مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال هشتم، شماره ۱، بهار ۱۳۹۹؛ ص ۳۳-۲۵

تحلیل امنیت و بهبود یک سامانه حمل‌ونقل هوشمند مبتنی بر امضای تجمعی فاقد گواهینامه

نصراله پاک‌نیت[۱]، زیبا اسلامی[۲*]

۱- استادیار، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران، ۲- دانشیار، گروه علوم داده‌ها و کامپیوتر، دانشکده علوم ریاضی، دانشگاه شهید بهشتی، تهران، ایران

(دریافت:۹۷/۱۲/۲۶، پذیرش: ۹۸/۳/۲۸)

چکیده

«شبکه‌های اقتضایی خودرویی» (VANET) اساس سامانه‌های حمل‌ونقل هوشمند هستند و نیازمندی‌های کلیدی آن‌ها عبارتند از تضمین جامعیت و اصالت پیام‌های تولیدشده توسط وسایل نقلیه، حفظ حریم خصوصی مشروط و کارایی. اخیراً، ژانگ و همکاران با ارائه یک طرح امضا تجمعی فاقد گواهینامه، یک سامانه حمل‌ونقل هوشمند ارائه کرده‌اند. در این سامانه، اصالت پیام‌ها با استفاده از امضای دیجیتال، حفظ حریم خصوصی مشروط با استفاده از نام‌های مستعار و کارایی با استفاده از امضای تجمعی فاقد گواهینامه تأمین شده است. طرح امضا تجمعی فاقد گواهینامه ارائه‌شده توسط ژانگ و همکاران بسیار کارا بوده و در آن، طول امضا تجمعی و همچنین تعداد عملگر زوج‌سازی دوخطی موردنیاز برای بررسی اصالت یک امضا، ثابت و مستقل از تعداد امضاهای تجمعی است. ژانگ و همکاران ادعا کرده‌اند که تحت فرض سختی مساله محاسباتی دیفی-هلمان CDH، طرح ارائه‌شده توسط آن‌ها در برابر حمله متن و شناسه منتخب وفقی جعل‌ناپذیر است. در این مقاله، در ابتدا، اثبات می‌شود که این ادعا نادرست بوده و نشان داده خواهد شد که در طرح ارائه‌شده هر متخاصمی قادر است تنها با دیدن یک زوج (پیام و امضا) متناظر با یک وسیله نقلیه، به‌راحتی امضای آن وسیله نقلیه را بر روی هر پیام دیگری جعل کند. در ادامه، با اعمال تغییراتی بر روی طرح ژانگ و همکاران، یک طرح امضا تجمعی بهبودیافته ارائه می‌شود که در مقابل حمله جعل مطرح‌شده امن باشد.

کلیدواژه‌ها: VANETT، حفظ حریم خصوصی، امضا تجمعی، رمزنگاری فاقد گواهینامه، جعل‌پذیری، Computational Diffie-Hellman

۱. مقدمه

طراحی یک سامانه هوشمند برای حل مسئله ایمنی حمل‌ونقل و افزایش بهره‌وری آن همواره از مسائل موردتوجه محققان بوده است. بخصوص در سال‌های اخیر، به دلیل پیشرفت‌های فناوری شبکه و مخابرات بی‌سیم «شبکه‌های اقتضایی خودرویی»[۱] (VANET) به‌طور ویژه به کانون توجه محققان این حوزه تبدیل گشته‌اند. در این شبکه‌ها، وسایل نقلیه از طریق شبکه‌های بی‌سیم با یکدیگر در ارتباط بوده و در فواصل زمانی مشخص اطلاعاتی مرتبط با ترافیک جاده‌ای را منتشر می‌کنند. این اطلاعات سپس توسط سرورهایی جمع‌آوری و تحلیل شده و به مرکز کنترل ترافیک ارسال می‌شود تا راهبرد بهینه جهت مدیریت وضعیت ترافیک را اتخاذ کند.

موجودیت‌های موجود در یک VANET عبارتند از یک مرکز مورد اعتماد[۲] (TA)، مجموعه‌ای از واحدهای کنار جاده‌ای[۳] (RSU) و مجموعه‌ای از وسایل نقلیه که به یک واحد خاص[۴] (OBU) مجهز هستند. روال انجام کار در VANET (طبق پروتکل «ارتباطات کوتاه برد اختصاصی»[۵] (DSRC))، به‌صورت زیر است: هر وسیله نقلیه‌ای اطلاعات مربوط به ترافیک شامل اخبار ازدحام، وضعیت آب و هوایی، اطلاعات در مورد تصادفات، سرعت وسیله نقلیه، مکان و ... را هر ۱۰۰ تا ۳۰۰ میلی‌ثانیه منتشر می‌کند. RSU پس از دریافت پیام‌های مرتبط با ترافیک، جامعیت و اعتبار آن‌ها را مورد بررسی قرار داده و اطلاعات معتبر را به مرکز کنترل ترافیک ارسال می‌کند. در ادامه، مرکز کنترل ترافیک با توجه به اطلاعات دریافتی راهبردهای مناسب جهت بهبود ترافیک اتخاذ می‌کند.

چالش مهم VANET، جلوگیری از دست‌کاری اطلاعات توسط یک وسیله نقلیه مخرب است. به‌طور واضح، استفاده از پیام‌های اشتباه ممکن است منجر به تصادف و اتخاذ راهبرد غلط توسط مرکز کنترل ترافیک شود؛ بنابراین، بدون تردید لازم است جامعیت و اصالت پیام‌ها قبل از استفاده بررسی شود. علاوه‌براین، یکی دیگر از نیازمندهای امنیتی VANET حفظ حریم خصوصی

*رایانامه نویسنده پاسخگو: z_eslami@sbu.ac.ir

1- Vehicular Ad-hoc Network
2 -Trusted authority
3- Road side unit
4- On-board unit
5- Dedicated short range communication protocol

مشروط[1] است. حفظ حریم خصوصی مشروط بدین معنی است که درعین‌حال که سایرین قادر به شناسایی وسایل نقلیه بر اساس پیام‌های ارسالی آن‌ها نیستند، ردیابی هر وسیله نقلیه‌ای در صورت نیاز ممکن باشد. همچنین با توجه به محدوده تحت پوشش یک RSU و حجم ترافیک موجود در این محدوده، فشرده‌سازی نیز مسئله مهم دیگری است که باید در VANET به آن پرداخته شود [۲-۱].

۲. کارهای مرتبط

پیشینه پژوهش نشان می‌دهد که روش‌های زیادی برای تأمین نیازمندی‌های امنیتی VANET ارائه شده است. در [۳] یک طرح احراز اصالت با حفظ حریم خصوصی با استفاده از سامانه‌های کلید عمومی سنتی PKI[2] ارائه شده است. این روش متأسفانه به دلیل نیاز به ذخیره‌سازی تعداد زیادی کلید و گواهینامه مربوطه بر روی OBU وسایل نقلیه و محاسبات سنگین موردنیاز برای مدیریت گواهینامه‌ها و ردیابی شناسه واقعی یک وسیله نقلیه متخلف از کارایی مناسب برخوردار نیست. در [۴]، نویسندگان یک پروتکل با قابلیت حفظ حریم خصوصی مشروط کارا برای ارتباط امن بین خودرویی ارائه کرده‌اند. این روش نیز مبتنی بر سامانه‌های کلید عمومی سنتی (PKI) بوده و درنتیجه از مشکل مدیریت گواهینامه‌ها رنج می‌برد. برای حل مسئله مدیریت گواهینامه‌ها، روش‌هایی مبتنی بر رمزنگاری مبتنی بر شناسه ارائه‌شده است. در یک سامانه رمزنگاری مبتنی بر شناسه [۵]، کلید عمومی هر وسیله نقلیه‌ای را می‌توان به‌راحتی با استفاده از شناسه آن محاسبه کرد. در [۶]، یک روش احراز هویت دسته‌ای مبتنی بر شناسه ارائه‌شده است. در این روش، حفظ حریم خصوصی مشروط با استفاده از فن زنجیره چکیده‌ساز[3] تأمین شده که این مهم منجر به کارایی مناسب این روش شده است. [۲] نیز یک روش احراز هویت دسته‌ای مبتنی بر شناسه دیگر ارائه کرده است. متأسفانه، همانند سایر روش‌های رمزنگاری مبتنی بر شناسه، روش ارائه‌شده در [۲ و ۶] نیز از مسئله امان‌سپاری کلید[4] رنج می‌برد.

برای حل هم‌زمان مسائل مدیریت گواهینامه‌ها در سامانه‌های سنتی و امان‌سپاری کلید در سامانه‌های مبتنی بر شناسه، در [۷] مفهوم رمزنگاری فاقد گواهینامه معرفی شده است. همانند سامانه‌های رمزنگاری مبتنی بر شناسه، در سامانه‌های رمزنگاری فاقد گواهینامه نیز مرکز تولید کلید[5] (KGC) وجود داشته اما در این‌جا این مرکز تنها بخشی از کلید خصوصی کامل کاربر به نام کلید خصوصی جزئی را با توجه به شناسه او تولید کرده و در اختیار او قرار می‌دهد. قسمت دیگری از کلید خصوصی کاربر توسط خود او انتخاب و محرمانه نگهداری می‌شود. در این سامانه‌ها، هر کاربر علاوه بر شناسه دارای یک کلید عمومی نیز بوده که با استفاده از قسمتی از کلید خصوصی او و مقادیر عمومی محاسبه‌شده و بدون نیاز به گواهینامه اعلام عمومی می‌شود.

مفهوم امضا تجمعی برای اولین بار در [۸] توسط بونه و همکاران ارائه‌شده است. با استفاده از یک طرح امضا تجمعی، می‌توان n امضا ایجادشده بر روی n پیام از طرف n کاربر را در یک امضا تجمیع و ارسال کرد و بدین طریق هم حجم داده‌های ارسالی و هم بار محاسباتی موردنیاز برای تصدیق درستی امضاها را کاهش داد. این ویژگی امضاهای تجمعی، آن‌ها را به ابزاری کاربردی به‌خصوص در محیط‌های با محدودیت در حجم ارسال داده‌ها یا محدودیت در محاسبات تبدیل می‌کند. پس از ارائه اولین طرح امضا تجمعی در [۸]، طرح‌های امضا تجمعی زیادی هم در بستر رمزنگاری کلید عمومی سنتی و هم در زمینه مبتنی بر شناسه ارائه‌شده که علاقه‌مندان می‌توانند برای اطلاعات بیشتر به [۱۵-۹] مراجعه کنند. در سالیان گذشته، با توجه به مزیت‌های رمزنگاری فاقد گواهینامه، چندین طرح امضا تجمعی فاقد گواهینامه[6] (CLAS) ارائه‌شده است [۲۲-۱۶]. علی‌رغم کاهش هزینه‌های محاسباتی در تصدیق امضاهای تجمعی، اغلب طرح‌های امضا تجمعی فاقد گواهینامه امن ارائه‌شده تا به امروز همچنان ناکارا هستند. در [۲۳]، نویسندگان یک طرح CLAS کارا ارائه کرده‌اند که تعداد عمل زوج‌سازی دوخطی موردنیاز در آن برای تصدیق یک امضا تجمعی ثابت است اما متأسفانه، در [۲۴]، نویسندگان نشان داده‌اند که این طرح ناامن است. در [۲۵]، نویسندگان یک طرح CLAS کارای دیگر ارائه کرده‌اند که در [۲۶] نشان داده شده این طرح نیز ناامن است.

در [۱]، نویسندگان با ارائه یک طرح CLAS با قابلیت حفظ حریم خصوصی یک سامانه هوشمند مدیریت ترافیک ارائه کرده‌اند که بسیار کاراست. در این طرح تعداد عمل زوج‌سازی موردنیاز برای تصدیق اصالت یک امضا تجمعی و همچنین اندازه امضا تجمعی ثابت بوده و وابسته به تعداد امضاکنندگان و پیام‌ها نیست. نویسندگان [۱] ادعا کرده‌اند که طرح CLAS ارائه‌شده توسط آن‌ها در برابر حمله متن و شناسه منتخب وفقی[7] امن است. حمله متن و شناسه منتخب وفقی نوعی تعاملی از حمله انتخاب متن و شناسه منتخب است که در آن حمله‌کننده قادر

1- Conditional privacy-preserving
2- Public key infrastructure
3- Hash chain technique
4- Key escrow
5- Key Generation Center
6- Certificateless Aggregate Signature
7- Adaptive chosen-message and chosen-identity attack

است به صورت وفق‌پذیر امضا متناظر با پیام‌ها و شناسه‌های مختلف را درخواست کرده و با استفاده از نتایج، امضا یک کاربر دلخواه روی یک پیام دلخواه را جعل کند. در این مقاله نشان داده خواهد شد که ادعای نویسندگان اشتباه بوده و طرح CLAS ارائه‌شده توسط آن‌ها در برابر این حمله ناامن است. به بیان دقیق‌تر، در این مقاله نشان داده خواهد شد که تنها با دسترسی به یک زوج (پیام و امضا) که توسط یک وسیله نقلیه در طرح ارائه‌شده در [۱] تولید شده است، هر متخاصمی قادر است امضای این وسیله نقلیه را روی هر پیام دیگری جعل کند. درنتیجه این جعل‌پذیری، سامانه هوشمند مدیریت ترافیک ارائه‌شده توسط نویسندگان نیز ناامن بوده و جامعیت و امکان بررسی اصالت پیام‌ها را ارائه نمی‌کند. در ادامه این مقاله و پس از اثبات ناامنی طرح ژانگ و همکاران، با اعمال تغییراتی بر روی این طرح، یک طرح امضا تجمعی بهبودیافته ارائه خواهد شد که در مقابل حمله جعل ارائه‌شده امن باشد.

سایر بخش‌های مقاله به صورت زیر سازمان‌دهی شده‌اند. در بخش ۳ شمای کلی و مدل امنیتی یک طرح امضا تجمعی فاقد گواهینامه مناسب برای استفاده در VANET بررسی خواهد شد. حمله پیشنهادشده بر روی طرح ژانگ و همکاران در بخش ۴ ارائه می‌شود. در بخش ۵، طرح ژانگ و همکاران به‌گونه‌ای بهبود داده خواهد شد که در مقابل حمله پیشنهادی امن باشد. تأمین الزامات امنیتی موردنیاز توسط طرح پیشنهادی در بخش ۶ بررسی خواهد شد و درنهایت، نتیجه‌گیری‌های این مقاله در بخش ۷ ارائه خواهد شد.

۳. تعاریف و مدل امنیت طرح‌های امضای تجمعی فاقد گواهینامه (CLAS)

در این بخش، در ابتدا شمای کلی یک طرح امضا تجمعی فاقد گواهینامه قابل‌استفاده در VANET توضیح داده شده و سپس مدل امنیت آن مورد بررسی قرار خواهد گرفت.

۳-۱. شمای کلی یک طرح CLAS

در یک طرح امضا تجمعی فاقد گواهینامه مناسب برای استفاده در VANET موجودیت‌های زیر دخیل هستند: مرجع مورد اعتماد (TA)، مرکز تولید کلید (KGC)، مجموعه‌ای از واحدهای کنار جاده‌ای ($RSU_1, RSU_2, \dots$)، مرجع ردیابی[1] (TRA) و مجموعه‌ای از وسایل نقلیه ($V_1, V_2, \cdots, V_n$). همچنین الگوریتم‌های تشکیل‌دهنده چنین طرحی عبارتند از:

الگوریتم راه‌اندازی سامانه: این الگوریتم با ورودی پارامتر امنیت، پارامترهای عمومی سامانه params، کلید مخفی اصلی[2] MSK و یک کلید ردیابی تولید می‌شود.

الگوریتم تولید نام مستعار: این الگوریتم با ورودی شناسه واقعی یک وسیله نقلیه (RID_i) که به‌صورت یکتا وسیله نقلیه موردنظر را مشخص می‌کند شناسه مستعار متناظر با این وسیله نقلیه (PID_i) را تولید می‌کند.

الگوریتم تولید کلید خصوصی جزئی: این الگوریتم با ورودی شناسه مستعار یک وسیله نقلیه PID_i، کلید خصوصی جزئی psk_i متناظر با این شناسه را تولید می‌کند.

الگوریتم تولید کلید وسیله نقلیه: این الگوریتم با ورودی شناسه مستعار PID_i متناظر با یک وسیله نقلیه، مقدار مخفی vsk_i و کلید عمومی متناظر با این مقدار vpk_i را تولید می‌کند.

الگوریتم امضا: این الگوریتم با ورودی کلید امضا (psk_i, vsk_i) و پیام $m_i \in \{0,1\}^*$ امضا σ_i را روی این پیام تولید می‌کند.

الگوریتم تائید اصالت: این الگوریتم با ورودی شناسه مستعار PID_i، کلید عمومی vpk_i، پیام m_i و امضا σ_i، اعتبار امضا σ_i را بررسی می‌کند.

الگوریتم تجمیع امضا: این الگوریتم n امضا σ_1، σ_2، ...، σ_n را دریافت کرده و امضا تجمعی σ را تولید می‌کند.

الگوریتم تائید اصالت تجمیعی: این الگوریتم شناسه‌های مستعار PID_1، PID_2، ...، PID_n، کلیدهای عمومی متناظر یعنی vpk_1، vpk_2، ...، vpk_n، پیام‌های m_1، m_2، ...، m_n و امضا تجمعی σ را دریافت کرده و در صورت معتبر بودن امضا تجمعی σ خروجی ۱ و در غیر این صورت خروجی ۰ را می‌دهد.

۳-۲. مدل امنیت طرح‌های امضا تجمعی فاقد گواهینامه

با توجه به استفاده از امضا تجمعی فاقد گواهینامه برای ارائه یک روش سامانه هوشمند مدیریت ترافیک در [۱]، در این بخش مدل در نظر گرفته شده برای بررسی امنیت این طرح‌ها بررسی می‌شود. به‌طورمعمول، در بررسی امنیت سامانه‌های رمزنگاری فاقد گواهینامه دو نوع متخاصم در نظر گرفته می‌شود: ۱) متخاصم نوع I (A_1) که به کلید مخفی اصلی دسترسی نداشته اما می‌تواند کلید عمومی هر وسیله نقلیه‌ای را با هر مقدار دلخواهی تعویض کند. این نوع متخاصم، یک کاربر مخرب بیرونی را شبیه‌سازی می‌کند؛ ۲) متخاصم نوع II (A_2) که به کلید

1- Trace Authority

2- Master Secret Key

مخفی اصلی دسترسی داشته اما قادر به تعویض کلید عمومی وسایل نقلیه نیست. این نوع متخاصم مرکز تولید کلید مخربی را شبیه‌سازی می‌کند که قصد سوءاستفاده از اختیارات خود را دارد.

امنیت یک طرح CLAS را با استفاده از دو بازی بین یک چالشگر C و دو نوع متخاصم در نظر گرفته‌شده در سامانه‌های رمزنگاری فاقد گواهینامه (A_1 و A_2) مدل‌سازی می‌کنند [۲۸-۲۷]. در ادامه این بخش، جزئیات بازی‌های موردنظر بازبینی خواهد شد.

بازی I: فرض کنید C چالشگر و l پارامتر امنیت باشد.

۱. C الگوریتم راه‌اندازی سامانه را با ورودی l اجرا کرده، پارامترهای عمومی سامانه params و کلید مخفی اصلی MSK را تولید کرده، params را به A_1 ارسال کرده و MSK را محرمانه نگهداری می‌کند.

- در طول شبیه‌سازی A_1 قادر است تعدادی درخواست (محدود به چندجمله‌ای) به C ارائه کند و C پاسخ‌های مناسب را به او بازمی‌گرداند. درخواست‌های قابل انجام از طرف متخاصم عبارتند از ایجاد وسیله نقلیه، کلید خصوصی جزئی وسیله نقلیه، مقدار مخفی وسیله نقلیه، کلید عمومی وسیله نقلیه، تعویض کلید عمومی وسیله نقلیه و امضا که C در پاسخ به این درخواست‌ها، خروجی مناسب را بازمی‌گرداند. در این بازی A_1 تنها قادر است درخواست امضا از طرف کاربرانی را انجام دهد که کلید عمومی آن‌ها تعویض نشده باشد.

۲. A_1 امضا تجمعی فاقد گواهینامه σ^* امضاشده توسط n وسیله نقلیه با شناسه‌های مستعار $L^*_{PID}=\{PID^*_1, PID^*_2, \cdots, PID^*_n\}$ و کلیدهای عمومی $L^*_{vpk}=\{vpk^*_1, vpk^*_2, \cdots, vpk^*_n\}$ بر روی پیام‌های $L^*_m=\{m^*_1, m^*_2, \cdots, m^*_n\}$ را خروجی می‌دهد. A_1 برنده این بازی است اگر دو شرط زیر برقرار باشند:

- شرط اول: σ^* یک امضا تجمعی معتبر بر روی پیام‌های $L^*_m=\{m^*_1, m^*_2, \cdots, m^*_n\}$ از طرف وسایل نقلیه با شناسه‌های $L^*_{PID}=\{PID^*_1, PID^*_2, \cdots, PID^*_n\}$ و کلیدهای عمومی $L^*_{vpk}=\{vpk^*_1, vpk^*_2, \cdots, vpk^*_n\}$ باشد.
- شرط دوم: به‌ازای حداقل یکی از شناسه‌های مستعار ($PID^*_1 \in L^*_{PID}$ باشد)، «درخواست مقدار مخفی وسیله نقلیه» با ورودی PID^*_1 و درخواست امضا با ورودی (PID^*_1, m^*_1) صورت نگرفته باشد.

بازی II: فرض کنید C چالشگر و l پارامتر امنیت باشد.

۱. C الگوریتم راه‌اندازی سامانه را با ورودی l اجرا کرده، پارامترهای عمومی سامانه params و کلید مخفی اصلی MSK را تولید کرده و آن‌ها را به A_2 ارسال می‌کند.

- در طول شبیه‌سازی A_2 قادر است تعدادی درخواست (محدود به چندجمله‌ای) به C ارائه کند و C پاسخ‌های مناسب را همانند بازی قبل به او بازمی‌گرداند. درخواست‌های قابل انجام از طرف متخاصم در این بازی عبارتند از: ایجاد وسیله نقلیه، مقدار مخفی وسیله نقلیه، کلید عمومی وسیله نقلیه و امضا.

۲. A_2 امضا تجمعی فاقد گواهینامه σ^* امضاشده توسط n وسیله نقلیه با شناسه‌های مستعار $L^*_{PID}=\{PID^*_1, PID^*_2, \cdots, PID^*_n\}$ و کلیدهای عمومی $L^*_{vpk}=\{vpk^*_1, vpk^*_2, \cdots, vpk^*_n\}$ بر روی پیام‌های $L^*_m=\{m^*_1, m^*_2, \cdots, m^*_n\}$ را خروجی می‌دهد. A_2 برنده این بازی است اگر:

- شرط اول: σ^* یک امضا تجمعی معتبر بر روی پیام‌های $L^*_m=\{m^*_1, m^*_2, \cdots, m^*_n\}$ از طرف وسایل نقلیه با شناسه‌های $L^*_{PID}=\{PID^*_1, PID^*_2, \cdots, PID^*_n\}$ و کلیدهای عمومی $L^*_{vpk}=\{vpk^*_1, vpk^*_2, \cdots, vpk^*_n\}$ باشد.
- شرط دوم: به‌ازای حداقل یکی از شناسه‌های مستعار (که بدون از دست رفتن کلیت مسئله فرض می‌شود این شناسه مستعار $PID^*_1 \in L^*_{PID}$ باشد)، «درخواست مقدار مخفی وسیله نقلیه» با ورودی PID^*_1 و درخواست امضا با ورودی (PID^*_1, m^*_1) صورت نگرفته باشد.

تعریف ۱. یک طرح امضا تجمعی فاقد گواهینامه را امن گویند هرگاه هیچ متخاصم احتمالاتی محدود به زمان چندجمله‌ای A_1 یا A_2 ای وجود نداشته باشد که بتواند با احتمالی غیرقابل‌چشم‌پوشی به ترتیب در بازی I یا II پیروز شود.

نکته: توجه شود که در بازی I مدل امنیتی در نظر گرفته شده در بالا (که آن را مدل امنیت عقلانی می‌نامیم) A_1 تنها قادر به درخواست امضا از طرف کاربرانی است که کلید عمومی آن‌ها تعویض نشده باشد. علاوه‌بر این مدل، مدل امنیتی قوی‌تری نیز

برای طرح‌های امضا فاقد گواهینامه تعریف شده که تفاوت آن با مدل ارائه‌شده در بالا در این است که در مدل جدید A_1 حتی قادر به درخواست امضا از طرف کاربرانی که کلید عمومی آن‌ها تغییر یافته نیز می‌باشد. در این مقاله مدل امنیت دوم را مدل امنیت قوی می‌نامیم. به راحتی قابل بررسی است که در صورتی که یک طرح در مدل امنیت قوی امن باشد در مدل عقلانی نیز امن خواهد بود.

۴. تحلیل امنیت طرح ژانگ و همکاران

در این بخش، نشان داده خواهد شد که علی‌رغم ادعای مطرح‌شده مبنی بر جعل‌ناپذیر وجودی بودن طرح ارائه‌شده در [۱] در برابر حمله متن و شناسه منتخب وفقی در مدل امنیت قوی، این طرح حتی در مدل عقلانی نیز ناامن است. به عبارت دیگر، در این بخش نشان می‌دهیم که با توجه به مدل عقلانی ارائه‌شده در بخش ۳، هر دو نوع متخاصم در نظر گرفته‌شده در سامانه‌های رمزنگاری فاقد گواهینامه به‌راحتی قادر هستند تا تنها با مشاهده یک زوج (پیام و امضا) مربوط به یک وسیله نقلیه، امضا آن وسیله نقلیه را بر روی هر پیام دلخواه دیگری در طرح ژانگ و همکاران جعل کنند. جزئیات انجام کار و جعل امضا در طرح ژانگ و همکاران در قضیه زیر و به صورت دقیق بیان شده است. جزئیات طرح ارائه‌شده در [۱] توسط ژانگ و همکاران در اینجا بررسی نشده و خوانندگان علاقمند به [۱] ارجاع داده می‌شوند.

قضیه ۱: با توجه به تعریف ۱، طرح امضا تجمعی فاقد گواهینامه ارائه‌شده توسط ژانگ و همکاران جعل‌پذیر است؛ به‌عبارت‌دیگر، در این طرح، هر دو نوع متخاصم در نظر گرفته‌شده در سامانه‌های رمزنگاری فاقد گواهینامه می‌توانند با احتمال ۱ در بازی‌های متناظر با آن‌ها یک امضا تجمعی جعل‌شده ایجاد کنند.

اثبات: برای سادگی و بدون کاستن از کلیت فرض کنید n برابر با یک باشد. فرض کنید V_1 وسیله نقلیه‌ای با شناسه مجازی PID_1 و کلید عمومی vpk_1 در طرح ژانگ و همکاران باشد. برای ایجاد یک امضا جعل‌شده معتبر σ' بر روی پیام m' از طرف V_1، متخاصم A (که می‌تواند A_1 در طول بازی I یا A_2 در طول بازی II باشد) در مقابل چالشگر C در بازی مربوطه به صورت زیر عمل می‌کند.

۱) به C اجازه می‌دهد تا الگوریتم راه‌اندازی سامانه را اجرا کند.

۲) درخواست امضا از طرف وسیله نقلیه V_1 با شناسه مستعار PID_1 و کلید عمومی vpk_1 بر روی پیام m را صادر کرده و در پاسخ $\sigma_1 = (R_1, T_1)$ را دریافت می‌کند که $R_1 = r_1 P$ و $T_1 = r_1 H_j + h_1 S_1$.

۳) برای جعل امضا V_1 روی پیام دلخواه m':

a. مقدار

$$h_1 = H_2(m||t_1, PID_1, vpk_1, ID_j) \quad (۸)$$

را محاسبه می‌کند.

b. وارون ضربی h_1 در پیمانه q (که با h_1^{-1} نمایش داده می‌شود) را محاسبه می‌کند.

c. برچسب زمانی معتبر جدید t'_1 را در نظر گرفته و مقدار

$$h'_1 = H_2(m'||t'_1, PID_1, vpk_1, ID_j) \quad (۹)$$

را محاسبه می‌کند.

d. مقادیر

$$R'_1 = h'_1 h_1^{-1} R_1 \quad (۱۰)$$

و

$$T'_1 = h'_1 h_1^{-1} T_1 \quad (۱۱)$$

را محاسبه می‌کند.

e. $\sigma'_1 = (R'_1, T'_1)$ را به عنوان امضا V_1 روی پیام m' خروجی می‌دهد.

f. مقدار T' را برابر با T'_1 و R' را برابر با R'_1 قرار می‌دهد.

در ادامه نشان داده خواهد شد که $\sigma'_1 = (R'_1, T'_1)$ یک امضا معتبر از طرف وسیله نقلیه V_1 با شناسه مستعار PID_1 و کلید عمومی vpk_1 روی پیام m' است. برای این منظور کافی است برقراری رابطه زیر بررسی شود:

$$e(P, T') = e\left(P_{pub}, \sum_{i=1}^{n} h_i Q_i\right) e(H_j, R' + \sum_{i=1}^{n} h_i vpk_i) . \quad (۱۲)$$

داریم:

$$\begin{aligned}
e(P, T') &= e(P, T'_1) \\
&= e(P, h'_1 h_1^{-1} T_1) \\
&= e\big(P, h'_1 h_1^{-1}(r_1 H_j + h_1(psk_1 + vsk_1 H_j))\big) \\
&= e\big(P, h'_1 h_1^{-1}((r_1 + h_1 vsk_1) H_j + h_1 psk_1)\big) \\
&\quad e\big(P, h'_1 h_1^{-1}(r_1 + h_1 vsk_1) H_j) e(P, h'_1 h_1^{-1} h_1 psk_1)\big) \\
&\quad e\big(P, (h'_1 h_1^{-1} r_1 + h'_1 vsk_1) H_j) e(P, h'_1 psk_1\big) \\
&= e\big(R'_1 + h'_1 vpk_1, H_j\big) e\big(P_{pub}, h'_1 Q_1\big) \\
&= e\big(H_j, R'_1 + h'_1 vpk_1\big) e(P_{pub}, h'_1 Q_1) \\
&= e(P_{pub}, h'_1 Q_1) e(H_j, R'_1 + h'_1 vpk_1)
\end{aligned}$$

$$= e\left(P_{pub}, \sum_{i=1}^{n} h_i Q_i\right) e\left(H_j, R' + \sum_{i=1}^{n} h_i vpk_i\right).$$

درنتیجه رابطه موردنظر برقرار بوده و امضا جعل‌شده موردپذیرش واقع خواهد شد.

لازم به ذکر است که در اثبات فوق تنها یک امضاکننده در نظر گرفته شده است؛ اما گسترش آن به حالت‌هایی با بیش از یک امضاکننده به راحتی قابل انجام است. در این راستا، ابتدا یک امضا تکی جعل‌شده ایجاد کرده و به راحتی و با جمع کردن آن را در امضا تجمعی جایگذاری کرده و امضا تجمعی جعل‌شده با تعداد کاربر بیشتر ایجاد می‌شود. ■

توجه به این نکته مهم است که در حمله ارائه‌شده تنها نیاز به انجام یک درخواست امضا، ۲ محاسبه مقدار تابع چکیده‌ساز، یک محاسبه مقدار وارون، ۲ محاسبه ضرب پیمانه‌ای و ۲ محاسبه ضرب اسکالر وجود دارد. بنابراین حمله ارائه‌شده کارا بوده و پیچیدگی محاسباتی آن O(1) است.

۵. بهبود طرح ژانگ و همکاران

در بخش قبل نشان داده شد که با توجه به حتی مدل امنیت عقلانی، امضای تجمعی ژانگ و همکاران [۱] توسط هر دو نوع متخاصم در نظر گرفته شده در رمزنگاری فاقد گواهینامه، جعل‌پذیر است.

همان‌طور که مشاهده شد حمله ارائه‌شده در بخش قبل بدین دلیل بر طرح ژانگ و همکاران موثر است که حمله‌کننده به راحتی می‌تواند با ضرب امضا در وارون $h_i = H_2(m_i||t_i, PID_i, vpk_i, ID_j)$ اثر پیام را از امضا حذف و مقداری را به دست آورد که به پیام وابسته نباشد. در این بخش، با استفاده از یک تابع چکیده‌ساز جدید ($H_4(.)$)، طرح ژانگ و همکاران به‌گونه‌ای تغییر داده خواهد شد که چنین چیزی ناممکن شود. در طرح پیشنهادی و در راستای افزایش مشاهده‌پذیری، مراحل تغییریافته نسبت به مراحل متناظر در الگوریتم‌های مشابه در طرح ژانگ و همکاران برجسته شده‌اند.

الگوریتم راه‌اندازی سامانه:

- ورودی: پارامتر امنیت 1^{λ}.
- پردازش: در این الگوریتم:
  - TA:
    - گروه جمعی G_1 و گروه ضربی G_2، هر دو از مرتبه عدد اول q را تولید می‌کند.
    - مولد P در گروه G_1 و نگاشت دوخطی $e: G_1 \times G_1 \to G_2$ را انتخاب می‌کند.
    - توابع چکیده‌ساز $H_0: \{0,1\}^* \to G_1$، $H_1: \{0,1\}^* \to G_1$، $H_2: \{0,1\}^* \to Z_q^*$، $H_3: \{0,1\}^* \to G_1$ و $H_4: \{0,1\}^* \to$ G_1 را انتخاب می‌کند.
  - KGC:
    - عدد تصادفی $s \in Z_q^*$ را به عنوان کلید مخفی اصلی انتخاب کرده و مقدار $P_{pub} = sP$ را محاسبه می‌کند.
  - TRA:
    - عدد تصادفی $\alpha \in Z_q^*$ را انتخاب کرده و مقدار $T_{pub} = \alpha P$ را محاسبه می‌کند. از α برای تولید شناسه مستعار استفاده خواهد شد و TRA تنها موجودیتی است که به این مقدار دسترسی خواهد داشت.

خروجی: مقدار s که به عنوان کلید مخفی اصلی توسط KGC محرمانه نگهداری شده، مقدار α که محرمانه توسط TRA نگهداری شده و پارامترهای عمومی سامانه $params = \left(q, G_1, G_2, e, P, P_{pub}, T_{pub}, H_0, H_1, H_2, H_3, H_4\right)$ که اعلام عمومی می‌شوند.

الگوریتم تولید نام مستعار:

- ورودی: شناسه واقعی یک وسیله نقلیه (RID_i) که به صورت یکتا وسیله نقلیه موردنظر را مشخص می‌کند.
- پردازش: در این الگوریتم:
  - وسیله نقلیه V_i:
    - مقدار تصادفی $k_i \in Z_q^*$ را انتخاب کرده، $PID_{i,1} = k_i P$ را محاسبه کرده و $(RID_i, PID_{i,1})$ را از طریق یک کانال امن به TRA ارسال می‌کند.
  - TRA:
    - پس از دریافت $(RID_i, PID_{i,1})$، ابتدا وجود RID_i را در پایگاه داده محلی خود بررسی کرده، $PID_{i,2} = RID_i \oplus H_0(\alpha PID_{i,1}, VP_i)$ که VP_i دوره اعتبار PID_i است را محاسبه کرده و PID_i را برابر با $(PID_{i,1}, PID_{i,2}, VP_i)$ قرار می‌دهد.
- خروجی: PID_i که از طریق یک کانال امن به KGC ارسال می‌شود.

الگوریتم تولید کلید خصوصی جزئی:

- ورودی: params، MSK و شناسه مستعار یک وسیله نقلیه PID_i.
- پردازش: در این الگوریتم KGC مقدار $Q_i = H_3(PID_i)$ را محاسبه کرده و سپس با استفاده از آن، $psk_i = sQ_i$ را به عنوان کلید خصوصی جزئی محاسبه می‌کند.
- خروجی: (PID_i, psk_i) که از طریق کانال امن به وسیله نقلیه موردنظر ارسال می‌شود.

الگوریتم تولید کلید وسیله نقلیه:

- ورودی: params و شناسه مستعار PID_i متناظر با وسیله نقلیه.
- پردازش: در این الگوریتم:
  - وسیله نقلیه موردنظر:
    - مقدار مخفی $x_i \in Z_q^*$ را به عنوان کلید مخفی vsk_i انتخاب کرده و کلید عمومی متناظر با این مقدار $vpk_i = x_i P$ را محاسبه می‌کند.
- خروجی: vsk_i که محرمانه توسط وسیله نقلیه نگهداری شده و vpk_i که اعلام عمومی می‌شود.

الگوریتم امضا:

- ورودی: params، شناسه PID_i، کلید عمومی vpk_i، کلید امضا (psk_i, vsk_i)، شناسه ID_j و پیام $m_i \in \{0,1\}^*$.
- پردازش: پردازش‌های این الگوریتم در این روش از دو مرحله تشکیل شده است: مرحله اول تنها یک بار و در زمانی انجام می‌شود که وسیله نقلیه V_i وارد محدوده تحت پوشش یک RSU جدید شود و مرحله دوم هرگاه وسیله نقلیه نیاز به امضا پیام داشت انجام می‌شود:
  - مرحله اول: V_i:
    - مقادیر

$$H_j = H_1(ID_j) \quad (۱۳)$$

را محاسبه و ذخیره می‌کند.

  - مرحله دوم: V_i:
    - مقدار تصادفی $r_i \in Z_q^*$ را انتخاب کرده و

$$R_i = r_i P \quad (۱۴)$$

را محاسبه می‌کند.

- مقدار

$$h_i = H_2(m_i||t_i, PID_i, vpk_i, ID_j) \quad (۱۵)$$

را محاسبه می‌کند، که t_i برچسب زمانی است.

- مقدار

$$T_i = r_i H_j + h_i(psk_i + vsk_i H_4(m_i)) \quad (۱۶)$$

را محاسبه کرده و σ_i را برابر با (R_i, T_i) قرار می‌دهد.

- خروجی: مقادیر $\{PID_i, m_i, vpk_i, t_i, \sigma_i\}$ که به RSU ارسال می‌شود.

الگوریتم تائید اصالت:

- ورودی: params، شناسه مستعار PID_i، کلید عمومی vpk_i، شناسه ID_j، پیام m_i، برچسب زمانی t_i و امضا σ_i.
- پردازش: در این الگوریتم:
  - RSU:
    - در ابتدا تازگی امضا را با بررسی رابطه $\Delta t_i \geq t_{RSU} - t_i$ که t_{RSU} زمان دریافت پیام توسط RSU و Δt حداکثر زمان تأخیر انتقال اجازه داده شده است، بررسی می‌کند.
    - مقادیر $H_j = H_1(ID_j)$، $Q_i = H_3(PID_i)$ و $h_i = H_2(m_i||t_i, PID_i, vpk_i, ID_j)$ را محاسبه می‌کند.
    - برقراری رابطه

$$e(P, T_i) = \frac{e(P_{pub}, h_i Q_i) e(H_j, R_i)}{e(h_i H_4(m_i), vpk_I)} \quad (۱۷)$$

را بررسی می‌کند.

- خروجی: 1 (پذیرش) درصورتی‌که رابطه فوق برقرار باشد و 0 (عدم پذیرش) در غیر این صورت.

الگوریتم تجمیع امضا:

- ورودی: params و زوج پیام-امضاهای $(m_1||t_1, \sigma_1 = (R_1, T_1))$، $(m_2||t_2, \sigma_2 = (R_2, T_2))$، ...، $(m_n||t_n, \sigma_n = (R_n, T_n))$ تولیدشده توسط وسایل نقلیه V_1، V_2، ...، V_n با شناسه‌های مستعار PID_1، PID_2، ...، PID_n با کلیدهای عمومی vpk_1، vpk_2، ...، vpk_n.
- پردازش: در این الگوریتم:
  - RSU:
    - مقادیر $R = \sum_{i=1}^{n} R_i$ و $T = \sum_{i=1}^{n} T_i$ را محاسبه می‌کند.
- خروجی: امضا تجمعی $\sigma = (R, T)$ که توسط خود RSU در الگوریتم تائید اصالت تجمیعی مورد استفاده قرار خواهد گرفت.

الگوریتم تائید اصالت تجمیعی:

- ورودی: params، شناسه ID_j، مجموعه پیام‌ها-برچسب‌های زمانی $(m_1||t_1)$، $(m_2||t_2)$، ...، $(m_n||t_n)$ تولیدشده توسط وسایل نقلیه V_1، V_2، ...، V_n با شناسه‌های مستعار PID_1، PID_2، ...، PID_n و کلیدهای عمومی vpk_1، vpk_2، ...، vpk_n و امضا تجمعی فاقد گواهینامه $\sigma = (R, T)$.
- پردازش: در این الگوریتم:
  - RSU:
    - مقدار $H_j = H_1(ID_j)$ را محاسبه می‌کند.
    - برای $i = 1, 2, \ldots, n$:
      - در ابتدا تازگی امضا را با بررسی رابطه $\Delta t_i \geq t_{RSU} - t_i$ بررسی می‌کند.
      - مقادیر $Q_i = H_3(PID_i)$ و $h_i = H_2(m_i||t_i, PID_i, vpk_i, ID_j)$ را محاسبه می‌کند.
      - برقراری رابطه

$$e(P,T) = \frac{e\left(P_{pub}, \sum_{i=1}^{n} h_i Q_i\right)}{e(H_j, R)\prod_{i=1}^{n} e(H_4(m_i)h_i vpk_i)} \quad (۱۸)$$

را بررسی می‌کند.

خروجی: 1 (پذیرش) درصورتی‌که رابطه فوق برقرار باشد و 0 (عدم پذیرش) در غیر این صورت.

۶. تحلیل امنیت در بهبود پیشنهادی

در این بخش نشان داده می‌شود بهبود ارائه‌شده ملزومات امنیتی موردنیاز در شبکه‌های VANET را تامین می‌کند. اهم این ملزومات عبارتند از احراز اصالت پیام، گمنامی، پیوندناپذیری، ردیابی مشروط و مقاومت در برابر حمله تکرار.

به سادگی دیده می‌شود که تغییرات پیشنهادی در بهبود ارائه‌شده تنها روی احراز اصالت پیام تاثیر می‌گذارند و اثبات‌های ارائه‌شده در مقاله ژانگ و همکاران در مورد گمنامی، پیوندناپذیری، ردیابی مشروط و مقاومت در برابر حمله تکرار، کماکان در مورد بهبود پیشنهادی برقرار خواهد بود. بنابراین، در اینجا صرفا به بررسی احراز اصالت پرداخته و خوانندگان علاقه‌مند را به [۱] برای کسب اطلاع در مورد نحوه تأمین سایر ملزومات امنیتی ارجاع می‌دهیم.

احراز اصالت پیام: احراز اصالت پیام از مهم‌ترین ملزومات امنیتی در شبکه‌های VANET بوده و به بررسی‌کننده پیام این اطمینان را می‌دهد که پیام از سوی کاربر مجاز ارسال شده و یکپارچگی آن نیز محفوظ مانده است.

همان‌طور که در بخش ۵ نشان داده شد دلیل مؤثر واقع‌شدن حمله ارائه‌شده بر طرح ژانگ و همکاران این بود که حمله‌کننده به راحتی قادر بود با دسترسی به پیام m_1 و امضا کاربر با شناسه موقت PID_I روی آن یعنی σ_1 با ضرب دو عنصر امضا در وارون $h_1 = H_2(m_1||t_1, PID_1, vpk_1, ID_j)$ (از طریق روابط (۱۰) و (۱۱)) اثر پیام m_1 را از امضا حذف و مقداری را به دست آورد که به پیام وابسته نباشد. در طرح بهبودیافته از یک تابع چکیده‌ساز جدید ($H_4(.)$) به‌گونه‌ای استفاده شده که چنین چیزی ناممکن شود. در طرح پیشنهادی، در صورت استفاده از حمله ارائه‌شده، حمله‌کننده به مقادیر $R'_1 = h'_1 h_1^{-1} R$ و $T'_1 = h'_1 h_1^{-1} T_1$ خواهد رسید که $R'_1 = h'_1 h_1^{-1} r_1 P$ و

$$T'_1 = h'_1 h_1^{-1} r_1 H_j + h'_1(psk_i + vsk_i H_4(m_i)) \quad (۱۹)$$

که

$$h'_1 = H_2(m'_1||t_I, PID_I, vpk_I, ID_j) \quad (۲۰)$$

با توجه به عدم یکسانی پیام‌های m_1 و m'_1 امضا فوق در رابطه تائید اصالت صادق نخواهد بود و درنتیجه روش ارائه‌شده نیازمندی احراز اصالت را، با توجه به مدل عقلانی در نظر گرفته شده، تأمین خواهد کرد.

۷. نتیجه‌گیری

در این مقاله به بررسی امنیت یک سامانه حمل‌ونقل هوشمند که اخیراً در مرجع [۱] و با استفاده از طرح امضا تجمعی فاقد گواهینامه ارائه‌شده پرداخته شده است. نتایج مقاله حاضر نشان می‌دهد سامانه هوشمند مدیریت ترافیک ارائه‌شده توسط نویسندگان ناامن بوده و برخلاف ادعاهای مطرح‌شده در قضایا (و اثبات‌های طولانی آن‌ها) امکان بررسی اصالت پیام‌های تولیدشده توسط خودروها در شبکه را فراهم نمی‌کند. به‌طور خاص در این مقاله اثبات شده که تنها با دسترسی به یک زوج (پیام و امضا) که توسط یک وسیله نقلیه با استفاده از طرح ارائه‌شده در [۱] تولید شده است، هر متخاصمی قادر است به سادگی امضا این وسیله نقلیه را روی هر پیام دیگری جعل کند. پس از اثبات ناامنی طرح ارائه‌شده در [۱]، نسخه‌ای بهبودیافته از این طرح ارائه‌شده که بر مشکل مطرح‌شده غلبه کند.

۸. مراجع

[1] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," Information Sciences, vol. 476, pp. 211–221, 2019.

[2] S. M. Pournaghi, M. Barmshoori, and M. Gardeshi, "An Improved Authentication Scheme with Conditional Privacy Preserving in VANETs," Journal of Electronic & Cyber Defence, vol. 3, pp. 1-12, 2015 (In Persian).

[3] M. Raya, and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15 pp. 39–68, 2007.

[4] R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, "Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications," IEEE INFOCOM 2008-The 27th Conference on Computer Communications, USA, 2008, pp. 1229-1237.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," Workshop on the theory and application of cryptographic techniques, Paris, France, 1984, pp. 47-53.

[6] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," IEEE INFOCOM 2008-The 27th Conference on Computer Communications, USA, 2008, pp. 246-250.

[7] S.S. Al-Riyami, and K.G. Paterson, "Certificateless public key cryptography," International conference on the theory and application of cryptology and information security, Taipei, Taiwan, 2003, pp. 452-473.

[8] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003, pp. 416-432.

[9] X. Cheng, J. Liu, and X. Wang, "Identity-based aggregate and verifiably encrypted signatures from bilinear pairing," International Conference on Computational Science and Its Applications, Singapore, 2005, pp. 1046-1054.

[10] C. Gentry, and Z. Ramzan, "Identity-based aggregate signature," International workshop on public key cryptography, New York, USA, 2006, pp. 257-273.

[11] S. Lu, R. Ostrovsky, and A. Sahai, "Sequential aggregate signatures and multi signatures without random oracles," Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, 2006, pp. 465-485.

[12] M. Ruckert, and D. Schrode, "Aggregate and verifiably encrypted signatures from multilinear maps without random oracles," International Conference on Information Security and Assurance, Seoul, Korea (Republic of), 2009, pp. 750-759.

[13] Z. Shao, "Enhanced aggregate signature from pairings," International Conference on Information Security and Cryptology, Seoul, Korea (Republic of), 2005, pp. 140-149.

[14] K. Shim, "An Id-based aggregate signature scheme with constant pairing computations," Journal of Systems and Software, vol. 83 pp. 1873-1880, 2010.

[15] B.Y. Kang, "ID-based aggregate signature scheme with constant pairing computations: attack and new construction," Journal of Computer Information System, vol. 16 pp. 6611- 6618, 2012.

[16] Z. Gong, Y. Long, and X. Hong, "Two certificateless aggregate signatures from bilinear maps," Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel Distributed Computing, Qingdao, China, 2007, pp. 188-193.

[17] N. Yanai, R. Tso, and M. Mambo, "Certificateless ordered sequential aggregate signature scheme," Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, 2011, pp. 662-667.

[18] L. Zhang, and F. Zhang, "A new certificateless aggregate signature scheme," Computer Communications, vol. 32 pp. 1079-1085, 2009.

[19] L. Cheng, Q. Wen, and Z. Jin, "Cryptanalysis and improvement of a certificateless aggregate signature scheme," Information Sciences, vol. 295 pp. 337-346, 2015.

[20] S. Horng, S. Tzeng, and P. Huang, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," Information Sciences, vol. 317 pp. 48-66, 2015.

[21] H. Du, M. Huang, and Q. Wen, "Efficient and provably-secure certificateless aggregate signature scheme," Acta Electronica Sinica, vol. 41 pp. 72-76, 2013.

[22] H. Chen, S. Wei, and C. Zhu, "Secure certificateless aggregate signature scheme," Journal of Software, vol. 26 pp. 1173-1180, 2015.

[23] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," Information Sciences, vol. 219 pp. 225–235, 2013.

[24] D. He, M. Tian, and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations," Information Sciences, vol. 268 pp. 458–462, 2014.

[25] H. Nie, Y. Li, W. Chen, and Y. Ding, "NCLAS: a novel and efficient certificateless aggregate signature scheme," Security and Communication Networks, vol. 9 pp. 3141-3151, 2016

[26] N. Pakniat, and M. Noroozi, "Cryptanalysis of a certificateless aggregate signature scheme," 9th Conference of Command, Control, Communications and Computer Intelligence, Tehran, Iran, 2016, pp. 1-5.

[27] Y. C. Chen, R. Tso, W. Susilo, X. Huang, and G. Horng, "Certificateless Signatures: Structural Extensions of Security Models and New Provably Secure Schemes," IACR Cryptology ePrint Archive, 2013, 193.

[28] K. Hashimoto, and W. Ogata, "Unrestricted and Compact Certificateless Aggregate Signature Scheme," Information Sciences, vol. 487 pp. 97-114, 2019.

Journal of Electronical & Cyber Defence
Vol. 8, No. 1, 2020, Serial No. 29

Security Analysis and Improvement of an Intelligent Transportation System based on Certificateless Aggregate Signature

N. Pakniat, Z. Eslami*

*Department of Data and Computer Science, Faculty of Mathematical Science, Shahid Beheshti University, Tehran, Iran.

(Received: 17/03/2019, Accepted: 18/06/2019)

ABSTRACT

A key component of intelligent transportation systems is the so-called Vehicular Ad-hoc Network (VANET). These networks refer to a set of smart vehicles which provide communication services on the road using wireless technologies. In addition to enhancing road safety, VANETs can contribute to vehicle and driver's security. Therefore, the research in this area is heavily centered around important security and privacy issues, in particular authentication of the messages exchanged while reducing communication overhead. In order to provide a solution to this problem, Zhong et al. recently proposed an efficient privacy-preserving authentication scheme for VANETs based on certificateless aggregate signatures. In their scheme, the length of the aggregated signature is fixed and does not depend on the number of input signatures. The goal of our paper is to show that the scheme of Zhong et al. fails to provide the required authentication for VANETs. We prove that it is easily possible to forge the signature of a vehicle on an arbitrary message after observing only one pair of (message, signature) signed by the target vehicle. We further propose an improvement over Zhong et al.'s scheme that overcomes the mentioned drawback and therefore provides the required authenticity in VANETs.

Keywords: VANET, Privacy-preserving, Aggregate signature, Certificateless Cryptography, Forgeability

* Corresponding Author Email: z_eslami@sbu.ac.ir