

## طرح بهبود یافته احراز اصالت با حفظ گمنامی مشروط در شبکه‌های اقتضایی بین خودرویی

سید مرتضی پورنقی<sup>۱\*</sup>، مصطفی برمشوری<sup>۲</sup>، محمود گردشی<sup>۳</sup>

۱- دانشجوی دکتری، دانشگاه قم

۲- کارشناسی ارشد، دانشکده علوم کامپیوتر، دانشگاه تهران

۳- استادیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۳/۰۹/۱۶؛ پذیرش: ۹۴/۰۷/۱۴)

### چکیده

شبکه‌های اقتضایی بین خودرویی (VANET) می‌توانند در ارتباط میان وسایل نقلیه و مدیریت ترافیک بهبود مناسبی ایجاد کنند. احراز اصالت پیام‌های منتشر شده توسط خودروها، از مهم‌ترین مسائل پیش‌رو در شبکه‌های اقتضایی بین خودرویی می‌باشد، زیرا ارسال پیام‌های اشتباه می‌تواند باعث بروز تصادفات و تغییر الگوی ترافیکی شبکه گردد. طرح‌های بسیار زیادی برای احراز اصالت در شبکه‌های اقتضایی بین خودرویی ارائه شده‌اند که هر کدام دارای مزایا و معایبی می‌باشند، اما معرفی یک طرح احراز اصالت امن و کارآمد در شبکه‌های اقتضایی بین خودرویی از مسائل باز تحقیقاتی بوده و مهم‌ترین چالش در این شبکه‌ها به‌شمار می‌آید. در این مقاله ابتدا به معرفی انواع روش‌های احراز اصالت در شبکه‌های اقتضایی بین خودرویی می‌پردازیم و سپس طرح ارائه‌شده توسط لی و لای را مورد تجزیه و تحلیل قرار می‌دهیم و سه سناریوی حمله به این طرح را معرفی می‌کنیم که امکان جعل امضای کاربر را به مهاجم می‌دهد. در ادامه یک طرح بهبود یافته از طرح لی و لای را پیشنهاد می‌دهیم که دارای ملزومات امنیتی و کارایی مناسبی می‌باشد سپس آن را شبیه‌سازی کرده و در پایان نتایج شبیه‌سازی طرح پیشنهادی خود را ارائه خواهیم کرد.

**واژه‌های کلیدی:** شبکه‌های اقتضایی بین خودرویی، احراز اصالت گمنام و مشروط، زوج‌سازی دوخطی، شناسه مستعار.

### ۱- مقدمه

شبکه‌های اقتضایی بین خودرویی توجه چندانی به امنیت آن‌ها نشده است، طراحی پروتکل‌های ارتباطی امن و کارآمد در این شبکه‌ها از چالش‌های اساسی این حوزه بوده و از موضوعات باز تحقیقاتی در مراکز علمی و دانشگاهی به‌شمار می‌آید.

در شبکه‌های اقتضایی بین خودرویی، خودروها به وسیله حسگرهایی که در آن‌ها نصب شده است اطلاعات ترافیکی محیط پیرامون خود را شناسایی کرده و شرایط ترافیکی و یا بروز حادثه را به سرعت به سایر خودروهای مجاور و ایستگاه‌های مدیریت ترافیک اعلام می‌کنند. مهم‌ترین نیاز امنیتی در شبکه‌های اقتضایی بین خودرویی قابل اعتماد بودن پیام‌های ارسالی توسط خودروها می‌باشد، زیرا ارسال پیام‌های نامعتبر می‌تواند امنیت خودروهای درون شبکه را به خطر اندازد و کارایی شبکه‌های اقتضایی بین خودرویی را مختل کند. به عنوان مثال تغییر پیام ارسالی و یا تکرار پیام‌های ارسال شده قبلی می‌تواند نمونه‌ای از این حملات باشد. احراز اصالت منبع منتشرکننده پیام می‌تواند یک راه حل مناسب برای کاهش این مخاطرات محسوب شود. در کنار این ویژگی، حفظ حریم خصوصی کاربر نیز یکی از نیازهای مهم در

با توجه به افزایش روز افزون حجم خودروها و به تبع آن افزایش تعداد تصادفات، در سال‌های اخیر گرایش عمومی سازندگان وسایل نقلیه و مدیران ترافیک شهری به خودروهای هوشمند افزایش یافته است و برقراری ایمنی در خودروها با استفاده از فرآیندهای هوشمند و مستقل از توانایی‌های راننده از اهداف مهم این مراکز قرار گرفته است. بنابراین نوع خاصی از شبکه‌های اقتضایی که در آن گره‌های شبکه، خودروها می‌باشند، با نام شبکه‌های اقتضایی بین خودرویی<sup>۱</sup> معرفی شدند. تفاوت عمده‌ی شبکه‌های اقتضایی با شبکه‌های بی‌سیم مبتنی بر استاندارد IEEE.802.11 این است که در این شبکه‌ها ارتباط بین گره‌های شبکه بدون هیچ زیرساخت مرکزی و یا ایستگاه پایه‌ای برای مدتی کوتاه برقرار می‌شود، از ویژگی‌های این شبکه‌ها تحرک پذیری بسیار بالای گره‌ها بوده که منجر به تغییرات بسیار زیادی در الگوی این شبکه‌ها می‌گردد. با توجه به این که هنگام طراحی پروتکل‌های

\* رایانامه نویسنده مسئول: sm.pournaghi@gmail.com  
1- VANET (Vehicular Ad hoc Network)

• دو خطی بودن<sup>۷</sup>: به‌ازای هر  $X, Y \in G_1$  و  $a, b \in \mathbb{Z}_p^*$  داریم:  

$$e(aX, bY) = e(X, Y)^{ab}$$

• زوال‌ناپذیری<sup>۸</sup>: برای هر  $X \in G_1$  و  $X \neq 0$  حداقل یک عضو  $Y \in G_1$  وجود دارد به‌طوری‌که  $e(X, Y) \neq 1$  است. همچنین برای هر  $Y \in G_1$  و  $Y \neq 0$  حداقل یک عضو  $X \in G_1$  وجود دارد به‌طوری‌که  $e(X, Y) \neq 1$  است [۳].

محاسبه‌پذیر بودن<sup>۹</sup>: برای هر  $X, Y \in G_1$  یک الگوریتم کارآمد برای محاسبه نگاشت  $e(X, Y)$  وجود داشته باشد.

تعریف ۲: مسئله لگاریتم گسسته بر روی منحنی بیضوی (ECDLP)<sup>۹</sup>: محاسبه عدد صحیح  $0 \leq l \leq q - 1$  با داشتن دو نقطه  $P, Q$  از مرتبه  $q$  بر روی منحنی بیضوی به‌طوری‌که  $Q = lP$  است.

تعریف ۳: مسئله دیفی-هلمن محاسباتی (CDH)<sup>۱۰</sup>: برای  $a, b \in \mathbb{Z}_q^*$ ، با معلوم بودن مقادیر  $P, aP, bP \in G_1$  محاسبه  $abP \in G_1$  را مسئله محاسباتی دیفی-هلمن گویند.

تعریف ۴: مسئله تصمیم دیفی-هلمن (DDH)<sup>۱۱</sup>: برای  $a, b, c \in \mathbb{Z}_q^*$ ، با معلوم بودن مقادیر  $P, aP, bP, cP \in G_1$  می‌خواهیم تصمیم بگیریم که آیا  $c = ab$  می‌باشد یا خیر؟

تعریف ۵: مسئله دیفی-هلمن دو خطی محاسباتی (CDBH)<sup>۱۲</sup>: به‌ازای پارامترهای نامعلوم  $a, b, c \in \mathbb{Z}_p$ ، مقادیر  $(g, g^a, g^b, g^c \in G)$  معلوم می‌باشد و مسئله یافتن مقدار  $e(g, g)^{abc}$  است.

تعریف ۶: مسئله تصمیم دیفی-هلمن دو خطی (DBDH)<sup>۱۳</sup>: به‌ازای پارامترهای نامعلوم  $a, b, c \in \mathbb{Z}_p$  و  $w \in G_2$ ، مقادیر  $(g, g^a, g^b, g^c \in G)$  معلوم هستند و می‌خواهیم تصمیم بگیریم که آیا  $w = e(g, g)^{abc}$  است یا خیر؟

### ۳- معرفی کارهای انجام شده

به‌طور کلی طرح‌های احراز اصالت گمنام و مشروط در شبکه‌های اقتضایی بین خودرویی به چهار دسته کلی تقسیم می‌شوند [۴].

- طرح‌های مبتنی بر گواهی‌های بی‌نام
- طرح‌های مبتنی بر امضاهای گروهی
- طرح‌های مبتنی بر RSU
- طرح‌های مبتنی بر TPD<sup>۱۴</sup>

شبکه‌های اقتضایی بین خودرویی می‌باشد، یعنی با توجه به ادوات الکترونیکی نصب شده در هر خودرو نباید امکان ردیابی و تحلیل رفتار کاربر برای هر موجودیتی امکان‌پذیر باشد. بنابراین احراز اصالت پیام باید به صورت گمنام صورت پذیرد یعنی اصالت پیام مورد تصدیق قرار گیرد بدون آن‌که هویت فرستنده‌ی پیام افشا شود. اما در کنار ویژگی احراز اصالت گمنام، در صورت تخلف کاربر باید بتوان هویت واقعی او را توسط مراجع ذی‌صلاح افشا کرد. بنابراین در شبکه‌های اقتضایی بین خودرویی نیازمند پروتکل‌های احراز اصالت گمنام و مشروط<sup>۱۵</sup> می‌باشیم و این بزرگ‌ترین چالش امنیتی در این شبکه‌ها محسوب می‌شود [۱].

در شبکه‌های اقتضایی بین خودرویی هر خودرو مجهز به یک واحد پردازنده داخلی به نام OBU<sup>۱۶</sup> بوده که وظیفه تولید و انتشار پیام‌های ترافیکی را بر عهده دارد، همچنین ایستگاه‌های کنار جاده‌ای به نام RSU<sup>۱۷</sup> برای ارتباط خودرو با مراکز ترافیکی در سطح شبکه نصب می‌گردد. ادامه مقاله به این صورت سازمان‌دهی شده است؛ در بخش ۲ مروری بر مفاهیم ریاضی مورد نیاز در پروتکل‌های احراز اصالت خواهیم داشت؛ در بخش ۳ راه‌حل‌های موجود برای برقراری احراز اصالت گمنام و مشروط در شبکه‌های اقتضایی بین خودرویی و کارهای صورت‌گرفته در این زمینه معرفی می‌شوند؛ سپس در بخش ۴ طرح لی و لای<sup>۱۸</sup> را معرفی می‌کنیم؛ در بخش ۵ سه سناریوی حمله‌ای که به طرح لی و لای انجام داده‌ایم را بیان می‌کنیم؛ سپس در بخش ۶ طرح بهبود یافته‌ای از طرح لی و لای را ارائه می‌دهیم؛ در بخش ۷ به تحلیل امنیتی طرح پیشنهادی خود و مقایسه آن با سایر طرح‌ها می‌پردازیم و شبیه‌سازی طرح پیشنهادی خود را در بخش ۸ ارائه می‌کنیم و در پایان در بخش ۹ به جمع‌بندی و نتیجه‌گیری می‌پردازیم.

### ۲- مقدمات ریاضی

در این بخش به‌صورت مختصر به معرفی مفاهیم ریاضی مورد نیاز در این مقاله می‌پردازیم.

تعریف ۱: زوج‌سازی دوخطی<sup>۱۹</sup>: فرض کنید  $G_1$  یک گروه جمعی دوری منحنی بیضوی با مولد  $P$  و  $G_2$  یک گروه ضربی دوری از مرتبه عدد اول  $p$  و با مولد  $g$  می‌باشد. نگاشت  $e: G_1 \times G_1 \rightarrow G_2$  یک زوج‌سازی دو خطی است اگر شرایط زیر را برآورده کند [۲-۴].

7- Non-Degeneracy  
 8- Computationality  
 9- Elliptic Curve Discret Logarithm  
 10- Computational Diffie-Hellman  
 11- Decisional Diffie-Hellman  
 12- Computational Bilinear Diffie-Hellman  
 13- Decisional Bilinear Diffie-Hellman  
 14- Tamper Proof Device

1- Conditional privacy preserving  
 2- On Board Unit  
 3- Road Side Unit  
 4- Lee & Lai  
 5- Bilinear Pairing  
 6- Bilinearity

### ۳-۱- طرح های مبتنی بر گواهی های بی نام

در این طرح ها با توجه به سطح گمنامی مورد نیاز در شبکه هر کاربر تعداد زیادی گواهی بی نام که توسط CA<sup>۱</sup> امضا شده و کلید خصوصی متناظر با آن ها را، به صورت امن از TA<sup>۲</sup> دریافت می کند، در این گواهی ها هیچ اطلاعاتی از هویت واقعی کاربر ثبت نشده است، لذا این گواهی ها گمنامی کاربران را کاملاً حفظ می کنند. برای ارسال هر پیام OBU به صورت تصادفی یکی از این گواهی ها را انتخاب کرده و سپس با کلید خصوصی متناظر با آن، پیام را امضا می کند و پیام، امضا و گواهی متناظر آن را منتشر می کند. در این روش TA مشخصات گواهی های تحویل داده شده به کاربران را ذخیره می کند و در صورت نیاز می تواند هویت واقعی کاربر را آشکار کند [۵]. ضعف عمده ای که در طرح های مبتنی بر گواهی های بی نام وجود دارد که باعث ناکارآمدی آن ها می گردد، فرآیند ابطال کاربران شبکه می باشد. در این طرح ها با افزایش تعداد کاربران ابطال شده حجم فهرست گواهی های ابطال شده (CRL<sup>۳</sup>) به شدت افزایش می یابد و این باعث افزایش زمان واریسی امضاها می گردد. زیرا هنگامی که یک کاربر متخلف شناخته می شود باید تمامی گواهی های بی نامی که در اختیار او قرار گرفته است در فهرست ابطال قرار گیرد، بنابراین با افزایش تعداد خودروهای ابطال شده حجم CRL به شدت افزایش می یابد و خودروها قبل از این که امضای پیامی را واریسی کنند باید CRL را بررسی کرده و از مجاز بودن کاربر اطمینان حاصل کنند. بررسی CRL با حجم زیاد برای شبکه های اقتضایی بین خودرویی که باید پیام ترافیکی مهمی را در کسری از ثانیه مورد بررسی قرار دهند بسیار زمان بر می باشد.

### ۳-۲- طرح های مبتنی بر امضای گروهی

در طرح های مبتنی بر امضای گروهی هر عضو گروه می تواند پیامی را از طرف گروه امضا کرده و این امضا می تواند توسط اعضای گروه مورد واریسی قرار گیرد بدون آن که مشخص باشد کدام عضو گروه پیام را امضا کرده است. در حالی که مرکز سوم مورد اعتمادی به نام TTP<sup>۴</sup> به عنوان مدیر گروه وجود دارد که می تواند هویت واقعی امضاکننده پیام را کشف کند [۹-۱۰].

از مشکلات پیش رو در طرح های مبتنی بر امضای گروهی این است که در این طرح ها زمان واریسی امضا به صورت خطی با تعداد خودروهایی که در فهرست ابطال قرار گرفته اند افزایش

می یابد و اگر تعداد خودروهای فسخ شده از آستانه تعیین شده بیشتر شود باید شبکه مجدداً راه اندازی گردد و هر گروه از خودروها کلیدهای جدیدی دریافت کنند. همچنین در بیشتر طرح های مبتنی بر امضای گروهی، خودرو باید توسط بالاترین مرجع مورد اعتماد ثبت نام گردد و کلید خصوصی خود را از طریق یک کانال امن به دست آورد، این فرآیند موجب می شود تا خودرو نتواند کلید خصوصی خود را به صورت پویا تغییر دهد و این باعث افزایش احتمال حمله می گردد.

در طرح های مبتنی بر امضای گروهی نیازمند برقراری مصالحه ای در اندازه گروه می باشیم، زیرا اگر اندازه گروه بزرگ باشد زمان واریسی امضا افزایش می یابد و در صورت کوچک بودن گروه، شناسایی اعضای گروه راحت تر بوده و گمنامی کاربران به خوبی حفظ نمی گردد.

### ۳-۳- طرح های مبتنی بر RSU

در این طرح ها خودروها برای امضای پیام ها و یا احراز اصالت آن ها نیازمند همکاری بر خط RSU می باشند. ژانگ<sup>۵</sup> یک روش جدید مبتنی بر RSU ارائه کرده است، که در آن RSU مسئول بررسی احراز اصالت پیام های رسیده از خودروها و پاسخ گویی به آن ها می باشد. همچنین در طرح ECPP احراز اصالت گمنام بر اساس تولید کلیدهای کوتاه مدت گمنام برای ارتباط خودروها با RSU پیشنهاد شده است. این کلیدها امکان احراز اصالت سریع و گمنام را با حفظ محرمانگی برآورده می کنند [۷-۱۲].

طرح های شامل RSU در مقایسه با سایر طرح های فاقد RSU کارآمدتر بوده و دارای محاسبات کمتری در سمت خودروها می باشند، اما این طرح ها برای امضا و بررسی پیام ها به شدت به زیرساخت کنار جاده ای RSU وابسته می باشند بنابراین این طرح ها عموماً فاقد ارتباط خودرو با خودرو (V2V<sup>۶</sup>) بوده و هر ارتباطی باید در حضور زیرساخت کنار جاده ای RSU انجام شود.

### ۳-۴- طرح های مبتنی بر TPD

TPD در واقع یک دیسک سخت غیر قابل نفوذ با قابلیت محاسباتی می باشد. در این طرح ها هر خودرو مجهز به یک TPD بوده و اطلاعات اصلی سامانه مانند کلید اصلی سامانه، توابع مورد نیاز و... بعد از ثبت نام توسط TA در TPD هر خودرو پیش ذخیره می گردد، حال TPD هر خودرو می تواند برای امضای هر پیام توسط کلید اصلی سامانه و شناسه واقعی خود یک شناسه مستعار و کلید خصوصی متناظر با آن را

1- Certificate Authority

2- Trusted Authority

3- Certificate Revocation List

4- Third Trusted Party

5- Zhang

6- vehicle to vehicle

را انتخاب کرده و شناسه مستعار  $ID^i = \{ID_1^i, ID_2^i\}$  و کلید خصوصی  $SK^i = \{SK_1^i, SK_2^i\}$  متناظر با آن را به صورت زیر محاسبه می کند.

$$ID^i = \{ID_1^i, ID_2^i\} = \{rP, RID_i \oplus H(rP_{pub_1})\} \quad (1)$$

$$SK^i = \{SK_1^i, SK_2^i\} = \{S_1 ID_1^i, S_2 h(ID_1^i \parallel ID_2^i \parallel T_i)P\} \quad (2)$$

#### ۴-۳- امضا و واریسی امضا در طرح لی و لای

خودروی  $V_i$  برای امضای پیام  $M_i$  یک شناسه مستعار مانند رابطه (۱) در زیر بخش قبل تولید کرده و به صورت زیر پیام را امضا می کند سپس چند تایی  $\langle ID^i, M_i, \delta_i, T_i \rangle$  را به عنوان امضای خود منتشر می کند که در آن  $T_i$  مهر زمانی می باشد.

$$\delta_i = SK_1^i + h(M_i)SK_2^i \quad (3)$$

برای واریسی پیام ابتدا شرط  $T_r - T_i < T_\Delta$  توسط واریسی کننده امضا بررسی می گردد که در آن  $T_r$  زمان فعلی سامانه و  $T_\Delta$  حداکثر تأخیر مجاز سامانه می باشد، اگر این شرط برقرار شد، آن گاه صحت امضا توسط برقراری شرط تصدیق زیر بررسی می گردد.

$$e(\delta_i, P) = e(ID_1^i, P_{pub_1}) \cdot e(h(M_i)h(ID_1^i \parallel ID_2^i \parallel T_i)P, P_{pub_2}) \quad (4)$$

این طرح امکان تصدیق گروهی را نیز دارد، واریسی کننده امضا برای بررسی امضاها  $\{M_n, ID^n, \delta_n, T_n\}, \dots, \{M_1, ID^1, \delta_1, T_1\}$  بردار اعداد تصادفی  $Vec_i$  را انتخاب کرده و با استفاده از رابطه (۵) امضاها را بررسی می کند.

$$e\left(\sum_{i=1}^n Vec_i \delta_i, P\right) = e\left(\sum_{i=1}^n Vec_i ID_1^i, P_{pub_1}\right) \cdot e\left(\left(\sum_{i=1}^n Vec_i h(M_i)h(ID_1^i \parallel ID_2^i \parallel T_i)\right) \cdot P, P_{pub_2}\right) \quad (5)$$

#### ۵- حمله به طرح لی و لای

در طرح لی و لای برای این که کارایی بهتری در تصدیق گروهی به دست آید به جای استفاده از نگاشت به نقطه  $H(\cdot)$  از تابع چکیده ساز  $h(\cdot)$  استفاده شده است که همین عامل باعث ایجاد یک ضعف بزرگ امنیتی در طرح آن ها گردیده است. حملاتی که در این مقاله ارائه می دهیم از این نقطه ضعف طرح لی و لای استفاده کرده و موفق به جعل امضا در طرح آن ها می شویم. در ادامه به معرفی سه سناریوی حمله ای که به این طرح انجام شد، می پردازیم.

تولید و پیام را امضا کند. با توجه به این که خودرو برای امضای هر پیام یک شناسه مستعار جدید تولید می کند بنابراین گمنامی و حریم خصوصی کاربر در این طرح ها کاملاً حفظ می شود. همچنین کلید اصلی سامانه فقط در اختیار TA می باشد بنابراین فقط TA می تواند هویت واقعی کاربر را افشا کرده و یا او را ردیابی کند. عمده مشکل طرح های مبتنی بر TPD نبود فرآیند واضحی برای ابطال کاربران متخلف می باشد زیرا با توجه به این که TPD هر خودرو شامل کلیدهای اساسی کل سامانه است، برای ابطال یک کاربر متخلف در شبکه باید آن کاربر را به صورت فیزیکی متوقف کرده و TPD آن را ضبط کرد [۱۲].

#### ۴- معرفی طرح لی و لای

طرح لی و لای یک طرح مبتنی بر TPD است که اطلاعات اصلی سامانه در TPD ذخیره می شود. این طرح شامل سه مرحله تولید و پیش توزیع کلید، تولید شناسه مستعار و کلید متناظر آن، امضا و واریسی پیام می باشد [۱۳].

#### ۴-۱- مرحله تولید و پیش توزیع کلید در طرح لی و لای

TA گروه دوری جمعی  $G$  تولید شده توسط  $P$  و گروه دوری ضربی  $G_T$  که  $G$  و  $G_T$  دارای مرتبه عدد اول  $q$  می باشند را تعیین کرده و تابع زوج سازی دو خطی  $e: G \times G \rightarrow G_T$ ، تابع چکیده ساز  $h: \{0,1\}^* \rightarrow \{0,1\}^n$  و تابع نگاشت به نقطه  $H: \{0,1\}^* \rightarrow G$  را تولید می کند. سپس TA دو مقدار تصادفی  $\langle S_1, S_2 \rangle$  را به عنوان کلید اصلی سامانه انتخاب کرده و مقادیر متناظر آن ها محاسبه می کند. سرانجام TA پارامترهای عمومی سامانه  $\langle G, G_T, q, P, P_{pub_1}, P_{pub_2}, e, h, H \rangle$  را در OBU و RSUها پیش ذخیره کرده و شناسه واقعی خودرو  $RID \in G$ ، گذرواژه PWD و کلیدهای اصلی سامانه  $\langle S_1, S_2 \rangle$  را در TPD هر خودرو ذخیره می کند. شناسه واقعی خودرو آن را به صورت منحصر به فرد از سایر خودروها تفکیک می کند و گذرواژه PWD برای احراز اصالت کاربر به TPD مورد استفاده قرار می گیرد.

#### ۴-۲- مرحله تولید شناسه مستعار در طرح لی و لای

خودروی  $V_i$ ، شناسه حقیقی  $RID_i$  و گذرواژه  $PWD_i$  را برای تولید شناسه مستعار وارد TPD می کند. TPD بعد از بررسی  $RID_i$  و  $PWD_i$ ، یک مقدار تصادفی  $r$  و مهر زمانی  $T_i$

$$SK_2^x = h(ID_1^x \parallel ID_2^x \parallel T_i)P_{pub_2} \quad (۶)$$

با این روش مهاجم می‌تواند برای هر مهر زمانی یک امضای دلخواه را تولید کند که مربوط به هیچ شناسه‌ای در شبکه نمی‌باشد و اگر TA سعی کند تا شناسه امضاکننده را به دست آورد به یک مقدار کاملاً تصادفی  $RID_x$  می‌رسد که مربوط به هیچ کاربری نیست. باید توجه کرد که این محاسبات خارج از TPD انجام می‌شود و هیچ نیازی به پارامترهای اساسی  $\langle S_1, S_2 \rangle$  ذخیره‌شده در TPD ندارد.

### ۵-۳- سناریوی سوم حمله

اگر مهاجم مقادیر  $\langle P_{pub_1}, P_{pub_2} \rangle$  را هم در اختیار نداشته باشد با توجه به این که TPD مقادیر  $\langle ID^i, SK^i \rangle$  را تولید کرده و در اختیار خودرو قرار می‌دهد، آن‌گاه مهاجم می‌تواند بر اساس این اطلاعات  $P_{pub_2}$  را به صورت زیر محاسبه کند.

$$P_{pub_2} = h(ID_1^i \parallel ID_2^i \parallel T_i)^{-1} SK_2^i \quad (۷)$$

حال مهاجم می‌تواند از سناریوهای اول و دوم حمله برای جعل امضا استفاده کند. بنابراین در این سناریوی حمله حتی اگر مهاجم عضو شبکه نباشد و مقادیر عمومی شبکه را هم در اختیار نداشته باشد، باز می‌تواند امضاهایی را در شبکه جعل کند که مورد تصدیق تمامی کاربران قرار خواهد گرفت.

بنابراین مهاجم با استفاده از سه سناریوی حمله مطرح شده قادر است تا امضای یک کاربر شبکه را جعل کرده و هر پیام اشتباهی را بدون آن که شناسایی شود در شبکه منتشر کند. حملات فوق به این علت به طرح لی و لای امکان پذیر شده‌اند که آن‌ها برای افزایش کارایی طرح خود به جای استفاده از نگاشت به یک نقطه  $H(\cdot)$ ، از تابع چکیده‌ساز  $h(\cdot)$  استفاده کرده‌اند، در بخش آتی طرح بهبود یافته لی و لای را ارائه خواهیم کرد.

### ۶- طرح پیشنهادی

برای مقابله با ضعف ایجادشده در طرح لی و لای در این بخش یک طرح بهبود یافته را ارائه می‌کنیم که در برابر حملات اشاره‌شده در بخش قبل مقاوم است. در طرح پیشنهادی ما مانند طرح لی و لای هر خودرو مجهز به یک TPD است که پارامترهای اساسی سامانه در آن ذخیره می‌گردند، این طرح شامل مراحل ثبت‌نام و پیش توزیع پارامترهای اساسی سامانه، تولید شناسه مستعار، امضا و واریسی پیام می‌باشد.

#### ۶-۱- ثبت‌نام و پیش توزیع کلید

در این طرح مانند طرح لی و لای TA مسئول ثبت‌نام، آماده‌سازی پارامترهای اساسی سامانه و پیش‌ذخیره آن‌ها در

### ۵-۱- سناریوی اول حمله

با توجه به این که در مرحله ثبت‌نام TA مقادیر کلیدهای اصلی  $\langle S_1, S_2 \rangle$  را در TPD و سایر مقادیر  $\langle G, G_T, q, P, P_{pub_1}, P_{pub_2} \rangle$  را در خودروها پیش‌ذخیره می‌کند، لذا هر کاربری به  $\langle P_{pub_1}, P_{pub_2} \rangle$  دسترسی خواهد داشت. حال اگر خودروی  $V_j$  امضای  $\langle ID^j, M_j, \delta_j, T_j \rangle$  را انجام داده باشد که در آن  $\delta_j = SK_1^j + h(M_j)SK_2^j$  است، آن‌گاه یک مهاجم که کاربر شبکه نیز است می‌تواند به صورت زیر کلیدهای خصوصی خودروی  $V_j$  را به دست آورده و در آن مهر زمانی هر پیامی را از طرف خودروی  $V_j$  امضا کند.

۱. با توجه به این که  $ID^j$  مشخص است و در امضای  $\langle ID^j, M_j, \delta_j, T_j \rangle$  ارسال شده است مهاجم می‌تواند  $h(ID_1^j \parallel ID_2^j \parallel T_i)$  را محاسبه کند.

۲. مهاجم با داشتن  $P_{pub_2}$  می‌تواند مقدار عبارت  $SK_2^j = h(ID_1^j \parallel ID_2^j \parallel T_i)P_{pub_2}$  را محاسبه کند.

۳. با تفریق دو نقطه از منحنی بیضوی می‌تواند عبارت  $SK_1^j = \delta_j - h(M_j)SK_2^j$  را به دست آورد.

بنابراین از این پس مهاجم با به دست آوردن مقادیر  $\langle SK_1^j, SK_2^j \rangle$  می‌تواند در مهر زمانی  $T_j$  هر پیامی را از طرف خودروی  $V_j$  امضا کند. باید توجه کرد که در این سناریوی حمله مهاجم می‌تواند هر پیام جعلی را از طرف یک کاربر مجاز شبکه امضا کند، در صورتی که آن کاربر هیچ اطلاعی از این امضا ندارد و در صورت بررسی هویت واقعی خودرو، TA به شناسه واقعی RID با زیروند  $i$  خواهد رسید که در واقع اصلاً تولید کننده این امضا نبوده است و مهاجم با استفاده از این شناسه یک پیام جعلی را امضا کرده است، در واقع این بسیار مخاطره آمیز است که مهاجم بتواند از طرف یک کاربر حقیقی امضایی را با شناسه او جعل کند.

### ۵-۲- سناریوی دوم حمله

مهاجم با در اختیار داشتن مقادیر  $\langle P_{pub_1}, P_{pub_2} \rangle$  که پارامترهای عمومی سامانه هستند می‌تواند یک امضای جعلی را در هر مهر زمانی به صورتی تولید کند که این امضا مربوط به هیچ کاربر شبکه نبوده اما حتماً تصدیق می‌شود و توسط TA هم قابل ردیابی نیست زیرا RID آن کاملاً جعلی می‌باشد.

۱. مهاجم با توجه به سناریوی اول حمله مقدار  $SK_1^j$  را بر اساس  $ID_1^j$  از خودروی  $V_j$  به دست می‌آورد، سپس از این شناسه به عنوان  $ID_1^x = ID_1^j$  استفاده می‌کند.

۲. مهاجم یک مقدار کاملاً تصادفی را به عنوان  $RID_x$  انتخاب کرده و سپس  $ID_2^x$  را به صورت زیر محاسبه می‌کند.

$$ID_2^x = RID_x \oplus H(rP_{pub_1})$$

۳. آن‌گاه  $SK_1^x = SK_1^j$  و  $SK_2^x$  را برای هر  $T_i$  به صورت زیر محاسبه می‌کند.

$$\delta_i = SK_1^i + h(M_i)SK_2^i \quad (8)$$

وارسی کننده امضا که می‌تواند خودروهای مجاور و یا RSU باشد با دریافت مقادیر  $\langle ID^i, M_i, \delta_i, T_i \rangle$  ابتدا معتبر بودن مهر زمانی  $T_i$  را بررسی کرده و سپس در صورت برقراری رابطه زیر امضا را تصدیق می‌کند.

$$e(\delta_i, P) = e(ID_1^i, P_{pub_1}) \cdot e(h(M_i)H(ID_1^i \parallel ID_2^i \parallel T_i), P_{pub_2}) \quad (9)$$

در ادامه صحت درستی رابطه (۹) نشان داده شده است.

$$\begin{aligned} e(\delta_i, P) &= e(sk_1^i + h(M_i)sk_2^i, P) = \\ &= e(SK_1^i, P) \cdot e(h(M_i)SK_2^i, P) \\ &= e(S_1 ID_1^i, P) \cdot e(h(M_i)S_2 H(ID_1^i \parallel ID_2^i \parallel T_i), P) \end{aligned}$$

$$\begin{aligned} &= e(ID_1^i, S_1 P) \cdot e(h(M_i)H(ID_1^i \parallel ID_2^i \parallel T_i), S_2 P) \\ &= e(ID_1^i, P_{pub_1}) \cdot e(h(M_i)H(ID_1^i \parallel ID_2^i \parallel T_i), P_{pub_2}) \end{aligned}$$

همچنین وارسی کننده پیام برای تصدیق گروهی امضاهای  $\{M_1, ID^1, \delta_1, T_1\}, \dots, \{M_n, ID^n, \delta_n, T_n\}$  می‌تواند صحت رابطه زیر را مورد بررسی قرار می‌دهد.

$$\begin{aligned} &e\left(\sum_{i=1}^n \delta_i, P\right) \\ &= e\left(\sum_{i=1}^n ID_1^i, P_{pub_1}\right) \cdot e\left(\sum_{i=1}^n h(M_i)H(ID_1^i \parallel ID_2^i \parallel T_i), P_{pub_2}\right) \quad (10) \end{aligned}$$

#### ۶-۴- بهبود طرح پیشنهادی در تصدیق گروهی

در طرح لی و لای با توجه به این که برای وارسی مجموعه پیام‌های  $\{M_1, ID^1, \delta_1, T_1\}, \dots, \{M_n, ID^n, \delta_n, T_n\}$  یک بردار تصادفی  $Vec_i$  انتخاب می‌شود، حال اگر مهاجم تعدادی پیام متفاوت و امضای آن‌ها را به صورت  $\langle ID^1, M_1, \delta_1 \rangle$ ،  $\langle ID^2, M_2, \delta_2 \rangle$ ،  $\langle ID^3, M_3, \delta_3 \rangle$  بسته‌های ارسالی را به صورت  $\langle ID^1, M_1, \delta_2 \rangle$ ،  $\langle ID^2, M_2, \delta_3 \rangle$ ،  $\langle ID^3, M_3, \delta_1 \rangle$  جابه‌جا کند، این مجموعه از امضاها مورد تصدیق واقع نخواهند شد. بنابراین مهاجم می‌تواند با کمترین توان ممکن یعنی فقط با تغییر ترتیب امضاها و پیام‌های ارسالی موجب شود تا تعدادی امضای صحیح اشتباه تلقی گردد، باید توجه کرد که طرح پیشنهادی ما فاقد این ضعف می‌باشد و تعدادی امضا صحیح که تنها ترتیب آن‌ها تغییر کرده است اشتباه تلقی نمی‌گردد.

$$e\left(\sum_{i=1}^3 Vec_i \delta_i, P\right) = e(Vec_1 \delta_2 + Vec_2 \delta_3 + Vec_3 \delta_1, P) \quad (11)$$

$$\neq e\left(\sum_{i=1}^n Vec_i ID_1^i, P_{pub_1}\right) \cdot e\left(\left(\sum_{i=1}^n Vec_i h(M_i)\right) h(ID_2^i), P, P_{pub_2}\right)$$

TPD خودروهای مجاز شبکه می‌باشد. مرحله ثبت‌نام و پیش توزیع کلید در طرح پیشنهادی ما نیز مشابه طرح لی و لای می‌باشد.

TA گروه دوری جمعی  $G$  تولیدشده توسط مولد  $P$  و گروه دوری ضربی  $G_T$  که  $G$  و  $G_T$  دارای مرتبه عدد اول  $q$  می‌باشند را تعیین کرده و تابع زوج‌سازی دو خطی  $e: G \times G \rightarrow G_T$ ، تابع چکیده‌ساز  $h: \{0,1\}^* \rightarrow \{0,1\}^n$  و تابع نگاشت به نقطه  $H: \{0,1\} \rightarrow G$  را تولید می‌کند. تابع نگاشت به نقطه  $H(\cdot)$  هر عضو از میدان  $Z_q^*$  را به یک نقطه از میدان منحنی بیضوی  $G$  نگاشت می‌کند. سپس TA دو مقدار تصادفی  $\langle S_1, S_2 \rangle$  را به‌عنوان کلید اصلی سامانه انتخاب کرده و مقادیر  $P_{pub_2} = S_2 P$  و  $P_{pub_1} = S_1 P$  را به‌عنوان کلید عمومی متناظر آن‌ها محاسبه می‌کند. سرانجام TA پارامترهای عمومی سامانه  $\langle G, G_T, q, P, P_{pub_1}, P_{pub_2}, e, h, H \rangle$  را در OBUها و RSUها پیش‌ذخیره کرده و شناسه واقعی خودرو  $RID \in G$  گذرواژه  $PWD$  و کلیدهای اصلی سامانه  $\langle S_1, S_2 \rangle$  را در TPD هر خودرو ذخیره می‌کند. شناسه واقعی خودرو آن را به صورت منحصر به فرد از سایر خودروها تفکیک می‌کند و گذرواژه  $PWD$  برای احراز اصالت کاربر به TPD می‌باشد. با توجه به این که این مقادیر در TPD خودرو ذخیره شده‌اند هیچ موجودیتی حتی صاحب خودرو امکان دسترسی به آن‌ها را ندارد.

#### ۶-۲- تولید شناسه مستعار

شناسه مستعار در طرح پیشنهادی مشابه طرح لی و لای تولید می‌شود، اما کلیدهای خصوصی متناظر با هر یک از شناسه‌های مستعار برای مقابله با حملات مطرح شده در بخش قبل به روش متفاوتی تولید می‌شود، و در تولید آن‌ها از تابع نگاشت به نقطه  $H(\cdot)$  استفاده می‌شود. خودروی  $V_i$  شناسه حقیقی  $RID_i$  و گذرواژه  $PWD_i$  را برای تولید شناسه مستعار وارد TPD می‌کند.

TPD بعد از بررسی  $RID_i$  و  $PWD_i$  یک مقدار تصادفی  $r$  و مهر زمانی  $T_i$  را انتخاب کرده و شناسه مستعار و کلید خصوصی را به صورت زیر تعیین و در اختیار کاربر قرار می‌دهد.

$$\begin{aligned} ID_1^i &= rP \\ ID_2^i &= RID_i \oplus H(rP_{pub_1}) \\ SK_1^i &= S_1 ID_1^i \\ SK_2^i &= S_2 H(ID_1^i \parallel ID_2^i \parallel T_i) \end{aligned}$$

#### ۶-۳- امضا و بررسی امضا

خودروی  $V_i$  برای امضای پیام  $M_i$  ابتدا یک شناسه مستعار و کلید خصوصی متناظر با آن را مانند زیر بخش قبل تولید کرده و سپس پیام را به صورت زیر امضا خواهد کرد و مقادیر  $\langle ID^i, M_i, \delta_i, T_i \rangle$  را به‌عنوان امضای خود ارسال می‌کند.

طرح بهبود یافته مهاجم نمی تواند با داشتن مقادیر  $\langle P_{pub_1}, P_{pub_2}, ID_1^i, ID_2^i, T_i \rangle$  کلید خصوصی  $SK_2^i$  و سپس  $SK_1^i$  را مانند سناریوهای مطرح شده در بخش های گذشته به دست آورد، زیرا با توجه به استفاده از تابع نگاشت  $H(\cdot)$  در تولید کلید خصوصی مهاجم برای به دست آوردن  $SK_2^i$  با استفاده از پارامترهای عمومی نیازمند حل مسئله لگاریتم گسسته بر روی منحنی های بیضوی می باشد که خود یک مسئله سخت محسوب می گردد. بنابراین اگر امضای پیامی تصدیق شود مطمئناً این پیام از سوی کاربر مجاز شبکه امضا شده و یک پارچگی آن نیز حفظ شده است.

### ۷-۲- گمنامی و پیوندناپذیری

با توجه به این که کاربر برای امضای هر پیام یک شناسه مستعار و کلید خصوصی جدید مستقل از شناسه های مستعار قبلی خود تولید می کند و با آن پیام را امضا می کند، بنابراین مهاجم نمی تواند هویت واقعی کاربر را به دست آورده و یا ارتباطی بین امضاهای مختلف او پیدا کند، لذا این طرح خاصیت گمنامی و پیوندناپذیری را بر آورده می کند.

### ۷-۳- ردیابی مشروط

با توجه به این که کاربر برای امضای هر پیام یک شناسه مستعار و کلید خصوصی جدید بر اساس شناسه حقیقی خود و کلید اصلی سامانه تولید می کند و با آن پیام را امضا می کند، لذا مهاجم با مشاهده تعدادی پیام مشخص، نمی تواند ارتباطی بین پیام های امضا شده و امضاکننده آن ها به دست آورد. همچنین مهاجم برای افشای هویت واقعی امضاکننده پیام نیازمند این است که مقادیر کلید اصلی سامانه یعنی  $(S_1, S_2)$  را به دست آورد که با توجه به این که آن ها در TPD خودرو ذخیره شده اند امکان بازیابی آن ها وجود ندارد و یا مهاجم باید قادر به حل مسئله ECDLP باشد تا بتواند با توجه به  $ID^i$  مقدار  $r$  را به دست آورد و به  $RID$  خودرو دست یابد. اما TA با داشتن مقادیر کلید اصلی سامانه  $(S_1, S_2)$  با محاسبه رابطه (۱۲) می تواند هویت واقعی خودرو را با توجه به شناسه مستعار آن به دست آورد.

$$SK_2^x = h(ID_1^x \parallel ID_2^x \parallel T_i) P_{pub_2} \quad (12)$$

بنابراین TA قادر به افشای هویت اصلی خودرو و ردیابی آن می باشد.

### ۸- پیاده سازی و کارایی طرح

شبیه سازی یکی از ابزارهای مهم برای تعیین و بررسی عملی بودن یک پروتکل و یا دستگاه می باشد. VANET برخلاف شبکه های دیگر از دو جنبه ترافیکی و شبکه بی سیم باید مورد بررسی قرار بگیرد. منظور از ترافیک، مجموعه ای از خودروها می باشد که در یک نقشه در حال حرکت هستند. از آن جا که ترافیک در شبکه مخابراتی تأثیر مستقیم دارد،

$$\begin{aligned} &= (Vec_1 ID_1^1 + Vec_2 ID_1^2 \\ &+ Vec_3 ID_1^3, P_{pub_1}). e(Vec_1 h(M_1) h(ID_1^1 \\ &\parallel ID_2^1) + Vec_2 h(M_2) h(ID_2^2 \parallel ID_2^2) \\ &+ Vec_3 h(M_3) h(ID_1^3 \parallel ID_2^3)). P, P_{pub_2} \end{aligned}$$

بنابراین در طرح لی و لای اختیار بیشتری به مهاجم داده شده است زیرا با این روش هر مهاجمی با کمترین توان محاسباتی و فقط با تغییر ترتیب تعدادی امضای صحیح می تواند باعث تصدیق نشدن این امضاهای صحیح گردد و عملکرد سامانه را تخریب کند، در صورتی که طرح پیشنهادی ما این مزیت را دارد که اگر یک تعداد امضای صحیح حتی اگر ترتیب آن ها هم تغییر کرده باشد باز هم صحیح تشخیص داده می شوند و مهاجم تنها با تغییر ترتیب امضاها نمی تواند مانع تصدیق تعدادی امضای صحیح گردد.

### ۷- تحلیل امنیتی طرح پیشنهادی

در این بخش طرح پیشنهادی خود را از منظر ملزومات امنیتی مهم در شبکه های VANET که شامل احراز اصالت پیام، گمنامی و حفظ حریم خصوصی کاربر و ردیابی مشروط خودروها می شود، مورد تحلیل قرار می دهیم.

#### ۷-۱- احراز اصالت پیام

احراز اصالت پیام از مهم ترین ملزومات امنیتی در شبکه های VANET می باشد تا بررسی کننده پیام مطمئن باشد که پیام از سوی کاربر مجاز شبکه ارسال شده و یک پارچگی آن نیز محفوظ مانده است.

با توجه به این که در این طرح هر پیام قبل از ارسال به صورت رابطه ۸ امضا می شود و این امضا شامل تابع چکیده ساز  $h(\cdot)$  می باشد، با فرض امن بودن این تابع چکیده ساز یک پارچگی پیام حفظ می شود، همچنین با توجه به استفاده از مهر زمانی  $T_i$  در تولید کلید خصوصی  $SK_2^i$  واریسی کننده پیام از تازه بودن پیام های امضا شده اطمینان حاصل می کند. استفاده از مهر زمانی در تولید امضا مانع بروز حمله تکرار به طرح می شود، یعنی مهاجم قادر نخواهد بود که پیام های امضا شده توسط کاربران مجاز شبکه در یک زمان را جمع آوری و در زمان دیگری منتشر کند تا شرایط ترافیکی جعلی را ایجاد کند. همچنین با توجه به این که برای امضای هر پیام از یک کلید خصوصی به صورت  $SK^i = (SK_1^i, SK_2^i) = \langle S_1 ID_1^i, S_2 H(ID_1^i \parallel ID_2^i) \rangle$  استفاده می شود، مهاجم برای جعل امضا باید قادر به محاسبه کلید خصوصی امضا باشد، محاسبه کلید خصوصی امضا با داشتن تنها مقادیر  $\langle ID^i, P_{pub}, P \rangle$  معادل حل مسئله لگاریتم گسسته بر روی زوج سازی های دوخطی می باشد که یک مسئله سخت محسوب می گردد. همچنین با توجه به اصلاح صورت گرفته در تولید کلید خصوصی  $SK_2^i$  در طرح پیشنهادی امکان برقراری حملات مطرح شده به طرح لی و لای به طرح وجود ندارد. در

می‌کند استفاده می‌کنیم. سپس تغییرات لازم را اعمال خواهیم کرد. برای شبیه‌سازی مراحل زیر انجام می‌شود:

- طراحی مدل شبیه‌سازی
- تعیین سناریوی شبیه‌سازی
- شبیه‌سازی و آنالیز داده‌ها

### ۸-۱- بررسی روش شبیه‌سازی

همان‌طور که در بالا اشاره شد شبیه‌سازی در دو بخش ترافیک و شبکه بی‌سیم انجام می‌گیرد. در ترافیک، تعداد زیادی از خودروها وجود دارند که هر کدام ویژگی‌های خاص خود مانند ابعاد، جهت حرکت و سرعت و غیره را دارند. الگوی حرکت نیز تأثیر زیادی بر جهت حرکت و بیشینه سرعت دارد. شکل (۲)، دو الگوی حرکت در شبیه‌سازی را نشان می‌دهد.

پارامترهای استفاده‌شده در شبیه‌سازی شبکه در جدول (۱) نشان داده شده است. در شبیه‌سازی تعداد خودروها را ثابت در نظر می‌گیریم و البته الگوی حرکت و زمان ورود و خروج خودروها در شبیه‌سازی تصادفی انتخاب می‌شوند. در این شبیه‌سازی در چهارراه حداقل سرعت ۳۰ و حداکثر آن ۶۰ است. درحالی‌که در بزرگراه این سرعت‌ها به ترتیب ۹۰ و ۱۱۰ می‌باشند.

یک شبکه بی‌سیم مجموعه‌ای از تبادل اطلاعات بین گره‌ها در خلال یک سیستم مخابراتی رادیویی می‌باشد. در این شبکه هر گره یک پشته پروتکلی دارد که پیام‌ها با کمک این پشته پروتکلی انتقال داده می‌شود. این پشته پروتکلی با توجه به استاندارد IEEE\_1609-2 شبیه‌سازی می‌شود که بخش‌های مختلفی از قبیل سرویس‌های پردازش<sup>۴</sup>، لایه فیزیکی، لایه ارتباط<sup>۵</sup> و غیره را در نظر دارد.

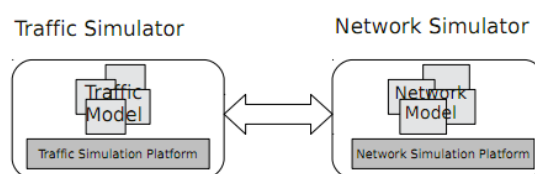


شکل (۲). دو الگوی حرکت (چهارراه و اتوبان)

پردازش پیام‌های امن در استاندارد IEEE\_1609-2 تعریف شده که انتقال امن اطلاعات، احراز اصالت و امضای پیام را شامل می‌شود. نمونه‌ای که برای شبیه‌سازی این استاندارد مناسب باشد در Veins لحاظ نشده و بنابراین باید این مدل به Veins اضافه شود.

می‌بایست در شبیه‌سازی اقتضایی بین خودرویی حتماً لحاظ شود. شبیه‌سازی اقتضایی بین خودرویی با دو شبیه‌ساز انجام می‌شود که یکی حرکت خودروها و دیگری شبکه مخابراتی را شبیه‌سازی می‌کند. شکل (۱) خلاصه‌ای از دو عامل شبیه‌سازی را بیان می‌کند.

آن چیزی که در شبیه‌سازی بسیار مهم است، حداقل کردن تفاوت شبیه‌سازی و واقعیت می‌باشد و از این رو برآورد دقیقی از پارامترهای دخیل در شبیه‌سازی ترافیک مانند، نقشه خیابان‌ها، اتوبان‌ها، ترافیک خودروها، قوانین رانندگی و غیره بسیار مهم است.



شکل (۱). دو عامل اصلی در شبیه‌سازی

شبیه‌سازی ترافیک به دو دسته ماکروسکوپی و میکروسکوپی تقسیم می‌شود. شبیه‌سازی ماکروسکوپی عواملی مانند چگالی ترافیک، نقشه و ساختار راه‌ها را در نظر می‌گیرد. شبیه‌سازی میکروسکوپی عواملی مانند انسان‌های در حال حرکت، ساختمان‌ها، آب و هوا را بررسی می‌کند [۱۷-۱۵]. در اقتضایی بین خودرویی عوامل میکروسکوپی خیلی تأثیری بر نتایج شبیه‌سازی ندارند و لذا از این به بعد منظور ما از شبیه‌سازی ترافیک، شبیه‌سازی ماکروسکوپی شبکه می‌باشد. شبیه‌سازی ترافیک، شامل محدودیت‌های حرکتی و تولید ترافیک است. محدودیت‌های ترافیکی مدل حرکت خودروها، قوانین رانندگی، مشخصات جغرافیایی، جهت خیابان‌ها و غیره را تعیین می‌کند. در ضمن چگالی و تابع توزیع ترافیک از عوامل مهم در تعیین محدودیت‌های ترافیکی است.

امروزه بسترهای مختلفی برای شبیه‌سازی مورد استفاده قرار می‌گیرند [۲۹-۱۸]. برای مثال Mobisim [۲۶]، SUMO [۲۹] و CityMob [۳۰]، مشهورترین آن‌ها و SUMO رایج‌ترین آن‌ها می‌باشد. SUMO یک بستر منبع باز است که اخیراً با شبیه‌سازهای شبکه NS2، NS3 و OMNet++ ترکیب و بستر مناسبی برای شبیه‌سازی اقتضایی بین خودرویی فراهم شده است. آنچه که ما در این شبیه‌سازی استفاده کرده‌ایم، OMNet++ به همراه بسته‌های زیر می‌باشد.

- MiXim
- Viens
- INET

این بسته‌ها در لایه کاربردی<sup>۱</sup>، WSMP<sup>۲</sup> و فیزیکی<sup>۳</sup> استفاده می‌شوند. احراز اصالت توسط لایه WSMP انجام می‌شود که بالاتر از لایه فیزیکی است. بنابراین ما برای شبیه‌سازی از بسته Viens که لایه فیزیکی را شبیه‌سازی

- 1- Application Layer
- 2- Wave Short Message Protocol
- 3- Physical
- 4- Process services
- 5- Link layer



جدول (۲). پارامترهای شبیه سازی ترافیک

تعداد ماشین	500
حداکثر سرعت شهری	60 Km/H
حداقل سرعت شهری	30 Km/H
بیشینه سرعت اتوبان	110 Km/H
کمینه سرعت اتوبان	90 Km/H

### ۸-۲- روش شبیه سازی

در شبیه سازی انجام شده، تمامی گره ها قادر به حرکت در شبکه ترافیکی و ارسال امن پیام های خود می باشند. قبل از ارسال پیام ها لازم است که پارامترهای عمومی سامانه [۳۱]، به گره ها اطلاع رسانی شده باشد. هدف اصلی ما از شبیه سازی برآورد تأخیر بررسی صحت پیام دریافتی می باشد.

### ۸-۳. نتیجه شبیه سازی:

در این بخش طرح پیشنهادی خود را با طرح های BLS، ECPP، DCS و LPA مقایسه می کنیم. جدول (۵) میزان پیچیدگی واریاسی امضای این طرح ها را در حالت واریاسی منفرد امضا و حالت واریاسی گروهی، با یکدیگر مقایسه می کند. با توجه به جدول (۵) میزان پیچیدگی طرح پیشنهادی ما با پیچیدگی طرح ECPP در حالت منفرد برابر است و از سایر طرح ها بهتر می باشد. همچنین طرح پیشنهادی ما در واریاسی گروهی امضاها از طرح های BLS، DCS، ECPP کارآمدتر است.

در فرآیند تولید و تأیید امضا، زمان اجرای الگوریتم شامل دو زمان ثابت و متغیر می باشد. به این صورت که زمان اجرای بعضی از عملگرها وابسته به طول پیام و بعضی دیگر از طول پیام مستقل هستند. از طرف دیگر زمان به توانایی پردازشگر و روش پیاده سازی نیز وابسته است. ما در شبیه سازی از بسته GMP [۳۲]، و پردازشگر X2 Ultra Dual-core Mobile ZM- AMD Turin (tm) 80 استفاده می کنیم. زمان اجرای عملگرها در جدول (۳) آمده است.

در طرح پیشنهادی از تابع چکیده ساز MD5 استفاده شده است که زمان اجرای آن به طول داده ورودی وابسته است. زمان اجرای الگوریتم پیشنهادی بر اساس مقادیر جدول (۳) در جدول (۴) آمده است. زمان سرپار، اختلاف زمان بین ورود داده به WSMP و خروج داده از آن است، که این زمان با رابطه زیر محاسبه می شود:

$$AD = \frac{1}{M} \sum_{i=1}^M T_{out}^i - T_{rec}^i \quad (13)$$

برای این منظور دو ماژول برای شبیه سازی WSMP و سرویس پردازش امنیت در نظر می گیریم، ماژول های سرویس پردازش امن و ماژول WSMP. ماژول های لایه کاربرد بسته های داده را با کمک WSMP ارسال و پردازش امن با کمک ماژول سرویس پردازش امن انجام می شود.

جدول (۱). پارامترهای شبیه سازی شبکه

20mW	بیشینه توان ارسال
18Mbps	نرخ بیت
-89dBm	حداقل آستانه میرایی سیگنال <sup>۱</sup>
2	کمینه ضریب تضعیف مسیر <sup>۲</sup>
5.890e9 Hz	کمینه فرکانس حامل کانال
Uniform(128bit, 131072bit)	طول بسته کاربردی <sup>۳</sup>

بالاترین لایه، لایه کاربرد است که پیام های امن با طول مختلف به گره های دیگر از مسیرهای مختلف ارسال می شود. این فرآیند برای هر گره یک ترافیک دریافت و آنالیز داده ایجاد می کند.

در لایه WSMP، پیام های دریافتی از لایه کاربرد و شبکه به سرویس پردازش امن برای امضا یا بررسی امضا داده می شود. در سرویس پردازش امن، زمان اجرای پردازش به روش پردازش، طول پیام ها و پردازشگر درون RSU و OBU بستگی دارد. لایه شبکه که یک لایه فیزیکی است و لایه های IEEE\_1609-4 پیام های لایه های بالاتر را به گره های دیگر از طریق کانال مخابراتی انتقال می دهند. همچنین پیام های دریافت شده از طریق کانال مخابراتی را به لایه های بالاتر منتقل می کنند. ماژول تحرک<sup>۴</sup>، مدل حرکت هر گره را بر اساس محدودیت های ترافیکی مانند آنچه در جدول ۲ آمده است، تعیین می کند. بر اساس استاندارد IEEE\_1609.2 هر پیام به طور جداگانه امضا و ارسال می شود. اگرچه روش های امضا طرح های امضا متفاوت هستند، اما فرآیند امضا و ارسال در همه طرح ها یکسان می باشد (شکل های ۳ و ۴). پیام های دریافتی همگی به سرویس پردازش امنیت منتقل و در آنجا اعتبار آن ها بررسی می شود.

- 1- Minimum signal attenuation threshold
- 2- Minimum path loss coefficient
- 3- Application packet length
- 4- Mobility module

جدول (۳). زمان عملگرها به ثانیه

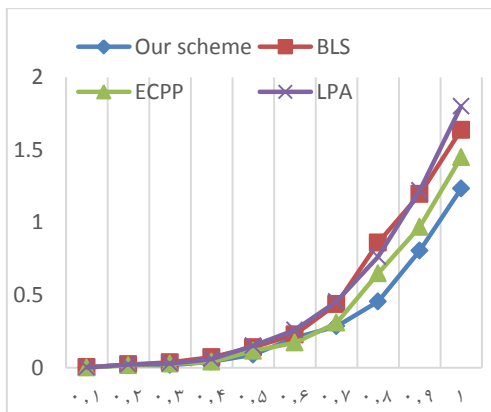
500	تعداد ماشین
4.41e-04	ضرب برداری
4e-08	جمع
2.8e-07	مولد تصادفی
8.820e-3	زوج‌سازی
1.1025e-4	نگاشت به نقطه
0.022Mbits/s	تابع چکیده ساز

جدول (۴). زمان اجرای طرح

بررسی	امضا	
0.022Mbit/s+0.0512 s	0.022Mbit/s+0.0157 4187s	طرح

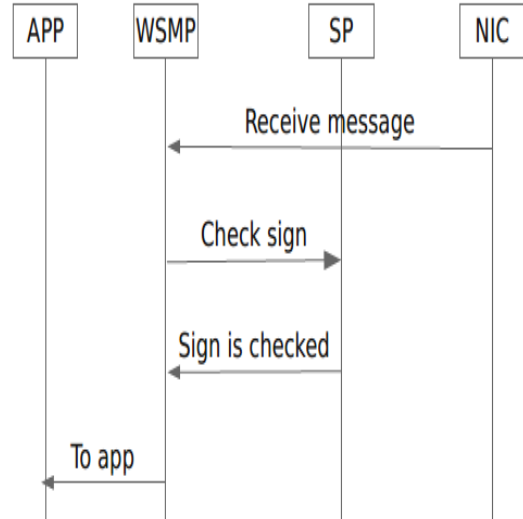
جدول (۵). میزان پیچیدگی و ارسی امضای طرح پیشنهادی با طرح‌های ECPP و LPA، DCS، BLS

نام طرح	وارسی منفرد	وارسی گروهی
BLS	$4T_{pair} + 2T_{mtp}$	$(2n + 2)T_{pair} + 2nT_{mtp}$
ECPP	$3T_{pair} + T_{mul} + T_{mtp}$	$3nT_{pair} + 11nT_{mul}$
DCS	$5T_{pair} + 3T_{mul}$	$5T_{pair} + 3nT_{mul}$
LPA	$4T_{pair} + T_{mul} + T$	-----
طرح پیشنهادی	$3T_{pair} + T_{mul} + T_{mtp}$	$3T_{pair} + nT_{mul} + nT_{mtp}$

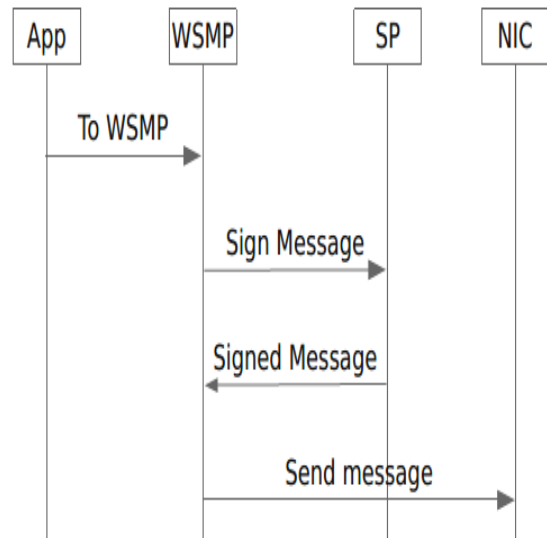


شکل (۵). متوسط تأخیر ناشی از اجرای طرح‌های ECPP، BLS، LPA و طرح پیشنهادی در چهار راه

که در آن،  $M$  تعداد پیام‌ها،  $T_{rec}^i$  زمان دریافت پیام در WSMP و  $T_{out}^i$  زمان ارسال پیام می‌باشد.



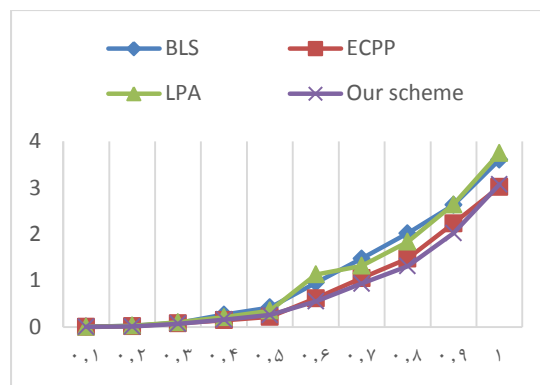
شکل (۳). گردش پیام برای دریافت داده در VANET



شکل (۴). گردش پیام برای ارسال داده در VANET

در این شبیه‌سازی درصد خودروها از ۱۰ درصد تا ۱۰۰ درصد تغییر و بر اساس آن کارایی طرح بررسی می‌شود. نتایج این شبیه‌سازی‌ها برای طرح‌های BLS، ECPP، LPA و طرح پیشنهادی برای دو حالت چهارراه و بزرگراه در شکل‌های (۵) و (۶) آمده است.

- [2] A. Menezes, "An introduction to pairing-based cryptography," 1991. Online: <http://www.math.uwaterloo.ca/~ajmeneze/publications/pairings>. Pdf (retrieved: January 2012).
- [3] D. Hankerson, V. Scott, and J. M. Alfred, "Guide to elliptic curve cryptography," Springer, 2004.
- [4] I. Blake, et al., "Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series), Cambridge University Press, 2005.
- [5] H. Xiong, et al., "Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview," Applied Cryptography and Network Security, 2012.
- [6] A. Wasef, Y. Jian, and X. Shen, "An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Transaction on Vehicular Technology, vol. 59, no. 2, P. 553, 2010.
- [7] R. Lu, et al., "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," INFOCOM 2008. The 27th Conference on Computer Communications IEEE, 2008.
- [8] D. Boneh, B. Lynn, and H. Shacham, "short signature from the weil pairing," In proceedings of Asiacrypt, p. 2248, pp. 514-532, 2001.
- [9] X. Sun, L. Xiaodong, and H. Pin-Han, "Secure vehicular communications based on group signature and ID-based signature scheme," Communications, 2007, ICC'07, IEEE International Conference on, IEEE, 2007.
- [10] H. Xiong, Z. Qin, and F. Li, "Identity-based Ring Signature Scheme based on quadratic residues," High Technology Letters, vol. 15, no. 1, pp. 94-100, 2011.
- [11] H. Xiong, C. Zhong, and L. Fagen, "Efficient and multi-level privacy-preserving communication protocol for VANET," Computers & Electrical Engineering vol. 38, no. 3, pp. 573-581, 2012.
- [12] C. Zhang, et al., "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," Communications, 2008. ICC'08, IEEE International Conference on, IEEE, 2008.
- [13] C. Zhang, H. Pin-Han, and T. Janos, "On batch verification with group testing for vehicular communications," Wireless Networks, vol. 17, no. 8, pp. 1851-1865, 2011.
- [14] Lee, Cheng-Chi, and L. Yan-Ming, "Toward a secure batch verification with group testing for VANET," Wireless Networks, pp. 1-9, 2013.



شکل (۶). متوسط تأخیر ناشی از اجرای طرح های BLS, ECPP, LPA و طرح پیشنهادی در بزرگراه

## ۹- نتیجه گیری

در این مقاله طرح احراز اصالت لی و لای را مورد تحلیل و ارزیابی قرار داده و سه سناریوی حمله را به آن مطرح کردیم که این حملات امکان جعل امضای کاربر مجاز و غیر مجاز شبکه را به مهاجم می دهد، سپس طرح بهبود یافته ای از آن را پیشنهاد داده ایم که در برابر جعل امضای کاربر مقاوم می باشد. آنچه امکان وقوع این حملات را به مهاجم در طرح لی و لای داده است آن است که آن ها برای بهبود عملکرد طرح خود در واریسی گروهی امضا از تابع چکیده ساز استفاده کرده اند، اما ما در طرح پیشنهادی خود از خواص تابع نگاشت به نقطه استفاده کرده ایم، و همین امر باعث مقاوم شدن طرح پیشنهادی ما در برابر حملات جعل امضا شده است. طرح پیشنهادی ما ملزومات امنیتی لازم در شبکه های VANET را که شامل احراز اصالت پیام، ردیابی مشروط، گمنامی و پیوندناپذیری کاربر می باشد را برآورده می کند. همچنین در طرح پیشنهادی ما قابلیت واریسی گروهی امضاها به صورت کارآمد وجود دارد. در پایان شبیه سازی طرح پیشنهادی خود را به همراه اصول استفاده شده در این شبیه سازی بیان کرده ایم. همچنین عملکرد طرح پیشنهادی خود را با طرح های BLS, DCS, ECPP و LPA در دو حالت واریسی منفرد و گروهی امضاها مورد مقایسه قرار دادیم، و همان طور که در شکل های (۵ و ۶) نشان داده شده است طرح پیشنهادی ما دارای کارایی بهتری نسبت به این طرح ها می باشد.

## ۱۰- مراجع

- [1] D. Antolino Rivas, et al., "Security on VANETS: Privacy misbehaving nodes false information and secure data aggregation," Journal of Network and Computer Applications, vol. 34, no. 6, pp. 1942-1955, 2011.

- Communications and Services (European Wireless), 11th European, VDE, 2005.
- [26] J. Miller and E. Horowitz, "A free real-time freeway trac simulator," in: Intelligent Transportation Systems Conference, ITSC2007. IEEE, pp.18-23, 2007.
- [27] J. Härrri, et al., "Vanet Mobi Sim: generating realistic mobility patterns for VANETs," Proceedings of the 3rd international workshop on Vehicular ad hoc networks, ACM, 2006.
- [28] Krajzewicz, Daniel, and R. Christian, "Simulation of urban mobility (SUMO)," Centre for Applied Informatics (ZAIK) and the Institute of Transport Research at the German Aerospace Centre, 2007.
- [29] Karnadi, K. Feliz, H. M. Zhi, and L. Kun-chan "Rapid generation of realistic mobility models for VANET," Wireless Communications and Networking Conference, WCNC 2007, IEEE, 2007.
- [30] K. Fall and K. Varadhan, *Ns Notes and Documents* 2011. URL:<http://www.isi.edu/nsnam/ns-documentation.html>. IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006) (2013)
- [15] H. Haj Salem, J. Chrisoulakis, M. Papageorgiou, N. Elloumi, and P. Papadakos, "The use of METACOR tool for integrated urban and interurban trac control," Evaluation in corridor peripherique, Paris, Vehicle Navigation and Information Systems Conference, Proceedings, pp. 645-650, 1994.
- [16] K. Nagel and A. Schleicher, "Microscopic traffic modeling on parallel high performance computers," *Parallel Computing*, vol. 20, no. 1, pp. 125-146, 1994.
- [17] S. Krau, "Microscopic modeling of trac Investigation of collision free vehicle dynamics," Ph. D. thesis, Universitat zu Koln, 1998.
- [18] M. Treiber, A. Hennecke, and D. Helbing, "Congested trac states in empirical observations and microscopic simulations," *Phys. Rev. E* 62, 2000. 18051824. doi:10.1103/PhysRevE.62.1805. Figure 9: Box chart of simulation time.
- [19] F. Bai, N. Sadagopan, and A. Helmy, "The fimportantg framework for analyzing the Impact of Mobility on Performance Of Routing protocols for Adhoc Networks," *Ad Hoc Networks* vol. 1, pp. 383-403, 2003. Doi: 10.1016/S1570-8705(03)00040-4.
- [20] N. Aschenbruck, et al., "Bonnmotion: a mobility scenario generation and analysis tool," Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques, ICST (Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), 2010.
- [21] A. K. Saha and B. J. David, "Modeling mobility for vehicular ad-hoc networks," Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, ACM, 2004.
- [22] R. Mangharam, et al., "GrooveSim: a topography-accurate simulator for geographic routing in vehicular networks," Proceedings of the 2nd ACMinternational workshop on Vehicular ad hoc networks, ACM, 2005.
- [23] M. Feeley, H. Norman, and R. Suprio, "ealistic mobility for mobile ad hoc network simulation," *Ad-Hoc, Mobile, and Wireless Networks*, Springer Berlin Heidelberg, pp. 324-329, 2004.
- [24] A. Mahajan, et al., "Evaluation of mobility models for vehicular ad-hoc network simulations," IEEE International Workshop on Next Generation Wireless Networks (WoNGeN), 2006.
- [25] Zimmermann, Hans-Martin, G. Ingo, and R. Christian, "A voronoi-based mobility model for urban environments," *Wireless Conference 2005-Next Generation Wireless and Mobile*

---

## An Improved Authentication Scheme with Conditional Privacy Preserving in VANETs

S. M. Pournaghi\*, M. Barmshoori, M. Gardeshi

Qom University

(Received: 07/12/2014, Accepted: 06/10/2015)

### ABSTRACT

*Vehicular Ad-hoc Networks (VANETs) can improve the communication between vehicles and traffic management to control appropriate. Authentication of messages which is issued by each vehicle is the most important problem in VANETs, because the wrong messages can cause crashes and change the traffic patterns of network. Many authentication schemes have been proposed in VANETs, each of which has advantages and disadvantages. In this paper first we introduce, a brief overview of these schemes. Then we analyse an authentication scheme for VANETs which introduced by Lee and Lai and introduce three scenarios that show their scheme is vulnerable to forgery attack. These attacks motivated us to design a novel and secure TPD based authentication scheme satisfying all security requirements in VANETs. Moreover, we introduce a simulation and comparison expressing the efficiency and performance of the proposed scheme.*

**Keywords:** VANET, conditional privacy preserving authentication, bilinear pairing, pseudo identity

---

\* Corresponding Author Email: sm.pournaghi@gmail.com