مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»
سال اول، شماره ۳، پاییز ۱۳۹۲، ص ۶۱-۵۳

پروتکل جدید در پرداخت سیار با استفاده از رمز- امضاء بر اساس خم بیضوی

آتنا لطفی[۱]، محمدعلی دوستاری[۲*]

۱- دانشجوی کارشناسی‌ارشد، دانشکده فنی و مهندسی دانشگاه شاهد ۲- استادیار، دانشکده فنی و مهندسی دانشگاه شاهد

(دریافت: ۹۱/۱۰/۹، پذیرش: ۹۲/۴/۹)

چکیده

با افزایش نفوذ تلفن همراه و توسعه تجارت سیار، استفاده از تلفن همراه به‌عنوان ابزار پرداخت، روزبه‌روز گسترش می‌یابد. با توجه به اهمیت امنیت در تجارت و پرداخت و به‌دلیل ویژگی‌های شبکه‌های بی‌سیم و محدودیت‌های موجود در ابزار پرداخت، پروتکل‌های پیشنهادی در حوزه پرداخت سیار می‌بایستی علاوه بر تأمین کارایی از امنیت مناسبی نیز برخوردار باشند. در این مقاله که در راستای اهداف فوق می‌باشد، یک پروتکل پرداخت امن و کارا مبتنی بر سناریوی ارتباطی فروشنده محور ارائه می‌شود. در پروتکل پیشنهادی با استفاده از طرح کلید عمومی خودگواهی مبتنی بر رمزنگاری خم بیضوی، امضای رقمی شانور و همچنین طرح رمز- امضاء، راه حلی جهت رمزنگاری تصدیق اصالت شده ارائه می‌شود. بنابراین به‌کارگیری راه حل پیشنهادی در پروتکل، سبب کاهش بار محاسباتی و پیچیدگی زمانی در مقایسه با دیگر طرح‌های رمزنگاری کلید عمومی می‌شود. به‌علاوه، پروتکل ارائه شده در برابر حملات امنیتی شناخته شده مقاوم می‌باشد و همچنین گمنامی مشتری و انجام تراکنش پرداخت منصفانه برای او را نیز فراهم می‌آورد.

واژه‌های کلیدی: سیستم پرداخت سیار، پروتکل پرداخت، رمزنگاری خم بیضوی، کلید عمومی خودگواهی، امضای رقمی شانور.

۱. مقدمه

پرداخت سیار، یک پرداخت الکترونیکی در محیط بی‌سیم است که در آن یکی از طرف‌های شرکت کننده حداقل در تراکنش از ابزار پرداخت سیار استفاده می‌کند[۱]. با توجه به اهمیت امنیت در تجارت و پرداخت، پروتکل‌های پیشنهادی در حوزه پرداخت سیار می‌بایست با دید همه جانبه نسبت به مباحث امنیتی در زمینه شبکه‌های سیار و محدودیت‌های موجود در ابزار پرداخت طراحی شوند[۲]. بنابراین برای غلبه بر مشکلات مرتبط با پرداخت سیار، توجه به دو بحث امنیت و کارایی در طراحی پروتکل‌های پرداخت سیار یک ضرورت محسوب می‌شود.

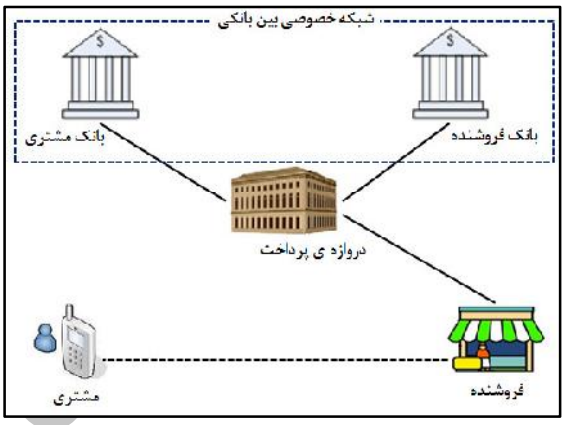
تاکنون تلاش‌های فراوانی در راستای ارائه پروتکل‌های پرداخت متناسب با نیازمندی‌های موجود در تجارت سیار صورت گرفته که در بسیاری از این پروتکل‌ها، جهت تأمین نیازمندی‌های امنیتی از سیستم‌های‌رمز کلید عمومی استفاده می‌شود. مسئله مهم در این سیستم‌ها، نیاز به برقراری ارتباط بین کلید عمومی و هویت شخص- اصالت کلید عمومی است. البته برای رفع این مسئله، راه حل‌هایی ارائه گردید که یک راه‌حل، سیستم‌های رمز کلید عمومی مبتنی بر گواهینامه است. اما استفاده از این سیستم‌ها در حوزه پرداخت سیار به‌دلیل نیاز به ساختار کلید عمومی، مدیریت و کنترل گواهینامه‌ها نامناسب است. پروتکل‌های SET [۵-۳] و iKP [۶ و ۷] نمونه‌هایی از پروتکل‌های پرداخت ارائه شده مبتنی بر طرح کلید عمومی مبتنی بر گواهینامه می‌باشند. جهت رفع مشکلات، طرح کلید عمومی مبتنی بر گواهینامه، طرح کلید عمومی مبتنی بر هویت اولین بار توسط شامیر[۱] در ۱۹۸۴ بیان گردید[۸]. اگرچه این طرح، مشکلات سیستم رمز کلید عمومی مبتنی بر گواهینامه را برطرف می‌کند ولی عیب آن وابستگی تمامی کلیدهای خصوصی به کلید اصلی مرکز تولید کلید[۲] است.

سیستم‌های رمز کلید عمومی خودگواهی[۳] برای مواجهه با مشکلات بیان شده در دو طرح فوق معرفی گردیدند. در سیستم رمز کلید عمومی خودگواهی، گواهینامه به‌طور ضمنی در خود کلید عمومی قرار می‌گیرد که این امر، کاهش هزینه ارتباطی و حافظه مصرفی را درمقایسه با طرح‌های مبتنی برگواهینامه سبب می‌شود. بنابراین استفاده از سیستم‌های رمز کلید عمومی خودگواهی در بحث پرداخت سیار، سبب بهبود فرآیند پرداخت می‌شود. البته در طراحی پروتکل‌های پرداخت سیار، استفاده از سیستم رمز متقارن اگرچه سبب کاهش بار محاسباتی تراکش پرداخت می‌شود، ولی مستلزم به اشتراک‌گذاری مقادیر محرمانه بین طرفین شرکت کننده در پروتکل می‌باشد. در نتیجه استفاده از سیستم‌های رمز متقارن در پروتکل پرداخت، محدودیت‌هایی را در طراحی پروتکل به‌وجود می‌آورد. از جمله پروتکل‌های مهم در حوزه پرداخت سیار مبتنی بر رمزنگاری متقارن، می‌توان به پروتکل‌های KSL [۹ و ۱۰] و Tellez [۱۵- ۱۱] اشاره نمود. بنابراین در طراحی پروتکل پیشنهادی از سیستم رمز

* ایمیل نویسنده پاسخگو: doostari@shahed.ac.ir

[1] Shamir
[2] Key Generation Center(Kgc)
[3] Self-Certified

کلید عمومی خودگواهی جهت برقراری خواسته‌های امنیتی استفاده می‌شود. در شکل ۱، یک سناریوی ارتباطی برای سیستم پرداخت سیار نشان داده شده است. در این سناریو، مشتری در زمان تراکنش پرداخت قادر به برقراری ارتباط مستقیم با بانک خود نمی‌باشد که دلیل آن می‌تواند، عدم دسترسی مشتری به اینترنت یا هزینه بالای پیاده‌سازی مکانیسم‌های دیگر جهت برقراری این ارتباط باشد. در این سناریو، مشتری با فروشنده فقط ازطریق یک کانال بی‌سیم بردکوتاه (مانند: بلوتوث، NFC، Infrared یا Wi-Fi) در ارتباط می‌باشد که این امر تسهیل فرآیند خرید را برای مشتریان (مانند: عابران و رانندگان) فراهم می‌آورد [۱۲ و ۱۴].



شکل ۱: سناریوی پرداخت سیار

پروتکل پیشنهادی ما در این مقاله، منطبق با این سناریوی ارتباطی است. در این پروتکل، طرحی جدید برای عملیات رمزنگاری کلید عمومی جهت استفاده در تراکنش پرداخت ارائه می‌شود که در این طرح پیشنهادی از سیستم رمز کلید عمومی خودگواهی، رمزنگاری خم بیضوی، طرح رمز- امضاء، طرح تصدیق هویت و امضای رقمی شانور[1] استفاده می‌شود. در این طرح استفاده از سیستم رمز کلید عمومی خودگواهی سبب بهبود فرآیند پرداخت و کاهش هزینه ارتباطی و حافظه مصرفی در مقایسه با طرح‌های امضای مبتنی بر گواهینامه می‌شود. از طرفی استفاده از خم بیضوی سبب کاهش طول کلید و حافظه مصرفی می‌شود. همچنین طرح شانور نیز به‌دلیل توان محاسباتی پایین یک طرح مناسب جهت استفاده در دستگاه‌هایی با منابع محدود می‌باشد. پروتکل پیشنهادی خواسته‌های امنیتی محرمانگی، تصدیق اصالت، عدم انکار فرستنده و دست نخوردگی اطلاعات را برآورده می‌نماید، همچنین گمنامی مشتری و انجام تراکنش پرداخت منصفانه برای او را نیز فراهم می‌آورد. این پروتکل در برابر حملات مردی در میان، تکرار و ایفای نقش نیز مقاوم می‌باشد. مقاله حاضر از بخش‌های مختلفی تشکیل شده است. در بخش ۲، مفاهیم و مقدماتی که برای ارائه پروتکل پرداخت مورد نیاز است بیان می‌شود. در بخش ۳، موجودیت‌ها و نمادهای استفاده شده در پروتکل پیشنهادی به‌همراه جزئیات پروتکل توضیح داده می‌شود. پروتکل ارائه شده، در بخش ۴ مورد تحلیل و بررسی قرار می‌گیرد و در بخش پایانی نتیجه کار انجام شده بیان می‌شود.

۲. پیش زمینه

در این بخش، به معرفی طرح‌هایی که مبنای کار در ارائه راه‌حل پیشنهادی قرار گرفته، پرداخته می‌شود.

۲-۱. سیستم رمزخم بیضوی

امنیت در این سیستم رمز، به سختی مسئله لگاریتم گسسته خم بیضوی‌بستگی دارد که از آن، برای تولید زوج کلید عمومی/ خصوصی در سیستم‌های رمز کلید عمومی استفاده می‌شود. از مزایای قابل توجه ECC، استفاده از تعداد بیت‌های کمتر نسبت به دیگر روش‌های رمزنگاری می‌باشد. در واقع ECC، با طول کلید کوتاه‌تر، امنیتی مشابه با دیگر سیستم‌های رمزنگاری کلید عمومی را فراهم می‌آورد که این امر سبب اجرای سریع‌تر و صرفه‌جویی بیشتر در پهنای باند می‌شود. بنابراین استفاده از سیستم‌های رمزخم بیضوی به‌ویژه برای برنامه‌های دستگاه سیار با منابع محدود بسیار مناسب می‌باشند [۱۸- ۱۶].

۲-۲. طرح رمز- امضاء

این طرح اولین بار در سال ۱۹۹۷ توسط زنگ[2] [۱۹] معرفی شد. این روش، نمونه‌ای جدید در رمزنگاری کلید عمومی است که در آن، عملیات امضاء و رمز به‌طور همزمان و تنها در یک گام منطقی انجام می‌گردد؛ یعنی این روش سبب کاهش زمان محاسبات و صرفه جویی در حجم پیام‌ها نسبت به روش «امضاء- سپس-رمز» می‌شود [۲۰].

۲-۳. طرح تصدیق هویت و امضای رقمی شانور

طرح‌های شانور، از پروتکل‌های «صفر-دانش»[3] می‌باشند. طرح‌های مبتنی بر صفر- دانش جزء روش‌های قوی برای بررسی صحت ادعای طرف مدعی است. به‌علاوه طرح شانور به‌علت داشتن توان محاسباتی پایین و تعداد گذرهای آن جهت استفاده در دستگاه‌هایی با توان محاسباتی پایین و حافظه محدود مناسب می‌باشد. طرح تصدیق هویت شانور از سه مرحله تشکیل شده که به‌ترتیب عبارتند از: «ادعای طرف مدعی»، «پرسش تصدیق‌کننده» و «پاسخ مدعی» که با قرار دادن این سه مرحله در پروتکل پرداخت پیشنهادی می‌توان عملیات پرداخت منصفانه‌ای را برای مشتری طراحی نمود. همچنین طرح امضای رقمی شانور نیز از سه مرحله تشکیل شده است ولی به‌صورت غیرتعاملی انجام می‌شود. به این منظور که در آن، هر سه مرحله را امضاء کننده انجام می‌دهد و نتیجه مرحله دوم و سوم به عنوان امضای پیام برای تصدیق‌کننده ارسال می‌شود تا بررسی صحت امضاء انجام گیرد [۲۱ و ۲۲].

[1] Schnorr

[2] Zheng

[3] Zero-Knowledge

۳. پروتکل پرداخت پیشنهادی

پروتکل پیشنهادی از پنج موجودیت:مشتری[1]، فروشنده[2]، بانک مشتری[3]، بانک فروشنده[4] و دروازه پرداخت[5] تشکیل شده است. دروازه پرداخت به‌عنوان یک رابط بین بانک مشتری/ فروشنده (شبکه خصوصی بین بانکی) و دو موجودیت دیگر مشتری و فروشنده، جهت انجام تسویه عمل می‌کند، یعنی توسط این شبکه خصوصی بین بانکی، انتقال واقعی پول انجام می‌گیرد و پول توسط بانک مشتری‌از اعتبار مشتری کسر و به اعتبار فروشنده اضافه می‌شود.

به‌علاوه، یک موجودیت مورد اعتماد به‌نام SA در سیستم پرداخت پیشنهادی وجود دارد و موجودیت‌های شرکت کننده در پروتکل، به‌منظور تولید زوج کلید عمومی/ خصوصی خود باید در آن ثبت نام نمایند.

۳-۱. نمادها

نمادها و علائم استفاده شده در پروتکل پیشنهادی در جدول **۱** نشان داده می‌شود.

جدول ۱: نمادها

نماد	شرح
$\{C, M, PG, I, A\}$	بیان کننده نام‌های طرفین شرکت کننده در پروتکل می‌باشند که به ترتیب عبارتند از: مشتری، فروشنده، دروازه پرداخت، بانک مشتری و بانک فروشنده.
ID_P	مشخصه‌ی هویتی موجودیت P
PK_P	کلید عمومی موجودیت P
S_P	کلید خصوصی موجودیت P
R_P	بیان کننده مقدار «شاهد»[6] برای موجودیت P می‌باشدکه توسط SA تولید می‌گردد و شرح آن در بخش ۲.۳ آمده است.
$\{m\}_K$	پیام m، رمزشده توسط کلید متقارن K
$sign_P$	امضاء توسط موجودیت P با استفاده از طرح امضای ارائه شده در بخش ۱.۳.۳
$signCrypt_{P-P'}$	رمز-امضاء روی پیام توسط فرستنده P برای گیرنده‌ی P' توسط طرح ارائه شده در بخش ۲.۳.۳
K_{AB}	کلید جلسه بین دو طرف شرکت کننده‌ی A و B
TID	شناسه تراکنش که توسط فروشنده به هر تراکنش تخصیص می‌یابد.
Date	تاریخ و زمان سفارش کالا یا خدمات
Nonce	یک مقدار دلخواه
OD	شرح سفارش که شامل اطلاعات: آدرس تحویل برای کالاهای فیزیکی و جزئیات سفارش خرید است.
Y/N	وضعیت کسر مبلغ از اعتبار مشتری و افزایش اعتبار به حساب فروشنده که توسط بانک مشتری و فروشنده اعلام می‌شود.
Price	قیمت کل کالا و خدمات
MID_{Req}	درخواست مشخصه هویتی فروشنده که این در خواست را مشتری از فروشنده می‌نماید.
H(m)	تابع درهم سازی یکطرفه روی پیام m
Acc_{Amt}	مانده حساب مشتری که توسط بانک مشتری در VSRes به مشتری اعلام می‌گردد.
Contract	قرارداد خریدکه شامل قیمت و شرح سفارش، شناسه منحصر به فرد قرارداد فی مابین فروشنده و مشتری، شناسه مشتری و فروشنده می‌باشد.
Reciption	رسید مشتری به فروشنده جهت دریافت سفارش با شرایط ذکر شده در قرارداد
InitReq/InitRes	تبادل اطلاعات لازم برای شروع پروتکل پرداخت بین مشتری و فروشنده
VSReq/VSRes	مجوز پرداخت به بانک جهت کسر از اعتبار مشتری که توسط مشتری برای بانک او صادر می‌شود و پاسخ مربوط به این درخواست توسط بانک مشتری برای مشتری برگردانده می‌گردد.
PReq/PRes	درخواست خرید توسط مشتری برای فروشنده ارسال می‌شود و پاسخ مربوط به این درخواست توسط فروشنده به مشتری برگردانده می‌شود.
VCReq/VCRes	درخواست افزایش اعتبار فروشنده توسط فروشنده برای PG ارسال می‌شود و پاسخ این درخواست توسط PG برای او بازگردانده می‌شود.

[1] Client
[2] Merchant
[3] Issuer
[4] Acquirer
[5] Payment Gateway
[6] Witness

۳-۲. روش‌های ارائه شده جهت استفاده در پروتکل پیشنهادی:

ابتدا روشی جهت امضاء رقمی بر اساس طرح امضای رقمی شانور پیشنهاد می‌شود که از تلفیق امضای رقمی شانور با کلید عمومی خودگواهی مبتنی برECC، این طرح امضاء ارائه می‌شود. در ادامه طرحی برای امضاء و رمز پیام به طور همزمان و در یک گام پیشنهاد شده است. این طرح از تلفیق امضای رقمی شانور، طرح رمز-امضاء و رمزنگاری کلید عمومی خودگواهی مبتنی برECC حاصل می‌شود.

جزئیات طرح پیشنهادی امضای رقمی شانور مبتنی بر رمزنگاری کلید عمومی خودگواهی و خم بیضوی: طرف A، می‌خواهد پیام m را امضاء نماید و برای B ارسال کند و B، تحیق صحت امضاء را انجام می‌دهد. برای این منظور طرف A، عدد دلخواهX را انتخاب وسپس مقادیر K، r و s را به شکل زیر محاسبه می‌کند. طرف A، (r,s) را به‌عنوان امضای پیام برای B ارسال می‌نماید و B بعد از دریافت امضای دریافتی، بررسی صحت آن را انجام می‌دهد.

generation

A: $X \in_R Z_q^*$

$K = XG$

$r = H(m||K)(modq)$

$s = X - rS_A$

(r,s)

verification

B: $\tilde{K} = sG + rPK_A = XG - rS_AG + rPK_A$

$r \stackrel{?}{\equiv} H(m||\tilde{K}) = \tilde{r}$

جزئیات طرح رمز- امضاء مبتنی بر رمزنگاری کلید عمومی خودگواهی، خم بیضوی و طرح امضای رقمی شانور: طرف A، پیام m را امضاء و رمز و برای B ارسال می‌کند. Bبعد از دریافت (r,s,c)، تحیق صحت امضاء را انجام می‌دهد و پیام m را بازیابی می‌نماید.

generation

A: $X \in_R Z_q^*$

$K = XPK_B = XS_BG$

$c = E_K(m)$

$r = H(m, H(XG), K) \bmod q$

$s = X - rS_A(\bmod q)$

A → B: (r,s,c)

verification

$sG + rPK_A = XG = *$

$\tilde{K} = (*)S_B = XGS_B = XPK_B$

$\tilde{m} = D_{\tilde{K}}(c)$

$r \stackrel{?}{\equiv} H(\tilde{m}, H(XG), \tilde{K})$

۳-۳. جزئیات پروتکل

گام ۱. C و M، اطلاعات لازم برای شروع پروتکل پرداخت را مبادله می‌کنند. این گام خود شامل دو مرحله می‌باشد:

- C، ابتدا پیغامی را که شامل شاهد و شناسه منحصر به‌فرد خود می‌باشد برای M ارسال می‌کند و درخواست خرید از M را می‌نماید. البته جهت حفظ گمنامی، مشتری می‌تواند از نام مستعار به‌جای هویت واقعی خود استفاده نماید.
- M، بعد از دریافت پیغام از C و انتخاب عدد تصادفی r_{MC}، کلید جلسه‌ای را جهت برقراری ارتباط امن با مشتری تشکیل می‌دهد و اطلاعات درخواستی مشتری را توسط این کلید جلسه، رمز و برای C ارسال می‌کند. M، مقدار درهم سازی فیلدی به نام Contractکه شامل اطلاعاتی از جمله: قیمت، شرح سفارش و شناسه منحصر به‌فرد قرارداد بین خود و مشتری است را در پیغام ارسالی به C قرار می‌دهد.

گام ۲. مشتری با دریافت پیغام InitRes و با استفاده از کلید خصوصی خود و مقدار $\{r_{MC}PK_M\}$ دریافتی، کلید جلسه را محاسبه می‌کند. سپس توسط آن، قسمت اول InitRes را رمزگشایی می‌نماید. بعد از بررسی آن، اگر قیمت و دیگر موارد مورد قبولش باشد درخواست خرید را برای فروشنده تحت عنوان PReq ارسال می‌کند. در پیغام PReq، مجوز پرداخت مشتری به بانک خود با نام VSReq قرار گرفته که VSReq مطابق با روش توضیح داده شده در بخش ۲.۳.۳ توسط مشتری، رمز و امضاء می‌شود. در پیغام VSReq، مقدار تصادفی K قرار گرفته که بانک مشتری در پاسخ به پیغام VSReq، از آن به‌عنوان کلید متقارن استفاده خواهد نمود. در این پروتکل در انتهای تراکنش خرید، مشتری باید رسیدی را جهت دریافت موفقیت‌آمیز کالا یا خدمات به فروشنده تحویل دهد که برای این منظور، از طرح تصدیق هویت شانور استفاده می‌گردد. این طرح شامل سه مرحله است که مرحله اول این طرح، ادعای طرف C می‌باشد که تحت عنوان r و با استفاده از مقدار تصادفی X تولید می‌شود. n یک مقدار تصادفی می‌باشد که توضیح آن در گام ۵ آمده است.

گام ۳. M ، بعد از رمزگشایی پیغام PReq، آن را چک می‌کند و اگر قیمت و دیگر موارد مورد قبولش باشد درخواست افزایش اعتبار را تحت عنوان VCReq برای PG ارسال می‌کند. این پیغام توسط M، امضاء و برای PG رمز شده است. در این پیغام مقدار تصادفی e، در واقع مرحله دوم از طرح تصدیق هویت شانور می‌باشد.

گام ۴. مراحل موجود در گام ۴، تحت شبکه خصوصی بین بانکی انجام می‌شود. بنابراین امنیت پیغام‌های مبادله شده برای ما مهم نمی‌باشد. در اولین مرحله PG، VSReq را به‌همراه برخی اطلاعات دیگر برای بانک مشتری ارسال می‌کند. بانک مشتری بعد از بررسی این پیغام و اطمینان از صحت آن، اعتبار مشتری را چک می‌نماید و نتیجه را به PG اعلام می‌کند. در پایان، PG بعد از دریافت پاسخ از I و A، پیغام VCRes را تشکیل می‌دهد.

گام ۵. PG، VCRes را برای M ارسال می‌کند. M با بررسی مقدار تابع

درهم‌سازی موجود در پیغام VCRes می‌تواند اطمینان حاصل نماید که PG پیغام VCRes را با توجه به پاسخ دریافتی از I تشکیل داده است. چون مقدار عدد تصادفی n راطرف I می‌داند ولی PG نمی‌داند.

گام ۶. M سپس مقدار دلخواه e، VSRes و اطلاعات دیگر را توسط کلید جلسه بین خود و C رمز می‌کند و در صورت افزایش اعتبار، مجوز استفاده از کالا و خدمات مورد درخواست مشتری را برای او ارسال می‌کند.

گام ۷. C بعد از دریافت موفقت‌آمیز کالا و خدمات، رسید را طبق مرحله سوم از طرح تصدیق هویت شانور تولید و برای M ارسال می‌کند. M نیز بعد از دریافت رسید، آن را اعتبارسنجی می‌نماید که برابری معادله زیر بیانگر دریافت یک رسید معتبر از مشتری می‌باشد.

$$yG + PK_c * e = XG - eS_cG + PK_c * e = XG \stackrel{?}{\equiv} r$$

۴. تحلیل و بررسی پروتکل پیشنهادی

۴-۱. خواسته‌های امنیتی

در این زیر بخش پروتکل پرداخت ارائه شده از لحاظ ویژگی‌های امنیتی مورد بررسی قرار گرفته و پس از آن در جدول **۲**، نتیجه مقایسه پروتکل پیشنهادی با پروتکل‌های دیگر از لحاظ خواسته‌های امنیتی نشان داده شده است ولی قبل از آن در جدول زیر، شرح گام‌های پروتکل بیان می‌شود:

Step1)

Step1.1) $C \rightarrow M$: $\text{InitReq} = \{ID_C, R_C, TID_{Req}, Nonce, MID_{Req}\}$

Step1.2) $M \rightarrow C$: $\text{InitRes} = \{TID, Date, H(Contract)\}_{K_{MC}}, ID_M, R_M, r_{MC}PK_M$
$Contract = TID, Date, Nonce, ID_M, ID_C, Price, OD$
$K_{MC}=S_M r_{MC}[H_2(ID_C, R_C)PK_S + R_C]$

step2) $C \rightarrow M$: $PReq = \{TID, Date, Nonce, ID_I, H(OD, Price), VSReq, n\}_{K_{MC}}, ID_C, Nonce$
$VSReq = \{ID_M, Price, H(Contract), r, K, n\}_{SignCrypt_{C-I}}$
$r = XG$

step3) $M \rightarrow PG$: $VCReq = \{TID, Date, Nonce, Price, ID_I, ID_C, R_C, H(Contract), e, VSReq\}_{SignCrypt_{M-PG}}, ID_M, R_M$

step4) "با استفاده از شبکه‌ی خصوصی بین بانکی"
1) $PG \rightarrow I$: $VSReq, TID, Date, Nonce, Price, ID_M, ID_C, R_C, H(Contract), e$
2) $PG \rightarrow A$: $Price, ID_M, TID, Date, Nonce$
3) $I \rightarrow PG$: $Y/N, TID, Date, Nonce, ID_M, H(Y/N, H(Contract), n), VSRes$
$VSRes = \{Y/N, TID, Date, Nonce, H(Contract), Acc_{Amt}, e\}_K$
4) $A \rightarrow PG$: $Y/N, TID, Date, Nonce, ID_M$

step5) $PG \rightarrow M$: $VCRes = \{Y/N, TID, Date, Nonce, H(Y/N, H(Contract), n), VSRes\}_{Sign_{PG}}, ID_{PG}, R_{PG}$

step6) $M \rightarrow C$: $PRes = Services \ \& \ Goods, \{TID, Date, Nonce, e, VSRes\}_{K_{MC}}, ID_M, Nonce$

step7) $C \rightarrow M$: $y = (X - e * S_C)$ رسید دریافت کالا و خدمات

جدول ۲: مقایسه پروتکل‌ها از لحاظ خواسته‌های امنیتی

ویژگی / پروتکل	SET	3KP	Ksl_{V_1}	Ksl_{V_2}	$Tellez_{V_1}$	$Tellez_{V_2}$	Proposed
محرمانگی	✓	✓	✓	✓	✓	✓	✓
عدم انکار تراکنش	✓	✓	✓	✓	✓	✓	✓
گمنامی مشتری	×	×	×	×	✓	✓	✓
مبادله منصفانه	×	×	×	×	×	×	✓
تصدیق اصالت موجودیت‌ها	✓	✓	✓	✓	✓	✓	✓
جامعیت و دست نخوردگی اطلاعات	✓	✓	✓	✓	✓	✓	✓
مقاوم در برابر حمله تکرار	✓	✓	✓	✓	✓	✓	✓
مقاوم در برابر حمله مردی در میان	✓	✓	✓	✓	✓	✓	✓
مقاوم در برابر حمله ایفای نقش	✓	✓	✓	✓	✓	✓	✓
عدم ثبت نام در فروشنده قبل از پرداخت	✓	✓	×	×	×	✓	✓
عدم ارسال گواهینامه و بررسی اعتبار آن	×	×	×	✓	✓	✓	✓

❖ **محرمانگی تراکنش:** در پروتکل پیشنهادی، کانال ارتباطی بین C، M و PG ناامن است، بنابراین می‌بایست اطلاعات مهم مبادله شده بین طرفین در طول انتقال برای افراد غیرمجاز آشکار نگردد. برای دست‌یابی به این امر، می‌بایست از رمزنگاری استفاده شود. بدین منظور در پروتکل ارائه شده، ارتباط بین C و M از طریق یک کلید جلسه مشترک به‌نام K_{MC}، رمز می‌شود و از طرفی اطلاعاتی که C برای I از طریق M ارسال می‌کند و VSReq نام دارد به‌وسیله تکنیک توضیح داده شده در بخش ۲.۳.۳ رمز شده و همچنین پیغام مبادله شده بین M و PG نیز با استفاده از همین تکنیک رمز می‌شود.

❖ **گمنامی:** به‌منظور محافظت از هویت واقعی مشتری، او می‌تواند ازنام مستعار(NID_C) به‌جای هویت واقعی خودش استفاده نماید؛ یعنی به‌جای استفاده از ID_C، هر مشتری باید دارای چندین NID_C باشد و این NID_Cها فقط برای خود مشتری و بانک او شناخته شده باشند و فروشنده نتواند ارتباطی بین NID_C و هویت واقعی مشتری برقرار نماید. بدین شکل گمنامی مشتری برقرار می‌شود. در ادامه سه ویژگی تصدیق اصالت موجودیت‌ها، دست نخوردگی تراکنش و عدم انکار در پروتکل پیشنهادی بررسی می‌شود:

- در پروتکل پیشنهادی، مشتری و فروشنده لازم نیست که یکدیگر را تصدیق اصالت نمایند بلکه این وظیفه PG و I می‌باشد که این ادعاها را بررسی نمایند و از طرفی چون اطلاعات مبادله شده بین C و M توسط کلید جلسه رمز می‌شود، بنابراین هر یک از این طرف‌ها، بعد از رمزگشایی پیغام دریافتی از طرف دیگر، می‌بایست معنادار بودن فیلدهای پیغام دریافتی را بررسی نماید. در صورت معنادار‌بودن، می‌توانند اطمینان داشته باشد که پیغام دریافتی در طول مسیر تغییر نیافته است.
- در پروتکل ارائه شده، اطلاعاتی که C برای I ارسال می‌کند با استفاده از روش SignCrypt ارائه شده در بخش۲.۳.۳ رمز و امضاء می‌شود. بنابراین I می‌تواند اطمینان داشته باشد که خودC مجوز درخواست کسر از اعتبار را صادر نموده و از طرفی چون C نیز آن را امضاء کرده، بنابراین نمی‌تواند ارسال این درخواست را انکار نماید. بعد از رمزگشایی پیغام دریافتی توسط I، در صورتی که فیلدهای این پیغام معنادار باشد I می‌تواند اطمینان داشته باشد که پیغام در طول انتقال تغییر نیافته است؛ بنابراین سه ویژگی فوق برآورده می‌شود و همین‌طور برای پیغام درخواست افزایش اعتباری که M به PG ارسال می‌کند نیز این سه ویژگی به دلیل استفاده از طرح بیان شده در بخش ۲.۳.۳برقرار است.
- در این پروتکل، پیغام پاسخ کاهش اعتبار، که I برای C از طریق M ارسال می‌کند، توسط کلید متقارن K که در پیغام VSReqوجود دارد رمز می‌شود. از طرفی، چون پیغام VSReq، فقط قابل رمزگشایی توسط I می‌باشد، بنابراین C می‌تواند اطمینان داشته باشد که پیغام حتما از طرف I ارسال شده است (تصدیق اصالت) و درصورت معنادار‌بودن فیلدهای پیغام دریافتی، C می‌تواند اطمینان داشته باشد که پیغام در مسیر انتقال تغییر نیافته است.
- پاسخ درخواست افزایش اعتبار فروشنده، توسط PG امضاء می‌شود. بنابراین M می‌تواند اطمینان داشته باشد که این پیغام حتماً از طرف PG فرستاده شده و اطلاعات دست نخورده می‌باشد و از طرفی، PG هم نمی‌تواند ارسال آن را انکار نماید. وجود فیلد$H(Yes/NO, H(Contract), n)$ در پیغام، تضمین می‌نماید که PG در راستای پیغام دریافتی از I، VCRes را تولید نموده است. چون مقدار تصادفیn، فقط در اختیار C می‌باشد و او این مقدار را برای M در گام دوم ارسال می‌کند و همچنین مقدار n در VSReq نیز قرار دارد. بنابراین M و I هر دو این مقدار را دارند ولی PG آن را ندارد.

❖ **ایستادگی در مقابل حمله مردی در میان:** یعنی فرد مهاجم خودش را بین دو طرف قانونی قرار دهد و بتواند یکی از این دو یا هر دو را فریب دهد. از آنجایی که پیام‌های مهم، به‌صورت رمزشده تصدیق اصالت شده می‌باشند، بنابراین دشمن و مهاجم نمی‌تواند نقش هیچ کدام از طرف‌های قانونی را ایفا کند. در نتیجه پروتکل پیشنهادی در برابر این حمله مقاوم می‌باشد.

❖ **مقاوم بودن در مقابل حمله تکرار:** ممکن است مهاجمی بخواهد با استراق سمع پیام‌های مبادله شده بین طرفین شرکت کننده در یک تراکنش، یک نشست جعلی تشکیل دهد. اما از آنجایی که TID به‌ازای هر تراکنش، مقدار منحصر به‌فردی دارد و همچنین به‌دلیل استفاده از مقدار دلخواه Nonce، بنابراین مهاجم قادر نخواهد بود اطلاعاتی که در تراکنش‌های قبلی جمع‌آوری کرده را در تشکیل یک تراکنش جدید به‌کار ببرد.

❖ **مقاوم بودن در مقابل حمله ایفای نقش:** ممکن است مهاجمی بخواهد از طرف مشتری، مجوز کسر از اعتبار را صادر نماید؛ ولی به‌دلیل اینکه در پروتکل‌های پیشنهادی، مجوز کسر از اعتبار، توسط مشتری امضاء و رمز می‌شود و از طرفی درخواست افزایش اعتبار نیز توسط فروشنده امضاء و رمز شده، بنابراین این حمله امکان پذیر نمی‌باشد.

❖ **تراکنش پرداخت منصفانه:** یکی از ویژگی‌های مهم در پروتکل‌های پرداخت، حفظ منافع شرکت‌کنندگان در پروتکل می‌باشد. در پروتکل پیشنهادی، در طول اجرای تراکنش پرداخت مشتری قبل از دریافت کالا یا خدمات درخواستی، پول را پرداخت می‌کند. بنابراین در این پروتکل، ریسکی برای فروشنده وجود ندارد اما مشتری ممکن است کالا یا خدمات را دریافت نکند. برای منصفانه کردن عملیات پرداخت، از طرح تصدیق هویت شانور استفاده گردید.

۴-۲. کارایی

مقایسه پروتکل پیشنهادی با پروتکل‌های دیگر از نظر تعداد عملیات مورد نیاز برای انجام تراکنش پرداخت در جدول **۳** نشان داده شده است و در ادامه پروتکل‌ها از نظر میزان بار محاسباتی و پیچیدگی زمانی مورد مقایسه قرار داده می‌شود.

جدول ۳: مقایسه پروتکل‌ها از لحاظ تعداد عملیات مورد نیاز

عملیات	پروتکل	SET	3KP	Ksl_{V_1}	Ksl_{V_2}	$Tellez_{V_1}$	$Tellez_{V_2}$	Proposed
رمزنگاری کلید عمومی	C	۱	۱	–	–	–	۲	۱
	M	۱	۱	۱	–	–	۳	۱
	PG	۱	–	۱	–	–	۱	–
رمزگشایی کلید عمومی	C	–	–	–	–	–	۲	–
	M	۱	–	۱	–	–	۲	–
	PG	۲	۲	۱	–	–	۱	۱
تولید امضاء	C	۱	۱	–	–	–	۲	۱
	M	۳	۱	۱	–	–	۳	۱
	PG	۱	۱	۱	–	–	۱	۱
بررسی صحت امضاء	C	۲	۲	–	–	–	۲	–
	M	۲	۲	۱	–	–	۲	۱
	PG	۲	۲	۱	–	–	۱	۱
رمزنگاری/ رمزگشایی کلیدمتقارن	C	۲	–	۴	۴	۵	–	۴
	M	۱	–	۳	۵	۶	–	۳
	PG	۲	–	–	۲	۲	–	–
توابع درهم‌سازی	C	۳	۲	۳	۳	۲	۱	۲
	M	۳	۴	۳	۳	۴	۲	۳
	PG	۲	۱	–	۱	۱	۱	۲
توابع درهم‌سازی کلیددار	C	–	–	۲	۲	۲	–	–
	M	–	۱	۱	۲	۲	–	–
	PG	–	–	–	۱	۱	–	–

Ksl_{V_1} (مبتنی بر رمزنگاری نامتقارن [۲، ۹ و ۱۰]) Ksl_{V_2} (مبتنی بر رمزنگاری متقارن [۲، ۹ و ۱۰])، $Tellez_{V_1}$ (مبتنی بر رمزنگاری متقارن- فروشنده محور [۱۱]) $Tellez_{V_2}$ (مبتنی بر رمزنگاری نامتقارن- فروشنده [۱۵- ۱۲]) Proposed(پروتکل پیشنهادی)

برای این منظور برای هر یک از عملیات استفاده شده توسط موجودیت‌های شرکت کننده در پروتکل، یک زمانی تخصیص داده می‌شود که نمادهای استفاده شده برای این امر به صورت زیر می‌باشد [۱۴و ۱۶]:

T_m: زمان برای ضرب بدون پیمانه N

T_{mm}: زمان برای ضرب با پیمانه N

T_h: زمان برای تابع درهم‌سازی

T_{kh}: زمان برای تابع درهم‌سازی کلیددار

T_{exp}: زمان برای توان رسانی پیمانه‌ای

T_{EC_m}: زمان برای ضرب خم بیضوی

T_{sym}: زمان برای انجام عملیات رمزنگاری و رمزگشایی متقارن

- ✓ از زمان جمع و تفریق صرف‌نظر می‌شود، چون زمان آن در مقایسه با دیگر زمان‌ها به‌نسبت کم است. بنابراین در تحلیل پیچیدگی زمانی از آن‌ها صرف نظر می‌گردد [۱۴].
- ✓ رمزنگاری/ رمزگشایی متقارن تقریبا صد برابر سریع‌تر از رمزنگاری/ رمزگشایی نامتقارن است[۱۶].
- ✓ زمان مورد نیاز برای انجام عمل ضرب خم بیضوی کندتر از عمل ضرب و سریع تر از عمل توان‌رسانی است[۱۶].

$1T_{EC_m} \cong 29\ T_m$

$1T_{exp} \cong 240\ T_m$

با توجه به نکات بیان شده در بالا، پیچیدگی زمانی پروتکل‌ها مورد بررسی قرار می‌گیرد. برای این منظور، ابتدا زمان مورد نیاز برای انجام عملیات رمزنگاری، رمزگشایی، امضاء و بررسی صحت امضاء در پروتکل $Tellez_{V_2}$ و پروتکل پیشنهادی در جدول **۴** نشان داده می شود و سپس بر اساس آن کار تحلیل و مقایسه پروتکل ها انجام می‌شود.

جدول۴: زمان انجام عملیات

زمان عملیات / پروتکل	رمز و امضا (T_{es})	رمزگشایی و بررسی صحت امضاء (T_{dv})	تولید امضاء (T_s)	بررسی صحت امضاء (T_v)
$Tellez_{V_2}$	$3T_h+3T_m+2T_{mm}+3T_{exp}$	$5T_h+T_m+5T_{mm}+11T_{exp}$	–	–
Proposed	$2T_h+1T_m+2T_{EC_m}$	$2T_h+3T_{EC_m}$	$1T_h+T_m+T_{mm}$	$1T_h+2T_{EC_m}$

جدول ۵: مقایسه پروتکل‌ها از لحاظ پیچیدگی زمانی

نام پروتکل	موجودیت شرکت‌کننده	زمان مورد نیاز
$Tellez_{V_1}$	C	$2T_h + 2T_{kh} + 5T_{sym}$
	M	$4T_h + 2T_{kh} + 6T_{sym}$
	PG	$1T_h + 1T_{kh} + 2T_{sym}$
KSL_{V_2}	C	$3T_h + 2T_{kh} + 4T_{sym}$
	M	$3T_h + 2T_{kh} + 5T_{sym}$
	PG	$1T_h + 1T_{kh} + 2T_{sym}$
$Tellez_{V_2}$	C	$2T_{es} + 2T_{dv} + 1T_h$
	M	$3T_{es} + 2T_{dv} + 2T_h$
	PG	$1T_{es} + 1T_{dv} + 1T_h$
Proposed	C	$1T_{es} + 4T_{sym} + 2T_h$
	M	$1T_{es} + 1T_v + 3T_{sym} + 3T_h$
	PG	$1T_s + 1T_{dv} + 1T_s + 2T_h$

نتیجه‌ای که از جدول ۵ حاصل می‌شود به‌صورت زیر است:

- ✓ از نظر پیچیدگی زمانی در سمت مشتری:

$$\mathrm{KSL}_{V_2} < \mathrm{Tellez}_{V_1} < Proposed < \mathrm{Tellez}_{V_2}$$

- ✓ از نظر پیچیدگی زمانی در سمت فروشنده:

$$\mathrm{KSL}_{V_2} < \mathrm{Tellez}_{V_1} < Proposed < \mathrm{Tellez}_{V_2}$$

- ✓ از نظر پیچیدگی زمانی در سمت دروازه پرداخت:

$$\mathrm{KSL}_{V_2} \cong \mathrm{Tellez}_{V_1} < Proposed < \mathrm{Tellez}_{V_2}$$

دو پروتکل KSL_{V_2} و Tellez_{V_1} مبتنی بر رمزنگاری متقارن می‌باشند که اگر چه سبب کاهش بار محاسباتی تراکش پرداخت می‌شوند، ولی نیاز به اشتراک گذاری مقادیر محرمانه بین طرفین شرکت کننده در پروتکل می‌باشد.

۵. نتیجه‌گیری

هدف مقاله حاضر، طراحی پروتکلی متناسب با نیازمندی‌های حوزه پرداخت سیار است. پروتکل ارائه شده در این مقاله، مبتنی بر سناریوی ارتباطی فروشنده محور می‌باشد. در این پروتکل، طرحی جدید برای عملیات رمزنگاری کلید عمومی جهت استفاده در تراکنش پرداخت ارائه شده که در طرح پیشنهادی از سیستم رمز کلید عمومی خودگواهی، رمزنگاری خم بیضوی، طرح رمز- امضاء، طرح تصدیق هویت و امضای رقمی شانور استفاده گردیده است. پروتکل ارائه شده ویژگی‌های محرمانگی، تصدیق اصالت، عدم انکار فرستنده و دست نخوردگی اطلاعات را برآورده می‌نماید. همچنین گمنامی مشتری و انجام تراکنش پرداخت منصفانه برای او را نیز فراهم می‌آورد. به‌علاوه، این پروتکل در برابر حملات مردی در میان، تکرار و ایفای نقش نیز مقاوم است. پروتکل پیشنهادی از لحاظ خواسته‌های امنیتی نسبت به سایر پروتکل‌های اشاره شده بهتر می‌باشد ولی از نظر بار محاسباتی و پیچیدگی زمانی تراکنش پرداخت نسبت به پروتکل‌های متقارن ضعیف‌تر و نسبت به پروتکل‌های نامتقارن قوی‌تر می‌باشد.

۶. مراجع

[1] M. V. alizadeh, R. A. Moghaddam, S. Momenebellah, "New Mobile Payment Protocol: Mobile Pay Center Protocol (MPCP)"; 3rd Int. Conf. Electronics Computer Tech., pp.74–78, 2011.

[2] S. Kungpisdan, "Modelling Design, and Analysis of Secure Mobile Payment Systems"; Ph.D.[Dissertation, Faculty of Information Technology, Monash University, 2005.

[3] S. M. Shedid, M. El-Hennawy, M. Kouta, "Modified SET Protocol for Mobile Payment: An Empirical Analysis"; IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010, pp. 289–295.

[4] X-y Ren, L-l Wei, J-f Zhang, X. Ma, "The Improvement of SET Protocol based on Security Mobile Payment"; Journal of Convergence Information Technology, Vol. 6, No. 7, pp. 22–28, 2011.

[5] S. Kungpisdan, B. Srinivasan, P. D. Le, "A Practical Framework for Mobile Set Payment"; IADIS Int. Conf. e-Society, pp. 321–328, 2003.

[6] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E.V. Herreweghen, M. Waidner, "Design, Implementation, and Deployment of the iKP Secure Electronic Payment System"; IEEE J. on selected areas in communications, vol. 18, No. 4, pp. 611–626, 2000.

[7] K. Ogata, K. Futatsugi, "Flaw and Modification of the IKP Electronic Payment Protocols"; Information Proc. Letters 86 [Online],www.elsevier.com/locate/ipl, pp. 57– 62, 2003.

[8] A. Shamir, "Identity-Based Cryptosystem and Signature Scheme"; in Proceedings of CRYPTO, pp. 47 –53, 1984.

[9] B. T. S. Toh, S. Kungpisdan, P. D. Le, "KSL Protocol: Design and Implementation"; Proc. IEEE, Conf. on Cybernetics and Intelligent Systems, pp. 544–549, 2004.

[10] S. Kungpisdan, B. Srinivasan, P.D. Le, "Accountability Logic for Mobile Payment Protocols"; Proc. IEEE, the Int. Conf. on Information Tech., Coding and Computing (ITCC'04) , pp. 40–44.

[11] J. T. Isaac, J. M. Sierra, A. Izquierdo, M. Carbonell, "A Secure for a Payment System Based on a Kiosk Centric Case Mobile Scenario"; Ingenieria UC, Universidad de Carabobo, VeneZuela, pp. 25–36, 2006.

[12] J. T. Isaac, J. S. Camara, A. I. Manzanares, J. T. Marquez, "Anonymous Payment in a Kiosk Centric Model using Digital Signature Scheme with Message recovery and Low Computational Power Devices"; J. of Theoretical and Applied Electronic Commerce Research, pp. 1–11, 2006.

[13] J. T. Isaac, J. S. Camara, "A Secure Payment Protocol for Restricted Connectivity Scenarios in M-Commerce"; Proc. 8th Int. Conf. on E-Commerce and Web Technologies, (EC-Web'07), pp. 1–10, 2007

[14] J. T. Isaac, J. S. Camara, S. Zeadally, J. T. Marquez, "A Secure Vehicle-to-Roadside Communication payment protocol in Vehicular ad hoc Networks"; Computer Communications, pp. 2478–2484, 2008.

[15] M. V. Astudillo, J. T. Isaac, D. S. Touceda, H. P. López, "Evaluation of a Client Centric Payment Protocol Using Digital Signature Scheme with Message Recovery Using Self-Certified Public Key"; ICCSA 2009, Part II, LNCS 5593, Springer-Verlag Berlin Heidelberg, pp. 155–163. 2009.

[16] W. Li, Q. Wen, Q. Su, Z. Jin, "An efficient and secure Mobile Payment Protocol for restricted Connectivity Scenarios In Vehicular Ad Hoc Network"; Computer Communications , vol. 35, pp. 188–195, 2012.

[17] A. Menezes, M. Qu, S. Vanstone, "Elliptic Curve Systems"; IEEE P1363 Part4 Standard, 1995.

[18] A. Babel "Elliptic Curve Cryptography"; F090740, Universiteit Utrecht, INFOB3CRP – Cryptography.

[19] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) <<Cost(Signature) + Cost (Encryption)"; CRYPTO '97 Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pp. 165–179, 2011.

[20] L. Savu, "Combining Public Key Encryption with Schnorr Digital Signature"; J. of Software Eng. and Applications"; pp.102–108, 2012.

[21] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography"; CRC-Press , 1996.

[22] J. Pieprzyk, T. Hardjono, J. Seberry, "Fundamentals of Computer Security", Springer, 2003.