مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۲، تابستان ۱۳۹۴، ص ۱۲- ۱

طرح بهبودیافته احراز اصالت با حفظ گمنامی مشروط در شبکه‌های اقتضایی بین خودرویی

سید مرتضی پورنقی[1*]، مصطفی برمشوری[2]، محمود گردشی[3]
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 بهبودیافته از طرح لی و لای را پیشنهاد می‌دهیم که دارای ملزومات امنیتی و کارآیی 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

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[1] 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 این‌که هنگام طراحی پروتکل‌های 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 به شمار 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 کارآیی 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

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

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[۱] 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[۲] بوده که وظیفه تولید و انتشار پیام‌های ترافیکی را بر عهده دارد، همچنین ایستگاه‌های کنار جاده‌ای به نام RSU[۳] 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[۴] 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[۵]: 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 $e: G_1 \times G_1 \to G_2$ یک زوج‌سازی دو خطی است اگر شرایط زیر را برآورده کند [۴-۲].

- دو خطی بودن[۶]: به‌ازای هر $X,Y \in G_1$ و $a,b \in Z_p^*$ داریم:
$$e(aX, bY) = e(X,Y)^{ab}$$
- زوال‌ناپذیری[۷]: 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[۸]: 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[۹]): 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[۱۰]): 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[۱۱]): 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[۱۲]): 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[۱۳]) 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

به‌طورکلی 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[۱۴]

1- Conditional privacy preserving
2- On Board Unit
3- Road Side Unit
4- Lee & Lai
5- Bilinear Pairing
6- Bilinearity
7- Non-Degeneracy
8- Computationality
9- Elliptic Curve Discret Logarithm
10- Computational Diffie-Hellman
11- Decisional Diffie-Hellman
12- Computational Billinear Diffie-Hellman
13- Decisional Billinear Diffie-Hellman
14- Tamper Proof Device

۳-۱- طرح‌های مبتنی بر گواهی‌های بی‌نام

در این طرح‌ها با توجه به سطح گمنامی مورد نیاز در شبکه هر کاربر تعداد زیادی گواهی بی‌نام که توسط CA[1] امضا شده و کلید خصوصی متناظر با آن‌ها را، به‌صورت امن از TA[2] دریافت می‌کند، در این گواهی‌ها هیچ اطلاعاتی از هویت واقعی کاربر ثبت نشده است، لذا این گواهی‌ها گمنامی کاربران را کاملاً حفظ می‌کنند. برای ارسال هر پیام OBU به‌صورت تصادفی یکی از این گواهی‌ها را انتخاب کرده و سپس با کلید خصوصی متناظر با آن، پیام را امضا می‌کند و پیام، امضا و گواهی متناظر آن را منتشر می‌کند. در این روش TA مشخصات گواهی‌های تحویل داده شده به کاربران را ذخیره می‌کند و درصورت نیاز می‌تواند هویت واقعی کاربر را آشکار کند [۵]. ضعف عمده‌ای که در طرح‌های مبتنی بر گواهی‌های بی‌نام وجود دارد که باعث ناکارآمدی آن‌ها می‌گردد، فرآیند ابطال کاربران شبکه می‌باشد. در این طرح‌ها با افزایش تعداد کاربران ابطال‌شده حجم فهرست گواهی‌های ابطال‌شده (CRL[3]) به‌شدت افزایش می‌یابد و این باعث افزایش زمان وارسی امضاها می‌گردد. زیرا هنگامی که یک کاربر متخلف شناخته می‌شود باید تمامی گواهی‌های بی‌نامی که در اختیار او قرار گرفته است در فهرست ابطال قرار گیرد، بنابراین با افزایش تعداد خودروهای ابطال شده حجم CRL به شدت افزایش می‌یابد و خودروها قبل از این‌که امضای پیامی را وارسی کنند باید CRL را بررسی کرده و از مجاز بودن کاربر اطمینان حاصل کنند. بررسی CRL با حجم زیاد برای شبکه‌های اقتضایی بین خودرویی که باید پیام ترافیکی مهمی را در کسری از ثانیه مورد بررسی قرار دهند بسیار زمان‌بر می‌باشد.

۳-۲- طرح‌های مبتنی بر امضای گروهی

در طرح‌های مبتنی بر امضای گروهی هر عضو گروه می‌تواند پیامی را از طرف گروه امضا کرده و این امضا می‌تواند توسط اعضای گروه مورد وارسی قرار گیرد بدون آن‌که مشخص باشد کدام عضو گروه پیام را امضا کرده است. درحالی‌که مرکز سوم مورد اعتمادی به‌نام TTP[4] به‌عنوان مدیر گروه وجود دارد که می‌تواند هویت واقعی امضاکننده پیام را کشف‌کند [۹-۱۰].

از مشکلات پیش رو در طرح‌های مبتنی بر امضای گروهی این است که در این طرح‌ها زمان وارسی امضا به‌صورت خطی با تعداد خودروهایی که در فهرست ابطال قرارگرفته‌اند افزایش می‌یابد و اگر تعداد خودروهای فسخ‌شده از آستانه تعیین‌شده بیشتر شود باید شبکه مجدداً راه‌اندازی گردد و هر گروه از خودروها کلیدهای جدیدی دریافت کنند. همچنین در بیشتر طرح‌های مبتنی بر امضای گروهی، خودرو باید توسط بالاترین مرجع مورد اعتماد ثبت‌نام گردد و کلید خصوصی خود را از طریق یک کانال امن به‌دست آورد، این فرآیند موجب می‌شود تا خودرو نتواند کلید خصوصی خود را به‌صورت پویا تغییر دهد و این باعث افزایش احتمال حمله می‌گردد.

درطرح‌های مبتنی بر امضای گروهی نیازمند برقراری مصالحه‌ای در اندازه گروه می‌باشیم، زیرا اگر اندازه گروه بزرگ باشد زمان وارسی امضا افزایش می‌یابد و درصورت کوچک بودن گروه، شناسایی اعضای گروه راحت‌تر بوده و گمنامی کاربران به خوبی حفظ نمی‌گردد.

۳-۳- طرح‌های مبتنی بر RSU

در این طرح‌ها خودروها برای امضای پیام‌ها و یا احراز اصالت آن‌ها نیازمند همکاری برخط RSU می‌باشند. ژانگ[5] یک روش جدید مبتنی بر RSU ارائه کرده است، که در آن RSU مسئول بررسی احراز اصالت پیام‌های رسیده از خودروها و پاسخ‌گویی به آن‌ها می‌باشد. 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 می‌کنند [۷-۱۲].

طرح‌های شامل RSU در مقایسه با سایر طرح‌های فاقد RSU کارآمدتر بوده و دارای محاسبات کمتری در سمت خودروها می‌باشند، اما این طرح‌ها برای امضا و بررسی پیام‌ها به‌شدت به زیرساخت کنار جاده‌ای RSU وابسته می‌باشند بنابراین این طرح‌ها عموماً فاقد ارتباط خودرو با خودرو (V2V[6])بوده و هر ارتباطی باید در حضور زیرساخت کنار جاده‌ای RSU انجام شود.

۳-۴- طرح‌های مبتنی بر TPD

TPD در واقع یک دیسک سخت غیرقابل نفوذ با قابلیت محاسباتی می‌باشد. در این طرح‌ها هر خودرو مجهز به یک TPD بوده و اطلاعات اصلی سامانه مانند کلید اصلی سامانه، توابع مورد نیاز و... بعد از ثبت‌نام توسط TA درTPD هر خودرو پیش ذخیره می‌گردد، حال TPD هر خودرو می‌تواند 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

تولید و پیام را امضا کند. با توجه به این‌که خودرو برای امضای هر پیام یک شناسه مستعار جدید تولید می‌کند بنابراین گمنامی و حریم خصوصی کاربر در این طرح‌ها کاملاً حفظ می‌شود. همچنین کلید اصلی سامانه فقط در اختیار TA می‌باشد بنابراین فقط TA می‌تواند هویت واقعی کاربر را افشا کرده و یا او را ردیابی کند. عمده مشکل طرح‌های مبتنی بر TPD نبود فرآیند واضحی برای ابطال کاربران متخلف می‌باشد زیرا با توجه به‌این‌که TPD هر خودرو شامل کلیدهای اساسی کل سامانه است، برای ابطال یک کاربر متخلف در شبکه باید آن کاربر را به‌صورت 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 می‌شود. این طرح شامل سه مرحله تولید و پیش توزیع کلید، تولید شناسه مستعار و کلید متناظر آن، امضا و وارسی پیام می‌باشد [۱۳].

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

TA گروه دوری جمعی G تولیدشده توسط 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 $e: G \times G \to G_T$، تابع چکیده‌ساز $h: \{0,1\}^* \to \{0,1\}^n$ و تابع نگاشت به نقطه $H: \{0,1\}^* \to G$ را تولید می‌کند. سپس TA دو مقدار تصادفی $\langle S_1, S_2 \rangle$ را به‌عنوان کلید اصلی سامانه انتخاب کرده و مقادیر $P_{pub_1} = S_1 P$, $P_{pub_2} = S_2 P$ را به‌عنوان کلید عمومی متناظر آن‌ها محاسبه می‌کند. سرانجام TA پارامترهای عمومی سامانه $\langle G, G_T, q, P, P_{pub1}, P_{pub2}, e, h, H \rangle$ 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 به‌صورت منحصربه‌فرد از سایر خودروها تفکیک می‌کند و گذرواژه PWD برای احراز اصالت کاربر به TPD مورد استفاده قرار می‌گیرد.

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 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 $ID^i = \{ID_1^i, ID_2^i\}$ و کلید خصوصی $SK^i = \{SK_1^i, SK_2^i\}$ متناظر با آن را به‌صورت زیر محاسبه می‌کند.

$$ID^i = \{ID_1^i, ID_2^i\} = \{rP, RID_i \oplus H(rP_{pub_1})\} \quad (۱)$$

$$SK^i = \{SK_1^i, SK_2^i\} = \{S_1 ID_1^i, S_2 h(ID_1^i \| ID_2^i \| T_i) P\} \quad (۲)$$

۴-۳- امضا و وارسی امضا در طرح لی و لای

خودروی V_i برای امضای پیام M_i یک شناسه مستعار مانند رابطه (۱) در زیر بخش قبل تولیدکرده و به‌صورت زیر پیام را امضا می‌کند سپس چند تایی $\langle ID^i, M_i, \delta_i, T_i \rangle$ را به‌عنوان امضای خود منتشر می‌کند که در آن T_i مهر زمانی می‌باشد.

$$\delta_i = SK_1^i + h(M_i) SK_2^i \quad (۳)$$

برای وارسی پیام ابتدا شرط $T_r - T_i < T_\Delta$ توسط وارسی‌کننده امضا بررسی می‌گردد که در آن T_r زمان فعلی سامانه و T_Δ حداکثر تأخیر مجاز سامانه می‌باشد، اگر این شرط برقرار شد، آن‌گاه صحت امضا توسط برقراری شرط تصدیق زیر بررسی می‌گردد.

$$e(\delta_i, P) = e(ID_1^i, P_{pub_1}).\, e(h(M_i) h(ID_1^i \| ID_2^i \| T_i) P, P_{pub_2}) \quad (۴)$$

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

$$e\left(\sum_{i=1}^{n} Vec_i \delta_i, P\right) = e\left(\sum_{i=1}^{n} Vec_i ID_1^i, P_{pub_1}\right).\, e\left(\left(\sum_{i=1}^{n} Vec_i h(M_i)\, h(ID_1^i \| ID_2^i \| T_i)\right).P, P_{pub_2}\right) \quad (۵)$$

۵- حمله به طرح لی و لای

در طرح لی و لای برای این‌که کارآیی بهتری در تصدیق گروهی به‌دست آید به‌جای استفاده از نگاشت به نقطه $H(.)$ از تابع چکیده‌ساز $h(.)$ استفاده شده است که همین عامل باعث ایجاد یک ضعف بزرگ امنیتی در طرح آن‌ها گردیده است. حملاتی که در این مقاله ارائه می‌دهیم از این نقطه ضعف طرح لی و لای استفاده‌کرده و موفق به جعل امضا در طرح آن‌ها می‌شویم. در ادامه به معرفی سه سناریوی حمله‌ای که به این طرح انجام شد، می‌پردازیم.

۵-۱- سناریوی اول حمله

با توجه به این‌که در مرحله ثبت‌نام TA مقادیر کلیدهای اصلی $\langle S_1, S_2 \rangle$ را در TPD و سایر مقادیر $\langle G, G_T, q, P, P_{pub1}, P_{pub2} \rangle$ را در خودروها پیش‌ذخیره می‌کند، لذا هر کاربری به $\langle P_{pub1}, P_{pub2} \rangle$ 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 به‌دست‌آورده و در آن مهر زمانی هر پیامی را از طرف خودروی V_j امضا کند.

۱. با توجه به این‌که 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 به‌دست آورد.

بنابراین از این پس مهاجم با به‌دست 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، درصورتی‌که 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 $\langle P_{pub1}, P_{pub2} \rangle$ که پارامترهای عمومی سامانه هستند می‌تواند یک امضای جعلی را در هر مهر زمانی به‌صورتی 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 به‌دست می‌آورد، سپس از این شناسه به‌عنوان $ID_1^x = ID_1^j$ استفاده می‌کند.

۲. مهاجم یک مقدار کاملاً تصادفی را به‌عنوان RID_x انتخاب کرده و سپس ID_2^x را به‌صورت 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 به‌صورت زیر محاسبه می‌کند.

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

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 به‌دست 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 $\langle P_{pub1}, P_{pub2} \rangle$ را هم در اختیار نداشته باشد با توجه به این‌که TPD مقادیر $\langle ID^i, SK^i \rangle$ را تولیدکرده و در اختیار خودرو قرار می‌دهد، آن‌گاه مهاجم می‌تواند بر اساس این اطلاعات P_{pub2} را به‌صورت 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 مطرح‌شده قادر است تا امضای یک کاربر شبکه را جعل‌کرده و هر پیام اشتباهی را بدون آن‌که شناسایی شود در شبکه منتشر کند. حملات فوق به این علت به طرح لی و لای امکان‌پذیر شده‌اند که آن‌ها برای افزایش کارآیی طرح خود به‌جای استفاده از نگاشت به یک نقطه $H(.)$، از تابع چکیده‌ساز $h(.)$ 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 وارسی 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

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 تعیین‌کرده و تابع زوج‌سازی دو خطی $e: G \times G \to G_T$، تابع چکیده‌ساز $h: \{0,1\}^* \to \{0,1\}^n$ و تابع نگاشت به نقطه $H: \{0,1\} \to G$ را تولید می‌کند. تابع نگاشت به نقطه $H(.)$ 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 انتخاب‌کرده و مقادیر $P_{pub_1} = S_1P$ و $P_{pub_2} = S_2P$ را به‌عنوان کلید عمومی متناظر آن‌ها محاسبه می‌کند. سرانجام TA پارامترهای عمومی سامانه $\langle G, G_T, q, P, P_{pub1}, P_{pub2}, e, h, H \rangle$ را در OBUها و RSUها پیش‌ذخیره‌کرده و شناسه واقعی خودرو $RID \in G$، گذرواژه PWD و کلیدهای اصلی سامانه $\langle S_1, S_2 \rangle$ را در TPD هر خودرو ذخیره‌می‌کند. شناسه واقعی خودرو آن‌را به‌صورت منحصربه‌فرد از سایر خودروها تفکیک می‌کند و گذرواژه PWD برای احراز اصالت کاربر به TPD می‌باشد. با توجه به این‌که 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 $H(.)$ استفاده می‌شود. خودروی V_i، شناسه حقیقی $\mathrm{RID_i}$ و گذرواژه $\mathrm{PWD_i}$ را برای تولید شناسه مستعار وارد TPD می‌کند.

TPD بعد از بررسی $\mathrm{RID_i}$ و $\mathrm{PWD_i}$، یک مقدار تصادفی r و مهر زمانی T_i را انتخاب کرده و شناسه مستعار و کلید خصوصی را به‌صورت زیر تعیین و در اختیار کاربر قرار می‌دهد.

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

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 به‌صورت زیر امضا خواهد کرد و مقادیر $\langle ID^i, M_i, \delta_i, T_i \rangle$ را به‌عنوان امضای خود ارسال می‌کند.

$$\delta_i = SK_1^i + h(M_i) SK_2^i \quad (۸)$$

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 درصورت برقراری رابطه زیر امضا را تصدیق می‌کند.

$$e(\delta_i, P) = e\left(ID_1^i, P_{pub_1}\right). e\left(h(M_i) H\left(ID_1^i \parallel ID_2^i \parallel T_i\right), P_{pub_2}\right) \quad (۹)$$

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

$$e(\delta_i, P) = e(sk_1^i + h(M_i) sk_2^i, P) = e(SK_1^i, P). e(h(M_i) SK_2^i, P)$$
$$= e(S_1 ID_1^i, P). e(h(M_i) S_2 H(ID_1^i \parallel ID_2^i \parallel T_i), P)$$

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

همچنین وارسی‌کننده 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.

$$e\left(\sum_{i=1}^{n} \delta_i, P\right) = e\left(\sum_{i=1}^{n} ID_1^i, P_{pub_1}\right). e\left(\sum_{i=1}^{n} h(M_i) H(ID_1^i \parallel ID_2^i \parallel T_i), P_{pub_2}\right) \quad (۱۰)$$

۶-۴- بهبود طرح پیشنهادی در تصدیق گروهی

در طرح لی و لای با توجه به این‌که 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 به‌صورت $\langle ID^1, M_1, \delta_1 \rangle$، $\langle ID^2, M_2, \delta_2 \rangle$، $\langle ID^3, M_3, \delta_3 \rangle$ تولید و سپس محتویات بسته‌های ارسالی را به‌صورت $\langle ID^2, M_2, \delta_3 \rangle$، $\langle ID^1, M_1, \delta_2 \rangle$، $\langle ID^3, M_3, \delta_1 \rangle$ 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.

$$e\left(\sum_{i=1}^{3} Vec_i \delta_i, \mathrm{P}\right) = e(Vec_1 \delta_2 + Vec_2 \delta_3 + Vec_3 \delta_1, P) \quad (۱۱)$$
$$\neq$$
$$e\left(\sum_{i=1}^{n} Vec_i ID_1^i, P_{pub_1}\right). e\left(\left(\sum_{i=1}^{n} Vec_i h(M_i)\, h(I\right. \right.$$
$$\left. \left. ID_2^i)\right). P, P_{pub_2}\right)$$

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

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 می‌تواند 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 آن‌ها هم تغییر کرده باشد باز هم صحیح تشخیص داده می‌شوند و مهاجم تنها با تغییر ترتیب امضاها نمی‌تواند مانع تصدیق تعدادی امضای صحیح گردد.

۷- تحلیل امنیتی طرح پیشنهادی

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

۷-۱- احراز اصالت پیام

احراز اصالت پیام از مهم‌ترین ملزومات امنیتی در شبکه‌های VANET می‌باشد تا بررسی‌کننده پیام مطمئن باشد که پیام از سوی کاربر مجاز شبکه ارسال شده و یکپارچگی آن نیز محفوظ مانده است.

با توجه به این‌که در این طرح هر پیام قبل از ارسال به‌صورت رابطه ۸ امضا می‌شود و این امضا شامل تابع چکیده‌ساز $h(.)$ می‌باشد، با فرض امن بودن این تابع چکیده‌ساز یکپارچگی پیام حفظ می‌شود، همچنین با توجه به استفاده از مهر زمانی T_i در تولید کلید خصوصی SK_2^i وارسی کننده پیام از تازه بودن پیام‌های امضا شده اطمینان حاصل می‌کند. استفاده از مهر زمانی در تولید امضا مانع بروز حمله تکرار به طرح می‌شود، یعنی مهاجم قادر نخواهد بود که پیام‌های امضا شده توسط کاربران مجاز شبکه در یک زمان را جمع‌آوری و در زمان دیگری منتشر کند تا شرایط ترافیکی جعلی را ایجاد کند. همچنین با توجه به این‌که برای امضای هر پیام از یک کلید خصوصی به‌صورت $SK^i = \langle SK_1^i, SK_2^i \rangle = \langle S_1 ID_1^i, S_2 H(ID_1^i \parallel ID_2^i) \rangle$ استفاده می‌شود، 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 زوج‌سازی‌های دوخطی می‌باشد که یک مسئله سخت محسوب می‌گردد. همچنین با توجه به اصلاح صورت‌گرفته در تولید کلید خصوصی SK_2^i در طرح پیشنهادی امکان برقراری حملات مطرح‌شده به طرح لی و لای به طرح وجود ندارد. در طرح بهبودیافته مهاجم نمی‌تواند 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 مطرح‌شده در بخش‌های گذشته به‌دست آورد، زیرا با توجه به استفاده از تابع نگاشت $H(.)$ در تولید کلید خصوصی مهاجم برای به‌دست آوردن SK_2^i با استفاده از پارامترهای عمومی نیازمند حل مسئله لگاریتم گسسته بر روی منحنی‌های بیضوی می‌باشد که خود یک مسئله سخت محسوب می‌گردد. بنابراین اگر امضای پیامی تصدیق شود مطمئناً این پیام از سوی کاربر مجاز شبکه امضاشده و یک‌پارچگی آن نیز حفظ شده است.

۷-۲- گمنامی و پیوندناپذیری

با توجه به این‌که کاربر برای امضای هر پیام یک شناسه مستعار و کلید خصوصی جدید مستقل از شناسه‌های مستعار قبلی خود تولید می‌کند و با آن پیام را امضا می‌کند، بنابراین مهاجم نمی‌تواند هویت واقعی کاربر را به‌دست‌آورده و یا ارتباطی بین امضاهای مختلف او پیدا کند، لذا این طرح خاصیت گمنامی و پیوندناپذیری را برآورده می‌کند.

۷-۳- ردیابی مشروط

با توجه به این‌که کاربر برای امضای هر پیام یک شناسه مستعار و کلید خصوصی جدید بر اساس شناسه حقیقی خود و کلید اصلی سامانه تولید می‌کند و با آن پیام را امضا می‌کند، لذا مهاجم با مشاهده تعدادی پیام مشخص، نمی‌تواند ارتباطی بین پیام‌های امضاشده و امضاکننده آن‌ها به‌دست آورد. همچنین مهاجم برای افشای هویت واقعی امضاکننده پیام نیازمند این است که مقادیر کلید اصلی سامانه یعنی $\langle s_1, s_2 \rangle$ را به‌دست آورد که با توجه به این‌که آن‌ها در TPD خودرو ذخیره شده‌اند امکان بازیابی آن‌ها وجود ندارد و یا مهاجم باید قادر به حل مسئله ECDLP باشد تا بتواند با توجه به ID^i مقدار r را به‌دست آورد و به RID خودرو دست‌یابد. اما TA با داشتن مقادیر کلید اصلی سامانه $\langle s_1, s_2 \rangle$ با محاسبه رابطه (۱۲) می‌تواند هویت واقعی خودرو را با توجه به شناسه مستعار آن به‌دست آورد.

$$SK_2^x = h(ID_1^x \parallel ID_2^x \parallel T_i) P_{pub_2} \qquad (۱۲)$$

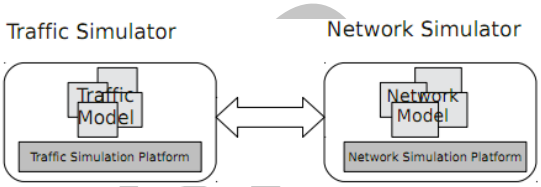
بنابراین TA قادر به افشای هویت اصلی خودرو و ردیابی آن می‌باشد.

۸- پیاده‌سازی و کارآیی طرح

شبیه‌سازی یکی از ابزارهای مهم برای تعیین و بررسی عملی بودن یک پروتکل و یا دستگاه می‌باشد. VANET برخلاف شبکه‌های دیگر از دو جنبه ترافیکی و شبکه بی‌سیم باید مورد بررسی قرار بگیرد. منظور از ترافیک، مجموعه‌ای از خودروها می‌باشد که در یک نقشه در حال حرکت هستند. از آن‌جا که ترافیک در شبکه مخابراتی تأثیر مستقیم دارد،

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 ماکروسکوپیک و میکروسکوپیک تقسیم می‌شود. شبیه‌سازی ماکروسکوپیک عواملی مانند چگالی ترافیک، نقشه و ساختار راه‌ها را در نظر می‌گیرد . شبیه‌سازی میکروسکوپیک عواملی مانند انسان‌های در حال حرکت، ساختمان‌ها، آب و هوا را بررسی می‌کند [۱۷-۱۵]. در اقتضایی بین خودرویی عوامل میکروسکوپیک خیلی تأثیری بر نتایج شبیه‌سازی ندارند و لذا از این به بعد منظور ما از شبیه‌سازی ترافیک، شبیه‌سازی ماکروسکوپیک 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++ به‌همراه بسته‌های زیر می‌باشد.

- MiXim
- Viens
- INET

این بسته‌ها در لایه کاربردی[1]، WSMP[2] و فیزیکی[3] 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 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 درشبیه‌سازی 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[4]، لایه فیزیکی، لایه ارتباط[5] 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.

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

برای این منظور دو ماژول برای شبیه‌سازی WSMP و سرویس پردازش امنیت در نظر می‌گیریم، ماژول‌های سرویس پردازش امن و ماژول WSMP. ماژول‌های لایه کاربرد بسته‌های داده را با کمک WSMP ارسال و پردازش امن با کمک ماژول سرویس پردازش امن انجام می‌شود.

جدول (۱). پارامترهای شبیه‌سازی شبکه

بیشینه توان ارسال	20mW
نرخ بیت	18Mbs
حداقل آستانه میرایی سیگنال[1]	-89dBm
کمینه ضریب تضعیف مسیر[2]	2
کمینه فرکانس حامل کانال	5.890e9 Hz
طول بسته کاربردی[3]	Uniform(128bit, 131072bit)

بالاترین لایه، لایه کاربرد است که پیام‌های امن با طول مختلف به گره‌های دیگر از مسیرهای مختلف ارسال می‌شود. این فرآیند برای هر گره یک ترافیک دریافت و آنالیز داده ایجاد می‌کند.

در لایه WSMP، پیام‌های دریافتی از لایه کاربرد و شبکه به سرویس پردازش امن برای امضا یا بررسی امضا داده می‌شود. در سرویس پردازش امن، زمان اجرای پردازش به روش پردازش، طول پیام‌ها و پردازشگر درون OBU و RSU بستگی دارد. لایه شبکه که یک لایه فیزیکی است و لایه‌های IEEE_1609-4 پیام‌های لایه‌های بالاتر را به گره‌های دیگر از طریق کانال مخابراتی انتقال می‌دهند. همچنین پیام‌های دریافت‌شده از طریق کانال مخابراتی را به لایه‌های بالاتر منتقل می‌کنند. ماژول تحرک[4]، مدل حرکت هر گره را بر اساس محدودیت‌های ترافیکی مانند آنچه در جدول ۲ آمده است، تعیین می‌کند. بر اساس استاندارد IEEE_1609.2 هر پیام به‌طور جداگانه امضا و ارسال می‌شود. اگرچه روش‌های امضا طرح‌های امضا متفاوت هستند، اما فرآیند امضا و ارسال در همه طرح‌ها یکسان می‌باشد (شکل‌های ۳ و ۴). پیام‌های دریافتی همگی به سرویس پردازش امنیت منتقل و در آنجا اعتبار آن‌ها بررسی می‌شود.

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

جدول (۲). پارامترهای شبیه‌سازی 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 شبیه‌سازی

درشبیه‌سازی انجام‌شده، تمامی گره‌ها قادر به حرکت در شبکه ترافیکی و ارسال امن پیام‌های خود می‌باشند. قبل از ارسال پیام‌ها لازم است که پارامترهای عمومی سامانه [۳۱]، به گره‌ها اطلاع‌رسانی شده باشد. هدف اصلی ما از شبیه‌سازی برآورد تأخیر بررسی صحت پیام دریافتی می‌باشد.

۸-۳. نتیجه شبیه‌سازی:

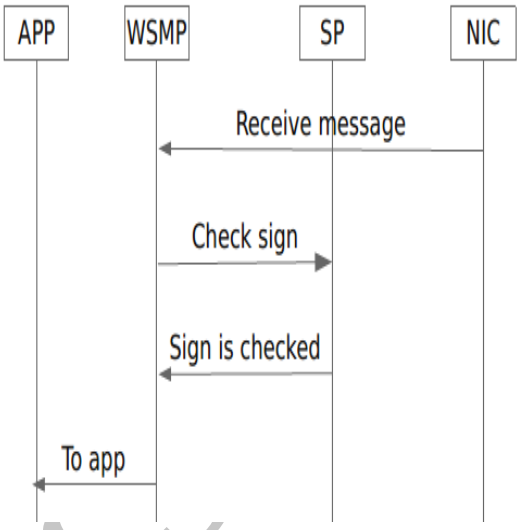
در این بخش طرح پیشنهادی خود را با طرح‌های BLS، ECPP، DCS و LPA مقایسه می‌کنیم. جدول (۵) میزان پیچیدگی وارسی امضای این طرح‌ها را در حالت وارسی منفرد امضا و حالت وارسی گروهی، با یکدیگر مقایسه می‌کند. با توجه به جدول (۵) میزان پیچیدگی طرح پیشنهادی ما با پیچیدگی طرح ECPP در حالت منفرد برابر است و از سایر طرح‌ها بهتر می‌باشد. همچنین طرح پیشنهادی ما در وارسی گروهی امضاها از طرح‌های BLS، DCS و ECPP کارآمدتر است.

در فرآیند تولید و تأیید امضا، زمان اجرای الگوریتم شامل دو زمان ثابت و متغیر می‌باشد. 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 پیاده‌سازی نیز وابسته است. ما در شبیه‌سازی از بسته GMP [۳۲]، و پردازشگر X2 Ultra Dual-core Mobile ZM-80 AMD Turin (tm) استفاده می‌کنیم. زمان اجرای عملگرها در جدول (۳) آمده است.

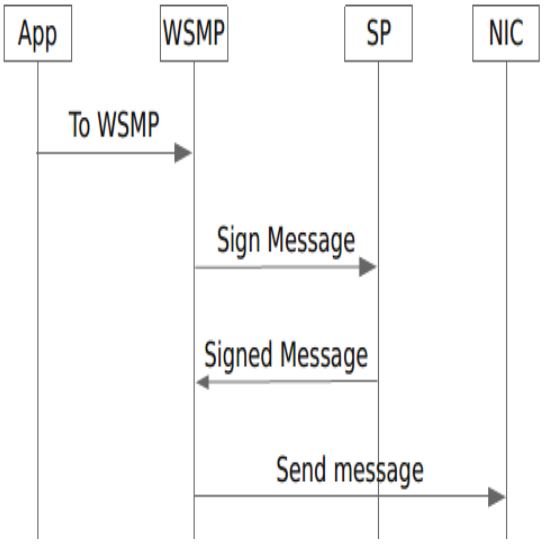
در طرح پیشنهادی از تابع چکیده‌ساز MD5 استفاده شده است که زمان اجرای آن به‌طول داده ورودی وابسته است. زمان اجرای الگوریتم پیشنهادی بر اساس مقادیر جدول (۳) در جدول (۴) آمده است. زمان سربار، اختلاف زمان بین ورود داده به WSMP و خروج داده از آن است، که این زمان با رابطه زیر محاسبه می‌شود:

$$AD = \frac{1}{M}\sum_{i=1}^{M} T_{out}^{i} - T_{rec}^{i} \qquad (۱۳)$$

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.

جدول (۳). زمان عملگرها به ثانیه

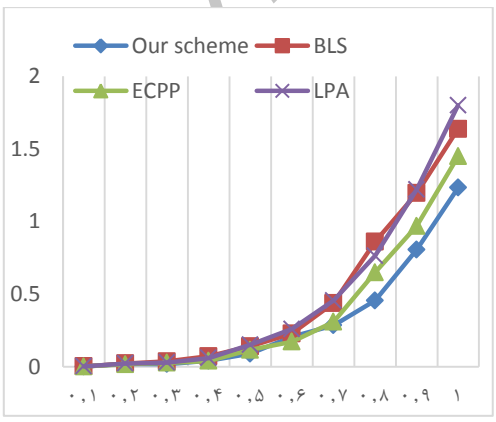
تعداد ماشین	500
ضرب برداری	4.41e-04
جمع	4e-08
مولد تصادفی	2.8e-07
زوج‌سازی	8.820e-3
نگاشت به نقطه	1.1025e-4
تابع چکیده ساز	0.022Mbits/s

جدول (۴). زمان اجرای طرح

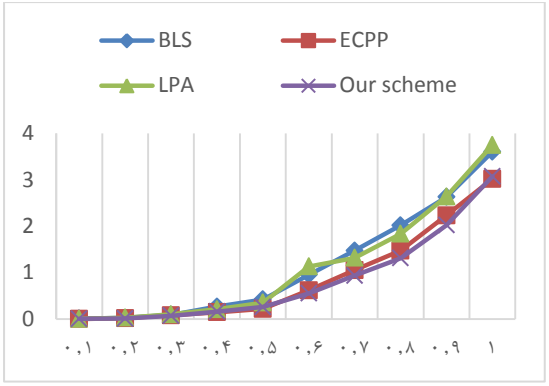
	امضا	بررسی
طرح	0.022Mbit/s+0.0157 4187s	0.022Mbit/s+0.0512 s

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

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 BLS، ECPP، LPA و طرح پیشنهادی در چهار راه



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

۹- نتیجه‌گیری

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 می‌دهد، سپس طرح بهبود یافته‌ای از آن را پیشنهاد داده‌ایم که در برابر جعل امضای کاربر مقاوم می‌باشد. آنچه امکان وقوع این حملات را به مهاجم در طرح لی و لای داده است آن است که آن‌ها برای بهبود عملکرد طرح خود در وارسی گروهی امضا از تابع چکیده‌ساز استفاده کرده‌اند، اما ما در طرح پیشنهادی خود از خواص تابع نگاشت به نقطه استفاده کرده‌ایم، و همین امر باعث مقاوم‌شدن طرح پیشنهادی ما در برابر حملات جعل امضا شده است. طرح پیشنهادی ما ملزومات امنیتی لازم در شبکه‌های VANET را که شامل احراز اصالت پیام، ردیابی مشروط، گمنامی و پیوندناپذیری کاربر می‌باشد را برآورده می‌کند. همچنین در طرح پیشنهادی ما قابلیت وارسی گروهی امضاها به‌صورت کارآمد وجود دارد. در پایان شبیه‌سازی طرح پیشنهادی خود را به‌همراه اصول استفاده‌شده در این شبیه‌سازی بیان کرده‌ایم. همچنین عملکرد طرح پیشنهادی خود را با طرح‌های BLS، DCS، ECPP و LPA در دو حالت وارسی منفرد و گروهی امضاها مورد مقایسه قرار دادیم، و همان‌طور که در شکل‌های (۵ و ۶) نشان داده شده است طرح پیشنهادی ما دارای کارآیی بهتری نسبت به این طرح‌ها می‌باشد.

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.

[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.

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. Härri, 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/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 dentity

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