به نام خدا

A Countermeasure for Garg et al. Scheme: An Authentication Method for V2G Networks

علیرضا اکرمی[۱]، سعید جعفری[۲]

۱- دانشجوی دانشکده برق و کامپیوتر دانشگاه تهران شماره دانشجویی: ۸۱۰۱۹۹۳۲۱
۲- دانشجوی دانشکده برق و کامپیوتر دانشگاه تهران شماره دانشجویی: ۸۱۰۱۹۹۱۳۰

چکیده

یکی از چالش‌های اساسی برای هر سیستمی بحث تامین امنیت آن سیستم است. با گسترش و پیشرفت تکنولوژی و داغ شدن بحث اینترنت اشیاء موضوع امنیت آن تبدیل به یک مسئله‌ی چالش برانگیز شده و طرح‌ها و پروتکل‌های بسیاری برای تامین امنیت در شبکه‌های مختلف مرتبط به اینترنت اشیاء ارائه شده است. یکی از این پروتکل‌ها، پروتکل Garg و همکارانش برای احراز هویت در شبکه‌ی V2G است که با بررسی‌هایی که در این پژوهش انجام شده است؛ ابتدا تحلیلی از این پروتکل ارائه شده و نقص‌های آن بیان شده و سپس یک پروتکل احراز هویت سریع و کارا برای رفع نقص‌های موجود در پروتکل Garg ارائه شده است. همچنین برای بررسی عملکرد پروتکل پیشنهادی، پروتکل جدید از لحاظ تامین ویژگی‌های امنیتی و سربار پردازشی و ارتباطی با پروتکل Garg مقایسه شده است.

واژگان کلیدی:

اینترنت اشیاء، ارتباط خودرو با شبکه(V2G)، امنیت شبکه، پروتکل احراز هویت

۱-مقدمه و پیشینه تحقیق

با گسترش و پیشرفت تکنولوژی ایده‌ی اینترنت اشیا به سرعت مورد توجه‌ی جامعه‌ی علمی و صنعتی قرار گرفت. به صورت کلی هدف از این ایده، ایجاد ارتباط بین تمامی اشیاء با یک دیگر بر بستر اینترنت بود. اما پیاده‌سازی این ایده به علت متفاوت بودن شبکه‌ها و اشیاء موجود در اینترنت و تعداد بسیار زیاد این اشیاء همواره با چالش‌های بسیاری همراه بوده و خواهد بود. برای مثال می‌توان دو شبکه‌ی Smart Grid و V2G را نام برد که در اینگونه شبکه‌ها هدف ایجاد یک ارتباط دو طرفه برای رساندن انرژی به دست مصرف کننده و محاسبه‌ی Real Time هزینه‌ی آن و ارسال قبض یا فاکنور برای مشتری است. همانطور که گفته شد در شبکه‌ی اینترنت اشیاء ما با چالش‌های بسیاری سر و کار داریم که یکی از مهم ترین آن‌ها، بحث تامین امنیت به وسیله‌ی احراز هویت و تبادل کلید بین مولفه‌های مختلف شبکه است. در ادامه به بررسی برخی پروتکل‌های پیشنهادی در زمینه‌ی Smart Grid و V2G می پردازیم.

در زمینه‌ی پروتکل‌های احراز هویت و تبادل کلید در Smart Grid فعالیت بسیاری انجام شده است که در این قسمت ما ۵ مقاله از سال ۲۰۱۸ تا ۲۰۲۰ را در این زمینه بررسی می‌کنیم. در [۱] یک طرح احراز هویت و تبادل کلید بر اساس رمزنگاری خم بیضوی ارائه شده است که ایده‌ی بسیار جالبی را به کار برده است و آن انتقال بار پردازشی از سمت Smart Meter(SM) ها که قدرت پردازشی کمتری دارند به سمت سرورهای با قدرت بیشتر است و به این ترتیب علاوه بر ایجاد امنیت، سربار پردازشی کمی نیز دارد. همچنین تعداد پیام‌های ارسالی و دریافتی این پروتکل بین SM و سرور برای اجرای فرآیند احراز هویت و تبادل کلید برابر با ۳ است که این نشان‌دهنده‌ی سربار ارتباطی کم آن است. این پروتکل در مقابل حملاتی مثل حمله‌ی بازپخش، مرد میانی، جعل هویت و نا همزمان کردن کلید مقاوم است اما در مقابل حمله‌ی منع سرویس آسیب پذیر بوده، نیازمندی ناشناسی را برآورده نمی‌کند و مشکل کلید سپاری نیز دارد. همچنین از امنیت رو جلو[۱] نیز برخوردار نیست و با لو رفتن کلید یک جلسه می‌توان به کلید سایر جلسات دسترسی داشت.

در تمامی پروتکلها ارتباط احراز هویت و تبادل کلید انتها به انتها بین Smart Meter و سرورهای سازمان تامین کننده‌ی انرژی در نظر گرفته نمی‌شود و یک سری گره میانی تحت عنوان دروازه[۲] نیز وجود دارند که اطلاعات خانه‌های یک منطقه را تجمیع و به سرورهای سازمان ارسال می‌کنند. در چنین شرایطی معمولا ارتباط بین دروازه و سرورها امن فرض می‌شود و پروتکل احراز هویت و تبادل کلید بین خانه‌ها و دروازه‌ی مربوط به آن منطقه تعریف می‌شود. نمونه‌ای از چنین پروتکلی در [۲] بیان شده است. در این طرح که از رمزنگاری خم بیضوی استفاده می‌شود، در مقابل حملات بازپخش، مرد میانی، جعل هویت و منع سرویس مقاوم است. دو حمله‌ی جدید نیز به نام حمله‌ی جعل کلید Smart Meter تصاحب شده و کلید جلسه‌ی آشکار نیز در این طرح مطرح می‌شود که پروتکل پیشنهادی توانایی جلوگیری از این دو نوع حمله را نیز دارد. در حالت اول زمانی که کلید یک Smart Meter لو می‌رود، این نشت اطلاعات نباید منجر به پیدا کردن کلید سایر SM ها شود. در حالت دوم نیز اگر کلید یک جلسه‌ی قدیمی لو برود نباید کلید جلسه‌ی فعلی با تهدیدی رو به رو شود. همچنین این پروتکل ویژگی امنیت رو به جلو و ناشناسی را نیز برآورده می‌سازد اما همچنان مشکل کلید سپاری را نیز دارد. از لحاظ سربار ارتباطی این پروتکل دارای دو تبادل پیام برای اجرای فرآیند احراز هویت و تبادل کلید می‌باشد.

پروتکل ارائه شده در [۳] مشابه پروتکل قبل می‌باشد و برای تبادل کلید بین خانه‌ها و دروازه طراحی شده است و از رمزنگاری خم بیضوی بهره می‌برد. این پروتکل در برابر حملات بازپخش، جعل هویت، کلید جلسه‌ی آشکار و منع سرویس مقاوم است و امنیت رو به جلو و ناشناسی را نیز پشتیبانی می‌کند. ولی همچنان مشکل کلید سپاری در این پروتکل نیز وجود دارد. این پروتکل از سه پیام برای تبادل کلید استفاده می‌کند ولی سربار پردازشی و ارتباطی آن کمتر از پروتکل قبل است.

مشکل کلید سپاری موضوعی بود که در سه پروتکل قبلی حل نشده باقی مانده بود. برای حل این مشکل در [۴] با استفاده از خم بیضوی و نگاشت دو خطی یک پروتکل تبادل کلید و احراز هویت انتها به انتها بین SM و سرورهای سازمان تامین کننده‌ی انرژی ارائه شد که در برابر حملات جعل هویت، مرد میانی، کلید جلسه‌ی آشکار مقاوم است و همچنین امنیت رو جلو و ناشناسی را نیز تامین می‌کند و همانطور که گفته شد مشکل کلید سپاری ندارد. با اینکه این مشکل در این پروتکل رفع شده اما به خاطر استفاده از نگاشت دو خطی، سربار پردازشی زیادی را به عناصر درگیر در فرآیند احراز هویت و تبادل کلید تحمیل می‌کند. همچنین فرآیند تبادل کلید و احراز هویت به وسیله‌ی تبادل دو پیام انجام می‌شود.

پروتکل‌هایی تا کنون بحث شد همگی بر اساس رمز نامتقارن فرآیند تبادل کلید و احراز هویت خود را انجام می‌دادند اما در [۵] با استفاده از AES 128 بیتی، XOR و تابع چکیده ساز یک طرفه این فرآیند انجام می‌شود که به دلیل استفاده از رمز

---

[۱] Forward Secrecy

[۲] Gateway

متقارن، کارایی و سرعت اجرای این پروتکل بسیار بیشتر از طرح‌های قبلی است. اما استفاده از رمزمتقارن نیاز به حافظه برای نگهداری دارد و برای جلوگیری از حمله‌ی نا همگام سازی کلید نیاز به دو برابر حافظه برای نگهداری کلیدها دارد. این پروتکل در مقابل حملات مرد میانی، جعل هویت، کلید جلسه‌ی آشکار، نا همگام سازی کلید مقاوم است و همچنین ویژگی‌های امنیت رو به جلو، ناشناسی و غیر قابل ردیابی بودن پیام‌ها را دارا است. این پروتکل از ۴ پیام برای انجام فرآیند تبادل کلید و احراز هویت استفاده می‌کند.

در زمینه‌ی تبادل کلید و حفظ حریم خصوصی در V2G مقالات و طرح‌های بسیاری ارائه شده است که در این قسمت به بررسی ۳ مورد از آن‌ها می‌پردازیم. در [۶] یک تبادل کلید و احراز هویت سبک دو عاملی[۱] شامل رمزعبور[۲] و اثر انگشت کاربر برای شبکه‌ی توزیع انرژی بین خودروهای الکتریکی و شبکه‌ی هوشمند توزیع انرژی الکتریکی(V2G) ارائه شد که بر اساس استخراج کننده‌ی فازی[۳] کار می‌کند و اثبات امنیت آن با استفاده از اوراکل تصادفی[۴] انجام شده است.

پس از این در [۷] ابتدا ضعف‌های پروتکل قبل شامل ایجاد مشکل همزمانی [۵]در زمان ورود کاربر و ضعف در برابر حملات مرد میانی و حمله‌ی بازپخش[۶] بیان شد و سپس پروتکلی مشابه طرح [۶] برای بهبود آن ارائه شد. این طرح نیز با استفاده از اوراکل تصادفی و همچنین ابزار AVISPA و اثبات غیر رسمی، اثبات امنیت شد. علاوه بر جلوگیری از حملات مرد میانی و بازپخش، این پروتکل در مقابل حملات جعل هویت و منع سرویس مقاوم است و ویژگی‌های امنیت رو به جلو و ناشناسی را تامین می‌کند.

احراز هویت سه عاملی شامل رمزعبور، اثر انگشت و کارت هوشمند برای شبکه V2G در [۷] مطرح شد. ایده‌ی کلی این طرح ارائه‌ی یک پروتکل کارا با استفاده از نگاشت آشوب چبیشف تعمیم یافته بود و به این دلیل ارائه شد که بیشتر طرح‌های قبل از آن از سیستم رمزنگاری و ضرب روی خم بیضوی استفاده می‌کردند که عملی پر هزینه برای وسایل با منبع محدود در شبکه بود و با استفاده از این سیستم جدید، وسایل با منبع محدود در شبکه می‌توانستند با صرف انرژی و هزینه‌ی کمتری عملیات احراز هویت و توافق برای کلید را انجام دهند.

امن بودن پروتکل یاد شده با استفاده از اوراکل تصادفی اثبات شده است. لازم به ذکر است این پروتکل در برابر حملات بازپخش، مرد میانی و جعل هویت مقاوم است و ویژگی امنیت رو به جلو و حریم خصوصی را حفظ می‌کند. لازم به ذکر است که به علت محدودیت فضا، مقایسه‌ی پروتکل‌های بیان شده به صورت کامل در گزارش تکمیلی پیوست شده، قابل مشاهده خواهد بود.

۲- آنالیز پروتکل احراز هویت Garg

سیستم ارتباطی خودرو با شبکه این بخش دارای چهار جز اصلی می‌باشد؛ اتومبیل الکتریکی(EV)، ایستگاه شارژ اتومبیل (CS)، جمع‌آوری اطلاعات مرکزی (CAG)، شبکه بلاکچین

در سیستم طراحی شده بر مبنای بلاکچین تلاش شده است تا ساختاری انگیزشی برای خودروها مهیا شود و خودروهایی که در ساعات پیک مصرف به انرژی الکتریکی خود نیاز ندارند آن را به جایگاه‌های تامین انرژی بفروشند و عملیات سوخت‌گیری را در ساعات خاموشی با قیمت به مراتب پایین انجام دهند. اختلاف قیمت به وجود آمده و پاداش داده شده از سوی جایگاه‌های تامین سوخت به اتومبیل‌ها، از اختلاف قیمت فروش سوخت در ساعت‌های مختلف برای جایگاه‌ها تامین می‌شود. واحد جمع‌آوری اطلاعات مرکزی تراکنش‌های معتبری که از جایگاه‌های تامین انرژی دریافت می‌شود را در شبکه بلاکچین ثبت می‌کند. هم‌چنین این واحد وظیفه ثبت‌نام خوروها و واحدهای معتبر در شبکه را دارد و به کمک ساختار بلاکچینی مکانیزم تشویقی را بین خودروهای الکتریکی ایجاد می‌کند. لازم به ذکر است که به علت محدودیت فضا، مراحل انجام احراز هویت و تحلیل پروتکل Garg و همکاران به صورت کامل در گزارش تکمیلی پیوست شده، قابل مشاهده خواهد بود.

۲-۱- مراحل انجام احراز هویت در شبکه

در این شبکه از وارد شدن یک خودرو یا جایگاه به شبکه تا احراز هویت و معرفی جایگاه‌ها و خودروها چهار مرحله اساسی طی خواهد شد؛ ۱-مقداردهی اولیه سیستم، ۲-ثبت‌نام خودروها و جایگاه‌های تامین انرژی، ۳-احراز هویت دوطرفه و ۴-اجماع و انجام تراکنش

۲-۱-۱-مقداردهی اولیه سیستم

ساختار احراز هویت این سیستم بر مبنای خم بیضوی انجام می‌شود، در نتیجه در این مرحله خم بیضوی مناسب، یک عدد پایه روی خم و یک عدد اول بزرگ انتخاب می‌شود. سپس واحد جمع‌آوری اطلاعات مرکزی یک نقطه روی خم به عنوان کلید

---

[۱] Factor
[۲] Password
[۳] Fuzzy Extractor
[۴] Random Oracle
[۵] Synchronization
[۶] Replay

خصوصی انتخاب کرده و ضرب آن در پایه را به عنوان کلید عمومی خود اختیار می‌کند.

۲-۱-۲-ثبت‌نام خودروها و جایگاه‌های تامین انرژی

این مرحله برای خودروها و جایگاه‌های تامین انرژی فقط یک بار صورت می‌گیرد و به واسطه آن، خودرو و جایگاه معتبر به واحد جمع‌آوری اطلاعات مرکزی معرفی می‌شود و هر خودرو و جایگاه پس از ثبت‌نام از واحد جمع‌آوری اطلاعات مرکزی هویت پنهان و کلید خصوصی دریافت می‌کند. هم‌چنین هویت و کلید عمومی آن‌ها نیز در مرکز جمع‌آوری اطلاعات مرکزی ذخیره شده و بعدا از این مقادیر جهت احراز هویت این اجزا شبکه از آن‌ها بهره گرفته خواهد شد.

۲-۱-۳- احراز هویت دوطرفه

فرآیند احراز هویت جایگاه‌ها و اتومبیل‌ها در شش مرحله انجام می‌شود. این فرآیند پیش از ثبت تراکنش سوختی در جایگاه‌ها برای تایید هویت جایگاه و اتومبیل و معرفی این دو به یکدیگر صورت می‌گیرد.

۲-۲- آنالیز امنیت پروتکل ارائه شده

در مرجع [۹] پروتکل Garg جهت احراز هویت دوطرفه در شبکه ارتباطی خودرو با شبکه تعریف شده است. اکنون قصد داریم برخی از چالش‌های امنیتی رعایت نشده در پروتکل را مطرح نماییم.

۲-۱-۱- آنالیز سرعت و راه‌حل‌های موجود

ضرب در خم بیضوی یکی از زمان‌بر ترین عملیات‌های رمزنگاری موجود می‌باشد و وجود ضرب‌های متعدد در پروتکل ارائه شده منجر به کند شدن این پروتکل خواهد شد.

۲-۲-۲- بررسی هویت مخفی کاربران شبکه

در پایان ثبت‌نام، هر جز از شبکه از مرکز جمع‌آوری اطلاعات یک هویت پنهان دریافت می‌کند. در این پروتکل تلاش شده است با هدف حفظ هر چه بیشتر حریم خصوصی جایگاه‌ها و اتومبیل‌ها بجای استفاده از هویت اصلی خود، یک هویت پنهان به هر جز اختصاص داده شود و پیام‌های مبادله شده اجزا با این هویت صورت گیرد.

۲-۲-۳- بررسی مسئله کلید سپاری

یکی از مواردی که باید در مسئله‌ی احراز هویت یا تبادل کلید در نظر گرفته شود، عدم تولید تمامی مقادیر مخفی توسط یک واحد معتمد است؛ به این خاطر که در صورت لو رفتن اطلاعات این واحد امنیت تمامی مولفه‌های مجاز موجود در شبکه به خطر می‌افتد و بهتر است تبادل این مقادیر مخفی به گونه‌ای باشد که هر مولفه واحد معتمد قسمتی از مقادیر مخفی را داشته و پس از تبادل اطلاعات با یک دیگر قادر به ساخت مقدار مخفی باشند تا امنیت کل سیستم به خطر نیفتد.

۲-۲-۴- بررسی فرآیند احراز تازگی پیام در پروتکل

در این پروتکل ارائه شده، هر زمان که نیاز به احراز تازگی[۱] پیام وجود دارد از برچسب زمانی استفاده می‌شود. قرار دادن برچسب زمانی بر روی پیام‌هایی که در شبکه مبادله می‌شود، مشکلات بسیاری را ایجاد می‌کند. اولین مشکل به وجود آمده، مسئله هماهنگ‌سازی زمان[۲] در اجزا شبکه می‌باشد. با توجه به غیرمتمرکز بودن شبکه هماهنگ‌سازی زمان بین اجزا بسیار سخت بوده و خود می‌تواند بستر مخاطراتی برای شبکه باشد.

۲-۲-۵- بررسی بار پردازشی مرکز جمع‌آوری اطلاعات برای تشخیص کاربران نامعتبر

اگر یک خودرویی اقدام به احراز هویت با هویت جعلی یا اشتباه نماید، شبکه تا مرحله چهارم متوجه نخواهد شد. علاوه بر آن واحد جمع‌آوری اطلاعات مرکزی مجبور است که عملیات‌های رمزنگاری ضرب روی خم بیضوی و چکیده گرفتن را انجام دهد تا نامعتبر بودن یک کاربری برای او احراز شود. اگر یک یا چند خودرو دائما درخواست احراز هویت با هویت جعلی ارسال نمایند، واحد جمع‌آوری اطلاعات مرکزی دائما مشغول این عملیات‌های سنگین رمزنگاری شده و عملیات سرویس‌دهی به کابران معتبر نیز دچار مشکل خواهد شد و حمله منع سرویس صورت می‌گیرد.

۲-۲-۶- بررسی احراز هویت تمام بخش‌ها به یکدیگر

بررسی مقادیر ارسال شده بر روی کانال‌های ارتباطی به ما نشان می‌دهد که جایگاه‌های تامین انرژی تقریبا تمامی مقادیر مخفیانه و غیرمخفیانه را روی کانال ارسال می‌کند. این اتفاق می‌تواند منجر به آن شود که اطلاعات مهاجم برای احراز هویت به جای دیگران را افزایش دهد و در نتیجه مهاجم هر زمان که خواست به جای دیگران در جایگاه‌ها عملیات احراز هویت را انجام دهد.

۲-۲-۷- شخصی‌سازی فرآیند احراز هویت در شبکه ارتباطی خودرو با شبکه

فاش شدن هر کدام از مقادیر مخفی اجزا شبکه باعث می‌شود هر کس که مقادیر مخفی کاربران دیگر را دارد، خود را در شبکه به

---

[۱] Freshness

[۲] Time Synchronization

جای آن‌ها معرفی سازد. این اتفاق در شبکه‌ای که منافع دیگران با جعل هویت به خطر می‌افتد اصلا قابل قبول نمی‌باشد. در نتیجه باید مکانیزهایی پیاده‌سازی نماییم تا در هر مرحله احراز هویت شخصی سازی شود و مهاجمین صرف دستیابی به برخی مقادیر محرمانه کاربران نتوانند حملات جعل هویتی طراحی نمایند.

۳- ارائه پروتکل احراز هویت در ارتباطات خودرو با شبکه

این بخش یک پروتکل احراز هویت برای ارتباط وسیله نقلیه به شبکه را ارائه می دهیم. این مدل بر اساس پروتکل احراز هویت و توافق کلید ارائه شده در مرجع [۷] آورده شده است، اما با توجه به آن که هدف ما ارائه راه‌حل برای احراز هویت می‌باشد با کمی تغییر بخش توافق کلید پروتکل را حذف کرده‌ایم. اجزای این مدل شامل کاربر، رابط کاربری با دستگاه تلفن همراه، ایستگاه شارژ اتومبیل (CS_j) و واحد مرکزی خدمات کاربردی (CAG) می‌باشد. در مدل ارائه شده دو مرحله ثبت نام کاربر و احراز هویت متقابل را جهت ارائه خدمت پشت سر می‌گذاریم.

۳-۱- مرحله ثبت‌نام کاربر

هر کاربر برای دریافت خدمات از شبکه نیاز دارد تا فاز ثبت‌نام اولیه را نزد CAG در یک کانال امن پشت سر بگذارد. مراحل ثبت‌نام کاربران به صورت زیر است:

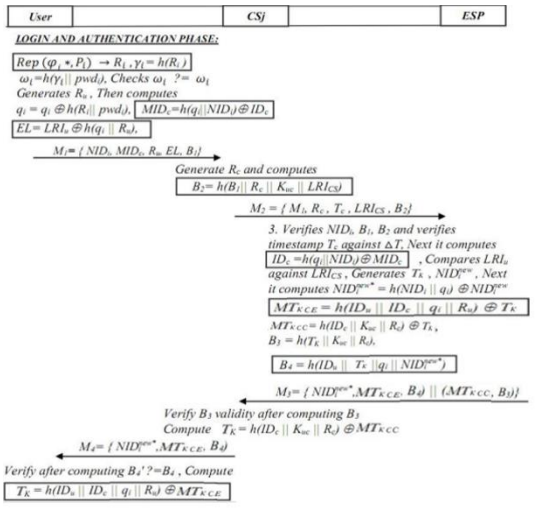
۱. در این مرحله کاربر از طریق یک کانال امن شناسه (ID_u) خود را برای CAG به عنوان درخواست ثبت‌نام ارسال می‌کند.
۲. در مرحله دوم CAG این کاربر را نیز به پایگاه داده خود اضافه می‌کند و برای کاربر یک شناسه گم‌نام و یک مقدار مخفی(کلید خصوصی) و یک مجموعه SID تولید و تحویل خودرو می‌دهد، هم‌چنین این مقادیر در CAG نیز ذخیره می‌شوند. مقادیر SID زمانی استفاده می‌شود که خودرو و CAG سنکرون بودن خود را از دست دهند.
۳. خودرو هم بعد از دریافت مقادیر مرحله دوم از CAG مقادیر پسورد و رمز اثر انگشت خود را اعمال کرده و در کنار سایر مقادیر ذخیره می‌نماید.

۳-۲- مرحله احراز هویت

پس از انجام مراحل اولیه و اختصاص دادن مقادیر پنهان و هماهنگ شدن خودرو و CAG می‌توان وارد مرحله احراز هویت دو طرفه خودرو با CAG و CS شد.

۱. خودرو پسورد و اثر انگشت خود را وارد می‌نماید. اگر مراحل ورود به درستی انجام شود، یعنی پسورد و احراز هویت به درستی انجام شود، مقدار کلید خصوصی خودرو به روز شده و شناسه ماسک شده خودرو تولید می‌شود. پس از تولید شناسه پنهان خودرو پیام B_1 را برای احراز هویت خود تولید و ارسال می‌کند.
۲. در مرحله بعدی CS مقادیر دریافتی را برای احراز هویت به سمت CAG ارسال می‌کند. در این مقادیر برای احراز تازگی، یک عدد تصادفی که توسط CS تولید می‌شود، تاثیر داده می‌شود.
۳. مرحله سوم اختصاص دارد به بررسی اطلاعات ارسالی به CAG و در صورت صحت این اطلاع یک بلیط برای خودرو درخواست دهنده تولید می‌شود.
۴. ·برای تولید بلیط و احراز هویت خودرو به جایگاه، ابتدا شناسه گم‌نام خودرو به‌روز می‌شود. سپس با استفاده از شناسه‌های ثبت شده در مرحله ثبت‌نام بلیط احراز هویت برای جایگاه و خودرو تولید می‌شود. در این مرحله جایگاه پیام دریافتی از CAG را بررسی می‌کند و به گونه‌ای سرور هم برای جایگاه احراز هویت می‌شود. پس از این اتفاق جایگاه پیامی که CAG برای خودرو تولید کرده است را تحویل خودرو می‌دهد.
۵. خودرو پیام دریافتی را بررسی می‌نماید و در صورت صحت، جایگاه و CAG برای او احراز هویت می‌شوند چرا که هیچ‌کس جز آن‌ها قادر به ساخت پیام احراز هویت نبودند.

جزییات مرحله احراز هویت کاربر در شکل ۱ آمده است.



شکل ۱ مرحله‌ی احراز هویت متقابل در پروتکل ارائه شده

۴- ارائه نتایج و ارزیابی

۴-۱- مقایسه‌ی ویژگی های امنیتی

در این قسمت ویژگی‌های امنیتی پروتکل پیشنهادی و پروتکل Garg و همکارانش [۹] بررسی شده است و نتیجه‌ی حاصل حاکی از این است که پروتکل پیشنهادی تمامی ایرادات موجود در پروتکل Garg را برآورده می‌سازد اما همچنان در مورد مسئله‌ی کلید سپاری چالش وجود دارد.

جدول ۱ مقایسه‌ی ویژگی‌های امنیتی

ویژگی‌های امنیتی	پروتکل پیشنهادی ما	پروتکل پیشنهادی Garg و همکاران
حمله‌ی بازپخش	T	F
حمله‌ی جعل هویت	T	F
حمله ی مرد میانی	T	T
حمله‌ی منع سرویس	T	F
حفظ ناشناسی	T	F
احراز هویت دو طرفه تمام مولفه‌ها	T	F
مشکل کلید سپاری	F	F
امنیت رو جلو	T	F

T: از حمله‌ی گفته شده جلوگیری کرده یا ویژگی امنیتی گفته شده را فراهم می‌کند.

F: از حمله‌ی گفته شده جلوگیری نکرده یا ویژگی امنیتی گفته شده را فراهم نمی‌کند.

۴-۲- مقایسه‌ی سربار پردازشی و ارتباطی

برای بررسی سربار پردازشی و ارتباطی با استفاده از اطلاعات موجود در [۷]، به محاسبه‌ی سربار پردازشی و ارتباطی دو پروتکل پرداخته شده است و نتیجه‌ی حاصل از این محاسبات، برتری پروتکل پیشنهادی را در هر دو زمینه‌ی سربار پردازشی و ارتباطی اثبات می‌کند. لازم به ذکر است که پروتکل پیشنهادی در زمینه‌ی تعداد پیام‌های مبادله شده برای انجام فرآیند احراز هویت نیز با تبادل ۴ پیام از پروتکل Garg و همکاران با ۵ تبادل پیام عملکرد بهتری دارد.

	User (ms)	Server (ms)
T_{BP}	13.662	7.318
T_{ECM}	10.235	5.387
T_{Exp}	8.341	3.362
T_M	5.012	2.002
T_H	0.019	0.012
T_{SYM}	0.063	0.048
T_{Bio_Rep}	0.015	-
T_{CertG}	69.326	-
T_{CertV}	-	21.257

شکل ۱: هزینه‌ی پردازشی محاسبه شده در [۷]

Primitive operations	Comm. cost (bits)
Bilinear Pairing	320 bits
Elliptic Curve Point	320 bits
User/CSj identity	60 bits
Hash function	160 bits
Random number	160 bits
Time Stamp	32 bits
Digital signature	1024 bits
Symmetric encryption	256 bits

شکل ۲: هزینه‌ی پردازشی محاسبه شده در [۷]

جدول ۲: مقایسه‌ی پروتکل پیشنهادی و پروتکل Garg و همکاران

Schemes	EV	CS/CAG	Communicational Cost(bits)
Garg et al.	$1\,T_{ECM} + 3\,T_H = 10.292ms$	$4\,T_{ECM} + 6\,T_H = 21.62ms$	2752
Ours	$1\,T_{Bio\_Rep} + 7\,T_H = 0.148ms$	$9\,T_H = 0.108ms$	2176

۵- چالش‌های باقی مانده و زمینه‌های تحقیقاتی آینده

همانطور که در بخش مقایسه‌ی ویژگی‌های امنیتی اشاره شد، یکی از مشکلات پروتکل پیشنهادی ما بحث کلید سپاری است و ایجاد پروتکلی که ویژگی عدم وابستگی به کلید سپاری را داشته باشد و در عین حال سبک نیز باشد یکی از مسائل چالش برانگیز این حوزه خواهد بود. در طرح پیشنهادی از رمزنگاری متقارن استفاده شده است اما، می‌توان از رمزنگاری نامتقارن نیز استفاده کرد و با استفاده از تکنیک انتقال بار یا استفاده از نگاشت آشوب طرح‌های سبک‌تر و کاراتری نسبت به طرح‌های مبتنی بر خم بیضوی ارائه داد.

۶- مراجع

[1] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. M. Nodooshan, “A novel identity-based key establishment method for advanced metering infrastructure in smart grid,” IEEE Transactions on Smart Grid, Vol. 9 (4), pp. 2834-2842, 2018.

[2] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, “Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks,” IEEE Transactions on Smart Grid, Vol. 10 (4), pp. 4349-4359, 2019.

[3] S. Garg; K. Kaur; G. Kaddoum; J. J. P. C. Rodrigues; M. Guizani, “Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid,” IEEE Transactions on Industrial Informatics, Vol. 16 (5), pp. 3548 - 3557, 2020.

[4] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, S. M. Mazinani, “A Secure and Efficient Key Establishment Scheme for Communications of Smart Meters and Service Providers in Smart Grid,” IEEE Transactions on Industrial Informatics, Vol.16 (3), pp. 1495-1502, 2020.

[5] L. Zhang, L. Zhao, S. Yin, C.H. Chi, R. Liu, Y. Zhang, “A lightweight authentication scheme with privacy protection for smart grid communications,” Future Generation Computer Systems, Vol. 100, pp. 770-778, 2019.

[6] P. Gope, & B. Sikdar, “An Efficient Privacy-preserving Authentication Scheme for Energy Internet-based Vehicle-to-Grid Communication”. IEEE Transactions on Smart Grid, Vol. 10 (6), pp. 6607 – 6618, 2019.

[7] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, “A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework,” IEEE Transactions on Industry Applications, vol. 00, pp. 1–11, 2020.

[8] D. Abbasinezhad-Mood, A. Ostad-Sharif, S.M. Mazinani, M. Nikooghadam, “Provably-secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection,” IEEE Transactions on Industrial Informatics, Vol. 16 (12), pp. 7287 – 7294, 2020.

[9] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. Rodrigues, “An efficient blockchain-based hierarchical authentication mechanism for energy trading in v2g environment,” in 2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2019, pp. 1–6.