

رسالة محمد



دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر
گرایش هوش مصنوعی

**حفظ حریم مکانی برای انجام پرس و جوهای نزدیک‌ترین همسایه‌ی گروهی در
خدمات مکان‌مبنا**

استاد راهنما:
دکتر بهروز ترک‌لادانی

پژوهشگر:
فهیمة بلورکش

مهر ماه ۱۳۹۱

کلیه حقوق مادی مترتب بر نتایج مطالعات، ابتکارات
و نوآوری‌های ناشی از تحقیق موضوع این پایان‌نامه
متعلق به دانشگاه اصفهان است.



دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر گرایش هوش
مصنوعی خانم فهیمه بلورکش تحت عنوان

حفظ حریم مکانی برای انجام پرس و جوهای نزدیک‌ترین همسایه‌ی گروهی در
خدمات مکان‌مبنا

در تاریخ ۹۱/۷/۲۹ توسط هیأت داوران زیر بررسی و با درجه بسیار خوب به تصویب نهایی رسید.

۱- استاد راهنمای پایان‌نامه دکتر بهروز ترک لادانی با مرتبه‌ی علمی دانشیار امضا

۲- استاد داور داخل گروه دکتر افسانه فاطمی با مرتبه‌ی علمی استادیار امضا

۳- استاد داور خارج از گروه دکتر حمید ملا با مرتبه‌ی علمی استادیار امضا



سپاسگزارى

سپاس خداى را كه انسان را به بهترين شكل آفريد و به راه شناخت خويش هدايت كرد. خدايى كه به آدمى فرصت آموختن داد و در اين فرصت به او آموخت آنچه را كه نمى دانست؛ به آدمى فرصت بيان داد تا او را بخواند به اسماء الحسنى؛ و هر آن كه او را خواند، پاسخش گفت بدان سان كه او را كفايت كند. سپاس او را كه كفايتش، بندگان را غرق عنايت كرده و حمايتش در مهيب ترين گردابها، امن ترين ساحل هاست. سپاس و ستايش خدايى را كه در سپاس و ستايش او ناتوانيم و او به مرحمت خويش وسع تنگ ما را در وسعت بي منتهايش لحاظ مى كند.

به مصداق جمله‌ى

«من لم يشكر المخلوق، لم يشكر الخالق»

از راهنمايى‌هاى ارزشمند و بي دريغ استاد گراندرد، جناب آقاى دكتور بهروز ترك لادانى جهت انجام اين پايان نامه و هم‌چنين از تلاش و زحمات بي وقفه‌ى ايشان در جهت پيشرفت و توسعه‌ى سطح علمى دانشگاه، كمال قدردانى را داشته و علو مدارج علمى ايشان را از خداوند منان مسئلت مى نمايم.

تقدیم بہ

روح پاک پدرم کہ عالمانہ بہ من آموخت تا چگونہ در عرصہ زندگی، ایستادگی را تجربہ نمایم؛
و بہ مادرم، دریای بی کران فداکاری و عشق کہ وجودم برایش ہمہ رنج بود و وجودش برایم ہمہ مهر؛
و تقدیم بہ خواهران عزیزم، مہربان فرشتگانی کہ لذت و غرور دانستن، جسارت خواستن، عظمت رسیدن و تمام تجربہ های یکتا
و زیبای زندگیم، دیون حضور سبز آنهاست.

چکیده

توسعه و افزایش روزافزون دستگاه‌های قابل حمل گوناگون، که دارای ابزارهای مکان‌یابی و قابلیت برقراری ارتباطات بی‌سیم هستند، موجب پیدایش و توسعه سیستم‌هایی برای ارائه خدمات مکان‌مبنا شده‌است. این سیستم‌ها با دریافت پرس‌وجوهای مکان‌مبنای کاربران، اطلاعات متناسب با مکانشان را در اختیار آن‌ها قرار می‌دهند. از آن‌جا که برای انجام این پرس‌وجوها، کاربران باید اطلاعات مکانی خود را در اختیار فراهم‌کنندگان خدمت قرار دهند، امکان ردیابی و نقض حریم خصوصی کاربران وجود دارد. بنابراین هدف تحقیقات فعلی در این زمینه، بهبود روش‌های حفظ حریم مکانی با وجود ارائه خدمات با کیفیت بالا، و همچنین ارائه انواع جدید و مختلفی از خدمات کاربردی به کاربران می‌باشد. یکی از خدمات جدید در این زمینه، پرس‌وجوهای نزدیک‌ترین همسایه‌ی گروهی هستند که در آن‌ها اعضای یک گروه نزدیک‌ترین مکان به کل افراد گروه را درخواست می‌کنند. تاکنون راهکارهای مختلفی جهت حفظ حریم مکانی کاربران در پرس‌وجوهای فردی طراحی شده‌اند، اما در مورد پرس‌وجوهای گروهی تا به حال تحقیقات کمی صورت گرفته‌است. در این پایان‌نامه، دو روش برای انجام پرس‌وجوهای نزدیک‌ترین همسایه‌ی گروهی ارائه و بررسی شده‌است. در روش اول، یک شناسه‌ی منحصر به فرد برای پرس‌وجو انتخاب شده و سپس هر یک از اعضای گروه با استفاده از روش‌های مخفی‌سازی مکان که در پرس‌وجوهای فردی استفاده می‌شوند، ناحیه‌ی بی‌نشانی خود را به فراهم‌کننده‌ی خدمت اعلام می‌کند؛ فراهم‌کننده‌ی خدمت پس از دریافت تمام نواحی بی‌نشانی، پرس‌وجو را پردازش کرده و مجموعه‌ای از جواب‌های کاندیدا را به کاربران بازمی‌گرداند که شامل جواب حقیقی می‌باشد. در نهایت کاربران با استفاده از الگوریتم‌های شایعه‌ی مورد استفاده در تجمیع داده‌ها، جواب حقیقی را به دست می‌آورند، به طوری که هیچ یک نتوانند مکان حقیقی دیگری را حدس بزنند. در روش دوم که روشی تقریبی است، ابتدا کاربران با استفاده از الگوریتم‌های شایعه روی یک شاخص مکانی مشترک به توافق رسیده و یکی از اعضای گروه، این شاخص مکانی را به فراهم‌کننده‌ی خدمت ارسال می‌کند. پس از آن فراهم‌کننده‌ی خدمت جواب‌های تقریبی را به آن کاربر ارسال کرده و کاربر مذکور نیز این جواب‌ها را به سایر اعضای گروه ارسال می‌کند. کاربران می‌توانند برای محاسبه‌ی جواب‌های دقیق، مجموعه جواب بزرگ‌تری را از فراهم‌کننده‌ی خدمت درخواست کرده و سپس با استفاده از الگوریتم شایعه جواب حقیقی را پیدا کنند. نتایج حاصل از ارزیابی‌های انجام شده نشان می‌دهد که هر دو روش ارائه‌شده میزان حفاظت از حریم مکانی و زمان پاسخ به کاربران را نسبت به روش‌های پیشین بهبود می‌بخشند. در روش دوم هزینه‌ی پردازش پرس‌وجو در فراهم‌کننده‌ی خدمت نیز کاهش می‌یابد.

واژگان کلیدی: خدمات مکان‌مبنا، حریم مکانی، پرس‌وجوی نزدیک‌ترین همسایه‌ی گروهی، الگوریتم شایعه.

فهرست مطالب

صفحه

عنوان

فصل اول

- ۱-۱ مقدمه..... ۱
- ۲-۱ شرح مسئله و روش انجام پژوهش..... ۳
- ۳-۱ ساختار پایان نامه ۵

فصل دوم

- ۱-۲ مقدمه..... ۶
- ۲-۲ محاسبات فراگیر..... ۷
- ۱-۲-۲ محاسبات آگاه به زمینه ۷
- ۳-۲ خدمات مکان مبنا..... ۸
- ۱-۳-۲ انواع پرس وجوهای درخواستی..... ۹
- ۴-۲ حریم خصوصی..... ۱۱
- ۱-۴-۲ حریم مکانی..... ۱۱
- ۵-۲ حفظ حریم خصوصی در خدمات مکان مبنا..... ۱۲
- ۱-۵-۲ اهمیت حفظ حریم خصوصی در خدمات مکان مبنا..... ۱۲
- ۲-۵-۲ روش های حفظ حریم خصوصی در خدمات مکان مبنا..... ۱۳
- ۳-۵-۲ مخفی سازی مکان با استفاده از بی نشانی..... ۱۹
- ۴-۵-۲ پردازش پرس وجو..... ۲۴
- ۵-۵-۲ پرس وجوهای نزدیک ترین همسایه ی گروهی..... ۲۶
- ۶-۲ مفهوم شایعه در تجمیع داده ها..... ۲۷
- ۷-۲ جمع بندی..... ۳۰

فصل سوم

- ۱-۳ مقدمه..... ۳۲
- ۲-۳ روش های حفظ حریم خصوصی در خدمات مکان مبنا..... ۳۳
- ۱-۲-۳ روش های حفظ حریم مکانی در خدمات مکان مبنا..... ۳۴

۳-۳ پرس و جوهای نزدیک ترین همسایه‌ی گروهی در خدمات مکان مبنا.....	۴۱
۱-۳-۳ پرس و جوهای kGNN.....	۴۱
۲-۳-۳ روش هاشم و همکارانش.....	۴۳
۳-۳-۳ روش هوانگ و همکارانش.....	۵۰
۴-۳-۳ روش عاشوری و همکارانش.....	۵۱
۴-۳ الگوریتم‌های شایعه در تجمیع داده.....	۵۵
۵-۳ کاستی‌های موجود.....	۵۸
۶-۳ جمع‌بندی.....	۵۹

فصل چهارم

۱-۴ مقدمه.....	۶۰
۲-۴ تعریف مسئله.....	۶۱
۳-۴ روش اول برای انجام پرس و جوهای kGNN.....	۶۵
۱-۳-۴ فیلتر خصوصی مجموع مبتنی بر حداکثر فواصل تجمعی.....	۶۹
۲-۳-۴ فیلتر خصوصی مجموع مبتنی بر شایعه‌ی امن.....	۷۲
۳-۳-۴ فیلتر خصوصی بیشینه‌ی مبتنی بر شایعه‌ی امن.....	۷۵
۴-۳-۴ بررسی خصوصیات فیلترهای خصوصی مبتنی بر شایعه.....	۷۹
۴-۴ روش دوم برای انجام پرس و جوهای kGNN.....	۸۲
۱-۴-۴ مرحله‌ی ارسال پرس و جوی kGNN.....	۸۳
۲-۴-۴ پردازش پرس و جو در فراهم‌کننده‌ی خدمت.....	۸۷
۳-۴-۴ استخراج جواب‌های حقیقی از مجموعه جواب کاندیدا.....	۸۹
۵-۴ مقایسه‌ی خصوصیات روش‌های پیشنهادی.....	۸۹
۶-۴ جمع‌بندی.....	۹۲

فصل پنجم

۱-۵ مقدمه.....	۹۴
۲-۵ نحوه‌ی شبیه‌سازی.....	۹۵

۳-۵ نتایج تجربی	۹۹
۱-۳-۵ ارزیابی و مقایسه‌ی فیلترهای خصوصی	۱۰۰
۲-۳-۵ ارزیابی روش‌های حفاظت از حریم مکانی گروهی	۱۰۷
۴-۵ تحلیل و مقایسه	۱۲۲
۵-۵ جمع‌بندی	۱۲۴

فصل ششم

۱-۶ مقدمه	۱۲۶
۲-۶ خلاصه‌ی مباحث و نتایج به‌دست‌آمده	۱۲۶
۳-۶ کارهای آینده	۱۲۸
واژه‌نامه	۱۲۹
منابع و مآخذ	۱۳۱

فهرست شکل‌ها

صفحه

عنوان

- شکل ۱-۲: الف) خدمات مکان‌مبنا، اشتراکی از خدمات شبکه‌های بی‌سیم هستند. ب) اجزای ۸
- شکل ۲-۲: اهمیت مخفی کردن مکان ۱۴
- شکل ۳-۲: معماری سه لایه با حضور شخص ثالث مورداستناد ۱۶
- شکل ۴-۲: معماری نظیربه‌نظیر سیار ۱۸
- شکل ۵-۲: نمونه‌ای از ناحیه‌ی مخفی‌ساز با بی‌نشانی مرتبه‌ی سه ۲۲
- شکل ۶-۲: الف) یک منبع گرما و چهار حسگر با مقادیر حس‌شده. ب) میزان واریانس مقادیر گره‌ها ۲۸
- شکل ۷-۲: الگوریتم شایعه جهت محاسبه‌ی مقادیر تجمعی ۲۹
- شکل ۱-۳: الف) یک نمونه از مناطق مخلوط‌سازی که با سه منطقه‌ی کاربرد در ارتباط است ۳۲
- شکل ۲-۳: الف) ناحیه‌ی بی‌نشانی مرتبه‌ی ۳ برای u_3 ، u_4 و u_5 . ب) ناحیه‌ی بی‌نشانی مرتبه‌ی ۳ برای ۳۵
- شکل ۳-۳: روش بازیابی خصوصی اطلاعات ۳۶
- شکل ۴-۳: نمونه‌ای از پرس‌وجوهای نزدیک‌ترین همسایه‌ی گروهی ۴۰
- شکل ۵-۳: الگوریتم MAX_IPPF ۴۷
- شکل ۶-۳: روش متمرکز محاسبه‌ی GNN به روش ارزیابی عملکرد امن ۵۰
- شکل ۷-۳: حمله‌ی تباری جزئی در پروتکل هاشم و همکارانش، خطوط پررنگ Δ_i را نشان می‌دهند. ۵۳
- شکل ۸-۳: الگوریتم شایعه‌ی جلاسیتی و همکارانش ۵۴
- شکل ۹-۳: الگوریتم شایعه با قوانین خاموش‌سازی ۵۶
- شکل ۱-۴: مرکز ثقل و نقطه‌ی q زمانی که n برابر با ده است ۶۳
- شکل ۲-۴: مرکز ثقل و نقطه‌ی q زمانی که n برابر با صد است ۶۳
- شکل ۳-۴: ارتباط سرگروه با فراهم‌کننده‌ی خدمت در مرحله‌ی اول ۶۵
- شکل ۴-۴: ارسال درخواست ملاقات توسط سرگروه به سایر اعضا ۶۶
- شکل ۵-۴: مرحله‌ی دوم و سوم از روش اول ۶۷
- شکل ۶-۴: الگوریتم شایعه‌ی محافظ حریم خصوصی ۷۲
- شکل ۷-۴: الگوریتم به‌روزرسانی بردارها در فیلتر خصوصی پیشینه‌ی مبتنی بر شایعه‌ی امن ۷۵
- شکل ۸-۴: الگوریتم تغییر نویز در فیلتر خصوصی پیشینه‌ی مبتنی بر شایعه‌ی امن ۷۶
- شکل ۹-۴: الگوریتم فیلتر خصوصی پیشینه‌ی مبتنی بر شایعه‌ی امن برای فرآیند فعال ۷۷
- شکل ۱۰-۴: الگوریتم فیلتر خصوصی پیشینه‌ی مبتنی بر شایعه‌ی امن برای فرآیند منفعل ۷۷

- شکل ۴-۱۱: نحوه‌ی نمایش یک مستطیل در صفحه‌ی مختصات ۸۴
- شکل ۴-۱۲: نمونه‌ی ای از ناحیه‌ی بی‌نشانی گروهی که با توجه به نواحی بی‌نشانی اعضا ساخته می‌شود ۸۵
- شکل ۴-۱۳: (۱) ساخت ناحیه‌ی بی‌نشانی گروهی با استفاده از الگوریتم شایعه (۲) ارسال پرس‌وجو ۸۶
- شکل ۴-۱۴: روند کلی مرحله‌ی دوم از روش دوم ۸۷
- شکل ۵-۱: هزینه‌ی ارتباطی فیلترهای خصوصی در k های مختلف ($n=64$) ۱۰۳
- شکل ۵-۲: هزینه‌ی ارتباطی فیلترهای خصوصی در n های مختلف ($k=8$) ۱۰۴
- شکل ۵-۳: تغییرات درصد خطای جواب نهایی با تغییر ضریب k درخواستی ۱۰۷
- شکل ۵-۴: اثر تغییر اندازه‌ی گروه بر درصد خطای جواب نهایی ۱۰۸
- شکل ۵-۵: اثر تغییر اندازه‌ی گروه بر اندازه‌ی مجموعه جواب کاندیدا ۱۰۹
- شکل ۵-۶: اثر تغییر اندازه‌ی گروه بر هزینه‌ی محاسباتی فراهم‌کننده‌ی خدمت ۱۱۰
- شکل ۵-۷: اثر تغییر اندازه‌ی گروه بر تعداد دسترسی‌های صفحه در فراهم‌کننده‌ی خدمت ۱۱۱
- شکل ۵-۸: اثر تغییر اندازه‌ی گروه بر درصد خطای جواب نهایی ۱۱۱
- شکل ۵-۹: اثر تغییر اندازه‌ی مقدار k بر اندازه‌ی مجموعه جواب کاندیدا ۱۱۲
- شکل ۵-۱۰: اثر تغییر مقدار k بر هزینه‌ی محاسباتی فراهم‌کننده‌ی خدمت ۱۱۳
- شکل ۵-۱۱: اثر تغییر مقدار k بر تعداد دسترسی‌های صفحه در فراهم‌کننده‌ی خدمت ۱۱۳
- شکل ۵-۱۲: اثر تغییر اندازه‌ی MBR بر اندازه‌ی مجموعه جواب کاندیدا ۱۱۴
- شکل ۵-۱۳: اثر تغییر اندازه‌ی MBR بر هزینه‌ی محاسباتی فراهم‌کننده‌ی خدمت ۱۱۵
- شکل ۵-۱۴: اثر تغییر اندازه‌ی MBR بر تعداد دسترسی‌های صفحه ۱۱۶
- شکل ۵-۱۵: اثر تغییر اندازه‌ی نواحی بی‌نشانی بر اندازه‌ی مجموعه جواب کاندیدا ۱۱۷
- شکل ۵-۱۶: اثر تغییر اندازه‌ی نواحی بی‌نشانی بر هزینه‌ی محاسباتی فراهم‌کننده‌ی خدمت ۱۱۷
- شکل ۵-۱۷: اثر تغییر اندازه‌ی نواحی بی‌نشانی بر تعداد دسترسی‌های صفحه ۱۱۸
- شکل ۵-۱۸: اثر تغییر اندازه‌ی مجموعه‌ی نقاط داده بر اندازه‌ی مجموعه جواب کاندیدا ۱۱۹
- شکل ۵-۱۹: اثر تغییر اندازه‌ی مجموعه‌ی نقاط داده بر هزینه‌ی محاسباتی فراهم‌کننده‌ی خدمت ۱۱۹
- شکل ۵-۲۰: اثر تغییر اندازه‌ی مجموعه‌ی نقاط داده بر تعداد دسترسی‌های صفحه ۱۲۰

فهرست جدول‌ها

عنوان	صفحه
جدول ۱-۲: یک پایگاه داده‌ی منتشرشده با حذف شناسه‌ها	۲۰
جدول ۲-۲: لیست رأی‌دهندگان الکترونیکی	۲۰
جدول ۳-۲: جدول منتشرشده با بی‌نشانی مرتبه‌ی چهار	۲۱
جدول ۱-۳: فاصله‌ی حقیقی کاربران تا نقاط داده‌ی موجود در مجموعه جواب کاندیدا	۴۶
جدول ۲-۳: به‌روزکردن حداقل و حداکثر فواصل تجمعی و هرس افزایشی	۴۷
جدول ۱-۴: مقایسه‌ی فیلترهای خصوصی	۸۰
جدول ۲-۴: مقایسه‌ی دو روش پیشنهادی	۹۰
جدول ۱-۵: محدوده‌ی تغییر پارامترها برای بررسی فیلترهای خصوصی	۹۹
جدول ۲-۵: اثر تغییر تعداد تراکنش‌های شایعه بر عملکرد Diff_GPF	۱۰۰
جدول ۳-۵: اثر تغییر تعداد تراکنش‌های شایعه بر عملکرد Safe_GPF	۱۰۰
جدول ۴-۵: درصد خطای جواب با توجه به تغییر پارامترهای C و thaw در I_Diff_GPF	۱۰۱
جدول ۵-۵: درصد خطای جواب با توجه به تغییر پارامترهای C و thaw در I_Safe_GPF	۱۰۱
جدول ۶-۵: درصد خطای فیلترهای خصوصی در مقادیر مختلفی از n ($k=8$)	۱۰۲
جدول ۷-۵: درصد خطای فیلترهای خصوصی در مقادیر مختلفی از k ($n=64$)	۱۰۲
جدول ۸-۵: محدوده‌ی عوامل مورد بررسی جهت ارزیابی کارایی روش‌های پیشنهادی	۱۰۶

فصل اول

کلیات

۱-۱ مقدمه

با پیشرفت روزافزون تکنولوژی‌های بی‌سیم، دستگاه‌های شخصی سیار و قابل حمل^۱ مختلف (مانند تلفن همراه، PDA و...) توانایی دسترسی گسترده به اینترنت را در زمان‌ها و مکان‌های مختلف فراهم نموده‌اند. علاوه بر آن، امروزه سیستم‌های مکان‌یابی جهانی^۲ یک جزء اساسی و رایج در دستگاه‌های قابل حمل دستی به شمار می‌روند. در نتیجه در حوزه‌ی محاسبات فراگیر^۳ سیستم‌های جدیدی به نام خدمات مکان‌مبنا^۴ (LBS) طراحی شده‌اند که این امکان را برای کاربران فراهم می‌کنند که پرس‌وجوهای مبتنی بر مکان خود را از هر جایی به یک فراهم‌کننده‌ی خدمت مکان‌مبنا ارسال کرده و جواب آن را دریافت کنند. این پرس‌وجوها می‌تواند درباره‌ی یک مکان موردعلاقه^۵ یا اطلاعاتی مانند میزان ترافیک یا آلودگی هوا باشد؛ به عنوان مثال، یک

^۱ Mobile and Portable Devices

^۲ Global Positioning System(GPS)

^۳ Pervasive Computing

^۴ Location Based Service(LBS)

^۵ Points Of Interest(POI)

پرس وجو می تواند این باشد که «نزدیک ترین عابربانک (ATM) به من کجا می باشد؟» و یا «کدام پمپ بنزین ها فاصله ی کمتر از یک کیلومتر به من را دارند و کدام یک در مسیر من قرار دارد؟»

برای استفاده از خدمات مکان مینا و انجام چنین پرس وجوهایی کاربران باید اطلاعات مربوط به مکان خود را برای فراهم کنندگان خدمت فاش سازند. در نتیجه، این امکان وجود دارد که این سیستم ها حریم خصوصی^۱ افراد را به خطر بیندازند؛ به این صورت که فراهم کننده ی خدمت یا یک فرد مهاجم می تواند با دنبال کردن پرس وجوهای کاربر او را شناسایی کند. اگر حفاظت لازم صورت نگیرد، یک مهاجم می تواند اطلاعات مربوط به مکان یا مسیرهای شخص را با اطلاعات قبلی خود ترکیب کرده و با انجام استنتاج هایی روی آن ها به دیگر اطلاعات خصوصی او نیز دسترسی پیدا کند [۱]. به عنوان مثال، با بررسی مسیرهای روزانه ی فرد و مکان هایی که روزانه به آن ها رفت و آمد دارد، می توان علاقه ها، عقاید و سبک زندگی او را تا حد زیادی تشخیص داد. بنابراین در توسعه ی خدمات مکان مینا، یک نکته ی اساسی که باید در نظر گرفته شود، حفظ حریم مکانی^۲ کاربران است که تأثیر زیادی روی موفقیت و محبوبیت آن خدمت دارد.

به طور کلی اهداف و کاربردهای خدمات مکان مینا را می توان مشتمل بر موارد زیر دانست:

- ارائه ی روش های جدید برای ارتباط بهتر و راحت تر کاربران،
- اطلاع رسانی بهتر و آگاهی سریعتر کاربران از اطلاعات، اخبار و امکانات جدید،
- ایجاد سیستم های سرگرمی،
- کاربردهای تجاری و آگهی های بازرگانی،
- توانایی بهتر در دنبال کردن مواردی مانند پیگیری افراد و وسائل گم شده،
- کاربردهای نظامی.

کاربران مختلف با توجه به نوع خدمت مکان مینایی که استفاده می کنند، نیازمندی های امنیتی متفاوتی دارند. تاکنون راه های مختلفی برای حفظ حریم مکانی کاربران، در انجام پرس وجوهای فردی پیشنهاد داده شده اند، اما در مورد حریم مکانی کاربرانی که با هم مرتبط هستند و پرس وجوهای گروهی، تا به حال تحقیقات کمی صورت گرفته است. یک نمونه از این پرس وجوها می تواند به این صورت باشد: «رستورانی که به یک گروه از دوستان نزدیک تر می باشد، کدام است؟» در این پرس وجو باید مکانی انتخاب شود که حاصل جمع فاصله اش به تمام

¹ Privacy

² Location Privacy

کاربران پرس و جو کننده کمترین مقدار را داشته باشد. این نمونه از پرس و جوها استفاده‌ی زیادی در زندگی و فعالیت‌های اجتماعی کاربران دارند.

هدف این پایان‌نامه، بررسی چگونگی انجام پرس و جوهای گروهی مکان‌مبنا است به طوری که حریم مکانی اعضای گروه به خطر نیفتد. در این فصل، به شرح مسئله‌ای که در این پایان‌نامه مطرح شده است پرداخته و اهمیت و کاربردهای آن را بیان می‌کنیم. برای این منظور مسئله‌ی مورد بحث را از جوانب مختلف بررسی کرده و پس از مرور روش انجام تحقیق، نتایج حاصله را شرح می‌دهیم. در نهایت ساختار کلی پایان‌نامه معرفی می‌شود.

۱-۲ شرح مسئله و روش انجام پژوهش

خدمات مکان‌مبنا در صورتی پیشرفت خواهند کرد که نیازمندی‌های امنیتی و کارایی دلخواه کاربران را برآورده سازند؛ از این رو، تحقیقات فعلی در زمینه‌ی خدمات مکان‌مبنا، سعی در بهبود روش‌های حفظ حریم خصوصی کاربران و بالا بردن کیفیت خدمات دارند و نیز در صدد ارائه‌ی خدمات جدید و مطابق با نیاز روز می‌باشند.

یکی از اصلی‌ترین جنبه‌های زندگی انسان‌ها، ارتباطات اجتماعی بین آن‌ها است که منجر به تصمیم‌گیری‌های جمعی و فعالیت‌های اجتماعی می‌شود. بنابراین پشتیبانی از درخواست‌های گروهی و تسهیل ارتباط بین افراد مختلف، می‌تواند به عنوان یکی از مهم‌ترین عوامل پیشرفت خدمات مکان‌مبنا در نظر گرفته شود. از طرفی با پیدایش شبکه‌های اجتماعی، ارتباطات مجازی گروهی نیز افزایش پیدا کرده است و بسیاری از افراد تعاملات روزانه و بخشی از فعالیت‌های اجتماعی خود را به صورت مجازی انجام می‌دهند. از این رو، با پیشرفت خدمات مکان‌مبنا نیز سیستم‌هایی ایجاد شده‌اند که خدمات بلادرنگ جدیدی را به کاربران ارائه می‌دهند، بدین ترتیب که گروهی از کاربران را قادر می‌سازند که یک پرس و جوی مبتنی بر مکان مشترک را با هم انجام دهند؛ به عنوان مثال، ممکن است گروهی از کاربران مایل به یافتن نزدیک‌ترین مکان مناسب برای ملاقات باشند، یعنی مکانی که مجموع فواصل پیموده شده توسط آن‌ها را کمینه می‌کند و یا مکانی که زمان رسیدن تمام اعضای گروه به آن مکان کمینه است. هم‌چنین ممکن است اعضای گروه بخواهند فردی را در گروه انتخاب کنند که کمترین فاصله به یک مکان مورد علاقه (مانند فروشگاه، رستوران، مرکز اینترنت و ...) را دارد. چنین پرس و جوهای در زندگی روزانه‌ی افراد و فعالیت‌های روزانه‌ی سازمان‌ها و هم‌چنین در زمینه‌های اورژانسی و خدمات نظامی و ... کاربرد دارند.

در این پایان‌نامه فرض بر این است که گروهی از کاربران، می‌خواهند با استفاده از دستگاه‌های بی‌سیم مجهز

به مکان‌یاب جهانی، نزدیک‌ترین نقاط موردعلاقه به خود را بیابند به طوری که حریم خصوصی آن‌ها به خطر نیفتد. این کاربران می‌توانند با استفاده از دستگاه‌های خود با انواع خدمات موجود در اینترنت ارتباط برقرار کرده و هم‌چنین می‌توانند با سایر کاربران موجود در شبکه (سلولی یا اینترنت) ارتباط نظیربه‌نظیر برقرار سازند. برای حفظ حریم خصوصی کاربران در پرس‌وجوهای گروهی باید مکان اعضای گروه از یکدیگر و از فراهم‌کننده‌ی خدمت و از سایر افراد مهاجم موجود در شبکه مخفی بماند. در این پایان‌نامه برای انجام پرس‌وجوهای گروهی سه مرحله‌ی کلی در نظر گرفته شده‌است که این مراحل باید به صورتی انجام شوند که مکان هیچ یک از اعضا برای هیچ موجودیتی فاش نگردد. مراحل مذکور عبارتند از:

(۱) ارسال پرس‌وجوی درخواستی به فراهم‌کننده‌ی خدمت

(۲) پردازش پرس‌وجو در فراهم‌کننده‌ی خدمت و ارسال مجموعه‌ی جواب‌های کاندیدا به کاربران

(۳) تشخیص نزدیک‌ترین همسایه‌ی حقیقی از بین مجموعه جواب کاندیدا.

در این پایان‌نامه، برای انجام این مراحل دو روش کلی ارائه شده‌است. در روش اول مکان هر یک از اعضای گروه (با توجه به نیازمندی‌های امنیتی آن‌ها) در یک ناحیه‌ی مستطیل شکل مخفی شده و این ناحیه‌ها برای فراهم‌کننده‌ی خدمت ارسال می‌شود. فراهم‌کننده‌ی خدمت نمی‌تواند با استفاده از این نواحی، نزدیک‌ترین همسایه‌ی دقیق را به کاربران اعلام کند، بنابراین نزدیک‌ترین نقاط موردعلاقه به این نواحی را به عنوان مجموعه جواب کاندیدا به اعضای گروه بازمی‌گرداند. پس از آن اعضای گروه باید جواب دقیق را از مجموعه جواب کاندیدا استخراج کنند به طوری که مکان هیچ یک از آن‌ها برای دیگران فاش نگردد. این مرحله با استفاده از سازوکاری به نام فیلتر خصوصی انجام می‌شود. در این پایان‌نامه سه فیلتر خصوصی ارائه می‌شود که برای محاسبه‌ی نزدیک‌ترین همسایه‌های حقیقی از روش‌های تجمیع داده‌ی موجود در شبکه‌های نظیربه‌نظیر استفاده می‌کنند. در این روش، جواب‌های دقیق در اختیار کاربران قرار می‌گیرد، اما هزینه‌ی ارتباطی کاربران و هزینه‌ی محاسباتی و ارتباطی فراهم‌کننده‌ی خدمت نسبت به روش دوم بیشتر است.

در روش دوم تنها یک شاخص مکانی از اعضای گروه به فراهم‌کننده‌ی خدمت ارسال می‌گردد. این شاخص مکانی، یا به صورت مرکز ثقل هندسی کاربران و یا به صورت یک ناحیه‌ی مستطیل شکلی حاوی این مرکز ثقل است که با استفاده از روش‌های تجمیع داده در شبکه‌های نظیربه‌نظیر محاسبه می‌گردند. فراهم‌کننده‌ی خدمت با توجه به این شاخص مکانی، پرس‌وجوی درخواستی را پردازش کرده و نزدیک‌ترین نقاط موردعلاقه به این شاخص مکانی را به کاربران بازمی‌گرداند. این روش در تمام حالت‌ها جواب دقیق را به کاربران بازمی‌گرداند اما

نسبت به روش اول سربار ارتباطی بسیار کمتری برای کاربران دارد، هم‌چنین سربار ارتباطی و محاسباتی در فراهم‌کننده‌ی خدمت نیز کمتر از روش اول است و بدین ترتیب زمان دست یافتن کاربران به پاسخ نیز بسیار کمتر از روش اول می‌باشد. در صورتی که کاربران نیاز به دریافت جواب‌های دقیق داشته‌باشند، می‌توانند مجموعه جواب بزرگتری را از فراهم‌کننده‌ی خدمت درخواست کنند و سپس در مرحله‌ی بعد با استفاده از فیلترهای خصوصی نزدیک‌ترین همسایه‌های حقیقی را پیدا کنند.

برای ارزیابی دو روش ارائه‌شده، الگوریتم‌های پیشنهادی با استفاده از زبان جاوا پیاده‌سازی شده و عملکرد کاربران و فراهم‌کننده‌ی خدمت شبیه‌سازی می‌شود. با استفاده از نتایج حاصله، الگوریتم‌های پیشنهادی از لحاظ کارایی و هزینه‌های واردشده به کاربران با یکدیگر مقایسه می‌گردند.

۳-۱ ساختار پایان‌نامه

این پایان‌نامه از شش فصل تشکیل شده‌است. در فصل اول به بیان کلیات و شرح مسئله‌ی پژوهشی پرداخته شد و روش انجام تحقیق به طور خلاصه بیان گردید. سازماندهی ادامه‌ی پایان‌نامه به شرح زیر می‌باشد:

در فصل دوم، مفاهیم و تعاریف اولیه‌ای که برای آشنایی با موضوع این تحقیق لازم است، شرح داده می‌شوند. مفاهیم مربوط به حفظ حریم مکانی در خدمات مکان‌مبنا و روش‌های تجمیع داده‌ی مبتنی بر شایعه از جمله مفاهیم مورد بررسی هستند.

در فصل سوم، کارهای انجام‌شده در حوزه‌های مرتبط با موضوع این پایان‌نامه معرفی شده و نقاط قوت و ضعف آن‌ها بررسی می‌گردد.

در فصل چهارم جزئیات راهکارهای پیشنهادی جهت انجام پرس‌وجوهای نزدیک‌ترین همسایه‌ی گروهی شرح داده می‌شود؛ بدین ترتیب که ابتدا مسئله‌ی مورد پژوهش به طور دقیق تعریف شده و سپس دو روش کلی برای انجام پرس‌وجوهای نزدیک‌ترین همسایه‌ی گروهی معرفی می‌شوند.

در فصل پنجم، نحوه‌ی شبیه‌سازی کاربران و فراهم‌کنندگان خدمت مکان‌مبنا بیان شده و کارایی راهکارهای پیشنهادی معرفی شده در فصل چهارم مورد ارزیابی قرار می‌گیرد و با روش‌های قبلی مقایسه می‌شود.

در فصل ششم، ابتدا یک نتیجه‌گیری کلی از پروژه و نتایج به دست آمده انجام شده و در نهایت پیشنهادهایی برای ادامه‌ی کار در این زمینه به عنوان کارهای آینده مطرح می‌گردد.

فصل دوم

مروری بر مفاهیم پایه

۱-۲ مقدمه

در این فصل برای روشن شدن موضوع تحقیق و درک بهتر روش پیشنهادی، تشریحی از مفاهیم پایه‌ی موردنیاز، ارائه می‌گردد.

در ابتدا مفاهیم و اصطلاحات موجود در حوزه‌ی محاسبات فراگیر، خصوصاً مفاهیم مربوط به حفظ حریم مکانی در خدمات مکان‌مبنا بیان شده و پس از بررسی چالش‌های موجود در این زمینه، ساختارهای پیشنهادی جهت رفع این چالش‌ها را معرفی و طبقه‌بندی می‌کنیم. پس از آن، روش‌های ذخیره و بازیابی و نیز روش‌های پردازش اطلاعات مکانی در خدمات مکان‌مبنا، به طور خلاصه مرور می‌شوند.

در نهایت، از آن‌جا که در روش‌های پیشنهادی از الگوریتم‌های تجمیع داده‌ی مبتنی بر شایعه استفاده نموده‌ایم، به شرح مفهوم تجمیع داده در شبکه‌های نظیربه‌نظیر پرداخته و جزئیات روش تجمیع داده‌ی مبتنی بر شایعه را بیان خواهیم کرد.

۲-۲ محاسبات فراگیر

محاسبات یا رایانش فراگیر، قدرت محاسبات را از قید کامپیوترهای رومیزی رها کرده و این امکان را ایجاد می‌کند که بتوان با استفاده از دستگاه‌های سیار در هر زمان و مکان دلخواه، به اطلاعات موردنیاز دسترسی پیدا کرد [۲]. این فناوری در سال ۱۹۹۱، با نام «محاسبات همه‌جا حاضر»^۱، در آزمایشگاه زیراکس پارک^۲ ایجاد شد که حاصل همکاری فناوری‌های مختلفی مانند محاسبات سیار^۳، شبکه‌های بی‌سیم^۴، محاسبات جاسازی‌شده^۵، آگاهی از زمینه^۶ با استفاده از فناوری حسگرها، و تعاملات انسان و رایانه^۷ می‌باشد [۳، ۴]. دستگاه‌های مورد استفاده در این زمینه، از لحاظ روش و قابلیت‌ها متفاوت بوده و دارای چالش‌هایی مانند محدودیت قدرت پردازش، عمر باتری، فضای حافظه و پهنای باند و هم‌چنین قطعی‌های متوالی می‌باشند؛ در نتیجه، یکی از نکات مهم در توسعه‌ی برنامه‌های کاربردی در این محیط‌ها، توجه به کارایی و استفاده‌ی بهینه از منابع است [۳].

۲-۲-۱ محاسبات آگاه به زمینه^۸

طبق تعریف، «هر نوع اطلاعاتی که بتوان از آن برای مشخص کردن وضعیت یک موجودیت استفاده کرد، زمینه نامیده می‌شود.» منظور از یک موجودیت، یک شخص، مکان و یا شیء می‌باشد که به تعاملات بین کاربر و سیستم مربوط است [۵]. در محاسبات فراگیر از سه نوع آگاهی از زمینه پشتیبانی می‌شود [۶]:

۱. زمینه‌ی محیط فیزیکی، که به پدیده‌ها و ابعاد محیط فیزیکی وابسته است؛ مانند مکان، زمان و دما.
۲. زمینه‌ی انسانی، که وابسته به نحوه‌ی تعامل کاربران با سیستم است؛ مانند هویت و علائق کاربر.
۳. زمینه‌ی محیط مجازی یا زمینه‌ی فناوری اطلاعات و ارتباطات^۹، نوع خدمات داخلی یا خارجی ارائه‌شده توسط سیستم‌های توزیع شده، زمینه‌های محیط مجازی را تشکیل می‌دهند.

آگاهی از زمینه یک مفهوم کلیدی در حوزه‌ی محاسبات فراگیر است و هدف آن مرتبط‌نمودن و هماهنگی

سیستم‌های کامپیوتری با تغییرات محیطی می‌باشد [۷].

¹ Ubiquitous Computing

² Xerox PARC (Palo Alto Research Center)

³ Mobile Computing

⁴ Wireless Networks

⁵ Embedded Computing

⁶ Context Awareness

⁷ Human Computer Interaction

⁸ Context-aware Computing

⁹ Information and Communication Technology (ICT)