پروتکل حفظ حریم خصوصی و احرازهویت در سیستم های موبایلی

سابینا نوبری[1] و مجید گودرزی[2]

1- عضو هیئت علمی دانشگاه آزاد اسلامی، واحد تهران جنوب، ایران،

maryamkamalian@yahoo.com

۲- دانشکده فنی مهندسی دانشگاه آزاد اسلامی، واحد الکترونیکی تهران ، ایران

چکیده

با رشد و نفوذ تکنولوژی سیار، وجود پروتکل پرداختی که علاوه بر تامین نیازهای امنیتیلازم از کارایی مطلوب در محیط سیار نیز برخوردار باشد یک ضرورت اساسی است. در این تحقیق ابتدا با توسعه SWPP، پروتکل پرداخت سیار پیشنهاد شده که بر خلاف SWPP ویژگیهای گمنامی و حفظ حریم خصوصی مشتری را نیز فراهم می کند. در پروتکل پرداخت سیار پیشنهاد شده از یک گواهینامه دیجیتالی مستعار و یک حساب بانکی گمنام برای مخفی نگه داشتن هویت مشتری استفاده می شود. ویژگیهای امنیتی پروتکلهای پیشنهادی به صورت غیررسمی و رسمی بررسی و با پروتکلهای مرتبط مقایسه شد.این پروتکل از لحاظ تامین معیارهای امنیتی و کارایی ارزیابی با پروتکلهای مشابه مقایسه شد. بررسیها نشان می دهد که پروتکلهای پیشنهادی علاوه بر تامین کلیه ویژگیهای امنیتی مورد نیازیک سیستم پرداخت و خرید امن، کارایی بهتری را فراهم می آورند.

کلمات کلیدی:

۱– مقدمه

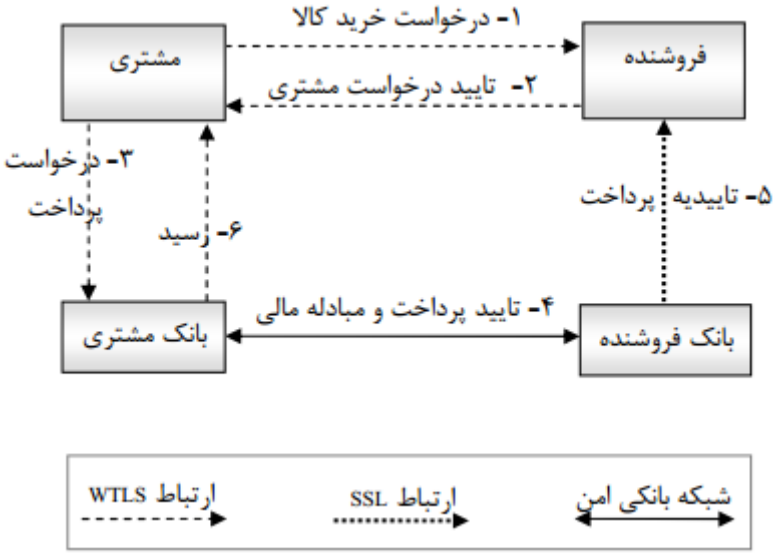
با افزایش استفاده از اینترنت بر روی گوشی های موبایل، روش‌های سنتی سرویس‌دهی به مشتریان مبدل به روش‌هایی شده است که به نحوی بتوانند از این سرویس بهره گیرند. بر اساس آمارهای موجود دامنه گسترش استفاده از ابزارهای موبایلی بالاتر از هر فناوری دیگری است و این مسأله، تجارت سیار را به شکل انقلابی جهانی درآورده است که با همان سرعت وقوع در کشورهای پیشرفته، در کشورهای در حال توسعه نیز در حال رخ دادن است. طبق تحقیقات بعمل آمده در طی سال های اخیر در سطح جهان، تعداد کاربران اینترنت از طریق ابزارهای سیار برای اولین بار از تعداد کاربران اینترنت از طریق رایانه‌های شخصی (خطوط ارتباطی ثابت) پیشی گرفته است. این مسأله خود بیانگر پتانسیل قوی تجارت سیار است که می تواند در آینده نزدیک بیشترین سهم از بانکداری الکترونیکی را به خود اخصاص دهد. بانکداری سیار بعنوان یکی از مهمترین حوزه های تجارت سیار، ارتباطات وسیع و تأثیرگذاری بر سایر حوزه های تجارت سیار دارد. بخش اعظمی از نقل و انتقالات پولی در شبکه تجارت سیار، از طریق بانکها و شبکه بانکداری سیار آنها انجام می شود، لذا بانکداری سیار از یک سو با مشتریان خود در ارتباط است و از سوی دیگر قادر است برای سایر بنگاههایی که در حوزه تجارت الکترونیکی فعالند، خدمات مالی مؤثری تأمین نماید. عواملی که توجه بانکها را شدیداً به سمت استفاده هرچه بهینه تر از ابزارهای موبایل جلب نموده است؛ امکان بی نظیر خدمات موبایلی در کاهش هزینه های ارائه خدمات بانکی و سرعت و امنیت بالای آنها می باشد همچنین به علت مشکلاتی از قبیل حمل کارت های پرداخت متعدد در کیف مشتریان، نگهداری رسیدهای کاغذی گوناگون، نبود یک سیستم خودکار ثبت سفارش، نبود مدیریت بر روی سیستم های پرداخت متنوع ناسازگار و عدم پشتیبانی پایانه های فروش از کلیه سیستم های پرداخت تمایل زیادی برای ایجاد یک سیستم پرداخت الکترونیک یکپارچه، که هزینه و ریسک مراودات را به شدت کاهش دهد، وجو دارد..به عنوان نمونه، بررسی که در German Bank آلمان صورت گرفت نشان می

دهد هزینه یک تبادل بانکی از طریق گیشه بانک به طور متوسط ۲ دلار می باشد در حالیکه ارائه همان خدمات از طریق شبکه بانکداری موبایلی تنها ۱۵ سنت هزینه در بر دارد.
از آنجایی که اطلاعات مهم در رابطه با هویت فرد و اطلاعات حساب بانکی او در داخل تراشه و درون تلفن همراه ذخیره می شود و تنها توسط دستگاه های خواننده NFC قابل بازیابی هستند و در هنگام بازیابی نیز توسط کلید خصوصی که در داخل گوشی همراه ذخیره شده است رمزنگاری می شود و به سمت مقصد ارسال می گردد تا حد بسیار زیادی امکان دستیابی افراد دیگر به این اطلاعات را کاهش داده است. همچنین برای امنیت بیشتر از ترکیب این روش با SIM کارت و PIN Code موجود در تلفن همراه استفاده می شود که بدلیل سرعت بالای برقراری ارتباط با دستگاه دیگر و انجام عملیات فرصت کافی برای سوء استفاده از اطلاعات را امکان پذیر نمی نماید همچنین در صورت سرقت گوشی همراه با وجود این تکنولوژی های رمزنگاری براحتی امکان رمزگشایی اطلاعات وجود نداشته و از آنجایی که بخشی از عملیات تائید هویت فرد با استفاده از SIM کارت و PIN Code او انجام می گیرد تنها با متوقف کردن SIM کارت تلفن همراه ربوده شده می توان تراشه NFC موجود در آن را برای همیشه از فعالیت باز داشت.
برای استفاده از کارت های Contact less در صورتیکه کاربر در بانک های مختلف دارای حساب باشد مجبور به حمل تعداد زیادی کارت های مختلف است و همچنینی باید چندین رمز مختلف را بخاطر بسپرد که بیشتر کاربران برای جلوگیری از فراموش کردن رمز خود یا آنها را یادداشت می کنند و یا اینکه برای تمامی کارت های خود از رمز یکسان استفاده می نمایند که این خود منجر به کاهش امنیت می گردد ولی در این تکنولوژی جدید می توان تمامی کارت های خود را در داخل یک تراشه NFC ذخیره نمود که در این صورت در تمامی زمان ها کاربر به تمامی حساب های خود دسترسی خواهد داشت و برای اینکه فرد دیگری بتواند از حساب او استفاده نماید ملزم به در اختیار داشتن گوشی همراه فرد، شماره PIN Code او، کلید خصوصی و SIM کارت او می باشد، بنابراین متوجه می شوید که این روش علاوه بر افزایش سهولت برای دسترسی به اطلاعات حساب های کاربر از امنیت بسیار بالایی نیز برخوردار می باشد.
رسیدن به روشی که دارای سهولت استفاده و امنیت اطلاعات بالا باشد چرا که بخش بسیار مهمی در این نوع تکنولوژی می باشد.
با استفاده از این تکنولوژی کاربر می تواند بصورت همزمان چندین نوع کارت یا Debit کارت را در تلفن همراه خود داشته باشد و بنا به نیاز خود بدون ایجاد هیچ اختلالی از آنها استفاده نماید که در این حالت تلفن همراه نقش یک کیف پول را بازی می کند و کاربر را بی نیاز از حمل دائمی تعداد زیادی کارت می نماید.

۲ - روش پیشنهادی ما

پروتکل روش پیشنهادی بـــر مبنـای جریـان پیام هـای موجود در پروتکـل پرداخت بی سیمِ امن پیشنهاد شده است [۴]. در این پروتکـل نیـز از مکـانیزم SSL، TLS و WTLS برای تامین نیازهای امنیتی از قبیل محرمانگی و جامعیت داده ها در حین انتقال استفاده می شود.
با بهینه سازی هایی که در پروتکل پیشنهادی صـورت گرفتـه تعـداد امضـاهای لازم جهـت تـامین ویژگی عدم انکار نسبت به پروتکـــل پرداخت بی سـیمِ امن کاهش یافته است. ویژگی اصلی این پروتکل این است که بدون ایجاد سربار اضافی در فرایند پرداخت، هویت مشتری در فراینـد خریـد کـالا و پرداخـت وجـه از فروشنده و بانک مخفی می ماند.
معماری، اجزاء اصلی و روند انجام پروتکل پیشنهادی در ۰بـه صـورت سـطح بـالا نشان داده شده است. این پروتکل از چهار عنصر کلیدی مشتری، فروشنده، بانک مشـتری و بانـک فروشنده تشکیل شده است. در سمت فروشنده، عامل فروشنده یک برنامه کاربردی مبتنـــی بـر وب ارائه می کند که روی سرور فروشنده اجرا می شود. مشتری از طریق دروازه WAP به ایـن

برنامه کاربردی دسترسی دارد. دروازه WAP محتوای HTML را به WML[1] تبدیل کرده و از پشته پروتکل WAP برای تعامل با دستگاه سیار مشتری استفاده می کند. در سمت مشتری، برنامه ای روی دستگاه سیار مشتری وجود دارد که عملیات ارسال و دریافت اطلاعات، رمزگذاری و سایر عملیات مربوط به پرداخت سیار را انجام می دهد. امنیت زیرساخت های بانکی فرض می شود که کافی بوده و خارج از بحث ما می باشد.



شکل ۱ - معماری پروتکل پیشنهادی

قبل از انجام پروتکل مراحل زیر باید انجام شده باشد:

مشتری ابتدا باید یک گواهینامه دیجیتال با نام مستعار برای خود تولید نماید. سپس در بانک خود یک حساب گمنام ایجاد کند. مشتری باید کلید عمومی خود را به این حساب پیوند دهد. به این منظور مشتری باید اثبات کند که صاحب کلید عمومی اش می باشد. به طریق زیر می توان به این هدف رسید:

پس از ایجاد حساب گمنام برای مشتری، بانک رمز مخفی KA و شماره حساب accA را به صورت امن برای وی ارسال می نماید. مشتری رمز KA را با کلید خصوصی اش امضا و با کلید عمومی بانک رمز نموده، به همراه گواهینامه گمنامش برای بانک می فرستد. بانک پیام را از حالت رمز خارج نموده و با کلید عمومی موجود در گواهینامه، امضای روی رمز KA را تایید اعتبار می کند. از آنجا که KA فقط در اختیار صاحب حساب قرار گرفته، بانک متوجه می شود که این گواهینامه متعلق به دارنده حساب گمنام مزبور می باشد، پس این گواهی را در بخش اطلاعات مربوط به آن حساب گمنام ثبت می نماید.

مشتری حساب خود را به صورت گمنام شارژ می کند تا برای پرداخت از آن استفاده نماید. این پروتکل از شش مرحله زیر تشکیل شده که در ادامه به شرح آنها می پردازیم.

۱- درخواست خرید کالا

۲- تایید درخواست مشتری

۳- درخواست پرداخت

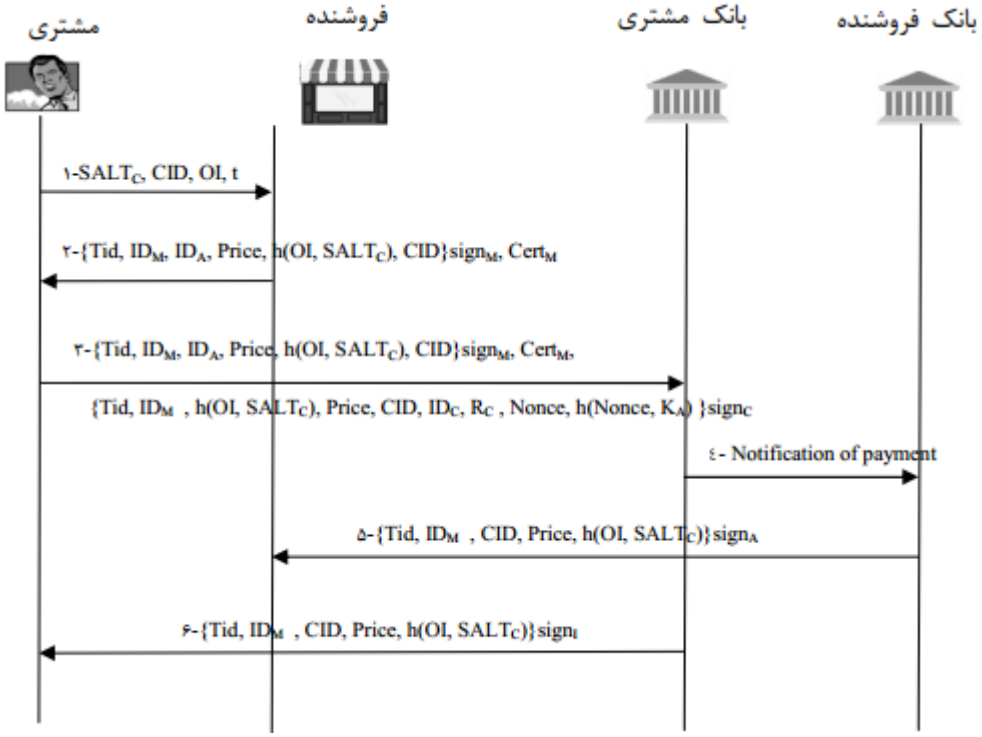
۴- تایید پرداخت و مبادله مالی

[1] Wireless Markup Language

۵- ارسال تاییدیه پرداخت به فروشنده

۶- ارسال رسید به مشتری

۰مراحل عبور پیغام ها و جزئیات تراکنش پرداخت در پروتکل پیشنهادی را نشـان می دهد.



شکل ۲ جریان تراکنش و پیغام ها در پروتکل پیشنهادی

پروتکل پیشنهادی جهت تامین تبادل منصفانه

در این پروتکل مسـائل دیگر یک سـیسـتم خرید الکترونیکی از قبیل اطمینان مشتری از دریافت کالا در قبال پرداخت وجه، اطمینان فروشـــنده از دریافت وجه در ازای تحو یل کالا و دریافت رســـید در قبال تحویل کالا به منظور جلوگیری از ادعای مشـتری مبنی بر عدم دریافت کالای صـحیح مورد بررسـی قرار نگرفته است. در این قسمت با توسعه پروتکل قبلی خودمان قصـد تامین ویژگی تبادل منصـفانه را داریم. بدین معنی که مشـتری باید مطمئن شود که در ازای پرداخت وجه حتما کالای مورد نظر خود را دریافت خواهد کرد. فروشنده نیز باید مطمئن شود که در قبال تحویل کالا وجه مورد نظر را دریافت می کند. به عبارتی در یک تراکنش یا هیچیک از طرفین چیزی دریافت نکنند و یا هر دو طرف خواسته خود را دریافت کنند. همچنین هیچیک از طرفین نباید قادر به انکار دریافت عنصر مورد نظر خود باشند. به این منظور مشتری باید رسید امضا شده ای مبنی بر پرداخت وجه به فروشـنده دریافت کند. فروشـنده نیز پس از تحویل کالا باید رسـید امضا شده ای مبنی بر تحویل کالا به مشـتری مورد نظر را دریافت کند. در این پروتکل از روش تبادل خوشبینانه[1] استفاده می شود. در چنین پروتکل هایی از یک شـخص ثالث مورد اعتماد کمک گرفته می شـود. نیازی نیسـت شـخص ثالث هنگام انجام تراکنش به صـورت برخط حضور داشـته باشـد بلکه تنها هنگام بروز اختلاف به این شخص ثالث جهت رفع اختلاف رجوع می شود. همچنین از ایده ارائه شده

[1] Optimistic Exchange Protocol

توسـط BaO جهت مبادله اطلاعات محرمانه و امضای روی آن، به منظور اطمینان فروشنده از دریافت رسید تحویل کالا به کار می رود [۱۲۴]. در ادامه پروتکل توسـعه یافته پیشـنهادی شـرح داده شـده و مورد تحلیل قرار می گیرد. فرض می کنیم مراحل زیر قبل از انجام تراکنش انجام شده است:

فروشـنده در یک قسـمت ثالث مورد اعتماد (TTP)[1] ثبت نام کرده است. فروشنده کالای m را به قسمت ثالث مورد اعتماد ارائـه می کنـد تا قسـمت ثالث آن را با کلید k رمزگذاری نموده و در یک مکان عمومی که ما آن را کاتالوگ می نامیم، به عنوان تبلیغ کالای m قرار دهد. زمانی که مشتری قصد خرید کالای m از فروشنده را دارد، باید [m, k] را از کاتالوگ دانلود کند. برای هر کالای m فروشـنده باید کالا را به همراه توصـیف آن و شـناسه مشخص کننده کالا برای قسمت ثالث ارسال نماید. قسـمت ثالث برای هر کالا یک کلید رمزنگاری k تولید کرده و آن را در اختیار فروشنده نیز قرار می دهد. قسمت ثالث قبل از قرار دادن کالا در کاتالوگ آن را توسـط کلید k رمزگذاری می کند. در این روش قسمت ثالث می تواند کالا را ارزیابی کرده و از تطابق آن با توصـیفی که برای آن ارائه شـده اطمینان یابد. جهت خرید کالا مشتری کالای رمز شده را از کاتالوگ قسـمت ثالث مورد اعتماد دانلود می کند، بنابراین می تواند از تطابق کالای رمز شده با توصیف آن مطمئن باشد، زیرا قسمت ثالث قبل از قرار دادن کالای رمز شده در کاتالوگ این مساله را بررسی نموده است.

مراحل انجام تراکنش

این پروتکل از ۱۰ مرحله زیر تشکیل شده که در ادامه شرح داده می شود:

درخواست خرید کالا.

تایید درخواست مشتری.

ایجاد و رمزگذاری رسید دریافت کالا.

امضای قرارداد تراکنش توسط فروشنده.

درخواست پرداخت.

تایید پرداخت و مبادله مالی.

ارسال رسید پرداخت به مشتری.

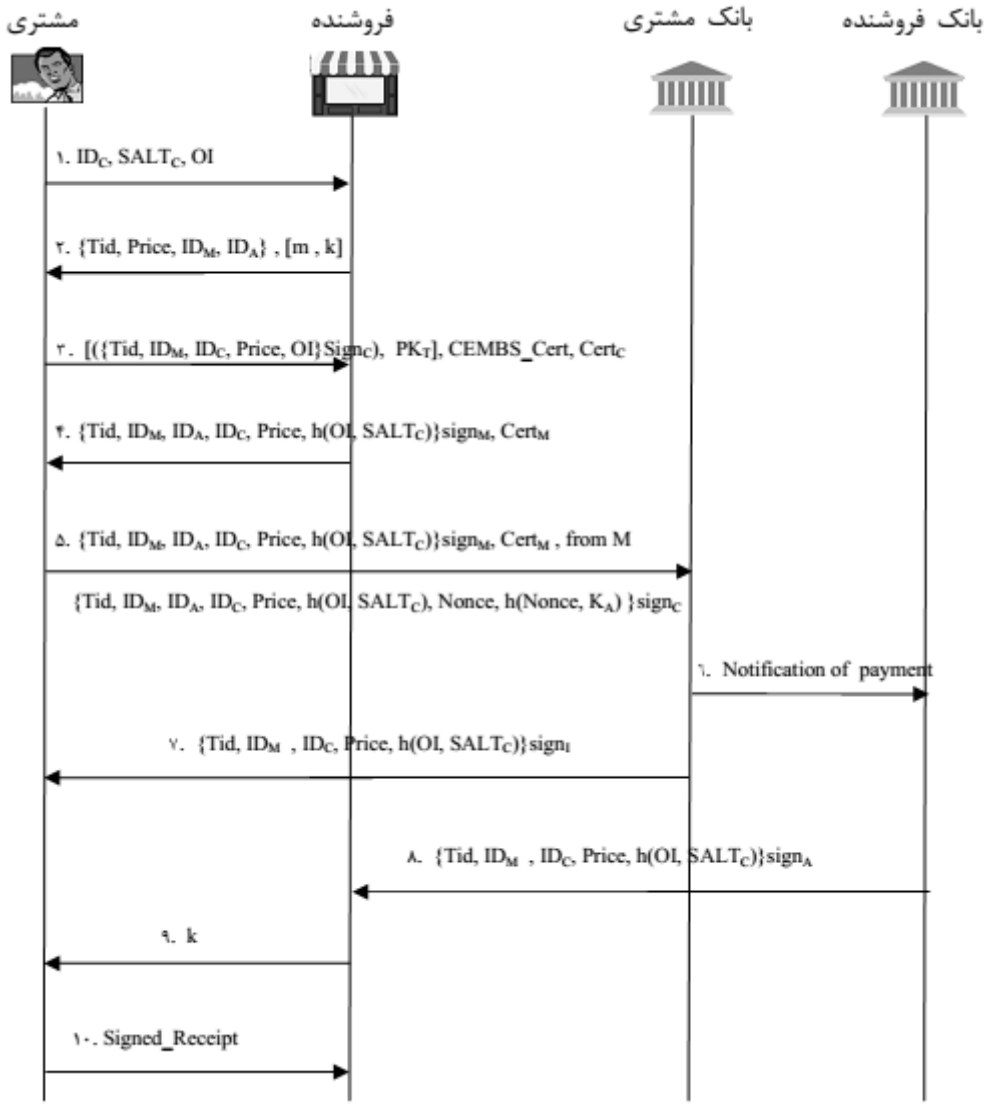
ارسال تاییدیه پرداخت به فروشنده.

تحویل کلید رمزگشایی کالا.

تحویل رسید دریافت کالا.

۰مراحل انجام پروتکل پیشنهادی منصفانه را در صورتیکه هیچیک از طرفین تخلفی انجام ندهد یا تراکنش را لغو نکند، نشان می دهد.

[1] Trusted Third Party



شکل ۳ جریان تراکنش و پیغام ها در پروتکل پیشنهادی منصفانه

در ۰ویژگی هـای امنیتـی پروتکل هـای پروتکـل پرداخت بی سیمِ امن، WPP، 3KP، SET و پروتکل پیشنهادی مورد مقایسه قـرار گرفتـه اسـت. همانگونـه کـه ملاحظـه مـی کنیـد، پروتکـل پیشنهادی تمام ویژگی های امنیتی مطلوب را فراهم می آورد.

جدول ۱- مقایسه ویژگی های امنیتی پروتکل های پرداخت بی سیمِ امن ، 3KP، WPP، SET و پروتکل پیشنهادی

ویژگی / پروتکل	محرمانگی	احراز هویت	جامعیت داده	انکار ناپذیری توسط مشتری	انکار ناپذیری توسط فروشنده	حفظ حریم خصوصی	گمنامی مشتری
SET	بله	بله	بله	بله	بله	بله	خیر
3KP	بله	بله	بله	بله	بله	بله	خیر
WPP	بله	بله	بله	بله	بله	بله	خیر
پروتکل پرداخت بی سیمِ امن	بله	بله	خیر	خیر	خیر	خیر	خیر
پروتکل پیشنهادی	بله	بله	بله	بله	بله	خیر	خیر

معیارهایی که در کارایی یک پروتکل موثر است عبارتند از: تعداد پیامهای مبادله شونده توسط هریک از نقشهای درگیر، تعداد عملیات رمزنگاری انجام شده و پهنای باند مورد نیاز که به تعداد و اندازه پیام ها بستگی دارد.
در ۰به مقایسه کارایی چند پروتکل از لحاظ سربار محاسباتی و ارتباطی پرداخته شده است.

جدول ۲- مقایسه کارایی پروتکل های پرداخت SET، 3KP، WPP، پروتکل پرداخت بی سیمِ امن و پروتکل پیشنهادی

عملیات / پروتکل	Publc-key encryption/decryption			Digital signiture/verification			Symmetric operation			Hash function			Communication overhead (number of messages)
	B	M	C	B	M	C	B	M	C	B	M	C	
SET	۳	۲	۱	۲	۵	۳	۱	۰	۱	۰	۲	۳	۹
3KP	۱	۴	۱	۳	۳	۴	۰	۰	۰	۱	۵	۲	۷
WPP	۲	۱	۱	۳	۱	۱	۰	۰	۰	۰	۰	۰	۷
پروتکل پرداخت بی سیمِ امن	۱	۱	۰	۵	۴	۴	۰	۰	۰	۰	۰	۰	۷
پروتکل پیشنهادی	۰	۰	۰	۴	۲	۲	۰	۰	۰	۵	۱	۳	۷

در جدول فوق علامت C بیانگر عملیات سمت مشتری، M عملیات سمت فروشنده و B بیانگر عملیات سمت بانک می باشد.

با توجه به ۰و همانگونه که در شرح پروتکل پیشنهادی نیز بیان شد، به دلیل بهینه سازی هایی که نسبت به پروتکل پرداخت بی سیمِ امن انجام شده نیازی نیست که فروشنده صورتحسابی را جداگانه امضا کند. این مساله باعث کاهش یک عمل امضا برای فروشنده و کاهش یک تاییـد امضا برای خریدار می شود. فروشنده در این پروتکل اطلاعات بانکی خود را از طریق کانال هـای ارتبـاطی مبادله نمی کند که این باعث کاهش یک عمل رمزنگاری نامتقارن در سمت فروشنده و کاهش یک عمل رمزگشایی نامتقارن در سمت بانک می شود. بنابراین در پروتکـل پیشـنهادی تعـداد عملیـات رمزنگاری نامتقارن ونیز تعداد عملیات امضا و تایید امضا نسبت به پروتکل های امـنِ SET و پروتکـل پرداخت بی سیمِ امن کاهش یافته است. تعداد عملیات امضای دیجیتال در این پروتکل نسبت به WPP افزایش یافته امـا در عوض تعداد عملیات رمزنگاری نامتقارن کاهش یافته است. در مجموع کارایی این پروتکل نسبت به پروتکل های امن بهبود یافته است.

۴– نتیجه گیری

پروتکل های پرداخت الکترونیکی امن و استاندارد فراوانی برای اینترنت وجود دارند، ولی محدودیت منابع در محیط سیار مانند هزینه بالا، نرخ انتقال و عرض باند پایین کانال ارتباطی، محدودیت ظرفیت های محاسباتی، محدودیت های باتری و حافظه دستگاه های سیار مانع اصلی استفاده مستقیم از پروتکل های موجود، در محیط سیار می باشد. به عبارت دیگر یک پروتکل جدید و مناسب برای محیط سیار لازم می باشد. به این منظور در این تحقیق تلاش شده پروتکلی ارائه گردد که علی رغم تامین ویژگی های امنیتی لازم، از کارایی قابل قبول برخوردار باشد. پروتکل پیشنهادی در این تحقیقی که پرداخت سیار گمنام و خصوصی نامیده شده بر پایه پروتکـل پرداخت بی سیمِ امن ارائه شده است. پروتکـل پرداخت بی سیمِ امن دارای ضعف های امنیتی شامل عدم حفظ حریم خصوصی و عدم گمنامی مشتری می باشد. در پروتکل پیشنهادی با استفاده از حساب بانکی گمنام و گواهینامه دیجیتالی با نام مستعار هویت واقعی مشتری مخفی می ماند. از توابع درهم سازی و شناسه های یکبار مصرف نیز برای حفظ حریم خصوصی مشتری استفاده می گردد.

اما در این پروتکل مسائل دیگر یک سیستم خرید الکترونیکی از قبیل اطمینان مشتری از دریافت کالا در قبال پرداخت وجه، اطمینان فروشنده از دریافت وجه در ازای تحویل کالا و دریافت رسید در قبال تحویل کالا به منظور جلوگیری از ادعای مشتری مبنی بر عدم دریافت کالای صحیح مورد بررسی قرار نگرفته است. در تراکنش های تجارت الکترونیک، مخصوصاً تراکنش هایی که شامل تبادل کالاهای الکترونیکی بین طرفین می باشد، نیازهای امنیتی مذکور نیز به چشم می خورد که در تراکنش های غیر الکترونیک وجود ندارد. در ادامه این تحقیق با توسعه پروتکل پرداخت سیار گمنام و خصوصی، ویژگی تبادل منصفانه تامین شده است که آن را پروتکلی تحت عنوان پروتکل تبادل منصفانه نام نهادیم. بدین معنی که در هر تراکنش مشتری مطمئن است که در ازای پرداخت وجه حتما کالای مورد نظر خود را دریافت خواهد کرد. فروشنده نیز اطمینان دارد که در قبال تحویل کالا، وجه مورد نظر و رسید تحویل کالا را دریافت می کند. همچنین هیچ یک از طرفین قادر به انکار دریافت عنصر مورد نظر خود نیستند. در این پروتکل توسعه یافته که از روش تبادل خوشبینانه استفاده می شود.

پروتکل های مزبور جهت بررسی میزان تامین ویژگی های امنیتی مورد تحلیل قرار گرفتند. همچنین میزان کارایی آنها بررسی و با دیگر پروتکل ها مقایسه شد. این پروتکل ها جهت بررسی میزان برآورده شدن اهداف امنیتی و مقاومت پروتکل در برابر آسیب پذیری های مختلف، توسط ابزار تحلیل رسمی Casper و FDR مورد ارزیابی قرار گرفتند. نتایج تحلیل بیانگر این است که پروتکل های مزبور کلیه ویژگی های امنیتی مورد انتظار را برآورده می نمایند.

۵- منابع

۱- سروش، الهه؛ هاشمی، محمود رضا. "پیشنهاد یک پروتکل پرداخت امن برای دستگاه های تلفن همراه." کنفرانس انجمن رمز ایران، دوره سوم، (۱۳۸۴): ۳-۸.

۲-دفتر توسعه تجارت الکترونیکی. "تجارت سیار". معاونت برنامه ریزی و امور اقتصادی، ویرایش دوم، (۱۳۸۴).

۳- گرمستانی، سمانه؛ بیات، نازیلا و حمیدی نوا، فاطمه. "بانکداری از طریق تلفن همراه در ایران: چالش ها، مزایا و زیرساخت ها". کنفرانس جهانی بانکداری الکترونیکی، دوره دوم (۱۳۸۷).

۴- احمدی، محمد حسین . "معرفی و تحلیل راهبردی کاربردهای سیار و فراگیر". دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف ، (۱۳۸۶).

[5[. Markus Mösenbacher. Preventing fraud in ePassports and eIDs Security Protocols for Today and Tomorrow. Technical Report 9397 750 17377. NXP Semiconductors. (2013).

[6].http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper.(۲۰۱۵)./

[7].https://www.cs.ox.ac.uk/projects/fdr/manual/command_line.html.(۲۰۱۵).

[8]. Payment news and resource center. "Statistics for Mobile Commerce ". October 20, www.ePaynews.com, (2016).

[9].Kungpisdan, Supakorn. Modelling, Design, and Analysis of Secure Mobile Payment Systems. Technology Monash University, (2005).

[10].O.Mahony, Donal; Peirce, Michael and Tewari, Hitesh. Electronic Payment Systems for E-Commerce. Norwood, ARTECH HOUSE, Second Edition, (2003).