
بسم الله الرحمن الرحيم

دانشگاه غیرانتفاعی شیخ بهایی

دانشکده فنی و مهندسی

پایان‌نامه‌ی کارشناسی ارشد رشته مهندسی کامپیوتر گرایش نرم‌افزار

ارائه راه‌حلی امن جهت حفظ محرمانگی مکان و هویت اعضا در شبکه‌های اجتماعی سیار

پژوهشگر

لیلا کاویانپور اصفهانی

استاد راهنما

دکتر احمد براآنی دستجردی

شهریورماه ۱۳۹۲

تقدیم به:

پدرم، که عالمانه به من آموخت تا چگونه در عرصه زندگی ایستادگی را تجربه نمایم

و به مادرم، دریای بی کران فداکاری و عشق که وجودم برایش همه رنج بود و وجودش برایم همه مهر

و به همسرم، اسطوره زندگیم، پناه خستگیم و امید بودنم.

از استاد گرامیم جناب آقای دکتر احمد براآنی بسیار سپاسگذارم چرا که بدون راهنماییهای ایشان تامین این پایان نامه بسیار مشکل مینمود.

از سرکار خانم مائده عاشوری به دلیل یاریها و راهنماییهای بی چشمداشت ایشان که بسیاری از سختیها را برایم آسانتر نمودند،

و سپاس بی‌دریغ از پدر ومادر و همسر عزیزم که همواره چراغ وجودشان روشنگر راه من در سختی ها و مشکلات بوده است.

چکیده

شبکه‌های اجتماعی رشد سریعی در دهه‌ی گذشته داشته‌اند. به علاوه بانفوذ دستگاه‌های قابل‌حمل که به شبکه دسترسی دارند و افزایش شدید استفاده از گوشی‌های همراه که مجهز به تجهیزات بی‌سیم با سیستم موقعیت‌یاب جغرافیایی هستند و می‌توانند به اینترنت متصل شوند نه تنها مردم قادرند به اطلاعات موجود در شبکه‌های اجتماعی خود در هر جا و هر زمان دسترسی داشته باشند، بلکه باعث به وجود آمدن بی‌شماری از سرویس‌های کاربردی مبتنی بر مکان در شبکه‌های اجتماعی سیار شده است. گسترش این سرویس‌ها می‌تواند سبب به خطر افتادن حفظ حریم خصوصی کاربران شود.

یکی از مشکلات اساسی در شبکه‌های اجتماعی سیار این است که کاربران تمایل ندارند مکان دقیق آن‌ها برای افراد ناشناس یا گروه‌ها و یا حتی بعضی از دوستانشان مشخص شود. در این شبکه‌ها کاربران باید به یک سرور مرکزی اعتماد کنند و اطلاعات شخصی موجود در شبکه‌های اجتماعی و موقعیت خود را برای این سرورها فاش کنند؛ اما کاربران دوست ندارند اطلاعاتشان حتی در یک سرور هم نگه داشته شود. شبکه‌های اجتماعی سیار به زمینه تحقیقاتی فعالی در طی چند سال اخیر تبدیل شده‌اند و در نتیجه این تحقیقات سیستم‌های متنوعی پیشنهاد شده‌اند. اغلب این سیستم‌ها و راه‌حل‌های پیشنهادی دارای محرمانگی و انعطاف‌پذیری کمی هستند یا پیاده‌سازی آن‌ها در دنیای واقعی غیرعملی و بسیار دشوار است. پیاده‌سازی یک ثالث معتمد امن در دنیای واقعی بسیار دشوار است. وجود تعداد زیادی سرور ناامن در دنیا که خدمات مختلفی ارائه می‌دهند، باعث افزایش ریسک اطلاعات مکانی کاربران شده است.

در این پژوهش راه‌حلی امن و مؤثر برای حفظ محرمانگی موقعیت کاربران شبکه‌های اجتماعی سیار ارائه شده است. هدف جلوگیری از افشا شدن مکان کاربر برای سرویس‌دهنده‌ی خدمت آگاه از موقعیت یا هر شخص ثالث معتمد دیگری، بر اساس تکنیک نادقیق‌سازی موقعیت است. الگوریتم EDA با این ساختار ارائه شده است ولی دارای مشکلاتی است:۱- مشکل بزرگ این است که همسایگان کاربر امن در نظر گرفته شده‌اند. ۲- سیستم آگاهی از محیط پیرامون ندارد و اگر مهاجم شناختی از اطراف داشته باشد می‌تواند مکان دقیق کاربر را در ناحیه‌ی نادقیق حدس بزند. ۳-معمولاً کاربر در مرکز ناحیه‌ی نادقیق قرار می‌گیرد. با توجه به محیط شبکه‌های اجتماعی سیار هیچ موجودیتی در این راه‌حل امن در نظر گرفته نشده است. راه‌حل ارائه‌شده LATEDA نام‌گذاری شده است که کاربران را قادر می‌سازد با یک روش نظیربه‌نظیر و بدون نیاز به یک سرور متمرکز ناحیه‌ی نادقیق بسازند و آن را به جای مکان واقعی به سرور بفرستند.

واژگان کلیدی: حریم خصوصی موقعیت، شبکه‌های اجتماعی سیار، خدمات مبتنی بر موقعیت، شبکه‌های نظیر به نظیر موبایل، نادقیق‌سازی موقعیت

Keywords: location privacy preserving, mobile social networks, location-based services, mobile peer to peer networks, spatial cloaking

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فصل اول

مقدمه

۱-۱- مقدمه‌ای بر حریم خصوصی در خدمات مبتنی بر موقعیت

در دهه‌های اخیر ارتباطات موبایل و فناوری اینترنت، در کنار یکدیگر به دو زمینه تحقیقاتی مهم تبدیل شده‌اند. راه‌حل‌ها و محصولات ارائه‌شده جهت حل چالش‌های موجود در این زمینه، تأثیر شگرفی بر شیوه‌های ارتباطی افراد و سبک زندگی آن‌ها داشته است. امروزه تحقیقات به سمت ادغام این دو فناوری پیش می‌رود به گونه‌ای که ایده‌ی محاسبات همه‌جا حاضر[1] در حال تحقق است؛ به این معنی که افراد قادر باشند اطلاعات مطلوب خود را به صورت حاضر در همه جا و نافذ دریافت کنند. برای مثال در هر مکانی و در هر زمانی اطلاعات مورد نظر خود را دریافت کنند [۱].

امروزه کاربران نه تنها قادرند خدمات اینترنت را روی شبکه‌های بی‌سیم دریافت کنند، بلکه این خدمات با توجه به اطلاعات زمینه[2] و محیط جاری قابل سفارشی شدن است؛ به عبارت دیگر افراد می‌توانند با توجه به وضعیت و

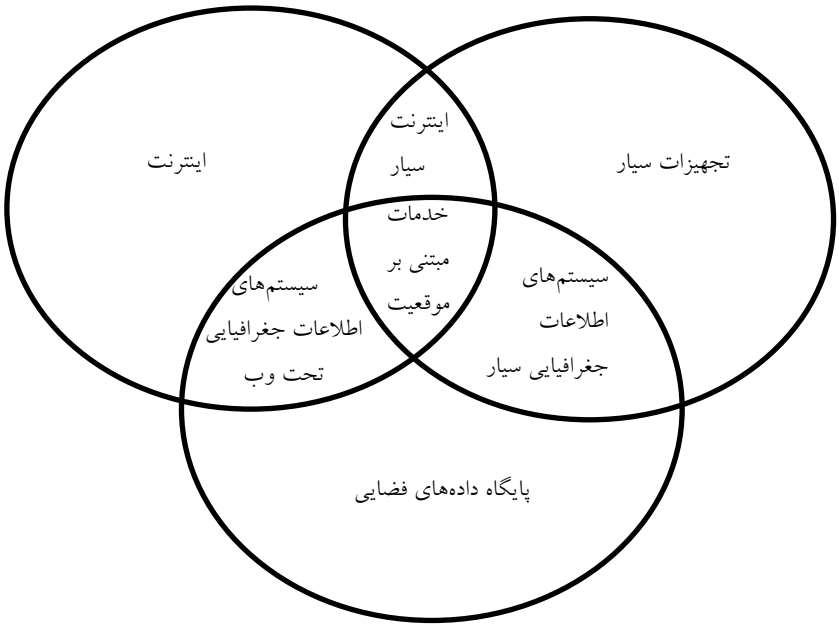
[1] Ubiquitous computing
[2] Context

ترجیحات فعلی خود، اطلاعات سفارشی شده را دریافت کنند. این‌گونه خدمات و کاربردها را خدمات آگاه به زمینه[۱] می‌نامند [۲]. اطلاعات زمینه هر نوع اطلاعاتی است که بتواند وضعیت یک فرد یا گروهی از افراد یا مکان یا شیئی که مرتبط با تعامل یک فرد با یک کاربرد یا خدمت است را مشخص می‌کند. برای مثال موقعیت کاربر[۲]، زمان، افراد مجاور کاربر[۳] و فعالیت کاربر نمونه‌هایی از اطلاعات زمینه هستند.

خدمات مبتنی بر مکان [۴] یکی از زمینه‌های بارز شبکه‌های اجتماعی سیار است که در شبکه‌های اجتماعی سنتی وجود ندارد. یک سرویس مبتنی بر مکان اطلاعاتی راجع به محل دستگاه موبایل در اختیار می‌گذارد و این اطلاعات همراه با اطلاعاتی که از شبکه اجتماعی به دست می‌آید برای کاربران شبکه‌های اجتماعی سیار خدماتی نظیر یافتن مکان دوستان، دوست‌یابی[۵] ، یافتن نزدیک‌ترین بانک یا رستوران،تبلیغات محلی و بازی‌های محلی فراهم می‌نماید.

یکی از پرکاربردترین انواع خدمات آگاه به زمینه، سرویس‌ها یا خدمات مبتنی بر موقعیت[۶] هستند. همان‌گونه که در شکل ۱-۱ نشان داده شده است [۳]. این‌گونه خدمات حاصل ادغام سه فناوری اینترنت، پایگاه داده‌های جغرافیایی[۷] و تجهیزات سیار[۸] است. پایگاه داده‌های جغرافیایی در سرویس‌دهنده‌های آگاه به موقعیت شامل مختصات یک سری نقاط جغرافیایی است که بر اساس موقعیت فعلی کاربر نقاط درخواست شده را به وی تحویل می‌دهد.

[1] Context-aware services
[2] Location
[3] Nearby people
[4] Location Based Service(LBS)
[5] Friends locator
[6] Location based services
[7] Spatial databases
[8] Mobile



شکل ۱-۱: همگرایی سه فناوری و خلق خدمات مبتنی بر موقعیت

انواع خدمات آگاه به موقعیت عبارتند از [۳] :

- خدمات جهت‌یابی[۱]
- خدمات هشدار ترافیک و وضعیت آب و هوایی[۲] مانند خدمت یافتن تعداد ماشین‌های فعلی موجود در بزرگراه یا اندازه‌ی تقریبی فاصله زمانی تا مقصد
- خدمات اطلاعات مجاور[۳] مانند خدمت یافتن نزدیک‌ترین رستوران یا پمپ‌بنزین به مکان فعلی کاربر و یا خدمت یافتن مشخصات رستوران‌هایی در فاصله‌ی معینی از کاربر
- خدمات حوادث اضطراری[۴]
- خدمات یافتن دوستان مجاور[۵]
- خدمات یافتن کودکان یا والدین سالخورده

[1] Navigation services
[2] Location-based traffic and weather alerts
[3] Nearby- information services
[4] Emergercy management services
[5] Nearby-friends services

- خدمات راهنمایی گردشگران
- تبلیغات مبتنی بر موقعیت مانند ارسال قهوه‌ی الکترونیکی برای همه‌ی مشتریان در فاصله‌ی پنج مایلی از فروشگاه کاربر

ازدیاد استفاده از خدمات آگاه به موقعیت، اگرچه منجر به تحقق ایده‌ی محاسبات حاضر در همه جا شده است، ولی باعث خلق مسائل و مشکلات جدیدی در زمینه‌ی امنیت و محافظت حریم خصوصی نیز شده است. مسئله‌ی اساسی در این میان این مطلب است که هر فناوری جدید به رغم مزایا و امکاناتی که به ارمغان می‌آورد، خطرات و تهدیدهای جدیدی را نیز معرفی می‌کند. گاهی سرعت ظهور تهدیدهای جدید بسیار بیشتر از سرعت تطبیق مکانیزم‌ها و راه‌حل‌های قانونی است. برای مثال خلق خدمات آگاه به موقعیت و کاهش هزینه جمع‌آوری اطلاعات کاربران در شبکه‌های موبایل، باعث آسان شدن فرآیند اشتراک دسته‌ی وسیعی از داده‌های خصوصی افراد شده است، به گونه‌ای که دامنه‌ی حریم خصوصی افراد را مورد تعرض قرار می‌دهد.

بنابراین اگرچه خلق خدمات آگاه به موقعیت باعث آسان شدن شیوه‌ی زندگی می‌شود، اما درعین‌حال می‌تواند باعث خلق خطرات جدی در حوزه‌ی حریم خصوصی افراد نیز شود. تعاریف مختلفی از حریم خصوصی ارائه شده است، در مرتبط‌ترین تعریف حریم خصوصی به صورت زیر تعریف می‌شود [۴]:

امتیاز و قدرت فرد یا گروهی از افراد یا موسسه در تعیین اینکه چه زمانی، چگونه و به چه میزانی اطلاعات خصوصی آن‌ها با دیگران مبادله شود، حریم خصوصی نامیده می‌شود.

در دسته‌بندی پینگلی [۳] حریم خصوصی در چهار گروه تقسیم‌بندی می‌شود:

- حریم خصوصی اطلاعات[1]
- حریم خصوصی جسمانی[2]

[1] Information privacy
[2] Bodily privacy

- حریم خصوصی ارتباطات[1]
- حریم خصوصی ارضی یا اقلیمی[2]

حریم خصوصی موقعیت نوع خاصی از حریم خصوصی اطلاعات است که به صورت زیر تعریف می‌شود [۳] :

امتیاز و قدرت کاربران در ممانعت و اجتناب دیگران از یادگیری و کشف موقعیت جاری و یا گذشته‌ی آن‌ها را حریم خصوصی موقعیت می‌نامند.

در رابطه با خدمات آگاه به موقعیت می‌توان گفت، استفاده از این خدمات نیاز به افشای بخشی از اطلاعات خصوصی کاربران در مورد موقعیت آن‌ها خواهد داشت؛ بنابراین کاربران این‌گونه خدمات، نگران چگونگی استفاده‌ی تأمین‌کنندگان خدمت از اطلاعات خصوصی خود هستند و این امر منجر به رد کردن این‌گونه خدمات از سوی کاربران می‌شود [۳].

فرض کنید یک کاربر قصد یافتن نزدیک‌ترین رستوران به موقعیت فعلی خود را دارد. او می‌تواند موقعیت خود به همراه پرس‌وجوی نزدیک‌ترین همسایگی[3] شامل یافتن نزدیک‌ترین رستوران را برای یک سرویس‌دهنده‌ی آگاه به موقعیت ارسال کند. در این سناریو مسئله‌ی امنیتی، حفاظت از موقعیت کاربر از دید سرویس‌دهنده است.

می‌توان از شبکه‌های اجتماعی سیار نیز برای ارتقا سرویس‌های مبتنی بر مکان استفاده کرد. در منبع [۵] یک سرویس مبتنی بر مکان بر اساس ارتباطات در شبکه‌های اجتماعی سیار ساخته می‌شود.

معمولاً در خدمات مبتنی بر مکان دو دیدگاه امنیتی وجود دارد:۱-امنیت مکان: که فرض می‌شود بخش سوم قابل‌اعتماد، هویت شخص را می‌داند اما از مکان دقیق وی اطلاع ندارد[۶] ۲-امنیت هویت: که در آن انتشار مکان کاربر نباید هویت او را فاش کند. برخی از راه‌حل‌های پیشنهادی ترکیبی از هر دو دیدگاه مذکور را به کار می‌برند و هدفشان این است که هم امنیت هویت و هم امنیت مکان را حفظ کنند[۷].

[1] Privacy of communication
[2] Territorial privacy
[3] Nearest Neighbor (NN) query

از آنجایی که مکان در شبکه‌های اجتماعی سیار برای پیدا کردن و ایجاد ارتباط با رویدادها، دوستان و موقعیت‌های شغلی مجاور نقش مهمی را ایفا می‌کند امنیت مکان به یک چالش مهم تبدیل شده است. مطالعات متعددی در این زمینه انجام شده است[۸، ۹] و محققان تلاش کرده‌اند راهنماهای مهمی را در زمینه چالش‌های محرمانگی مکان کاربر ایجاد کنند[۱۰] اما با این وجود اینکه چگونه محرمانگی مکان در برنامه‌های کاربردی به خصوص شبکه‌های اجتماعی سیار حفظ شود هنوز مبهم است[۱۱].

۱-۲- مسئله‌ی مورد پژوهش و اهمیت آن

در این تحقیق کاربرانی که عضو شبکه اجتماعی سیار هستند و هر یک مجهز به یکی از تجهیزات بی‌سیم با سیستم موقعیت‌یاب جغرافیایی هستند، در نظر گرفته شده است. این تجهیزات امکان برقراری ارتباط اینترنتی را فراهم می‌کنند. در این مجموعه کاربری خواهان دریافت خدمتی از یک سرویس‌دهنده‌ی خدمت آگاه به موقعیت است. حال در این پژوهش سعی بر این است که سطوح مختلف حریم خصوصی موقعیت برای فرد درخواست دهنده‌ی خدمت بررسی‌شده و سازوکارهای مناسب برای حفاظت از کاربران در هنگام استفاده از خدمات آگاه به موقعیت ارائه شود.

وجود تعداد زیادی سرور ناامن در دنیا که خدمات مختلفی ارائه می‌دهند، باعث افزایش ریسک اطلاعات مکانی کاربران شده است [۱۲].

در زمینه محافظت از حریم خصوصی موقعیت تاکنون فعالیت‌های زیادی انجام شده است [۱۳]. یک راه برای مشکلات امنیتی و حفظ محرمانگی استفاده از قابلیت‌های یک شخص ثالث معتمد[1] است که اطلاعات کاربران را جمع‌آوری می‌کند و خدمات مناسب را به آن‌ها ارائه دهد. به طور کلی روش‌های حفاظت از حریم خصوصی فردی در دو گروه دسته‌بندی می‌شوند:

۱) روش‌های مبتنی بر شخص ثالث معتمد

۲) روش‌های بدون نیاز به شخص ثالث معتمد

[1] Trusted third party

روش‌های مبتنی بر شخص ثالث معتمد به سادگی پیاده‌سازی می‌شوند و می‌توانند تعادل مناسبی بین کارایی، دقت و سطح حریم خصوصی مورد انتظار فراهم آورند. راه‌حل‌های مبتنی بر سرور به دلایل زیر برای شبکه‌های اجتماعی سیار زیاد مناسب به نظر نمی‌رسند:

- کاربران در شبکه‌های اجتماعی سیار دسترسی مستقیم به رایانه و اینترنت ندارند و با وجود اینکه محبوبیت این سرویس‌های داده‌ی سلولی[1] افزایش یافته است، اما به دلیل هزینه زیاد آن، تعداد مشترکین آن محدود هستند.
- کاربران به شدت در مورد اطلاعات شخصی و محرمانگی موقعیت مکانی خود حساس هستند و نمی‌خواهند موقعیت فعلی و دیگر اطلاعات شخصی خود را حتی برای یک سرور امن هم فاش کنند. ویلز و همکارانش سیزده شبکه اجتماعی مثل Facebook، Friendster، Hi5، LinkedIn، Myspace، Twitter را بررسی کردند و نشان دادند که همه‌ی آن‌ها تعدادی از اطلاعات شخصی را در اختیار سایت‌های ردیابی[2] قرار می‌دهند و تعدادی از آن‌ها اطلاعات مکان کاربران را در اختیار ثالث معتمد می‌گذارند [۱۴].
- یک سرور به راحتی می‌تواند به گلوگاه و یک نقطه شکست تبدیل شود و مورد حمله منع خدمت[3] قرار بگیرد [۱۵] که می‌تواند امنیت کل سیستم را تحت تأثیر قرار دهد. چهارم اینکه اکثریت این روش‌ها، حریم خصوصی موقعیت را تنها برای یک تصویر ایستا[4] از موقعیت کاربر فراهم می‌کنند؛ به عبارت دیگر این روش‌ها نسبت به حملات هم‌بسته[5] (همبند) مقاوم نیستند [۱۶، ۳]. لازم به ذکر است در حملات هم‌بسته، مهاجم اطلاعات موقعیت نادقیق فرد قربانی را به طور متوالی استخراج و از آن‌ها در جهت کشف موقعیت دقیق و یا دنبال کردن کاربر استفاده می‌کنند.

اگرچه روش‌های بدون نیاز به شخص ثالث معتمد، مشکلات روش‌های مبتنی بر شخص ثالث معتمد را تا حد زیادی برطرف کرده‌اند؛ اما دارای مشکلاتی نیز هستند برای مثال لازم است کاربر به همسایگان اطراف خود اعتماد کند. به

[1] Cellular data service
[2] Tracking site
[3] Denial-of-service attack
[4] Snapshot
[5] Correlation attacks

علاوه بعضی از این روش‌ها نیاز به تغییر ساختار تأمین‌کننده خدمت دارند و این مسئله مانع از به کارگیری این روش‌ها در واقعیت می‌شود [۱۶، ۱۷].

در شبکه‌های نظیر به نظیر[1] کاربران موبایل در میان خودشان ارتباطاتی دارند و با همکاری یکدیگر و بدون نیاز به ثالث معتمد موقعیت خود را در قالب یک ناحیه فضایی نادقیق می‌کنند؛ یعنی هنگامی‌که یک کاربر تقاضای خدمتی را از سرویس‌دهنده آگاه به موقعیت می‌کند، با بقیه افراد از طریق ارتباط چندهاپی[2] همکاری کرده و گروهی شامل همسایگان خود تشکیل می‌دهد و موقعیت نادقیق خود را به صورت ناحیه‌ای تعیین می‌کند که مکان خود و کلیه‌ی همسایگانش را در بر می‌گیرد. تنها یک الگوریتم تحت این مدل موجود است [۲۳]. به خاطر اینکه مدل‌های متمرکز یا توزیع‌شده دارای زیرساخت ارتباطی ثابت هستند و به سرورهای متمرکز یا توزیع‌شده متکی هستند برای محیط‌های ارتباطی نظیر به نظیر موبایل مناسب نیستند. به همین دلیل در این پژوهش نادقیق سازی موقعیت تحت مدل معماری نظیر به نظیر انجام می‌شود.

علاوه بر موارد فوق، اغلب مدل‌های پیشنهادی دانش پیش‌زمینه‌ای نسبت به محیط اطراف ندارند و آگاه به محیط نیستند، یعنی اگر شخص مهاجم شناختی از محیط اطراف فرد قربانی داشته باشد می‌تواند در ناحیه نادقیق مکان دقیق کاربر را حدس بزند. برای مثال اگر ناحیه‌ی نادقیق کاربر قربانی شامل قسمتی از رودخانه باشد که هیچ قایقی حق تردد در آن را ندارد شخص مهاجم می‌تواند این ناحیه را کوچک‌تر در نظر بگیرد و مکان واقعی کاربر را حدس بزند [۱۸].

با توجه به ماهیت شبکه‌های اجتماعی سیار در این تحقیق هیچ موجودیتی امن در نظر گرفته نشده است بنابراین مسئله‌ی مورد پژوهش این تحقیق به صورت زیر بیان می‌شود:

حفاظت از حریم خصوصی فردی برای کاربران شبکه‌های اجتماعی سیار هنگام استفاده از خدمات آگاه به موقعیت، به گونه‌ای که هویت و مکان کاربر در محیطی که هیچ موجودیتی امن در نظر گرفته نشده است، امن بماند.

[1] Peer-to-peer
[2] Multi-hop

۱-۳- اهداف، روش پژوهش و نوآوری‌ها

همان‌گونه که بیان شد، در این تحقیق سعی بر آن است که راه‌حلی امن برای حفظ محرمانگی مکان و هویت کاربران شبکه‌ی اجتماعی سیار ارائه شود به گونه‌ای که کاربران هنگام استفاده از خدمات آگاه به موقعیت در این‌گونه محیط‌ها، بدون نگرانی از حریم خصوصی خود از منافع این‌گونه سرویس‌ها بهره‌مند شوند.

جهت رسیدن به این هدف، با توجه به مدل در نظر گرفته‌شده برای مسئله، سناریوهای مختلف موجود در خدمات آگاه به محیط بررسی شده و اهداف امنیتی هر سناریو مشخص می‌شود. به علاوه استفاده از خدمات آگاه به موقعیت در شرایطی است که مهاجمانی در محیط وجود دارند، بنابراین لازم است پروتکل ارائه‌شده از حریم خصوصی فرد در چنین شرایطی محافظت کند.

سپس پروتکل ارائه‌شده از جهت کارایی و امنیت مورد ارزیابی قرار می‌گیرد. در تحلیل کارایی هدف بررسی عملکرد سیستم در محیط واقعی است. برای انجام این کار از روش آزمایش استفاده می‌شود و پروتکل ارائه‌شده پیاده‌سازی می‌شود. به علاوه تعدادی مجموعه‌ی داده‌ها فراهم می‌شود و با تغییر پارامترهای تأثیرگذار، سیستم ارزیابی و تست می‌شود و نتایج به دست آمده با کارهای قبلی مقایسه می‌شود.

زمینه‌های اصلی نوآوری این تحقیق در موضوع اصلی است: اول ارائه پروتکلی جهت تأمین حریم خصوصی و دوم بهبود کارایی پروتکل‌های ارائه‌شده که با انجام تغییراتی در اصول آن‌ها و اضافه کردن قابلیت‌های بیشتر صورت می‌گیرد. به طور کلی نوآوری پایان‌نامه به صورت زیر است:

ارائه پروتکلی با نام LATEDA[1] مبتنی بر روش نادقیق سازی فضایی موقعیت: در این پروتکل موقعیت یک فرد در قالب یک ناحیه‌ی منفرد نادقیق می‌شود به طوری که ترجیحات حریم خصوصی کاربران تأمین شود. این پروتکل همسایگان اطراف کاربر را امن در نظر نمی‌گیرد و با در نظر گرفتن برچسب اعتماد برای کاربران سیستم احتمال کشف شدن اطلاعات محرمانه فرد درخواست دهنده‌ی سرویس به دست فردی خرابکار را به صورت چشم‌گیری کاهش می‌دهد.

[1] Location-Aware Trusted Enhanced Dual-Active spatial cloaking