دانشگاه قم

دانشکده فنی مهندسی

پایان نامه دوره کارشناسی ارشد تجارت الکترونیک

عنوان:

ارائه یک پروتکل پرداخت سیار منصفانه

استاد راهنما:

آقای دکتر یعقوب فرجامی

استاد مشاور:

آقای دکتر مهدی شجری

نگارنده:

میلاد علی قندی دزفولی

شهریور ۱۳۸۹

تقدیم به :

پدر و مادرعزیزم؛ آموزگارانی که برایم زندگی؛ بودن و انسان بودن را معنا کردند

و همسر مهربانم، مژده، که همراه من در تمام لحظات زندگی است

تشکر و قدردانی:

حمد و سپاس خدای را که توفیق کسب دانش و معرفت را به ما عطا فرمود. در اینجا لازم می‌دانم از اساتید بزرگوار به ویژه اساتید دوره کارشناسی ارشد که در سالیان گذشته مرا در تحصیل علم و معرفت و فضائل اخلاقی یاری نمودند تشکر و قدر دانی کنم.

از استاد گرامی و بزرگوار جناب آقای دکتر یعقوب فرجامی که راهنمایی اینجانب را درانجام تحقیق و پژوهش و نگارش این پایان نامه تقبل نمودند نهایت تشکر و قدر دانی را دارم.

از جناب آقای دکتر مهدی شجری به عنوان مشاور که با راهنمایی خود مرا مورد لطف قرار دادند کمال تشکر را دارم.

چکیده:

بیطرفی یک خصوصیت حیاتی برای تجارت الکترونیک است. این بدین معنی است که در پایان مبادله هر دو طرف کالای طرف دیگر را دریافت می‌کنند و یا هیچ‌کدام چیزی دریافت نکنند. به‌طور تدریجی هدف پژوهش حذف ضعف‌ها است که با جمع‌آوری شواهد در طول اجرای پروتکل که با استفاده از یک طرف صادق بتوان مورد را ثابت کرد. در کل، پروتکل‌های مبادله منصفانه به قابلیتهای دسترسی مداوم به یک طرف سوم مورد اطمینان خارجی نیاز دارند. یک سایت مخصوص که مورد اطمینان طرفین شرکت‌کننده باشد. بیشتر پروتکلهای پرداخت الکترونیکی موجود از یک TTP برخط/ غیر برخط یا طرف سوم تا حدی مطمئن برای اطمینان از بی‌طرفی یک تراکنش استفاده می‌کنند که در این صورت معایبی وجود دارد: اولا طرف سوم حتما گلوگاه یک تراکنش می‌شود و منجر به انبوهی شبکه می‌شود. ثانیا TTP باعث کاهش کارایی پروتکل در حال اجرا و افزایش هزینه یک تراکنش می‌شود. و در آخر اینکه در هر زمانی جستجوی یک طرف سوم به عنوان TTP خیلی آسان نیست.اگر ما بتوانیم یک پروتکل بدون TTP طراحی کنیم تمام این مشکلات حل خواهد شد.

کلمات کلیدی: پروتکل پرداخت سیار، امضاهای همزمان، بی‌طرفی، انکارناپذیری، طرف سوم مورد اعتماد

فهرست مطالب

فهرست اشکال

فهرست جداول

فهرست علائم و اختصارات

C	Customer
CA	Certificate Athority
CAN	Customer Account Number
CCI	Credit Card Information
CDC	Connected Device Configuration
CDMA	Code Division Multiple Access
Cert	Certification
DESC	Description
EPO	Electronic Payment Order
ENC	Encryption
ETSI	European Telecommunications Standards Institute
EXP	Expiry
GSM	Global System for Mobile communications
GPRS	General Packet Radio System
HSCSD	High Speed Circuit Switched Data
IKP	I Key Protocol
J2ME	Java2 Micro Edition
NTT	Nippon Telegraph & Telephone
M	Merchant
MA	Merchant Agent
MAC	Message Authentication Code
MBI	Merchant Banking Information
OI	Order Information
PAM	Personal Assurance Massage
PDA	Personal Data Assistants
PG	Payment Gateway
PI	Payment Information
PK	Public Key
PSG	Public Signature Generator
SDMA	Space Division Multiple Access
SET	Secure Electronic Transaction
Sign	Signature

SIM	Subscriber Identity Module
SMS	Short Message Service
SSL	Secure Socket Layer
SWPP	Secure Wireless Payment Protocol
TID	Transaction Identification
TTP	Trusted Third Party
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WML	Wireless Markup Language
WPP	Wireless Payment Protocol
WTLS	Wireless Transport Layer Security

فصل اول:

مقدمه

فصل اول: مقدمه

۱– ۱ مقدمه

پیشرفت فناوری و توسعه فناوری‌های سیار منجر به شکل‌گیری نوع جدیدی از تجارت الکترونیکی تحت عنوان تجارت سیار شده‌است. در این نوع تجارت ارتباطات به‌صورت سریع و بی‌سیم[1]صورت می‌گیرد. تجارت سیار عبارت است از خرید و فروش کالاها و خدمات با استفاده از وسایل بی‌سیمی از قبیل تلفن‌های همراه یا کمک داده‌های شخصی[2]. با وجود آنکه هنوز بسیاری از سئوالات و ابهامات فنی، تجاری و قانونی در زمینه تجارت سیار باقی مانده است اما امتیازات منحصر به فرد این پدیده منجر به رشد سریع بکارگیری ابزارهای همراه در مبادلات تجاری و به تبع آن بازاریابی کالاها و خدمات، حتی در کشورهای در حال توسعه شده‌است، به گونه‌ای که در بسیاری از کشورهای در حال توسعه تجارت سیار به عنوان گزینه‌ای برای تسهیلات مخابراتی در نظر گرفته شده‌است. با رشد ضریب نفوذ تلفن همراه و توسعه تجارت سیار، پرداخت سیار یک نیاز اجتناب ناپذیر برای پرداخت هزینهٔ کالاها و خدمات خواهد بود. این امر مستلزم پیاده‌سازی پروتکل‌های بی سیمی است که بتواند مکانیزم‌های پرداخت از راه دور را به خوبی روشهای رودررو با استفاده از یک دستگاه واحد مدیریت نماید.

مشتریان همواره علاقمند به استفاده از روشهای ساده، سریع، شخصی، امن و قابل استفاده در هر مکان و زمان هستند و دستگاه‌های سیار بدلیل راحتی استفاده، بلادرنگ بودن، عدم نیاز به پول نقد جانشین خوبی می‌باشند. البته نباید ریسک‌ها و مشکلات امنیتی خاص این محیط را نادیده گرفت. براساس تحقیقات انجام شده توسط Forrester، مسائل امنیتی مانع اصلی برای حدود ۵۲ درصد کسانی است که هیچ نوع تراکنش تجاری با تلفنهای همراه انجام نمی‌دهند. امن کردن اطلاعات پرداخت روی اینترنت و شبکه تلفن همراه کار پرزحمت ولی ممکنی است. با دقت کافی، توجه به جزئیات، انتخاب و استفاده از ابزارهای مناسب می‌توان

[1].Wireless Communication
[2].Personal Data Assistants (PDA)

حریم‌های خصوصی و یکپارچگی را هم برای داده‌های مشتریان و هم برای سایر داده‌هـا فـراهم نمود. همیشه باید توجه داشت که هر راه‌حل امنیتی نیاز به توجه و نظارت دایمی دارد.

۱–۲ ضرورت ارائه پروتکل پرداخت سیار با ویژگی انصاف:

تجارت سیار نیز بدون یک محیط امن میسر نیست. در یک سناریوی پرداخت سیار، چالش‌های امنیتی متفاوتی وجود دارد. پرداخت سیار، برای جلب اطمینان خریداران، فروشندگان و اپراتورهای شبکه باید امین باشد. این خدمات از زیرساخت موجود شبکه‌های اپراتورها استفاده می‌کنند. قسمت مهمی از این شبکه‌ها واسط‌های رادیویی هستند که ارتباط شبکه ثابت با دستگاه‌های بیسیم را با کمک آنتن‌ها فراهم می‌نمایند.

در عین حال اطلاعات محرمانه کاربر، موجود در دستگاه تلفن همراه و خود دستگاه باید در مقابل استفاده غیر مجاز محافظت شوند.

یکی از موارد امنیتی که از حقوق مشتریان و فروشندگان محافظت می‌کند ویژگی انصاف در پرداخت سیار می‌باشد. یک پروتکل منصفانه به تمام افراد تضمینی برای بی‌طرفی ارائه می‌دهد که پروتکل به‌طور درست اجرا خواهد شد ولی همیشه این مهم امکان‌پذیر و یا مقرون به صرفه نیست. اگر بعضی از افراد (بازیگران) بعد از اجرای پروتکل متضرر شوند، می‌توان با اجرای مرحله حل و فصل مجادله[1]، بی‌طرفی را به آنها برگرداند. بنابراین یک پروتکل باید به اندازه کافی در کل اجرای مراحل برای درستکاری بازیگران دلیل و مدرک جمع‌آوری کند که بازیگران درستکار در مرحله حل و فصل برنده باشند.

با توجه به اهمیت موضوع انصاف، در این پژوهش سعی شده‌است که روش پرداختی ارائه شود که علاوه بر ویژگی‌های امنیتی استاندارد دارای ویژگی انصاف نیز باشد.

۱–۳ اهداف پژوهش:

با توجه به مطالب بیان شده اهداف کلی که در این پژوهش پیگیری می‌شود به شرح زیر می‌باشد:

[1] Dispute

- بررسی سیستم‌های پرداخت سیار و خصوصیت آنها
- آشنایی با زیرساخت‌های پرداخت سیار
- بررسی مسایل امنیتی در زیرساختهای سیار
- آشنایی با انواع مبادلات منصفانه و ویژگی‌های آنها
- ارایه یک روش پرداخت سیار منصفانه
- تحلیل و بررسی ویژگی‌های امنیتی در روش ارایه شده

در فصل دوم مروری بر ادبیات پژوهش و آشنایی با زیرساخت‌های سیار و مفهوم مبادلات منصفانه و انواع آنها است. سیستم‌های پرداخت الکترونیکی و سیار در فصل سوم بطور کامل مورد بررسی قرار خواهد گرفت. فصل چهارم با تمرکز برروی مسایل امنیتی ابتدا مدل‌های امنیتی در پرداخت‌های بی‌سیم بررسی می‌شود و سپس با اضافه کردن ویژگی و خصوصیت انصاف به یکی از آن مدلها یک روش پرداخت سیار منصفانه ارایه خواهیم کرد. در فصل پنجم اپتدا درستی و اعتبار مدل پیشنهادی را بررسی می‌کنیم و سپس میزان منابع مورد استفاده را بررسی خواهیم کرد. در نهایت نیز با ارایه پیشنهاداتی سعی در پیشرفت این حوزه از پرداخت خواهیم داشت.

فصل دوم:

مروری بر ادبیات تجارت سیار

فصل دوم: مروری بر ادبیات تجارت سیار

۲–۱ تکنولوژی‌های شبکه سیار:

شبکه موبایل از فنآوری مبتنی برسیستم آنالوگ به سیستم دیجیتال و سوئیچینگ مداری[۱] به سوئیچینگ‌های بسته ای[۲] تغییر پیدا کرده‌است. این تحولات را می‌توان توسط نسل‌های مختلف فن آوری موبایل شرح داد؛ نسل‌های مختلف این فنآوری عبارتند از:

- نسل اول (1G)
- نسل دوم (2G , 2.5G)
- نسل سوم (3G)

در این بین تنها نسل اول براساس سیستم‌های آنالوگ می‌باشد[33]. تعدادی از استانداردهای اصلی در هر یک از نسل‌های عبارتند از:

1G: AMPS[۳]، TACS[۴]، NTT[۵]، CDAMONE[۶]

2G: GSM[۷]، CDMA2000[۸]، HSCSD[۹]

2.5G: GPRS[۱۰]، EDGE[۱۱]

3G: UMTS[۱]

---

[4] Circuit switching
[5] Packet switch
[3] Advance Mobile Phone System
[4] Total Access Communication System
[5] Nippon Telegraph & Telephone
[6] Code Division Multiple Access One
[7] Global System for Mobile Communication
[8] Code Division Multiple Access 2000
[9] High Speed Circuit Switched Data Technology
[10] General Packet Radio System
[11] Enhanced Data Rate for GSM Evolution

: GSM.آ

سیستم جهانی برای ارتباطات سیار (GSM)، یک استاندارد نسل دوم برای ارتباطات سیار است که توسط ETSI (موسسه استانداردهای ارتباطی اروپا[2])توسعه داده شده‌است. این تکنولوژی درباند فرکانس900MHz تا 1800MHz کار می‌کند. GSM گسترده‌ترین استاندارد موبایل است که در اروپا و آسیا استفاده می‌شود. GSM برخلاف سیستم‌های سلولی آنالوگ قبلی نظیر AMPS , TACS برای استفاده از تکنولوژی‌های دیجیتالی طراحی شده‌است. GSM ترکیبی از TDMA , FDMA می‌باشد که اصولاً برای کنترل مخابره کردن صوت می‌باشد. به‌دلیل اینکه تمام کاربران باید از یک طیف رادیویی محدود استفاده کنند، تکنیک‌های زیر پهنای‌باند را بین تمام کاربران ممکن تقسیم می‌کند.[33]

: SDMA[3] برای تقسیم پهنای‌باند به مجموعه ای از ایستگاه‌های پایه‌ای که هر کدام یک منطقه محدود را پوشش می‌دهند، استفاده می‌شود.

FDMA[4]: فرکانس رادیوئی را به چندین حامل فرکانسی 200 Hz تقسیم می‌کند.

TDMA[5]: می‌تواند با تقسیم زمانی هر کدام از حامل فرکانسی 200 Hz را به 8 کانال تقسیم کند.

- سرویس‌های GSM:

- *Teleservice*: سرویس‌های ارتباطی می‌توانند به سرویس‌های حامل[6]، خدمات مخابراتی و سرویس‌های مکمل[7] تقسیم شوند، بیشترین سرویس ارتباطی پشتیبانی شده توسط GSM، تلفن می‌باشد.
- *سرویس‌های داده:*
  - سرویس‌های اینترنت[8]: کاربران GSM می‌توانند داده‌ها را با نرخ 9.6 kbps ارسال و دریافت کنند.
  - سرویس پیام کوتاه[9] SMS :GSMیک تکنولوژی منحصر به‌فرد برای GSM است که می‌تواند یک پیغام الفبا عددی تا ۱۶۰بایت را ارسال و دریافت کند.
  - Facsimile: ارسال و دریافت فکس توسط گوشی‌های GSM و لپ تاپ.

---

[1] Universal Mobile Telephone Standard
[2] European Telecommunications Standards Institute
[3] Space Division Multiple Access
[4] Frequency Division Multiple Access
[5] Time Division Multiple Access
[6] bearer services
[7] supplementary services
[8] Internet Services
[9] Short Messaging Service