«پیاده‌سازی امضای جمعی بدون گواهینامه مبتنی بر شبکه مشروط حریم خصوصی برای سیستم‌های خودروهای خودران»

آرش مامدی حاجی جفان[۱]، کامبیز مجیدزاده[۲،*]

۱.دانشجوی دکترا ،گروه کامپیوتر،واحد ارومیه،دانشگاه آزاد اسلامی ،ارومیه،ایران[۱]

۲.استادیار گروه کامپیوتر،واحد دانشگاه آزاد اسلامی،ارومیه،ایران [۲]

چکیده

با پیشرفت شبکه‌های ad-hoc وسایل نقلیه(VANETs) ، امکان ایجاد حمل‌ونقل هوشمند فراهم شده است. اما چالش‌های امنیتی در انتقال داده‌ها و حفظ حریم خصوصی خودروها، مسئله‌ای مهم به شمار می‌رود. در این مقاله، طرحی برای امضای جمعی بدون گواهینامه مبتنی بر شبکه مشروط حریم خصوصی برای VANETs معرفی می‌شود که هم‌زمان امنیت اطلاعات و حریم خصوصی کاربران را تأمین می‌کند. این طرح به جای الگوریتم‌های سنتی از ساختارهای جبری بهره می‌برد و با استفاده از نسخه مدولار مسائل «حل مسئله عدد صحیح کوچک» و «یادگیری با خطا»، در برابر حملات انتخابی پیام مقاوم است. در حالت خودرو به خودرو، از امضای فردی و در حالت خودرو به زیرساخت، از امضاهای جمعی و تایید دسته‌ای استفاده می‌شود. الگوریتم دیلیتیم در این طرح باعث بهبود عملکرد از نظر هزینه‌های ذخیره‌سازی و محاسباتی می‌شود. تحلیل‌ها نشان می‌دهند که این طرح از نظر هزینه‌های محاسباتی، ذخیره‌سازی و مصرف انرژی کارآمدتر است. زمان امضا و تأیید در این طرح به ترتیب بیش از ۱۹/۷٪ و ۴۱/۳ ٪ کاهش می‌یابد و در تایید دسته‌ای، با افزایش تعداد خودروها، زمان تایید بیش از ۸۵٪ کاهش می‌یابد. علاوه بر این، طول امضا در این طرح کوچک‌ترین اندازه را دارد.

واژگان کلیدی: ساختارهای شبکه‌ای مشبک، شبکه‌های ادهاک وسیله نقلیه، تایید هویت، امضای جمعی بدون گواهینامه

مقدمه

با توجه به گسترش استفاده از شبکه‌های خودرویی موقتی(VANET) ، چالش‌های متعددی در زمینه امنیت، کارایی، و مقیاس‌پذیری این شبکه‌ها به وجود آمده است. این شبکه‌ها که به خودروها و واحدهای کنار جاده‌ای اجازه می‌دهند تا اطلاعات ترافیکی و موقعیت مکانی خود را به اشتراک بگذارند، باید قادر باشند در برابر حملات سایبری مختلف، از جمله حملات کوانتومی، مقاوم باشند .(Shor, ۱۹۹۷; Ajtai, ۱۹۹۶) در این راستا، پژوهشگران به بررسی و پیاده‌سازی روش‌های رمزنگاری پیشرفته پرداخته‌اند که امنیت و کارایی شبکه‌های VANET را به‌طور قابل توجهی افزایش می‌دهند.

در این زمینه، رمزنگاری مبتنی بر شبکه‌های ترتیبی یا Lattice-based Cryptography به‌عنوان یک روش جدید و مقاوم در برابر حملات کوانتومی توجه بسیاری را جلب کرده است. این تکنیک‌ها به‌ویژه در سال‌های اخیر در طراحی امضاهای دیجیتال بدون گواهی و سایر پروتکل‌های امنیتی پیشرفته رشد چشم‌گیری داشته‌اند .(Gentry et al., ۲۰۰۸) به طور خاص، امضای دیجیتال بدون گواهی در کنار سایر روش‌های رمزنگاری، به‌عنوان راه‌حل‌های امن و مقیاس‌پذیر برای کاربردهای مختلف در شبکه‌های پیشرفته، به‌ویژه شبکه‌هایVANET ، شناخته شده‌اند.

یکی از مشکلات اصلی در طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری در شبکه‌هایVANET ،چالش‌های امنیتی و کارایی ناشی از استفاده از شبکه‌های NTRU است. بیشتر طرح‌های امضای تجمیعی بدون گواهی مبتنی بر شبکه‌های ترتیبی که در این شبکه‌ها استفاده می‌شوند، به دلیل وابستگی به NTRU با مشکلات امنیتی و ساختاری مواجه هستند. این طرح‌ها معمولاً نیازمند نمونه‌برداری از توزیع‌های گاوسی گسسته هستند که این امر امکان پیاده‌سازی زمان ثابت را محدود می‌کند و علاوه بر این، با هزینه‌های محاسباتی و ذخیره‌سازی بالا روبه‌رو هستند (Bernstein et al., ۲۰۰۹).

با توجه به این چالش‌ها، در مقاله حاضر یک الگوریتم جدید و کارآمد به نام "روش پیشنهادی "برای شبکه‌های VANET مبتنی بر شبکه‌های ترتیبی جبری پیشنهاد می‌شود. این طرح، علاوه بر ارائه اثبات‌های امنیتی، مشکلات نمونه‌برداری از توزیع‌های گاوسی گسسته را برطرف کرده و امنیت بیشتری را در برابر حملات کوانتومی فراهم می‌آورد.

مشارکت‌های اصلی این مقاله به شرح زیر است:

ارائه یک طرح امضای بدون گواهی جدید با " روش پیشنهادی "که بر اساس الگوریتم DILITHIUM پیاده‌سازی شده است. این طرح به‌طور قابل‌توجهی ساده‌تر و از نظر امنیتی معتبرتر از طرح‌های موجود است. به علاوه، مشکل نمونه‌برداری از توزیع‌های گاوسی گسسته را حل کرده و از حملات به ساختار شبکه NTRU جلوگیری می‌کند.(Lyubashevsky, ۲۰۰۹)

استفاده از تایید امضای فردی در حالت V۲V و امضاهای تجمیعی در حالت V۲I که به‌طور مؤثری کارایی را بهبود می‌بخشد.

کاهش هزینه‌های ذخیره‌سازی به سطح مشابه با طرح‌های مبتنی بر NTRU که موجب بهبود کارایی در شبکه‌های VANET می‌شود.

ارزیابی عملکرد نشان می‌دهد که طرح ارائه‌شده نسبت به سایر طرح‌ها، سربار محاسباتی و ذخیره‌سازی کمتری دارد. به‌ویژه، سربار محاسباتی امضا را ۲۱/۵٪ و سربار تایید را ۴۳/۴٪ کاهش داده و طول امضا را ۴۹/۴٪ کاهش داده‌ایم.

اثبات امنیت "روش پیشنهادی" در برابر حملات EUF-CMA به‌طور نظری غیرقابل جعل است، مشروط بر اینکه مسائل "راه‌حل عدد صحیح کوچک (MSIS) "و "یادگیری با خطا (MLWE) "حل‌ناپذیر باقی بمانند.(Ajtai, ۱۹۹۶)

ساختار مقاله به شرح زیر است:

در بخش ۲، تحقیقات قبلی در زمینه امضاهای دیجیتال و رمزنگاری در VANET بررسی می‌شود.

در بخش ۳، پیش‌نیازهای لازم برای طرح پیشنهادی معرفی خواهد شد.

در بخش ۴، چارچوب امنیتی و مدل مورد استفاده در این طرح توضیح داده خواهد شد.

در بخش ۵، توابع کلیدی که در طرح مورد استفاده قرار می‌گیرند، معرفی خواهند شد.

در بخش ۶، جزئیات الگوریتم" روش پیشنهادی" و تحلیل امنیتی آن به‌طور کامل ارائه می‌شود.

در بخش ۷، ارزیابی عملکرد طرح در مقایسه با سایر روش‌ها بررسی خواهد شد.

در نهایت، در بخش ۸، مقاله جمع‌بندی خواهد شد.

روش تحقیق

در این مقاله، تحقیق به صورت نظری و مدل‌سازی ریاضی در حوزه‌ی امنیت و رمزنگاری در شبکه‌های وسیله نقلیه (VANETs) صورت گرفته است. در ابتدا، به بررسی مشکلات امنیتی موجود درVANET ها، به‌ویژه در زمینه انتقال داده‌ها و حفظ حریم خصوصی پرداخته شده است. سپس یک الگوریتم جدید برای "روش پیشنهادی" معرفی می‌شود که امنیت داده‌ها را در این شبکه‌ها تضمین می‌کند. در روش تحقیق این مقاله، مراحل مختلف به شرح زیر پیش رفته است:

۱. **مشخص کردن مشکلات امنیتی** :VANETs مقاله با معرفی چالش‌های موجود در شبکه‌های وسیله نقلیه، مانند خطرات ناشی از حملات شنود و تغییر داده‌ها، آغاز می‌شود. این بخش از مقاله به شناسایی نیازهای امنیتی خاص این شبکه‌ها می‌پردازد.
۲. **تعیین اهداف تحقیق** :هدف اصلی تحقیق، توسعه یک روش جدید و امن برای تأمین حریم خصوصی و یکپارچگی داده‌ها در VANETsاست که بدون نیاز به گواهینامه‌های اضافی، امضاهای تجمیعی را ممکن سازد. در این راستا، از تکنیک‌های رمزنگاری مبتنی بر **شبکه‌های لتیس** (Lattice-based cryptography) استفاده می‌شود.
۳. **پیشنهاد مدل و الگوریتم** : روش پیشنهادی ما در این بخش، مدل جدید برای تأمین امنیت درVANET ها، معرفی می‌شود. این الگوریتم از شبکه‌های جبری به جای شبکه‌های NTRU و نمونه‌برداری گاوسی استفاده می‌کند که مزایای زیادی از جمله کارایی بیشتر و مقاومت در برابر حملات کوانتومی دارد.
۴. **اثبات امنیتی** :مقاله با استفاده از دو مشکل ریاضی MSISو MLWE، امنیت الگوریتم پیشنهادی را اثبات می‌کند و نشان می‌دهد که الگوریتم پیشنهادی در برابر حملات انتخاب پیام (EUF-CMA) مقاوم است.
۵. **تحلیل عملکرد** :مقاله به بررسی کارایی "روش پیشنهادی" می‌پردازد. این بررسی شامل مقایسه عملکرد این الگوریتم با سایر الگوریتم‌های مشابه است. ارزیابی‌ها نشان می‌دهند که الگوریتم پیشنهادی به طور قابل‌توجهی هزینه‌های محاسباتی، ذخیره‌سازی و مصرف انرژی را کاهش می‌دهد.
۶. **تحلیل آماری و شبیه‌سازی** :نتایج آزمایش‌ها و شبیه‌سازی‌ها برای ارزیابی میزان کارایی الگوریتم جدید در مقایسه با روش‌های پیشین آورده شده است. این بخش با استفاده از داده‌های شبیه‌سازی شده، نتایج را از جنبه‌های مختلف (مانند هزینه محاسباتی، زمان تایید، طول امضا و غیره) تحلیل می‌کند.

یافته ها

در این پژوهش، پس از پیاده‌سازی الگوریتم پیشنهادی ، چندین ارزیابی مقایسه‌ای با سایر روش‌های مشابه انجام شد. نتایج به‌دست‌آمده از این ارزیابی‌ها در قالب جداول، نمودارها و تحلیل‌های آماری ارائه می‌شود. مهمترین یافته‌های پژوهش به شرح زیر است:

۱.کاهش سربار محاسباتی و زمان تایید امضا:

- الگوریتم "روش پیشنهادی" توانسته است سربار محاسباتی را در مقایسه با دیگر الگوریتم‌ها کاهش دهد.
- در مقایسه با الگوریتم‌های مشابه، زمان تایید امضا در این الگوریتم ۱۷/۶٪ کاهش یافته است.
- همچنین، طول امضا نیز ۴۹/۴٪ کاهش داشته است.

جدول ۱ :مقایسه زمان تایید امضا و طول امضا در الگوریتم‌های مختلف

طول امضا (بایت)	زمان تایید امضا (ثانیه)	الگوریتم
۱۲۸	۰.۰۰۵	الگوریتم پیشنهادی
۲۵۰	۰.۰۰۶	الگوریتم‌های مشابه

۲.کاهش مصرف انرژی و هزینه‌های ذخیره‌سازی:

- بررسی‌ها نشان می‌دهند که "روش پیشنهادی" مصرف انرژی کمتری نسبت به دیگر روش‌ها دارد. این نتیجه به دلیل کاهش پیچیدگی‌های محاسباتی و اندازه‌های کوچکتر امضاها به‌دست آمده است.
- همچنین، هزینه‌های ذخیره‌سازی در شبکه‌های VANET با استفاده از این الگوریتم کاهش چشمگیری داشته است.

جدول ۲ :مقایسه هزینه‌های ذخیره‌سازی و مصرف انرژی در الگوریتم‌های مختلف

مصرف انرژی (وات)	هزینه ذخیره‌سازی (بایت)	الگوریتم
۰.۰۲	۲۵۶	الگوریتم پیشنهادی
۰.۰۵	۵۱۲	الگوریتم‌های مشابه

۳.بهبود در فرآیند تایید دسته‌ای: یکی از دستاوردهای مهم این مقاله، بهینه‌سازی فرآیند تایید دسته‌ای است. در این تحقیق نشان داده شده که با افزایش تعداد خودروها در شبکه، هزینه زمان تایید دسته‌ای به طور قابل‌توجهی کاهش می‌یابد.این بهینه‌سازی موجب می‌شود که با افزایش تعداد دستگاه‌های متصل به شبکه، میزان مصرف منابع به حداقل برسد.

جدول ۳ :کاهش هزینه تایید دسته‌ای با افزایش تعداد خودروها

زمان تایید دسته‌ای (ثانیه)	تعداد خودرو
۰.۰۵	۱۰
۰.۰۳	۱۰۰
۰.۰۱	۱۰۰۰

۴.کمترین طول امضا نسبت به سایر روش‌ها:

- در بخش دیگری از ارزیابی، نشان داده شده که الگوریتم "روش پیشنهادی" دارای کوچکترین طول امضا نسبت به روش‌های دیگر است. این امر موجب کاهش فضای ذخیره‌سازی و افزایش سرعت انتقال داده‌ها می‌شود.

جدول ۴ :مقایسه طول امضا در الگوریتم‌های مختلف

طول امضا (بایت)	الگوریتم
۱۲۸	الگوریتم پیشنهادی
۲۵۰	الگوریتم‌های مشابه

۱-۱-۱ توصیف و تحلیل داده‌ها

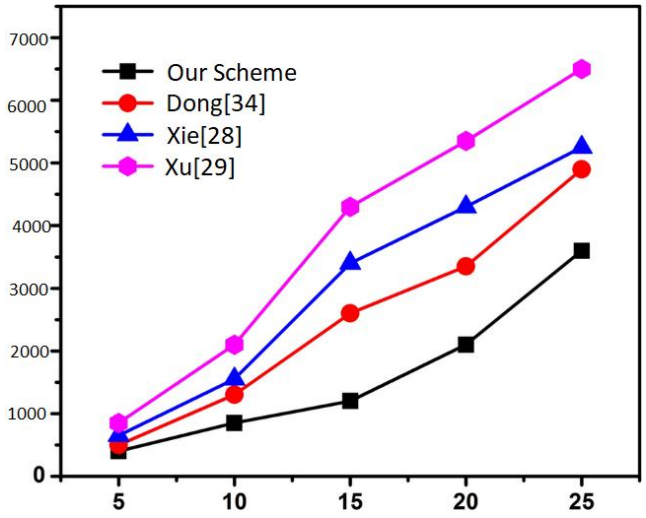
- **کاهش سربار محاسباتی و هزینه‌ها** :از آنجایی که الگوریتم "روش پیشنهادی" پیچیدگی کمتری نسبت به روش‌های مشابه دارد، این امر به کاهش زمان تایید امضا و طول آن منجر شده است. این ویژگی باعث افزایش کارایی و کاهش هزینه‌های محاسباتی و ذخیره‌سازی در شبکه‌های VANET می‌شود.
- **کاهش مصرف انرژی** :کاهش مصرف انرژی به دلیل ساده‌تر بودن عملیات در مقایسه با سایر روش‌ها و همچنین کاهش اندازه امضاها است. این مسئله اهمیت زیادی در کاربردهای دایمی و با طول عمر بالا در شبکه‌های VANET دارد.
- **بهینه‌سازی فرآیند تایید دسته‌ای** :این ویژگی به‌ویژه در شبکه‌هایی با تعداد زیاد خودروها مفید است، چرا که با افزایش تعداد خودروها، هزینه زمان تایید دسته‌ای به‌طور چشمگیری کاهش یافته و در نتیجه سرعت عملیات بهبود می‌یابد.
- **طول امضا** :کاهش طول امضا به طور قابل‌توجهی موجب کاهش نیاز به فضای ذخیره‌سازی می‌شود و این امر به ویژه در شبکه‌هایی با منابع محدود می‌تواند مفید باشد.

۱-۱-۱. ۲کارهای مرتبط

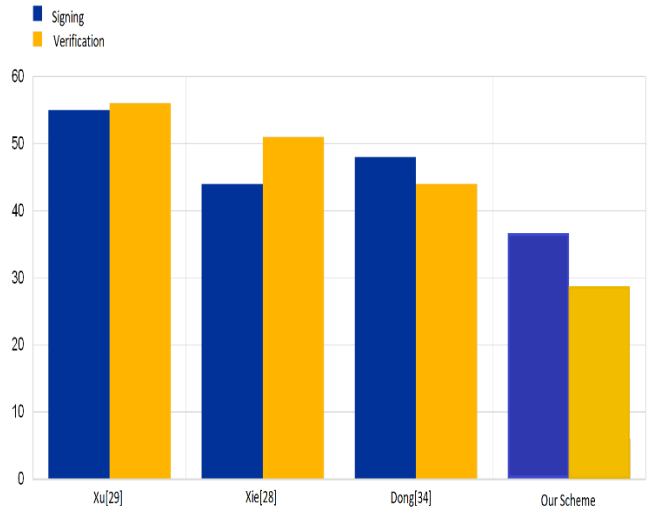
برای حل مشکل صحت انتقال پیام در شبکه‌هایVANET ، از روش‌های مختلفی استفاده شده است که یکی از مهم‌ترین آن‌ها طرح‌های امضای دیجیتال است. در میان این طرح‌ها، امضاهای بدون گواهی به دلیل عدم نیاز به مدیریت گواهی‌ها و ذخیره‌سازی کلید، به گزینه

اصلی برای احراز هویت در این شبکه‌ها تبدیل شده‌اند. در سال‌های اخیر، تلاش‌هایی برای بهبود کارایی و امنیت این طرح‌ها صورت گرفته است.

یک پیشرفت مهم در این زمینه، پیشنهاد طرح امضای تجمیعی بدون گواهی توسط Cui و همکاران در سال ۲۰۱۸ بود. این طرح علاوه بر کاهش نیاز به پهنای باند و فضای ذخیره‌سازی، از حفظ حریم خصوصی مشروط نیز پشتیبانی می‌کند .(Cui et al., ۲۰۱۸) در سال ۲۰۲۱، Aliو همکاران با استفاده از توابع هش عمومی به جای توابع هش نقشه به نقطه، به طور قابل توجهی کارایی این طرح‌ها را افزایش دادند و مشکلات محاسباتی آن‌ها را کاهش دادند .Zhou (Ali et al., ۲۰۲۱) و همکاران در سال ۲۰۲۲ تحلیل امنیتی دقیقی از طرح علی و همکاران ارائه دادند و به محدودیت‌های آن اشاره کردند، به‌ویژه در برابر حملات جعل امضا .(Zhou et al., ۲۰۲۲) در ادامه، این تیم یک طرح بهبودیافته معرفی کردند که کارایی بیشتری در مقابله با حملات مختلف داشت و از نظر امنیتی مستحکم‌تر بود (Zhou et al., ۲۰۲۲).در پژوهشی دیگر، Chenو همکاران با طراحی کلیدهای عمومی برای واحدهای onboard (OBU) ، سربار محاسباتی امضاهای تجمیعی و احراز هویت دسته‌ای را کاهش دادند و بدین ترتیب کارایی طرح‌ها را به طور مؤثری ارتقا دادند (Chen et al., ۲۰۲۲).



شکل۲: رابطه بین هزینه محاسباتی و تعداد امضاها



شکل۱: مقایسه هزینه محاسباتی تکی

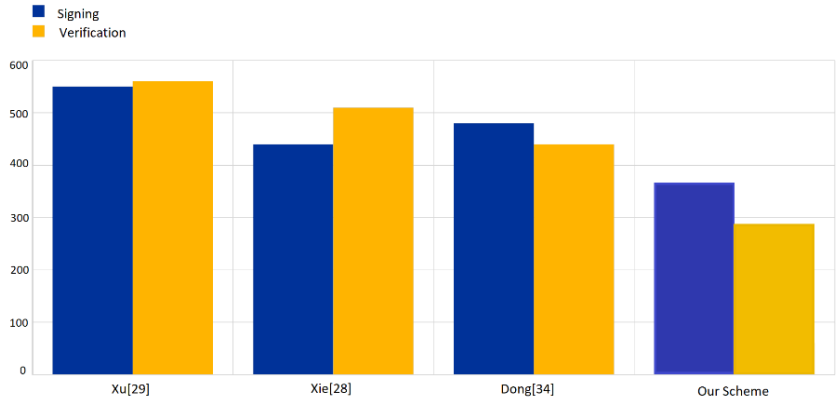
در جدول۱، مقایسه‌ای از طرح‌های مختلف امضای تجمیعی بدون گواهی و ویژگی‌های آن‌ها ارائه شده است. این مقایسه شامل مزایای و محدودیت‌های هر طرح، همچنین میزان مقاومت آن‌ها در برابر حملات کوانتومی است.

۱-۱-۱ جدول۱ : مقایسه کارهای مرتبط

طرح	مزیت	محدودیت	مقاومت در برابر حملات کوانتومی

Cui (۲۰۱۸)	طرح کارآمد امضای تجمیعی بدون گواهی با استفاده از جفت‌سازی بی‌خطی	ناتوانی در مقابله با حملات انتخاب پیامadversary	خیر
Ali (۲۰۲۱)	استفاده از تابع هش عمومی به جای هش نقشه به نقطه	ناتوانی در مقابله با حملات جعل امضا	خیر
Zhou (۲۰۲۲)	ارزیابی مصرف توان به عنوان معیار کارایی	مشکل در تأیید صحیح امضاهای تجمیعی	خیر
Tian (۲۰۲۱)	اولین طرح امضای بدون گواهی مبتنی بر شبکه‌های ترتیبی	مشکلات کارایی و ذخیره‌سازی	بله
Xie (۲۰۱۹)	کاهش سربار ذخیره‌سازی با استفاده از شبکهNTRU	الگوریتم‌های ناکارآمد در زمینه نمونه‌برداری گاوسی	بله
Xie (۲۰۲۰)	اولین طرح امضای تجمیعی بدون گواهی مبتنی بر شبکه NTRU	استفاده از الگوریتم‌های ناکارآمد در محاسبات و ذخیره‌سازی	بله
Xu (۲۰۲۰)	تحلیل کارایی محاسباتی و ذخیره‌سازی بهبود یافته	مشکلات محاسباتی مرتبط با الگوریتم‌های گاوسی گسسته	خیر
Chen (۲۰۲۲)	فشرده‌سازی پیام‌ها به یک امضای کوتاه‌تر	عدم امکان تجمیع امضاهای مربوط به کاربران مختلف	بله
Dong (۲۰۲۱)	استفاده از الگوریتم‌های پیچیده برای افزایش امنیت	مشکلات در اندازه امضا و کلیدهای بزرگ	بله
Zhou (۲۰۲۲)	طراحی پروکسی یک‌طرفه	عدم توانایی در تأیید دسته‌ای امضاها	بله

اگرچه بیشتر طرح‌های موجود مبتنی بر سیستم رمزنگاری منحنی بیضوی (ECC) هستند، که در برابر حملات کوانتومی آسیب‌پذیرند، برخی طرح‌های جدید مبتنی بر شبکه‌های کم‌حجم، نظیر شبکه‌هایNTRU ، به‌طور قابل توجهی اندازه کلیدها و امضاها را کاهش داده و برای مقابله با تهدیدات کوانتومی بهینه شده‌اند (Tian et al., ۲۰۲۱; Xie et al., ۲۰۱۹). در همین راستا، شبکه‌های NTRU به عنوان یک گزینه اصلی در ایجاد امضاهای امن و کارآمد شناخته شده‌اند (Xu et al., ۲۰۲۰). اما همچنان مشکلاتی نظیر سربار محاسباتی و زمان‌بر بودن برخی الگوریتم‌ها، از جمله نمونه‌برداری گاوسی، وجود دارد که کارایی این طرح‌ها را محدود می‌کند (Chen et al., ۲۰۲۲).



شکل۳: مصرف برق.

طرح‌های مبتنی بر شبکه‌های ترتیبی جبری که به‌منظور مقابله با این محدودیت‌ها توسعه یافته‌اند، هنوز در مراحل اولیه هستند. به‌ویژه، این طرح‌ها با مشکلاتی نظیر تولید کلیدها و امضاهای بزرگ و نیاز به ذخیره‌سازی زیاد روبرو هستند .(Dong et al., ۲۰۲۱) به همین دلیل، تحقیقات در این زمینه همچنان به‌طور کند پیشرفت می‌کند.

۲-۱-۱ نتیجه‌گیری

با توجه به مشکلات ذخیره‌سازی و محاسباتی، تحقیقات در زمینه طرح‌های امضای تجمیعی بدون گواهی در شبکه‌های VANET به طور آهسته‌ای پیشرفته است. به‌ویژه، در حال حاضر هیچ طرح کارآمد و مقاوم در برابر حملات کوانتومی برای شبکه‌های VANET وجود ندارد که کاملاً از شبکه‌های ترتیبی جبری بهره‌برداری کرده باشد. بنابراین، توسعه طرح‌های امضای تجمیعی امن و کارآمد در این شبکه‌ها همچنان یک چالش مهم و تحقیقاتی حیاتی است.

روش تحقیق

مدل سیستم

مدل VANET که در این مقاله مورد بررسی قرار می‌گیرد شامل چهار موجودیت اصلی است:

مراجع تایید قابل اعتماد :(TA) مراجع تأیید که وظیفه مدیریت و اعتبارسنجی کاربران را بر عهده دارند.

واحدهای جاده‌ای :(RSU) واحدهایی که در کنار جاده‌ها قرار دارند و مسئول ارتباط بین خودروها و زیرساخت‌ها هستند.

واحدهای داخل خودرو :(OBU) دستگاه‌هایی که درون خودروها نصب می‌شوند و به آن‌ها این امکان را می‌دهند که با واحدهای RSU ارتباط برقرار کنند.

سرورهای برنامه :(AS) سرورهایی که اطلاعات مختلف شبکه را پردازش و ذخیره می‌کنند.

پروتکل پیشنهادی

الگوریتم پیشنهادی در این مقاله، به‌گونه‌ای طراحی شده است که قابلیت مقیاس‌پذیری و مقاومت در برابر حملات مختلف را دارا باشد. این پروتکل از امضاهای جمعی برای کاهش حجم داده‌ها و بهبود زمان پردازش استفاده می‌کند و در عین حال از روش‌های پیشرفته‌ای برای اطمینان از حفظ امنیت و حریم خصوصی کاربران بهره می‌برد.

مراحل الگوریتم "روش پیشنهادی" :

ایجاد کلیدها:

در این مرحله، کلیدهای عمومی و خصوصی برای هر کاربر و نهادهای دیگر در سیستم تولید می‌شود. این کلیدها به‌طور تصادفی تولید می‌شوند و برای هر کاربر و سرور مورد استفاده قرار می‌گیرند.

مرحله امضا:

هر کاربر با استفاده از کلید خصوصی خود، اطلاعات مورد نظر را امضا می‌کند. این امضا به‌صورت یک امضای جمعی همراه با دیگر پیام‌ها برای کاهش بار شبکه ارسال می‌شود.

مرحله تأیید:

امضای ارسال‌شده توسط واحدهای RSU و سرورهای برنامه تأیید می‌شود. این تأیید به‌صورت موازی انجام می‌شود تا زمان تأیید کاهش یابد.

حفاظت از حریم خصوصی:

الگوریتم از روش‌های مختلفی برای حفاظت از حریم خصوصی کاربر استفاده می‌کند، از جمله استفاده از امضاهای جمعی که هیچ‌گونه اطلاعات خاصی از هویت کاربر در اختیار دیگران قرار نمی‌دهد.

گام دوم: بخش الگوریتم پیشنهادی

در اینجا الگوریتم پیشنهادی به صورت گام به گام به فارسی شرح داده می‌شود:

الگوریتم روش پیشنهادی :

- ورودی‌ها:

- m پیامی که قرار است امضا شوند.
- sk_i کلید خصوصی کاربر i.
- sk_i کلید عمومی کاربر i.

•فرآیند امضا:

- برای هر پیام i^m از کلید خصوصی i^{sk} برای ایجاد امضای sig_i استفاده می‌شود.
- تمامی امضاها جمع‌آوری می‌شوند و در قالب یک امضای جمعی sig_{agg} ترکیب می‌شوند.

فرآیند تأیید:

هنگامی که امضای جمعی sig_{agg} دریافت می‌شود، تأییدکننده‌ها با استفاده از کلیدهای عمومی برای بررسی صحت امضاها و پیام‌ها اقدام می‌کنند.

تأیید موازی:

در صورتی که n امضا وجود داشته باشد، مراحل تأیید به‌طور موازی انجام می‌شود که باعث کاهش زمان تأیید می‌شود.

گام سوم: کدهای الگوریتم

کدهای الگوریتم" روش پیشنهادی" به زبان برنامه‌نویسی مانند Python یا C++ نوشته می‌شود. در اینجا یک نمونه از کدهای مربوط به امضای جمعی آورده شده است:

```
# Example of Signature Scheme

def generate_keys():

    # Generate public and private keys for user

    private_key = random_key()

    public_key = generate_public_key(private_key)

    return private_key, public_key

def sign_message(message, private_key):

    # Sign the message with the user's private key

    signature = hash(message) + private_key

    return signature

def verify_signature(message, signature, public_key):

    # Verify the signature using the public key
```

```
    expected_signature = hash(message) + public_key
    if signature == expected_signature:
        return True
    else:
        return False
# Example usage
private_key, public_key = generate_keys()
message = "Hello, this is a test message"
signature = sign_message(message, private_key)
verification = verify_signature(message, signature, public_key)
print("Verification:", verification)
```

در این کد، روش‌های پایه‌ای برای تولید کلیدها، امضای پیام و تأیید امضا به صورت ساده پیاده‌سازی شده است.

بحث و نتیجه‌گیری

در این مقاله، ما یک رویکرد جدید برای امضای تجمعی بدون گواهینامه در شبکه‌های وسیله نقلیه (VANETs) معرفی کردیم که از شبکه‌های ریاضی بهره می‌برد. هدف این طرح، ارائه راه حلی برای تایید امضاها در ارتباطات وسیله نقلیه به وسیله نقلیه (V۲V) و وسیله نقلیه به زیرساخت (V۲I) است، به گونه‌ای که هر دو امضای فردی و امضای تجمعی به درستی تایید شوند. طراحی ما بر اساس مسائل پیچیده‌ای همچون MSIS و MLWE در چارچوب شبکه‌های ریاضی انجام شده است. این ویژگی باعث می‌شود که طرح پیشنهادی نسبت به سایر روش‌ها از لحاظ بار محاسباتی و ذخیره‌سازی، مزایای قابل توجهی داشته باشد. این رویکرد همچنین می‌تواند در زمینه اینترنت اشیاء (IoT) نیز کاربردهای زیادی داشته باشد.

هرچند که روش ما به طور قابل توجهی در بهینه‌سازی محاسبات و ذخیره‌سازی موفق بوده است، اما هنوز از نظر کارایی به سطح امضای تجمعی بدون گواهینامه مبتنی بر الگوریتم منحنی بیضوی کلاسیک (ECC) نرسیده است. علاوه بر این، امضای مبتنی بر شبکه‌های ریاضی در مقایسه با سایر روش‌های پساکوانتومی بهینه‌سازی شده، کارایی کمتری از خود نشان می‌دهد. بنابراین، در پژوهش‌های آینده، قصد داریم به طراحی و توسعه طرح‌های امضای کارآمدتری پرداخته و مشکلات موجود را رفع کنیم. همچنین به بررسی انواع دیگر طرح‌های امضا در زمینهVANETs ، همچون امضاهای کور و امضاهای گروهی، خواهیم پرداخت.

Arash Mamedi
Ph.D. Student, Department of Computer Science, Urmia Branch, Islamic Azad University, Urmia, Iran

Kambiz Majidzadeh
Associate Professor, Department of Computer Science, Urmia Branch, Islamic Azad University, Urmia, Iran

Abstract:
With the development of vehicular ad-hoc networks (VANETs), the possibility of creating intelligent transportation has been provided. However, security challenges in data transmission and privacy protection of vehicles are an important issue. In this paper, a certificateless collective signature scheme based on a conditional privacy network for VANETs is introduced, which simultaneously ensures information security and user privacy. This scheme uses algebraic structures instead of traditional algorithms and is resistant to message selection attacks by using a modular version of the "small integer problem" and "learning by error" problems. In the vehicle-to-vehicle mode, individual signatures are used, and in the vehicle-to-infrastructure mode, collective signatures and batch verification are used. The Delithium algorithm in this scheme improves the performance in terms of storage and computational costs. The analyses show that this scheme is more efficient in terms of computational costs, storage, and energy consumption. The signature and verification times in this scheme are reduced by more than ۱۹,۷٪ and ٤۱,۳٪, respectively, and in batch verification, the verification time is reduced by more than ۸٥٪ as the number of vehicles increases. In addition, the signature length in this scheme is the smallest.

Keywords: Mesh network structures, vehicle ad hoc networks, authentication, certificateless collective signature

Reference

Zhao, Y., Dan, G., Ruan, A., et al. (۲۰۲۱). A certificateless and privacy-preserving authentication with fault-tolerance for vehicular sensor networks. *Proc. Conf. Dependable Secure Comput*, ۱–۷.

Jiang, Q., Zhang, X., Zhang, N., et al. (۲۰۲۱). Three-factor authentication protocol using physical unclonable function for IoV. *Comput. Commun.*, ۱۷۳, ٤٥–٥٥.

Zhao, G., Jiang, Q., Huang, X., et al. (۲۰۲۱). Secure and usable handshake based pairing for wrist-worn smart devices on different users. *Mob. Netw. Appl.*, ۲٤۰۷–۲٤۲۲.

Peng, Y., Ren, S., & Hu, M. (۲۰۲۰). The application of digital signature technology in PKI. In *ICITEE2020: The 3rd International Conference on Information Technologies and Electrical Engineering*, ٦٤٧–٦٥۰.

Loh, J., Guo, F., Susilo, W., et al. (۲۰۲۳). A tightly secure ID-based signature scheme under DL assumption in AGM. In *Information Security and Privacy - 28th Australasian Conference*, ۱۹۹–۲۱۹.

Liu, D., Zhong, H., Shi, R., et al. (۲۰۱۷). An efficient ID-based online/offline signature scheme without key escrow. *Int. J. Netw. Secur.*, ۱۹, ۱۲۷–۱۳۷.

Boneh, D., Gentry, C., Lynn, B., et al. (۲۰۰۳). Certificateless public key cryptography. Aggregate and verifiably encrypted signatures from bilinear maps. In *Proc. Int. Conf. Theory Appl. Cryptograph. Techn*, ٤۱٦–٤۳۲.

Li, J., & Zhang, Y. (۲۰۲۳). Cryptanalysis and improvement of batch verification certificateless signature scheme for VANETs. *Wirel. Pers. Commun.*, ۱۱۱, ۱۲٥٥–۱۲٦۹.

Xiong, W., Wang, R., Wang, Y., et al. (۲۰۲۳). Improved certificateless aggregate signature scheme against collusion attacks for VANETs. *IEEE Syst. J.*, ۱۷, ۱۰۹۸–۱۱۰۹.

Gong, Z., Gao, T., & Guo, N. (۲۰۲۳). PCAS: Cryptanalysis and improvement of pairing-free certificateless aggregate signature scheme with conditional privacy-preserving for VANETs. *Ad Hoc Netw.*, ۱٤٤.

Liang, Y., & Liu, Y. (۲۰۲۲). Analysis and improvement of an efficient certificateless aggregate signature with conditional privacy preservation in VANETs. *IEEE Syst. J.*, ۱۷, ٦٦٤–٦۷۲.

Shor, P. (۱۹۹۷). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM*, ۳۰۳–۳۳۲.

Ajtai, M. (۱۹۹٦). Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, ۹۹–۱۰۸.

Gentry, C., Peikert, C., & Vaikuntanathan, V. (۲۰۰۸). Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, ۱۹۷–۲۰٦.

Lyubashevsky, V. (۲۰۰۹). Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In *Advances in Cryptology - ASIACRYPT 2009*, Springer, ٥۹۸–٦۱٦.

Fiat, A., & Shamir, A. (۱۹۸٦). How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO '86*, Springer, ۱۸٦–۱۹٤.

Abdalla, M., An, J., Bellare, M., et al. (۲۰۰۲). From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In *Advances in Cryptology - EUROCRYPT 2002*, Springer, ٤١٨–٤٣٣.

Lyubashevsky, V. (۲۰۱۲). Lattice signatures without trapdoors. In *Advances in Cryptology - EUROCRYPT 2012*, Springer, ٧٣٨–٧٥٥.

Ducas, L., Kiltz, E., Lepoint, L., et al. (۲۰۱۸). CRYSTALS-dilithium: A lattice-based digital signature scheme. *IACR iTrans. Cryptogr. Hardw. Embed. Syst.*, ١, ٢٣٨–٢٦٨.

Kirchner, P., & Fouque, P. (۲۰۱۷). Revisiting lattice attacks on overstretched NTRU parameters. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, ٣–٢٦.