوب می‌شود و همه توکن‌هایی که توسط وی یا دیگران مصرف شده است را در بانک اطلاعاتی خود ذخیره می‌کند. نحوه پرداخت به این صورت است که خودرو سرویس‌دهنده با دریافت توکن $<m , \sigma_m>$ از کارگزار، پایگاه‌داده خود را بررسی می‌کند و اگر m را در پایگاه‌داده خود داشته باشد متوجه می‌شود که توکن قبلا استفاده شده است؛ در غیر این صورت توکن را پذیرفته و m را در ابر منتشر می‌کند تا سایر اعضای ابر نیز آن را در پایگاه داده خود ذخیره کنند. باتوجه به این‌که اعضا ابر به σ_m دسترسی ندارند در نتیجه نمی‌توانند از توکن سوء استفاده کنند. و تنها می‌توانند به عنوان شاهدین توکن از این‌که آن توکن قبلا استفاده شده است یا نه مطلع گردند. (گام ۴ در شکل ۱)

در صورتی که کارگزار، به علت خروج عضوی از ابر، خودروی دیگری را به ابرخودرویی اضافه کند، آن خودرو در ابتدا می‌بایست در مورد تاریخچه ابر از سایر اعضای ابر پرس و جو کرده و پایگاه‌داده خود را به روز کند تا به این ترتیب بتواند شاهدی برای توکن‌ها محسوب گردد. در صورتی که بعد از اتمام مدت زمان اعتبار مجوز و منحل شدن ابرخودرویی توکنی برای خودرو کارگزار باقی‌مانده باشد می‌بایست مجددا آن توکن را برای استفاده در ابرخودرویی دیگر بازخرید کند و نمی‌تواند عینا آن توکن را در ابر دیگری مصرف کند. تخلفی که ممکن است در این‌جا صورت پذیرد عدم تعهد سرویس‌دهنده در اجرای درست وظایف‌اش است. در این صورت کارگزار می‌تواند مراتب را به سرور سلول اعلام کند و از وی بخواهد که خودرو متخلف را تنبیه کند. سرور بعد از اطمینان از صحت گزارش، تخلف را برای خودرو متخلف ثبت کرده و از اعتبار شهرت خودرو کسر می‌کند. فلوچارت مربوط به مدل و راهکار پیشنهادی را می‌توان در شکل ۱ مشاهده کرد.

۵- ارزیابی

در این بخش به ارزیابی راهکار پیشنهادی از نقطه نظر امنیت، حریم خصوصی، سربار ارتباطی، بارکاری، مقیاس‌پذیری و استفاده مجدد توکن پرداخته شده است.

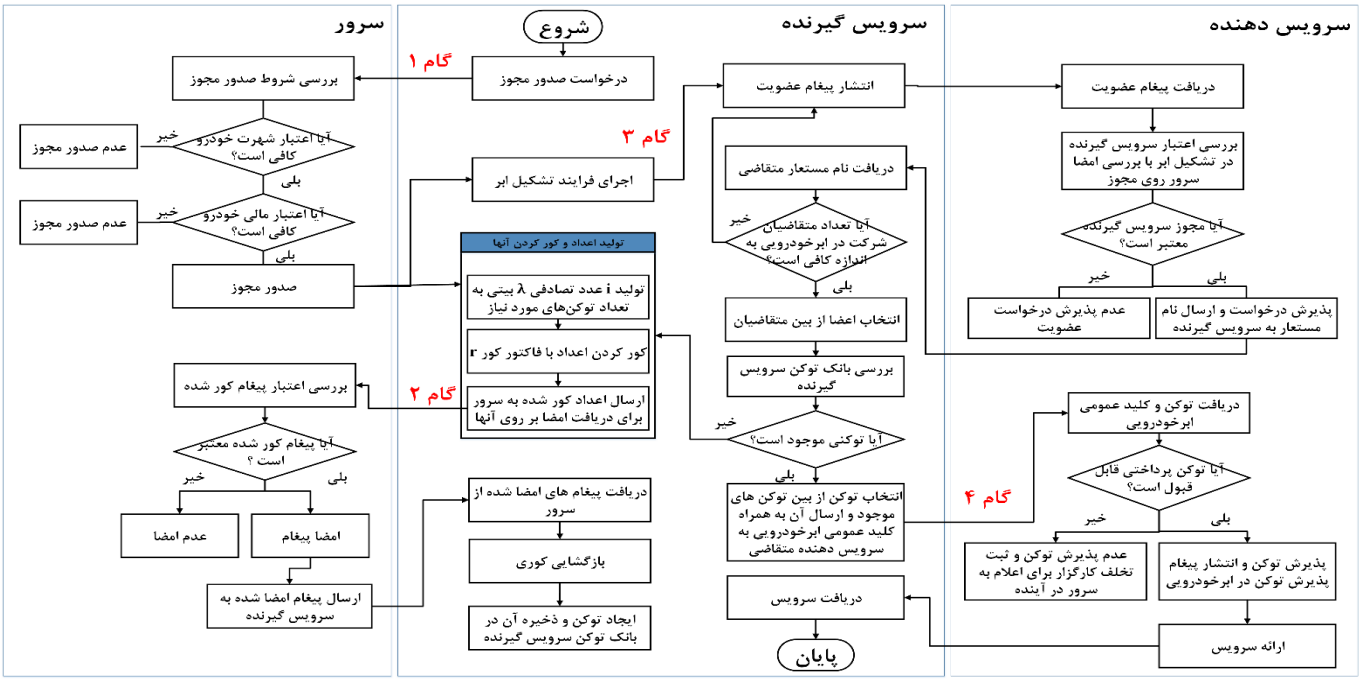
۵-۱- امنیت

غیرقابل‌جعل بودن: با توجه به ماهیت امضا دیجیتال، هیچ موجودیتی قادر نیست امضای موجودیت دیگری را جعل کند و همین مساله تاییدی بر غیرقابل جعل بودن توکن است.

حملات منع سرویس: با توجه به این‌که در هر سلول تنها یک سرور وجود دارد در نتیجه این سرور در معرض حمله منع‌سرویس قرار دارد. برای کاهش تاثیر این حمله می‌توان در نظر گرفت که اگر درخواست از خارج از محدوده سلول باشد و یا خارج از محدوده وظایف سرور باشد نادیده گرفته شود. همچنین با توجه به ظرفیت در نظر گرفته شده برای هر خیابان اگر تعداد درخواست‌های ارسالی از آن خیابان بیش از حد باشد در نتیجه به درخواست‌های مازاد پاسخ داده نمی‌شود.

www.SID.ir

Archive of SID



شکل ۱. فلوچارت مربوط به مدل و راهکار پیشنهادی

۵-۲- استفاده مجدد

در صورتی که مسئولیت کنترل تراکنش‌ها بر عهده سرور سلول باشد به طور قطع هیچ استفاده مجددی در آن سلول رخ نخواهد داد. در حالتی که این مسئولیت بین خودروها توزیع شود امکان استفاده مجدد وجود دارد. در راهکار پیشنهادی این مقاله، با توجه به این‌که توکن‌ها با کلید سرور سلول و کلید ابرخودرویی امضا شده‌اند ، در نتیجه تنها در همان سلول و همان ابرخودرویی قابل استفاده هستند. به این ترتیب کارگزار به هیچ وجه نمی‌تواند توکن خود را در ابر دیگری مصرف کند. از طرفی با توجه به این‌که اعضا ابر از تاریخچه ابر باخبر هستند امکان استفاده مجدد توکن درون همان ابر نیز امکان‌پذیر نیست.

۵-۳- گمنامی و حریم خصوصی

به منظور حفظ گمنامی و حریم خصوصی به ترتیب از نام مستعار به جای شناسه واقعی خودرو و تغییر نام مستعار در نواحی سکوت استفاده شده است. نواحی سکوت به نواحی گفته می‌شود که در آن خودروها هیچ پیامی را با نام مستعار خود رد و بدل نمی‌کنند و برای تبادل پیام‌های ایمنی از کلید آن ناحیه استفاده می‌کنند. با توجه به این‌که در هر چهارراه، احتمال تغییر مسیر خودروها وجود دارد، معمولا نواحی سکوت در این مکان‌ها شکل می‌گیرند چراکه قابلیت ردیابی خودروها کم می‌شود. علاوه بر موارد بیان شده، استفاده از توکن نیز می‌تواند ناقض گمنامی و حریم خصوصی سرویس‌گیرندگان باشد به همین دلیل در راهکار پیشنهادی این مقاله، با بهره‌گیری از امضا کور در تولید توکن به دنبال رفع این چالش بوده‌ایم. البته در صورتی که تعداد سرویس‌گیرندگان در سلول کم باشد همچنان امکان نقض گمنامی و حریم خصوصی آن‌ها در مقابل سرور سلول وجود دارد. به همین دلیل نیاز است که تعداد سرویس‌گیرندگان در هر واحد زمان در سلول از مقدار مشخصی کمتر نباشد. برای این منظور از معیار بی‌نظمی[1] (H) برای اندازه‌گیری گمنامی/حریم خصوصی استفاده شده است.

در صورتی که مجموعه گمنامی[2] (V) را تعداد سرویس‌گیرندگان در سلول در نظر بگیریم و احتمال این‌که خودرو V_i سرویس‌گیرنده باشد را p_{v_i} در نظر بگیریم ($\forall V_i \in V$) آنگاه مقدار بی‌نظمی خودرو V_i درمجموعه گمنامی V به صورت $H = -\sum_{i=1}^{|V|} p_{v_i} \times \log_2 p_{v_i}$ محاسبه می‌گردد. در صورتی که احتمال مربوط به سرویس‌گیرنده بودن هر خودرو $\frac{1}{|V|}$ باشد، آنگاه ماکزیمم بی‌نظمی رخ داده است و مقدار آن به صورت $H_{Max} = \log_2 p_{v_i}$ محاسبه می‌گردد. به این ترتیب هرچه میزان بی‌نظمی بیشتر باشد، گمنامی و حریم خصوصی سرویس‌گیرنده بیشتر محافظت می‌گردد. در صورتی که هدف حفظ گمنامی و حریم خصوصی سرویس‌گیرندگان در مقابل سایر خودروهای درون سلول باشد آنگاه مجموعه گمنامی تعداد خودروهای درون سلول در نظر گرفته می‌شود.

۵-۴- سربار ارتباطی، تاخیر و مقیاس پذیری

در راهکار پیشنهادی، مسئولیت کنترل تراکنش‌ها به خودروها سپرده شده است. همین مساله باعث افزایش مقیاس‌پذیری شبکه، کاهش سربار ارتباطی، و بارکاری[3] سرور و کاهش تاخیر در پاسخ‌دهی به درخواست‌ها

[1] entropy
[2] anonymity set
[3] load

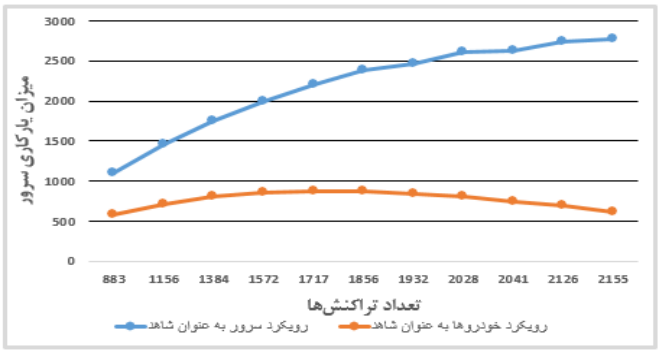
www.SID.ir

Archive of SID

شده است. میزان بهبود در بارکاری سرور در روش پیشنهادی با استفاده از شبیه سازی نشان داده شده است.

به منظور انجام شبیه‌سازی ابتدا با استفاده از نرم‌افزار SUMO، محیط و ترافیک شهری شبیه‌سازی شده سپس با استفاده از زبان برنامه‌نویسی جاوا، ابرخودرویی و راهکار پیشنهادی پیاده‌سازی شدند. با توجه به سلولی بودن محیط و ماکزیمم بازه ارتباطی DSRC (۱۰۰۰ متر)، اندازه سلول‌ها ماکزیمم ۷۰۰ * ۷۰۰ متر مربع در نظر گرفته شده است. تعداد سلول‌های در نظر گرفته شده در این شبیه‌سازی ۴ سلول است. سرور هر سلول در مرکز سلول مستقر شده است. در طول مدت ۱ ساعت شبیه سازی ۳۰۰۰ خودرو وارد شبیه‌ساز می‌شوند اما به طور میانگین ۱۵۰ خودرو در هر لحظه در شبیه‌ساز وجود دارد. خودروها در هر چهارراه با احتمال ۱/۴ یکی از مسیرها را برای ادامه حرکت خود انتخاب می‌کنند. میانگین سرعت در خیابان‌ها بین ۵ تا ۲۰ متر بر ثانیه (معادل ۱۸ تا ۷۲ کیلومتر بر ساعت) در نظر گرفته می‌شود. از میان خودروهای موجود در شبیه‌ساز، تعدادی از خودروها به صورت تصادفی به عنوان خودروهای سرویس‌گیرنده برچسب خورده‌اند. نرخ درخواست سرویس ۳۰۰ درخواست در ساعت می‌باشد. و بازه ارتباطی هر خودرو ۳۰۰ متر در نظر گرفته شده است.

همانطور که در شکل۲ قابل مشاهده است در رویکرد خودروها به عنوان شاهد (رویکرد پیشنهادی)، میزان بارکاری سرور بسیار کمتر از حالتی است که سرور به عنوان شاهد تراکنش‌ها انتخاب گردد. علت این امر نیز در این است که هر خودرو تنها هنگام خروج از سلول مراتب فعالیت خود را به سرور سلول اعلام می‌کند و در حین انجام تراکنش سرور را درگیر نمی‌کند. از طرفی در رویکرد خودروها به عنوان شاهد به نسبت افزایش تعداد تراکنش‌ها، میزان بارکاری سرور افزایش نیافته است و حتی از نقطه‌ای به بعد بارکاری سرور کاهش داشته است. علت این امر نیز در این است که وقتی سایز شبکه ثابت باشد و از طرفی تعداد تراکنش‌ها افزایش یابد در این صورت هر خودرو میزان کار بیشتری را در واحد زمان انجام می‌دهد در نتیجه هنگام ابلاغ به سرور خودروهای کمتری نیاز به برقراری ارتباط با سرور دارند.



شکل ۲. بارکاری سرور

۶- نتیجه گیری

در این مقاله به منظور پرداخت هزینه سرویس‌ها و به تبع آن تشویق خودروها به شرکت در ابرخودرویی، از مکانیزم انگیزشی مبتنی بر توکن استفاده کردیم. استفاده از توکن ممکن است منجر به نقض حریم خصوصی سرویس‌گیرنده گردد و یا به علت ماهیت مجازی توکن ممکن است چندین بار به صورت غیرقانونی مورد استفاده قرار گیرد. به منظور جلوگیری از مشکلات بیان شده از رویکرد مبتنی بر امضا کور و محدود کردن اعتبار توکن به ابرخودرویی و انتخاب شاهد از میان اعضای ابر استفاده کردیم. در نهایت راهکار پیشنهادی از نقطه نظر امنیت، حریم خصوصی، سربار ارتباطی، بارکاری، مقیاس‌پذیری و استفاده مجدد توکن مورد ارزیابی قرار گرفت و میزان بارکاری سرور در دو حالتی که سرور و خودروها به ترتیب به عنوان شاهد تراکنش‌ها انتخاب گردند شبیه‌سازی گردید. نتایج شبیه سازی نشان می‌دهد که میزان بارکاری سرور بسیار کمتر از حالتی است که سرور به عنوان شاهد تراکنش‌ها انتخاب گردد.

مراجع

[1] S. Olariu, M. Eltoweissy, and M. Younis, “Towards autonomous vehicular clouds,” *EAI Endorsed Trans. Mob. Commun. Appl.*, p. e2, 2011.

[2] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, “Security Challenges in Vehicular Cloud Computing,” *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, 2013.

[3] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, “Toward Cloud-based Vehicular Networks with Efficient Resource Management,” *IEEE Netw.*, pp. 48–55, Aug. 2013.

[4] P. Ghazizadeh, S. Olariu, A. G. Zadeh, and S. El-Tawab, “Towards Fault-Tolerant Job Assignment in Vehicular Cloud,” in *Services Computing (SCC), 2015 IEEE International Conference on*, 2015, pp. 17–24.

[5] Y. Zhu, L. Liu, J. Panneerselvam, L. Wang, and Z. Li, “Credit-Based Incentives in Vehicular Ad Hoc Networks,” in *Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on*, 2014, pp. 352–357.

[6] R. Zhang, Y. Zhang, and K. Ren, “Distributed privacy-preserving access control in sensor networks,” *IEEE Trans. Parallel Distrib. Syst.*, pp. 1427–1438, 2012.

[7] K. Lim, I. M. Abumuhfouz, and D. Manivannan, “Secure Incentive-Based Architecture for Vehicular Cloud,” in *International Conference on Ad-Hoc Networks and Wireless*, 2015, pp. 361–374.

[8] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, “Rethinking Vehicular Communications: Merging VANET with cloud computing,” *CloudCom 2012 - Proc. 2012 4th IEEE Int. Conf. Cloud Comput. Technol. Sci.*, pp. 606–609, 2012.

[9] G. Yan, S. Olariu, J. Wang, and S. Arif, “Towards providing scalable and robust privacy in vehicular networks,” *IEEE Trans. Parallel Distrib. Syst.*, pp. 1896–1906, 2014.

[10] E. Lee, E. Lee, M. Gerla, and S. Y. Oh, “Vehicular Cloud Networking : Architecture and Design Principles,” no. February, pp. 148–155, 2014.

[11] D. Chaum, “Blind Signatures for Untraceable Payments,” in *Advances in cryptology*, 1983, pp. 199–203.

[12] R. Zhang, Y. Zhang, and K. Ren, “DP^{2}AC: Distributed Privacy-Preserving Access Control in Sensor Networks,” in *INFOCOM 2009, IEEE*, 2009, pp. 1251–1259.

www.SID.ir