روشی برای ایجاد انگیزه در کاربران برای مشارکت در شبکه اجتماعی خودروها با حفظ حریم خصوصی مکانی

ساناز زمانی[1*]، بهروز ترک لادانی[2] و مائده عاشوری تلوکی[3]
[1]دانش آموخته کارشناسی ارشد امنیت اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، zamani.sanaz.11@gmail.com
[2]استاد، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، ladani@eng.ui.ac.ir
[3]استادیار، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، m.ashouri@eng.ui.ac.ir

چکیده : امروزه با گسترش استفاده از اینترنت در محیط خودرویی، مفهوم شبکه‌های اجتماعی خودرویی به عنوان نمونه‌ای از کاربرد اینترنت اشیاء در صنعت حمل و نقل، مورد توجه قرار گرفته است. تبادل اطلاعات میان کاربران در شبکه‌های خودرویی، باید با حفظ حریم خصوصی مکانی کاربران صورت بگیرد. همچنین برای مشارکت هرچه بیشتر کاربران در سامانه‌ی تبادل اطلاعات، نیاز به ایجاد انگیزه داریم. در این مقاله، روشی برای تبادل اطلاعات میان کاربران در شبکه‌ی اجتماعی خودرویی ارائه می‌شود که در آن ضمن حفظ حریم خصوصی کاربران، برای مشارکت در سامانه، انگیزه‌ی کافی ایجاد می‌شود. در این سامانه برای تبادل اطلاعات به جای استفاده از ارتباطات کوتاه-برد، از بستر اینترنت استفاده می‌شود (اینترنت خودروها). جهت ایجاد انگیزه در کاربران برای مشارکت در سامانه از پاداش‌دهی استفاده می‌شود. کاربران در ازای مشاهده شدن اطلاعاتشان، بلیط دریافت می‌کنند. جهت ارزیابی روش ارائه شده، از ابزار شبیه‌سازی ***Veins*** به همراه داده‌های واقعی موجود در مجموعه داده‌ای کرِتی استفاده شده است. نتایج ارزیابی و تحلیل روش ارائه شده نشان می‌دهد که میزان کیفیت پیام بر میزان پاداش دریافتی کاربران تاثیرگذار است و همچنین این سامانه منصفانه است، به طوری که طبق آزمایشات انجام شده بر اساس مشخصات سامانه، هیچ کاربری بالاتر از ۵۰۰ بلیط نخواهد داشت.

کلید واژه‌ها: اینترنت خودروها، انگیزه در شبکه‌های اجتماعی خودرویی، تبادل اطلاعات، حریم خصوصی مکانی، شبکه‌های اجتماعی خودرویی

۱-مقدمه

خودروهای هوشمند نسل جدید، بخشی از اینترنت اشیاء[1] هستند و خدمات و برنامه‌های کاربردی زیادی را به کاربران ارائه می‌دهند. هدف اصلی اینترنت اشیاء ارائه‌ی خدمات ارزش افزوده بر اساس دستگاه‌های هوشمند موجود است. به عبارتی دستگاه‌های هوشمند می‌توانند خدمات مختلف را از طریق تعامل با یک‌دیگر ارائه دهند [۱]. اینترنت اجتماعی اشیاء[2]، دستگاه‌های هوشمند را قادر می‌سازد تا در ارتباط با یک‌دیگر بر اساس محتوای به اشتراک گذاشته شده و منافع متقابل همکاری کنند.

اینترنت خودروها (IoV)، به عنوان شاخه‌ای از اینترنت اشیاء مطرح شده است که به عنوان یک بستر حساس جهت پردازش داده‌های اساسی برای سامانه‌های حمل‌ونقل هوشمند[3] (ITS) خدمت کند [۲]. در اینترنت خودروها، خودروها خدمات مبتنی بر مکان[4] مختلف را از ارائه دهندگان خدمات شخص ثالث[5] به دست می‌آورند (به عنوان مثال، پمپ بنزین‌های موجود در فاصله‌ی یک کیلومتری مکان فعلی) [۳]. همچنین اینترنت اجتماعی خودروها[6] از مفاهیم اینترنت اجتماعی اشیاء در حوزه‌ی خودرویی استفاده می‌کند [۱].

برای انتقال اطلاعات به کاربران در شبکه‌های اجتماعی خودرویی، می‌توان از روش متمرکز[7] یا غیر متمرکز[8] استفاده کرد.

با توجه به اینکه انتقال اطلاعات در میان کاربرها، و همچنین دریافت اطلاعات از طرف کارفرماها یک نیاز اساسی برای انجام سفری ایمن و راحت است، طراحی سامانه‌ای متمرکز برای انتقال امن این اطلاعات به کاربرها ضروری است. همچنین به لحاظ روانی، کاربران برای دریافت اطلاعات از کاربرهای دیگر تمایل

[1] Internet of Things (IoT)
[2] Social Internet of Things (SIoT)
[3] Intelligent Transport System (ITS)
[4] Location Based Services (LSB)
[5] Third Party
[6] Social Internet of Vehicles (SIoV)
[7] Centralised
[8] Decentralised

بیشـــتری دارند و اینکه بتوانند اطلاعات خود را با یک انگیزه‌ی مشخص با سایر کاربرهای حاضر در شبکه به اشتراک بگذارند، می‌تواند شبکه‌ای قوی از اطلاعات برای سفر ایمن و راحت ایجاد کند.

ما در این مقاله قصـــد داریم ســـامانه‌ای کاملاً متمرکز ارائه دهیم که در آن اطلاعات، توسط کارفرماها[1] تولید می‌شود و واحد مرکزی مورد اعتماد، این اطلاعات را به کاربران حاضر در شبکه (خودروها یا افراد) ارسال می‌کند. کاربران نیز می‌توانند اطلاعات موردنظرشان را به واحد مرکزی مورد اعتماد ارسال کنند. سایر کاربران در صورت تمایل می‌توانند این اطلاعات را از واحد مرکزی دریافت کنند.

در این طرح فرض می‌شـــود که کاربران برای دســـتیابی به اطلاعات یک‌دیگر کنجکاو هستند. بنابراین باید حریم خصوصی مکانی کاربران موجود در شبکه، از دید سایر کاربرها حفظ شود. کاربران برای انتقال داده‌های مورد نیاز به ســـایر کاربران، نیاز به انگیزه دارند. به همین منظور، آن‌ها به ازای ارســـال هر پیام مورد پسند کاربر مقصد، یک بلیط[2] (امتیاز مثبت) دریافت می‌کنند که بعدها می‌توانند این بلیط‌ها را برای دریافت خدمات خرج کنند. این بلیط‌ها در حقیقت اعتبارهایی اســـت که از ســـوی کارفرماها برای اعطای تخفیف به کاربران داده می‌شـــود. واحد مرکزی مورد اعتماد، روند اعطا و خرج کردن این اعتبارات را جهت عدم تخلف در جریان دریافت و خرج اعتبارات مدیریت خواهد کرد.

ساختار مقاله به صورت زیر است: در بخش ۲ مروری مختصر بر ادبیات موضوع انجام می‌شود. در بخش ۳ طرح پیشنهادی برای شـــبکه اجتماعی خودروها به همراه ملاحظات مربوط به انگیزه و حریم خصوصی آن‌ها شرح داده شده است. در بخش ۴ ارزیابی روش پیشـــنهادی انجام شـــده اســـت و در بخش ۵، نتیجه گیری مقاله آورده شده است.

۲-پژوهش‌های مرتبط

پژوهش‌های انجام شـــده در حوزه‌ی اینترنت خودروها را می‌توان از منظر امنیت در محیط خودرویی، شـبکه‌های اجتماعی خودرویی و طرح‌های ایجاد انگیزه در محیط خودرویی بررســـی کرد. از آن‌جا که ما قصد داریم یک شبکه‌ی اجتماعی خودرویی را با حفظ حریم خصـوصـی مکانی و ایجاد انگیزه در کاربران را ارائه کنیم، در این بخش پژوهش‌های مرتبط بررسی خواهد شد.

ژوو[3] و همکاران در [۴]، روشی ابتکاری برای ایجاد انگیزه در گره‌های خودخواه و تشویق آن‌ها به انتقال پیام‌های گره‌های دیگر و ارائه گزارش‌های صـــادقانه، ارائه دادند. در این روش، به آخرین گرهی که بســـته را به مقصـــد منتقل می‌کند، یک مقدار اعتبار اختصاص داده می‌شود.

لی[4] و همکاران در [۵] روشـــی را به نام FRAME برای حل مسـائل اضـافی محیط خودرویی پیشـنهاد دادند. FRAME از دو مؤلفه تشـکیل شـده اسـت، بخش پاداش دهی وزن‌دار و بخش قرعه‌کشی. در این روش، هر منبع پاداش وزنی دریافت می‌کند. از این رو، گره‌هایی که در حمل‌ونقل بسته شرکت می‌کنند، سهمی از پاداش را دریافت می‌کنند.

وو[5] و همکاران در [۶] یک مدل تئوری بازی از بارگیری و به اشـــتراک گذاری خوشـــه‌ها ارائه دادند. در این ســـامانه، گره‌ها به شـــبکه کمک می‌کنند و در رمزگشـــایی محتوا کمک می‌کنند. گره‌های خودخواه تا زمانی که داوطلبانه کمک نکنند، محتویات رمزگشایی نمی‌شود.

دیاس[6] و همکاران [۷]، دو روش جدید برای سازوکار تشویقی معرفی کردند: روش VBT[7] (حجم بایت‌های منتقل شـــده) و TSC[8] (زمان سپری شده برای همکاری).

شیائو[9] و همکاران [۸] یک سامانه متمرکز برای حفظ حریم خصـوصـی با نام CenLocShare در شـبکه‌های اجتماعی برخط موبـایـل (mOSNs[10]) پیشـــنهـاد کردنـد. در این ســـامـانـه، سرویس‌دهنده‌ی شبکه‌ی اجتماعی (SNS[11]) و سرویس‌دهنده‌ی مبتنی بر مکان (LBS[12]) ترکیب شـــده و به یک موجودیت «ســـرویس‌دهنده‌ی شـــبکه‌ی اجتماعی ذخیره کننده‌ی مکان» (LSSNS[13]) تبدیل می‌شـــود. در CenLocShare از مکان‌های

[1] به عنوان مثال، اداره‌ی پلیس، شرکت‌های تبلیغاتی یا کارخانه سازنده
[2] Ticket
[3] Zhu
[4] Li
[5] Wu
[6] Dias
[7] Volume of Bytes Transferred
[8] Time Spent to Cooperate
[9] Xiao
[10] Mobile Online Social Networks
[11] Socila Network Server
[12] Location Based Server
[13] Location-Storing Social Network Server

ساختگی و پروتکلهای اختصاصی نقشه برداری، برای به اشتراک گذاری مکان با حفظ حریم خصوصی میان LSSNS و برج سلولی (CT[1]) استفاده می‌شود.

ونگ[2] و همکاران [۹] یک طرح امن جدید برای شبکه‌های خودرویی اقتضایی ارائه داده‌اند که در آن حریم خصوصی، محرمانگی و عدم انکار فراهم می‌شود. این طرح بر پایه رمزنگاری کلید عمومی مبتنی بر گواهی‌نامه است.

ونگ و همکاران [۱۰] یک پروتکل تأیید هویت ناشناس، مبتنی بر رمزنگاری گواهی-مبنا، ارائه دادند که حریم خصوصی و عدم انکار را فراهم می‌کند. در این الگوریتم، پارامترهای عمومی سامانه با استفاده از توابع درهم‌ساز رمزنگاری تعیین می‌شود.

سان[3] و همکاران [۱۱] یک سامانه رمزنگاری برای شبکه‌های خودرویی ارائه کردند که مبتنی بر هویت می‌باشد. این طرح از نام مستعار برای تأمین حریم خصوصی و جلوگیری از ردیابی استفاده می‌کند. همچنین از رمزنگاری مبتنی بر هویت استفاده می‌کند که باعث می‌شود کلید عمومی از هویت عمومی کاربر مانند نام یا آدرس ایمیل گرفته شود.

وو[4] و همکاران [۱۲] یک روش جدید برای حفظ حریم خصوصی به نام «امضای گروهی قابل پیوند پیام[5]» پیشنهاد دادند. این طرح تأیید هویت ناشناس را ارائه می‌دهد. در این روش فرض بر این است که بیشتر خودروهای موجود در شبکه درست‌کار هستند.

هونگ لوو[6] و همکاران [۱۳] یک سامانه تأیید هویت برای شبکه‌های خودرویی پیشنهاد دادند. در این طرح برای حفظ حریم خصوصی، از نام‌های مستعار استفاده می‌شود.

جدول ۱ خلاصه‌ای از ویژگی‌های کارهای قبلی مربتط و اهداف پژوهش جاری را جهت مقایسه نشان می‌دهد.

جدول ۱: مقایسه کارهای قبلی و اهداف پژوهش جاری

روش	ارتباط اینترنتی	سازوکار انگیزه	حریم خصوصی مکانی	احراز اصالت	محرمانگی
[۴]	×	✓	×	×	×
[۵]	×	✓	×	✓	×
[۶]	×	✓	×	×	×
[۷]	×	✓	×	×	×
[۸]	✓	×	✓	×	×
[۹]	×	×	✓	✓	✓
[۱۰]	×	×	×	✓	×
[۱۱]	✓	×	✓	✓	✓
[۱۲]	×	×	✓	✓	✓
[۱۳]	✓	×	✓	✓	✓
پژوهش ما	✓	✓	✓	✓	✓

۳-طرح پیشنهادی

هدف ما طراحی سامانه‌ای متمرکز بر بستر اینترنت برای ارائه‌ی اطلاعات و خدمات جاده‌ای به مسافران است. این سامانه یک شبکه‌ی اجتماعی خودرویی است که به صورت متمرکز عمل می‌کند و بستر ارتباطی آن اینترنت خودروها است. بنابراین در حوزه‌ی اینترنت خودروها قرار می‌گیرد. به عبارتی در این سامانه، موجودیت‌ها از طریق واحد مرکزی با یک‌دیگر ارتباط برقرار می‌کنند.

موجودیت‌های حاضر در سامانه عبارت‌اند از واحد مرکزی یا مدیر سامانه، کاربران سامانه (خودروها یا افراد)، کارفرماها (می‌توانند به واحد مرکزی پیام ارسال کنند تا واحد مرکزی پیام آن‌ها را به کاربران سامانه برساند) و خریدار بلیط.

۳-۱-کلیات و معماری طرح پیشنهادی

در این سامانه، کارفرماها و کاربران می‌توانند به واحد مرکزی پیام ارسال کنند. این پیام‌ها در صورت درخواست سایر کاربران، به آن‌ها ارسال خواهد شد. کارفرماها در ازای مشاهده شدن پیام‌هایشان، به واحد مرکزی پول پرداخت می‌کنند. مقداری از

[1] Cellular Tower
[2] Wang
[3] Sun
[4] Wu
[5] Message Linkable Group Signature
[6] Hong Lu

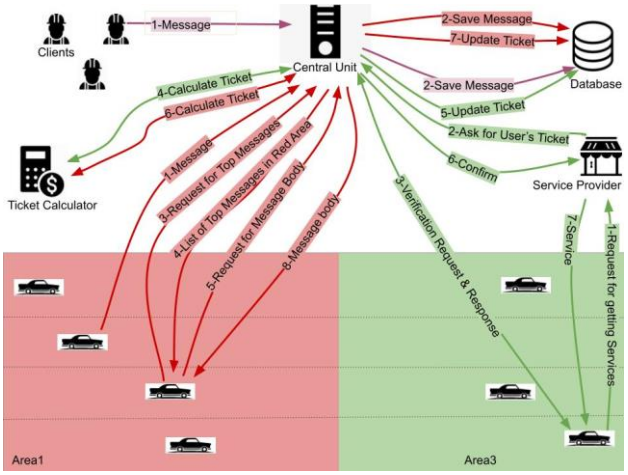
پول پرداختی کارفرماها، در قالب بلیط، به مالک پیامی تعلق می‌گیرد که پیامش مشاهده می‌شود. به عبارتی، بلیط‌ها به ازای مشاهده شدن اطلاعات کاربران، به آن‌ها اختصاص می‌یابد. کاربران می‌توانند بلیط‌های دریافتی‌شان را برای دریافت خدماتی از واحد مرکزی، کارفرماها یا تعمیرگاه‌های مجاز، خرج کنند.

انگیزه برای کاربران جهت شرکت در سامانه را می‌توان از دو منظر در نظر گرفت:

(۱) انگیزه‌ی ناشی از به اشتراک‌گذاری اطلاعات

(۲) بلیط‌های دریافتی به ازای تعداد مشاهده‌ی پیام

معماری سامانه در شکل ۱ نشان داده شده است.



شکل ۱: معماری سامانه

۳-۲-جزییات طرح پیشنهادی

طرح پیشنهادی را می‌توان در چهار بخش اساسی بررسی کرد: (۱) ثبت‌نام موجودیت‌ها در سامانه، (۲) ارسال پیام به واحد مرکزی، (۳) دریافت پیام از واحد مرکزی و (۴) خرج کردن بلیط‌های دریافتی کاربران.

هر کاربر u_i دارای یک جفت کلید عمومی و خصوصی (PU_{u_i}, PR_{u_i}) است. هویت و اطلاعات لازم درباره‌ی کاربر، در پایگاه‌داده‌ی واحد مرکزی ذخیره می‌شود.

۳-۳-ارسال پیام به واحد مرکزی

کاربران و کارفرماهای ثبت‌نام شده در سامانه می‌توانند در صورت تمایل، اطلاعات مورد نظرشان را به واحد مرکزی ارسال کنند تا واحد مرکزی آن اطلاعات را در پایگاه‌داده‌اش ذخیره کرده و در مراحل بعدی به کاربران ارسال کند.

پیام‌هایی که از طرف کاربر به واحد مرکزی ارسال می‌شود در سه دسته قرار می‌گیرند: پیام‌های حاوی اطلاعات برای ارسال به سایر کاربران، پیام‌های درخواست مشاهده‌ی فهرست اطلاعات جدید و درخواست دریافت یک پیام با شماره شناسه‌ی پیام

همچنین پیام‌هایی که از طرف کارفرما به واحد مرکزی ارسال می‌شوند، در دو دسته قرار می‌گیرند: اطلاعات درون‌پیامی (به عنوان یک تبلیغ، در درون پیام‌های مبادله شده میان کاربران قرار می‌گیرد) و اطلاعات مستقل (به صورت مستقل، یک پیام را تشکیل می‌دهند و می‌توانند در جایگاه رزرو شده قرار گیرند). کارفرما برای اطلاعات مستقل، پول بیشتری نسبت به اطلاعات درون‌پیامی به واحد مرکزی می‌پردازد.

پس از آن‌که اطلاعات به واحد مرکزی ارسال شد، مکان فرستنده‌ی پیام به ناحیه‌ی مربوطه نگاشت می‌شود. همچنین به هر پیام یک شماره شناسه تعلق گرفته و همراه با ناحیه‌ی مقصد و سایر جزئیات در پایگاه‌داده‌ی واحد مرکزی ذخیره می‌شود.

قبل از برقراری ارتباط موجودیت‌ها با واحد مرکزی، با استفاده از پروتکل تبادل کلید دیفی هلمن احراز اصالت شده [۱۴]، یک کلید مشترک با نام k با استفاده از کلید عمومی آن موجودیت رمز شده و توسط واحد مرکزی به او ارسال می‌شود. سپس موجودیت مذکور، پیام دریافتی را رمزگشایی می‌کند و به مقدار k دست پیدا می‌کند. هنگامی که کاربر u_i می‌خواهد پیام m_{u_i} را به واحد مرکزی بفرستد، جهت جلوگیری از به خطر افتادن محرمانگی، اصالت منبع و اصالت پیام، پیام خود را در قالب زیر به واحد مرکزی ارسال می‌کند:

$$Enc_k(m_{u_i}||Sign_{PR_{u_i}}(H(m_{u_i})))$$

واحد مرکزی پس از دریافت، ابتدا آن را رمزگشایی می‌کند:

$$Dec_k(Enc_k(m_{u_i}||Sign_{PR_{u_i}}(H(m_{u_i}))))$$
$$= m_{u_i}||Sign_{PR_{u_i}}(H(m_{u_i}))$$

واحد مرکزی زمان ارسال موجود در پیام m_{u_i} را بررسی می‌کند. در صورت قدیمی بودن، پیام بررسی نخواهد شد. در غیر این صورت، نام و شماره شناسه‌ی کاربر که در سرآیند پیام موجود است را در پایگاه‌داده‌اش جستجو می‌کند. با استفاده از کلید عمومی فرستنده که برابر با PU_{u_i} می‌باشد، امضای کارفرما اعتبارسنجی می‌شود. در صورت درستی، مقدار درهم شده پیام را به دست می‌آورد و با $H(m_{u_i})$ امضا شده مقایسه می‌کند. در صورتی که برابر بودند، مکان فرستاده شده توسط کارفرما، به مختصات جغرافیایی تبدیل شده و با توجه به اطلاعات موجود در جدول مربوط به ناحیه‌ها، مشخص می‌شود که مکان فرستاده شده مربوط به کدام ناحیه است. به عبارتی، پیام فرستاده شده،

برای کاربرهای کدام ناحیه ارسال شود. پیام m_{u_i} همراه با نام کاربر u_i، ناحیه‌ی به دست آمده با استفاده از مکان فرستاده شده، عنوان پیام و نوع پیام، در پایگاه‌داده‌ی واحد مرکزی ذخیره می‌شود.

محتویات پیام ارسالی از طرف کارفرما به واحد مرکزی شامل عنوان پیام، نام و شماره شناسه‌ی کارفرما، زمان ارسال پیام، ناحیه یا ناحیه‌های مقصد، نوع پیام (درون پیامی یا مستقل) و متن پیام می‌باشد. به طرز مشابه، محتویات پیام ارسالی از کاربر به واحد مرکزی شامل عنوان پیام، نام کاربری و شماره شناسه‌ی کاربر، زمان ارسال پیام، مکان فرستنده، نوع پیام (اطلاعات سرگرمی، اطلاعات توریستی و سایر اطلاعات) و متن پیام می‌باشد.

در ارسال پیام‌ها توسط کاربران به واحد مرکزی، حریم خصوصی مکانی کاربر حفظ شود. اما مکان کاربر، تنها از دید سایر کاربران و کارفرماها مخفی می‌شود و واحد مرکزی پس از دریافت پیام، مکان کاربر را خواهد دید. به عبارتی حریم خصوصی مکانی به صورت جزئی یا بخشی[1] می‌باشد.

۴-۳-دریافت پیام از واحد مرکزی

کاربران می‌توانند اطلاعات مورد نیازشان را از واحد مرکزی دریافت کنند. فرض کنیم کاربر u_j در ناحیه‌ی Area1 قرار دارد. این کاربر به محض برخط شدن در حساب خود، می‌تواند درخواستی برای دریافت عناوین اطلاعات جدید موجود در ناحیه‌اش را به واحد مرکزی ارسال کند. فرض کنیم $reqTopMsgs$ پیامی برای مشاهده‌ی اطلاعات است که کاربر u_i به واحد مرکزی ارسال می‌کند. این پیام حاوی نام و شماره شناسه کاربر، زمان ارسال پیام و مکان کاربر می‌باشد و به صورت زیر به واحد مرکزی ارسال می‌شود:

$$Enc_k(reqTopMsgs_{u_j}||Sign_{PR_{u_j}}(H\left(reqTopMsgs_{u_j}\right))$$

واحد مرکزی پس از دریافت پیام بالا، ابتدا پیام دریافتی را رمزگشایی می‌کند. سپس ویژگی زمان ارسال را بررسی می‌کند. در صورتی که زمان منقضی نشده باشد، واحد مرکزی به وسیله‌ی کلید عمومی کاربر، امضا را اعتبار سنجی می‌کند. در صورت درستی امضا، مقدار درهم شده‌ی پیام را به دست می‌آورد تا با مقدار درهم شده‌ی فرستاده شده، مقایسه کند. اگر این مرحله نیز درست بود، واحد مرکزی مکان موجود در پیام را گرفته و به ناحیه‌ای که در آن قرار دارد نگاشت می‌کند. سپس در پایگاه‌داده‌ی پیام‌ها، این ناحیه را جستجو می‌کند و نتیجه را بر اساس سیاست‌های مرتب‌سازی و نمایش پیام‌ها، به کاربر درخواست کننده می‌فرستد. بنابراین اطلاعات بازگردانده شده توسط واحد مرکزی، مبتنی بر مکان کاربر می‌باشد پیام ارسالی از طرف واحد مرکزی که حاوی فهرست پیام‌ها است را با $TopMsgs$ نشان می‌دهیم و به صورت زیر ارسال می‌شود:

$$TopMsgs_{CU}||Sign_{PR_{CU}}(H(resTopMsgs_{CU}))$$

پس از آن، کاربر در صورت تمایل به دریافت یک پیام، درخواستی به واحد مرکزی ارسال می‌کند. این پیام را با $reqMsgBody$ نشان می‌دهیم و به صورت زیر ارسال می‌شود:

$$E_k(reqMsgBody_{u_j}||Sign_{PR_{u_j}}(H\left(reqMsgBody_{u_j}\right))$$

هر پیامی که به کاربر نشان داده می‌شود، حاوی یک تبلیغ از جلنب یکی از کارفرماهاست. به ازای هر بار مشاهده شدن اطلاعات، از کارفرما پول دریافت می‌کنیم و یک بلیط به کاربر مالک آن پیام (که پیامش حاوی تبلیغات است و دیده می‌شود) اعطا می‌شود. همچنین یک جایگاه رزرو شده مختص به پیام‌های مستقل کارفرماها وجود دارد که کارفرما در ازای قرار دادن اطلاعات در این بخش، پول بیشتری نسبت به اطلاعات درون‌پیامی به واحد مرکزی می‌پردازد.

پیامی که برای مشاهده‌ی اطلاعات است و از طرف کاربر به واحد مرکزی ارسال می‌شود شامل نام و شماره شناسه‌ی کاربر، زمان ارسال پیام و مکان فرستنده می‌باشد.

مواردی که بر میزان دریافت یک بلیط اثرگذار خواهد بود، «میزان احتمال تولید پیام توسط کاربر»، «احتمال انتخاب پیام توسط واحد مرکزی برای نمایش به سایر کاربران»، «میزان جذابیت عنوان پیام» و «میزان درخواست‌های موجود در ناحیه‌ی خودروی فرستنده‌ی پیام» می‌باشد.

۵-۳-خرج کردن بلیط توسط کاربر

کاربران می‌توانند بلیط‌هایی که به دست می‌آورند را خرج کنند. مراکزی برای ارائه‌ی خدمات به کاربران وجود دارد، مانند کارفرماها، کارخانه‌ی سازنده‌ی خودروها، تعمیرگاه‌ها، فروشگاه‌ها، رستوران‌ها، پارکینگ‌ها و غیره. کاربر می‌تواند با مراجعه به این

[1] Partial Location Privacy

مراکز و درخواست دریافت خدمات به مرکز ارائه‌ی خدمات، در ازای بلیط‌هایی که دارد، تخفیف دریافت کند. بلیط‌ها و مقدار آن‌ها برای هر کاربر، در پایگاه‌داده‌ی واحد مرکزی نگهداری می‌شود و توسط او قابل نقد شدن خواهد بود.

کاربر ابتدا درخواستی را به مرکز ارائه‌ی خدمات ارسال می‌کند. سپس این مرکز درخواستی را به مدیر واحد مرکزی ارسال می‌کند تا مدیر، تراکنش را تایید کند. مدیر از کاربر سوال می‌کند که آیا مایل به کسر بلیط هست؟ (برای او کد تایید ارسال می‌کند). پس از تایید کاربر، مدیر واحد مرکزی به موتور محاسبه‌ی بلیط درخواست محاسبه‌ی میزان بلیط کاربر و کارفرما را می‌دهد. پس از پاسخ موتور محاسبه‌ی بلیط، مدیر واحد مرکزی میزان بلیط‌ها را در پایگاه‌داده به‌روز رسانی می‌کند. حال پیام تایید را به مرکز ارائه‌ی خدمات ارسال می‌کند. مرکز نیز خدمت مورد نظر کاربر را به او ارائه می‌دهد.

به دلیل کسر بلیط توسط مدیر واحد مرکزی قبل از ارائه‌ی خدمات و نیاز به تایید مدیر واحد مرکزی، امکان بروز حمله‌ی دو بار خرج کردن[1] وجود ندارد. همچنین تاریخچه‌ی تمام تراکنش‌های خرج کردن بلیط در پایگاه داده ذخیره می‌شود. بنابراین در صورتی که مرکز ارائه‌ی خدمات پس از کسر بلیط از کاربر، خدمات را به او ارائه نکند، به دلیل وجود فهرست تمام تراکنش‌ها، قابل پیگیری خواهد بود.

۴-تحلیل و ارزیابی طرح پیشنهادی

در این بخش قصد داریم سامانه را از لحاظ تامین حریم خصوصی مکانی، تاثیر میزان کیفیت پیام و منصفانه بودن بررسی نماییم.

برای شبیه‌سازی محیط و دنیای خودروها از یک مجموعه داده‌ای استفاده شده که اطلاعات آن از رفتار واقعی خودروهای موجود در محله‌ای در جنوب شرقی پاریس به نام کرِتی[2] استخراج شده است [۱۵]. این مجموعه داده‌ای بصورت رایگان بر روی بستر گیت[3] قرار دارد که در آن اطلاعات حرکتی خودروها بصورت ثانیه‌ای ثبت شده است. این اطلاعات شامل شماره‌شناسه‌ی خودرو، سرعت خودرو، شماره‌ی جاده‌ای که خودرو بر روی آن در حرکت است، جهت حرکت و موقعیت جغرافیایی می‌باشد.

همچنین جهت سازگاری بیشتر با طرح این مقاله، ویژگی‌های «جذابیت پیام»، «احتمال تولید پیام توسط خودرو» و «میزان درخواست فهرست پیام» به اطلاعات مجموعه داده‌ای اضافه شد. ویژگی جذابیت پیام بر اساس توزیع نرمال و احتمال تولید پیام و ارسال درخواست فهرست پیام با توزیع یکنواخت اختصاص یافته است.

فرض می‌کنیم هر خودرو در هر دو دقیقه، با احتمال ثابت تصمیم به تولید و ارسال پیام به واحد مرکزی دارد. برای پیام‌های تولید شده توسط خودروها در سامانه شاخص «سطح کیفیت» در نظر گرفته می‌شود. میزان کیفیت با عددی صحیح در بازه‌ی (۵ و ۱) به عنوان یک پارامتر به پیام اضافه می‌شود. همچنین فرض شده است که میزان احتمال انتخاب یکی از پیام‌ها برای مشاهده، تابعی از میزان جذابیت عنوان پیام است. جذابیت عنوان پیام در بازه (۱و۰) نرمال شده است.

برای شبیه‌سازی از شبیه‌ساز OM-Net++ استفاده شده است. برای پشتیبانی از مدل حرکت، پروژه Veins به شبیه‌ساز OM-Net++ اضافه شده است. Veins نقش یک افزونه را دارد که از امکانات پایه‌ی OM-Net++ برای شبیه‌سازی مدل حرکت در شبکه‌های خودرویی استفاده می‌کند. مدل حرکت در قالب فایل‌های با فرمت زبان نشانه‌گذاری قابل توسعه (XML)[4] به پروژه‌ی Veins اضافه می‌شود. مسیر حرکت و نحوه حرکت در این فایل‌ها را می‌توان با نرم‌افزار شبیه‌ساز با قابلیت حرکت شهری SUMO طراحی کرد و در قالب نقشه‌ی تصویری مشاهده کرد. با این نرم‌افزار می‌توان هر نوع مسیری را در جاده‌های درون شهری طراحی کرد. همچنین می‌توان نحوه‌ی حرکت خودروها، شامل سرعت و مکان جاده‌ای حرکت را تعیین کرد، و در نهایت رفتار و حرکت خودروها بر روی نقشه را مشاهده کرد.

۴-۱-تامین حریم خصوصی مکانی

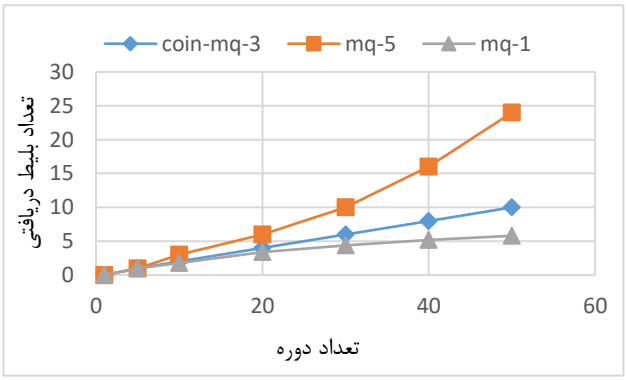
واحد مرکزی قابل اعتماد است. جهت ارائه‌ی خدمات با کیفیت‌تر، کاربران می‌توانند اطلاعات مکانی خود را در اختیار واحد مرکزی قرار دهند. به دلیل استفاده از رمزنگاری، مهاجم نمی‌تواند به اطلاعات پیام، از جمله مکان کاربر، دست پیدا کند. واحد مرکزی نیز اطلاعات مکانی کاربر را در اختیار سایر کاربران

[1] Double Spending
[2] Créteil
[3] GitHub
[4] Extensible Markup Language

قرار نخواهد داد. گیرندگان و مشاهده کنندگان پیام، تنها ناحیه‌ای که کاربر فرستنده در آن قرار دارد را می‌دانند و مکان دقیق را نمی‌دانند.

۴-۲-تاثیر میزان کیفیت پیام

در این آزمایش کاربران با احتمال ۰/۲ در یک دوره‌ی زمانی (دو دقیقه) پیام تولید می‌کنند. میزان جذابیت پیام‌های تولید شده عددی نرمال می‌باشد. همچنین شهرت کاربران و سطح کیفیت پیام به صورت تصادفی اختصاص یافته است. اما سه کاربر با شهرت اولیه‌ی ۰/۷ و سطح کیفیت‌های پیام ثابت (اعداد یک، سه و پنج برای هر کدام از سه کاربر) را در نظر می‌گیریم. فرض می‌کنیم نظردهی کاربرها در مورد این پیام، معادل سطح کیفیت است. نمودار این آزمایش در شکل ۲ نشان داده شده است.



شکل ۲: مقایسه بلیط دریافتی برای ارائه پیام با کیفیت‌های مختلف

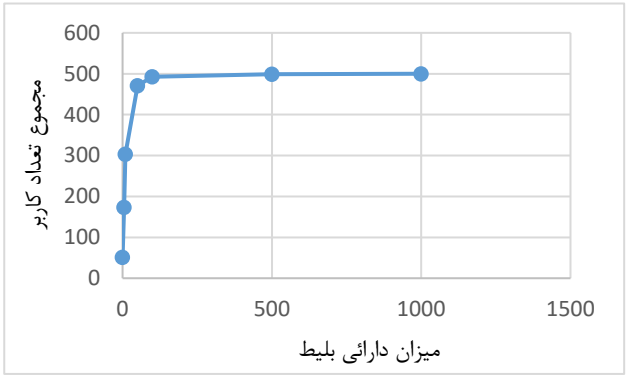
مشاهده می‌شود که هرچه پیام با کیفیت‌تر باشد، میزان بلیط دریافتی بیشتر است. به عبارتی میزان کیفیت پیام در میزان پاداش دریافتی‌اش تأثیر دارد. بنابراین در این سامانه، میزان کیفیت پیام بر میزان پاداش‌دهی تاثیر خواهد گذاشت.

۴-۳-منصفانه بودن سامانه

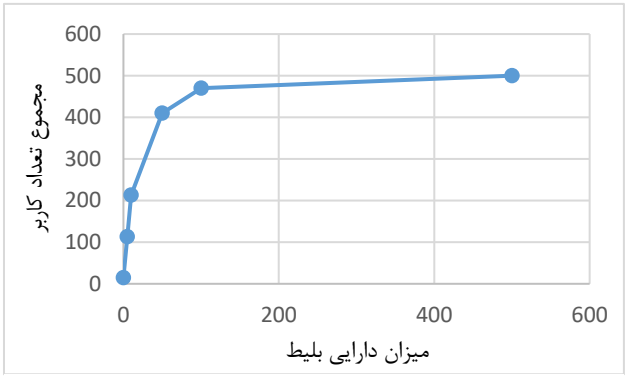
در این آزمایش می‌خواهیم پخش میزان دارایی بلیط را میان کاربران بررسی کنیم. به عبارتی می‌خواهیم بدانیم که در مجموع چه تعداد کاربر، صاحب چه تعداد بلیط هستند. نمودار این آزمایش در شکل ۳ نشان داده شده است.

مشاهده می‌شود که ۴۹۹ کاربر دارای ۵۰۰ بلیط یا کمتر هستند و تنها یک کاربر دارای بلیط بیشتر از ۵۰۰ عدد می‌باشد. همچنین حدود ۳۰ کاربر تنها ۱۰ بلیط دارند. با افزایش احتمال حضور پیام کاربران به صورت تصادفی در فهرست پیام‌ها (افزیش احتمال انتخاب پیام توسط واحد مرکزی) می‌توان سامانه را منصفانه‌تر نمود. نمودار پخش دارایی بلیط با تعداد انتخاب تصادفی بیشتر در میان پیام‌ها در شکل ۴ مشاهده می‌شود.

مشاهده می‌شود که اگر در میان پیام‌های انتخاب شده توسط واحد مرکزی، تعداد پیام‌های تصادفی بیشتر شود، نمودار پخش دارایی بلیط متعادل‌تر می‌شود. در شکل ۴ تعداد ۵۱ کاربر بلیط ندارند. همچنین تنها یک کاربر ۵۰۰ بلیط دارد. اما در شکل ۳، تنها ۱۵ کاربر بلیط ندارند و هیچ فردی بالاتر از ۵۰۰ بلیط ندارد.



شکل ۳: تعداد تجمعی کاربرها بر اساس میزان دارایی بلیط



شکل ۴: تعداد تجمعی کاربرها بر اساس دارایی بلیط با تعداد پیام تصادفی بیشتر

۵-نتیجه‌گیری

در این مقاله، طرح سامانه‌ای را ارائه کردیم که در آن می‌توان ضمن ایجاد انگیزه برای کاربران حاضر در سامانه، اطلاعات آن‌ها را با حفظ حریم خصوصی مبادله کنیم. این سامانه به صورت متمرکز عمل کرده و بستر ارتباطی آن اینترنت است. موجودیت‌های سامانه پس از ثبت‌نام در سامانه، بسته به میزان و کیفیت فعالیتشان در سامانه، پاداشی تحت عنوان بلیط دریافت می‌کنند که این بلیط‌ها برای دریافت خدمات از مراکز ارائه‌ی خدمات خرج خواهد شد.

در داخل پیام‌های مبادله شده میان کاربرها با مدیریت واحد

مرکزی، اطلاعات کارفرماها وجود دارد. کارفرما در ازای مشـــاهده شدن اطلاعاتش به واحد مرکزی پول می‌پردازد. واحد مرکزی نیز بخشی از این پول را به کاربری که میزبان پیام کارفرما بوده است می‌پردازد.

با طراحی چنین سامانه‌ای، کاربران برای مشارکت در سامانه انگیزه خواهنـد داشـــت. همچنین مکـان کـاربر از دیـد ســـایر موجودیت‌ها مخفی باقی می‌ماند.

در کارهای آتی ما قصـد داریم این امکان را برای کاربر فراهم کنیم که بتواند در پیام‌های موجود جســتجو انجام دهد. همچنین شـــاخص شـــهرت برای هر کاربر، جهت ترغیب کاربران به رفتار صادقانه در نظر گرفته شود.

مراجع

[1] Butt, T.A., et al., *Social Internet of Vehicles: Architecture and enabling technologies.* Computers & Electrical Engineering, 2018. **69**: p. 68-84.
[2] Kang, J., et al., *Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles.* IEEE Transactions on Intelligent Transportation Systems, 2017. **19**(8): p. 2627-2637.
[3] Kang, J., et al., *Location privacy attacks and defenses in cloud-enabled internet of vehicles.* IEEE Wireless Communications, 2016. **23**(5): p. 52-59.
[4] Zhu, Y., et al. *Credit-based incentives in vehicular ad hoc networks.* in *2014 IEEE 8th International Symposium on Service Oriented System Engineering*. 2014. IEEE.
[5] Li, F. and J. Wu. *Frame: An innovative incentive scheme in vehicular networks*. in *2009 IEEE International Conference on Communications*. 2009. IEEE.
[6] Wu, C., M. Gerla, and N. Mastronarde. *Incentive driven LTE content distribution in VANETs*. in *2015 14th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*. 2015. IEEE.
[7] Dias, J.A., et al. *A hybrid system to stimulate selfish nodes to cooperate in vehicular delay-tolerant networks.* in *2015 IEEE International Conference on Communications (ICC)*. 2015. IEEE.
[8] Xiao, X., et al., *CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks.* Future Generation Computer Systems, 2018. **86**: p. 863-872.
[9] Wang, N.-W., Y.-M. Huang, and W.-M. Chen, *A novel secure communication scheme in vehicular ad hoc networks.* Computer communications, 2008. **31**(12): p. 2827-2837.
[10] Wang, X., T. Liu, and G. Xiao, *Certificate-based anonymous authentication protocol for vehicular Ad-hoc network.* IETE Technical Review, 2012. **29**(5): p. 388-393.
[11] Sun, J., et al., *An identity-based security system for user privacy in vehicular ad hoc networks.* IEEE Transactions on Parallel and Distributed Systems, 2010. **21**(9): p. 1227-1239.
[12] Wu, Q., J. Domingo-Ferrer, and U. González-Nicolás, *Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications.* IEEE Transactions on Vehicular Technology, 2009. **59**(2): p. 559-573.
[13] Lu, H., J. Li, and M. Guizani. *A novel ID-based authentication framework with adaptive privacy preservation for VANETs*. in *2012 Computing, Communications and Applications Conference*. 2012. IEEE.
[14] Sarr, A.P., P. Elbaz-Vincent, and J.-C. Bajard. *A secure and efficient authenticated Diffie–Hellman protocol*. in *European Public Key Infrastructure Workshop*. 2009. Springer.
[15] *Microscopic vehicular mobility trace of Europarc roundabout, Creteil, France*. [cited ۲۰۲۰ January; Available from: https://vehicular-mobility-trace.github.io./