بررسی روش‌های حفاظت از حریم مکانی گروهی در خدمات مبتنی بر مکان و چالش‌های موجود

شادیه عزیزی[1]، مائده عاشوری تلوکی[2*] و حمید ملا[3]

[1] گروه مهندسی فناوری اطلاعات، دانشگاه اصفهان ، اصفهان، ایران
sh.azizi93@eng.ui.ac.ir

[2*] استادیار، مهندسی فناوری اطلاعات، دانشگاه اصفهان، اصفهان، ایران
m.ashouri@eng.ui.ac.ir

[3] استادیار، مهندسی فناوری اطلاعات، دانشگاه اصفهان، اصفهان، ایران
h.mala@eng.ui.ac.ir

چکیده

در خدمات میتنی بر مکان با توجه به موقعیت مکانی کاربران، خدمات ارائه می‌شود. این خدمات می‌تواند توسط یک فرد یا گروهی از افراد استفاده شود؛ در هر دو حالت لازم است، مکان افراد برای فراهم‌کنندهٔ خدمات آشکار شود، بنابراین به‌منظور تأمین امنیت کاربران، لازم است حریم مکانی آنها حفظ شود. از این رو راه‌کارهایی برای حفظ حریم مکانی افراد در هنگام استفاده از خدمات مبتنی بر مکان ارائه شده‌اند. در این مقاله راه‌کارهای حفظ حریم مکانی گروهی از کاربران در هنگام استفاده از خدمات مبتنی بر مکان بررسی شده‌اند که در آنها، گروهی از کاربران با حفظ حریم مکانی قصد استفاده از خدمات مبتنی بر مکان را دارند. راه‌کارهای موجود در دو دسته طبقه‌بندی و بررسی شده‌اند؛ دستهٔ نخست راه‌کارهای فردی هستند که حریم مکانی فرد را با همکاری گروه کاربران مجاور حفظ می‌کنند و دستهٔ دوم راهکارهای گروهی یافتن نزدیک‌ترین همسایهٔ گروهی با حفظ حریم مکانی هستند. در ادامه، روش‌های موجود از نظر کارایی و امنیت مقایسه شده و چالش‌های آن‌ها بررسی می‌شود؛ درنهایت پیشنهادهایی برای راه‌کارهای آینده ارائه خواهد شد.

واژگان کلیدی: خدمات مبتنی بر مکان، حفظ حریم مکانی فرد، نزدیک‌ترین همسایه به گروهی از کاربران، حمله تبانی.

۱- مقدمه

در خدمات مبتنی بر مکان با توجه به مکان افراد، به آن‌ها خدمات ارائه می‌شود. در این خدمات دو نوع پرس‌وجو وجود دارد: پرس‌و جوی فردی و پرس‌وجوی گروهی. در پرس‌وجوی فردی، فرد موقعیت جغرافیایی و درخواست خود را برای فراهم‌کنندهٔ خدمات مبتنی بر مکان ارسال می‌کند و فراهم‌کننده به درخواست او پاسخ می‌دهد؛ به‌عنوان مثال رانندهٔ یک اتومبیل، درخواست یافتن نزدیک‌ترین پمپ بنزین را برای فراهم‌کننده ارسال کرده، و در پاسخ فهرستی از نزدیک‌ترین پمپ بنزین‌ها به مکان خود را دریافت می‌کند.

در پرس‌وجوهای گروهی، گروهی از افراد یک درخواست را برای فراهم‌کننده ارسال می‌کنند و فراهم‌کننده به درخواست آن‌ها پاسخ می‌دهد (فراهم‌کننده خدمات مبتنی بر مکان، سروری است که بر اساس مکان کاربر، به درخواست کاربر پاسخ می‌دهد و اطلاعات مطلوب را به وی می‌فرستد). گروهی از دوستان قصد یافتن نزدیکترین رستوران به گروه را داشته باشند، و یا از بین چند پزشک نزدیک‌ترین آن‌ها هر چه سریع‌تر به نزد بیمار اورژانسی مراجعه کند، نمونه‌هایی از پرس و جوی گروهی هستند. افشای اطلاعات مکانی افراد ممکن است، باعث افشای اطلاعات شخصی آن‌ها شود؛ از

این‌رو در خدمات مبتنی بر مکان، باید حفظ حریم خصوصی افراد مورد توجه قرارگیرد و حتی داده‌هایی که در مورد مکان کاربر، اطلاعاتی را افشا می‌سازند، خطرآفرین هستند [15]؛ از این رو افشای اطلاعات حساس باعث افزایش نگرانی کاربران [16] و درنتیجه کاهش استفاده از خدمات می‌شود. در پرس‌وجوهای فردی حریم مکانی فرد باید در برابر فراهم‌کننده و مهاجم بیرونی حفظ شود؛ اما در پرس‌وجوهای گروهی علاوه‌بر حفظ امنیت افراد در برابر مهاجم بیرونی و فراهم‌کننده (حریم مکانی برون گروهی) باید حریم مکانی هر فرد در برابر سایر اعضای گروه نیز حفظ شود (حریم مکانی درون گروهی).

در این مقاله راه‌کارهای حفظ حریم مکانی در خدمات مبتنی بر مکان که در آن گروهی از افراد با یکدیگر در ارتباط هستند در دو دسته مرور شده‌اند. این راه‌کارها از سال‌های ۲۰۰۶ تا ۲۰۱۵ ارائه شده‌اند. دستهٔ نخست راه‌کارهایی هستند که به پرس‌وجوی گروهی یافتن نزدیک‌ترین همسایه گروهی[1](GNN) با حفظ حریم مکانی پرداخته‌اند و دستهٔ دوم راه‌کارهایی هستند که در پرس‌وجوی فردی قصد دارند حریم مکانی فرد را با همکاری کاربران مجاور او حفظ کنند.

ساختار مقاله بدین صورت است: در بخش دوم، راه‌کارهای حفظ حریم مکانی گروهی و در بخش سوم راه‌کارهای حفظ حریم مکانی فرد با همکاری کاربران مجاور مرور می‌شود؛ در بخش چهارم، راه‌کارهای مرورشده مقایسه و چالش‌های آنها بررسی و پیشنهادهایی ارائه می‌شود. در بخش پنجم مطالب ذکرشده جمع‌بندی می‌شوند.

۲- راه‌کارهای حفظ حریم مکانی گروهی

نمونه‌ای از پرس‌وجوهای گروهی یافتن مکان جلسه‌ای است که کم‌ترین فاصلهٔ جمعی را از کل گروه داشته باشد. در راه‌کارهای گروهی از لحاظ امنیتی تنها این پرس‌وجو بررسی شده است و راه‌کارهای مربوطه در این بخش مرور می‌شوند.

نخستین راه‌کار در این زمینه مقالهٔ هاشم[2] و همکاران [1] است. اعضای گروه P_1، P_2، ... و P_n به‌ترتیب در مکان‌های l_1، l_2، ... و l_n هستند و قصد یافتن نزدیک‌ترین مکان ملاقات به کل گروه را دارند. به‌طور تصادفی کاربری به‌عنوان هماهنگ‌کننده[3] گروه انتخاب می‌شود که اعضای گروه و شناسه پرس‌وجو را مشخص می‌کند. هر عضو P_i شناسهٔ پرس‌وجو و موقعیت تقریبی خود را در قالب ناحیه پنهانی R_i برای فراهم‌کنندهٔ خدمات، به‌طور گمنام ارسال می‌کند. مقدار R_i را فقط فراهم‌کننده و P_i می‌داند. فراهم‌کننده با توجه به مکان‌های تقریبی گروه، مجموعه‌ای از نزدیک‌ترین مکان‌های جلسه $\{O_1, O_2, \dots, O_m\}$ و مجموع بیشینه فاصله اقلیدسی بین ناحیه نادقیق کاربران (R_i) و هر نقطه از مجموع پاسخ را تحت عنوان $d_{max}(O_h)$ محاسبه و برای گروه ارسال می‌کند که در رابطه (۱) نشان داده شده است. در این رابطه $\boldsymbol{m}$ برابر تعداد نقاط مجموعه پاسخ است.

$$d_{max}(O_h) = \sum_{i=1}^{n} MaxDist(R_i, O_h), \quad O_h \in \{O_1, O_2, \dots, O_m\} \tag{۱}$$

سپس، به‌ترتیب هر عضو P_i مطابق رابطهٔ (۲) از مقدار $d_{max}(O_h)$ مقدار بیشینه فاصلهٔ خود تا O_h $(MaxDist(R_i, P_h))$ را کم کرده و مقدار فاصلهٔ واقعی خود $(Dist(l_i, O_h))$ را اضافه و نتیجه را برای عضو بعدی ارسال می‌کند.

$$d'_{max}(O_h) = d_{max}(O_h) - MaxDist(R_i, O_h) + Dist(l_i, O_h) \tag{۲}$$

پس از انجام این محاسبه توسط اعضای گروه، درنهایت، برای هر نقطه مجموع فاصله واقعی کاربران محاسبه و نزدیک‌ترین نقطه یافت می‌شود. فراهم‌کننده می‌تواند به‌منظور انجام هرس روی مجموعه پاسخ به همراه محاسبه $\boldsymbol{d_{max}(O_h)}$، مجموع کمینه فاصلهٔ هر کاربر $\boldsymbol{P_i}$ در ناحیه پنهانی از نقاط مجموعه پاسخ را تحت عنوان $\boldsymbol{d_{min}(O_h)}$ مطابق رابطه (۳) نیز ارسال کند:

$$d_{min}(O_h) = \sum_{i=1}^{n} MinDist(R_i, O_h), \quad O_h \in \{O_1, O_2, \dots, O_m\} \tag{۳}$$

سپس اعضا با توجه به رابطه (۴) مقادیر را به‌روز می‌کنند، در این رابطه $MinDist(R_i, O_h)$ حداقل فاصله‌ی کاربر P_i در ناحیهٔ پنهانی R_i از نقطهٔ O_h است.

$$d'_{min}(O_h) = d_{min}(O_h) - MinDist(R_i, O_h) + Dist(l_i, O_h) \tag{۴}$$

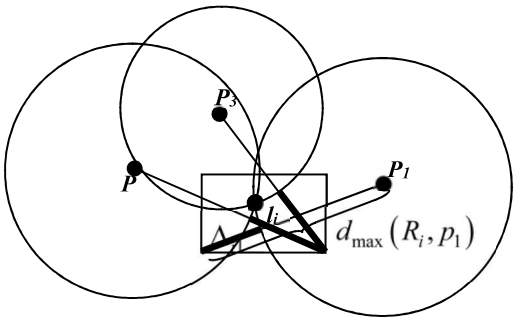
هر عضو مقادیر $d'_{min}(O_h)$ و $d'_{max}(O_h)$ را به‌روز و درصورتی‌که $d'_{min}(O_j)$ از $d'_{max}(O_h)$ بیشتر باشد O_j را از مجموعه پاسخ هرس می‌کند و مجموعه پاسخ هرس‌شده و

[1] Group Nearest Neighbor
[2] Hashem
[3] Coordinator

مقادیر به‌روزشده را برای عضو بعدی می‌فرستد؛ روال به‌ترتیب توسط n عضو انجام می‌شود. درنهایت می‌توان پاسخ بهینه و یا k نزدیک‌ترین همسایه گروه[1] را یافت. در این روش مدل مهاجمان شبه‌درستکار است؛ چون فرض می‌شود کاربران از روال پروتکل تبعیت می‌نمایند و قادر به انجام عملیات دلخواه نیستند. طبق مقاله [3] در برابر تبانی جزئی فراهم‌کننده و کاربر ماقبل و کاربر مابعد قربانی، امن نیست؛ در این حمله فراهم‌کننده ناحیه‌های پنهانی را برای کاربر ماقبل و کاربر مابعد قربانی P_i افشا می‌سازد؛ و آن‌ها تفاضل ایجادشده برای $d'_{max}(O_j)$ توسط P_i را محاسبه می‌کنند؛ (یعنی Δ_{ij}). در واقع Δ_{ij} برابر تفاضل حداکثر فاصله کاربر P_i در ناحیهٔ پنهانی و فاصله دقیق P_i از نقطه O_j است:

$$\Delta_{ij} = MaxDist(R_i, O_j) - Dist(l_i, O_j) \qquad (۵)$$

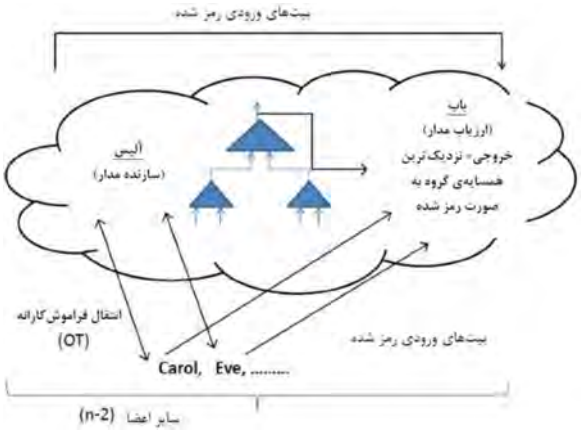
در رابطهٔ (۵) اگر $MaxDist(R_i, O_j)$ افشا شود، مقدار فاصلهٔ حقیقی کاربر از نقطه O_j محاسبه و با آشکارشدن فاصله کاربر از سه نقطه، مکان دقیق او محاسبه می‌شود؛ کاربر ماقبل و مابعد برای محاسبهٔ $MaxDist(R_i, O_j)$ از ناحیه‌های پنهانی استفاده می‌کنند. بدین صورت که به‌ازای هر ناحیهٔ پنهانی فرض می‌شود کاربر P_i در آن ناحیه است و با رابطهٔ (۵) فاصله دقیق کاربر از دست‌کم سه نقطه محاسبه می‌شود. سپس به‌ازای هر نقطه یک دایره به مرکز آن نقطه و شعاع فاصلهٔ کاربر از آن نقطه رسم می‌شود. درصورتی‌که به‌ازای سه نقطه دایره‌های رسم‌شده در یک نقطه در داخل ناحیهٔ پنهانی یکدیگر را قطع کنند، ناحیهٔ پنهانی انتخاب شده، صحیح و مکان دقیق کاربر در نقطه تقاطع سه دایره است. در شکل (۱) این حمله نشان داده شده است.



(شکل-۱): به‌دست آوردن مکان دقیق کاربر با حمله تبانی جزئی [3]

[1] K-Group Nearest Neighbor (KGNN)

هوانگ[2] و همکارانش در مقاله [2]، راهکاری بر مبنای رمزنگاری در مدل شبه‌درستکار ارائه داده‌اند که از مدارهای آشفته استفاده می‌کند. آن‌ها دو مدل متمرکز و توزیع‌شده ارائه کرده‌اند. در مدل متمرکز، یکی از کاربران (آلیس) باید مدار آشفته را برای محاسبه تابع GNN بسازد و کاربر دیگری (باب) آن را ارزیابی کند. سایر اعضای گروه، بیت ورودی‌های رمزشده خود را از سازنده مدار با انتقال فراموش‌کارانه[3] دریافت می‌کنند و بیت‌های ورودی خود را برای ارزیابی‌کنندهٔ مدار می‌فرستند تا او مدار را برای به‌دست‌آوردن GNN ارزیابی کند؛ سپس، آلیس نتیجه را تفسیر می‌کند. مراحل کار در شکل (۲) نشان داده شده است.



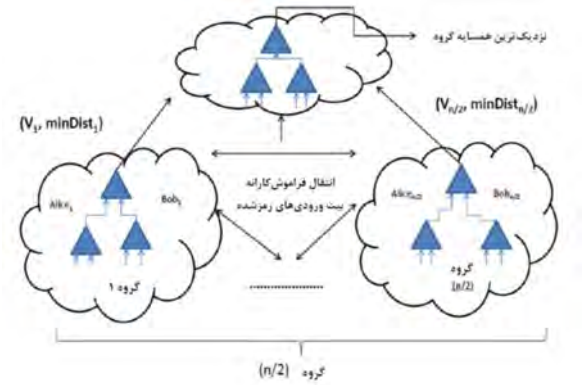
(شکل-۲): نمایی از مدل متمرکز [2]

در مدل توزیع‌شده، مدارهای بیشتری ساخته می‌شود؛ هر مدار یک سازنده و یک ارزیاب[4] دارد. حداکثر به تعداد نصف تعداد اعضای گروه، مدار ساخته می‌شود. در این صورت، در هر مدار، دو کاربر، یکی به‌عنوان سازنده و دیگری، ارزیاب مدار وجود دارد؛ مکان‌های نامزد به‌طور مساوی در بین مدارها توزیع و مدارها به‌طور موازی، و جداگانه، ارزیابی می‌شوند. در پایان، ارزیاب‌ها، مداری را به‌منظور محاسبه کمینه مقدارهای محاسبه‌شده توسط سایر مدارها می‌سازند. شکل (۳) مراحل این روش را نشان می‌دهد.

مزیت مدل توزیع‌شده، کاهش هزینهٔ محاسباتی و هزینه زمانی است. هزینه ارتباطی در دو مدل برابر و متعلق به انتقال فراموش‌کارانه است و تعداد انتقال‌های فراموش‌کارانه هر کاربر برابر تعداد مکان‌های جلسه نامزد

[2] Huang
[3] Oblivious Transfers (OT)
[4] Evaluator

است. مشکل اصلی این روش هزینهٔ زمانی و ارتباطی بالای آن به‌دلیل استفاده از مدارهای آشفته است.



(شکل-۳): مدل توزیع شده با (n/2) گروه [2]

عاشوری[1] و همکاران در مقاله [3] راه‌کاری تحت عنوان GLP[2] در مدل بدخواه ارائه کرده‌اند. در این راهکار اعضا با انجام محاسبات چندسویهٔ امن مرکز ثقل مکان‌های اعضای گروه را محاسبه و برای فراهم‌کننده ارسال می‌کنند؛ و فراهم‌کننده در پاسخ، نزدیک‌ترین مکان جلسه به مرکز ثقل را ارسال می‌کند. از شبکه وتوی گم‌نام[3][6] و رمزنگاری هم‌ریخت پیلیه[4] [8] به‌طور هم‌زمان استفاده می‌شود؛ گروه گردشی G از مرتبه عدد اول بسیار بزرگ q انتخاب می‌شود؛ به‌طوری‌که G گروهی از نوع پیلیه $(Z^*_{N^2})$ است. دو مولد غیریکسان g_s, g انتخاب می‌شوند، مولد g در شبکه‌وتوی گم‌نام و مولد g_s با شرط $g_s = 1 \bmod N$ برای رمزنگاری پیلیه استفاده می‌شود؛ سپس، دو مرحلهٔ زیر طی می‌شود:

در مرحلهٔ نخست، اعضای گروه مقادیر شبکهٔ وتوی گم‌نام را به اشتراک می‌گذارند. بدین منظور هر کاربر P_i یک عدد تصادفی $a_i \in_R Z_{N^2}$ را انتخاب و مقدار g^{a_i} را پخش همگانی ؛ سپس هر کاربر P_i مقدار $g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^{n} g^{a_j})$ را محاسبه می‌کند.

در مرحلهٔ دوم، به‌منظور محاسبهٔ مرکز ثقل، هر کاربر P_i غیر از نماینده، مختصات مکان دقیق خود (x_i, y_i) را با مولد g_s و مقادیر شبکه وتوی گمنام به‌صورت رابطه (۶) مخفی و پخش همگانی می‌کند.

$$(g_s^{x_i} g^{a_i b_i}, g_s^{y_i} g^{a_i b_i}) \qquad (۶)$$

نمایندهٔ گروه (P_α) برای انجام رمز پیلیه با استفاده از کلید عمومی فراهم‌کننده، دو عدد تصادفی r_1, r_2 را انتخاب و مکان خود را مطابق رابطه (۷) رمز و پخش همگانی می‌کند. لازم به ذکر است به طور تصادفی، یکی از اعضای گروه به‌عنوان نماینده انتخاب می‌شود.

$$(g_s^{x_\alpha} g^{a_i b_i} {r_1}^N, g_s^{y_\alpha} g^{a_i b_i} {r_2}^N) \qquad (۷)$$

سپس P_α مقادیر ارسالی کل گروه را در هم ضرب می‌کند که برابر مقدار رابطه (۸) است:

$$\begin{aligned}&(g_s^{x_\alpha} g^{a_i b_i} {r_1}^N \prod_{i=1, i\neq\alpha}^{n} g_s^{x_i} g^{a_i b_i},\\ &g_s^{y_\alpha} g^{a_i b_i} {r_2}^N \prod_{i=1, i\neq\alpha}^{n} g_s^{y_i} g^{a_i b_i})\end{aligned} \qquad (۸)$$

با ضرب مقادیر، ماسک شبکه وتوی گم‌نام ازبین می‌رود و مجموع مختصات رمز شده‌ی گروه با کلید عمومی فراهم‌کننده به روش پیلیه محاسبه می‌شود که در رابطه (۹) نشان داده شده است؛ این مقدار به‌همراه تعداد اعضای گروه برای فراهم‌کننده ارسال می‌شود.

$$\begin{aligned}&(Enc_{pk}(\sum x), Enc_{pk}(\sum y), n)\\ &= (g_s^{\sum x} r_1^N mod N^2, g_s^{\sum y} r_2^N mod N^2, n)\end{aligned} \qquad (۹)$$

فراهم‌کننده با رمزگشایی رابطه (۹) مرکز ثقل گروه را محاسبه و نزدیک‌ترین همسایه به آن را برای P_α ارسال می‌کند تا مکان جلسه را برای اعضای گروه پخش همگانی کند.

در مدل مهاجم بدخواه کاربران مجاز به رفتار دلخواه (خارج از روال پروتکل) هستند؛ در این مقاله برای مقابله با مهاجم بدخواه از اثبات صفر دانش اشنور [9] استفاده می‌شود. مختصات کاربر P_i، با استفاده از مقادیر شبکهٔ وتوی گم‌نام پنهان می‌ماند؛ بنابراین با توجه به امنیت ساختار شبکهٔ وتوی گم‌نام [6]، پروتکل GLP در برابر تبانی جزئی تا سطح $n-2$ نفر امن است. مرکز ثقل گروه فقط توسط فراهم‌کننده قابل محاسبه است. هزینهٔ محاسباتی این راه‌کار $O(n)$ نمارسانی است و مشکل اصلی این راه‌کار به‌دست‌آوردن نزدیک‌ترین مکان جلسه به مرکز ثقل گروه و نه مکان کل گروه است و ممکن است این مکان جلسه پاسخ دقیق نباشد.

[1] Ashouri
[2] Group Location Privacy
[3] Anonymous Veto Network
[4] Paillier

در سال ۲۰۱۲ راه‌کار مقاله [17] ارائه شده است که در آن اعضای گروه پس از ارسال نواحی پنهانی و دریافت مجموعه پاسخ از فراهم‌کننده، با استفاده از رمزنگاری هم‌ریخت پاسخ دقیق را می‌یابند. روال بدین صورت است که یکی از اعضای گروه به‌طور تصادفی به‌عنوان مدیر گروه انتخاب می‌شود و جفت کلید عمومی و خصوصی برای گروه تولید می‌کند؛ کلید عمومی را بین اعضای گروه به اشتراک می‌گذارد و کلید خصوصی را نزد خود نگه‌می‌دارد. حال هر عضو گروه با برخی از اعضای گروه اعداد تصادفی به‌اشتراک می‌گذارد؛ به‌طوری‌که مقداری که P_i با P_j به‌اشتراک می‌گذارد ($\boldsymbol{s_{ij}}$)، قرینهٔ مقدار به اشتراک گذاشته‌شدهٔ P_j با P_i است $s_{ij} = -s_{ji}$. در ادامه هر کاربر P_i مجموع فاصلهٔ خود از هر نقطه و مجموع مقادیر تصادفی خود را ($MSK_i = \sum s_{ij}$) با کلید عمومی گروه رمز کرده و برای مدیر گروه ارسال می‌کند. براساس خاصیت رمزنگاری هم‌ریخت، مدیر گروه با ضرب مقادیر دریافتی مجموع فاصله از هر نقطه و مجموع ماسک‌های اعضای گروه را محاسبه می‌کند و چون مقادیر تصادفی اعضای گروه قرینه هستند، مجموع ماسک‌های اعضای گروه برابر صفر است و مدیر گروه قادر است با رمزگشایی مقادیر، نقطه با کم‌ترین مجموع را انتخاب کند. در این مقاله به‌طودقیق نحوهٔ رمزگذاری و اشتراک مقادیر بین اعضای گروه تعیین نشده است و به‌طوردقیق هزینه‌های محاسباتی آن قابل محاسبه نیست.

در سال ۲۰۱۳ عاشوری و همکاران در مقاله [18] راه‌کار دیگری ارائه دادند، که در آن اعضای گروه با استفاده از شبکهٔ وتوی گم‌نام مرکز ثقل گروه را محاسبه می‌کنند. راه‌کار [18] را GLP-2 می‌نامیم. ابتدا گروه گردشی $\boldsymbol{G}$ از مرتبه عدد اول بسیار بزرگ q انتخاب می‌شود؛ سپس دو مرحله طی می‌شود: در مرحلهٔ نخست اعضای گروه دو شبکه وتوی گم‌نام راه‌اندازی می‌کنند؛ بنابراین هر کاربر P_i دو عدد تصادفی $a_i, a_i' \in_R Z_q$ را انتخاب و مقادیر ($g^{a_i}, g^{a_i'}$) را پخش همگانی می‌کند. سپس هر کاربر P_i مقادیر g^{b_i} و $g^{b_i'}$ را محاسبه می‌کند ($g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^{n} g^{a_j})$) و ($g^{b_i'} = (\prod_{j=1}^{i-1} g^{a_j'} / \prod_{j=i+1}^{n} g^{a_j'})$). در مرحله دوم هر کاربر P_i مختصات مکانی خود را با مقادیر شبکه پنهان و ارسال می‌کند. بنابراین در این راستا مقادیر ($g^{x_i} g^{a_i b_i}, g^{y_i} g^{a_i' b_i'}$) را پخش همگانی می‌کند. حال هر کاربر P_i مقادیر ($X = \prod_{i=1}^{n} g^{x_i} g^{a_i b_i}$، $Y = \prod_{i=1}^{n} g^{y_i} g^{a_i' b_i'}$) را محاسبه می‌کند و یکی از اعضای گروه آن را به‌همراه تعداد اعضای گروه برای فراهم‌کننده ارسال می‌کند. فراهم‌کننده پس از محاسبهٔ مرکز ثقل گروه، و نزدیک‌ترین مکان جلسه به مرکز ثقل را برای گروه ارسال می‌کند. این راه‌کار در برابر مهاجم بدخواه امن و دارای هزینهٔ محاسباتی از مرتبهٔ $O(n)$ نمارسانی است؛ اما پاسخ بهینه یافت نمی‌شود و مکان جلسه نیز آشکار است.

در مقاله [4] عاشوری و همکاران پروتکل Cloaked-Centroid را ارائه کردند که علاوه‌بر تأمین حریم مکانی اعضای گروه، حریم مکانی محل جلسه را نیز تأمین می‌کند؛ در این روش P_1، P_2، ...، P_n اعضای گروه هستند و گروه گردشی G از مرتبه عدد اول بسیار بزرگ q انتخاب می‌شود. راه‌کار شامل دو مرحله است: مرحلهٔ پنهان‌سازی مکان[1] و مرحلهٔ محاسبه محرمانه مرکز ثقل[2].

در مرحلهٔ نخست، هر عضو P_i مکان نادقیق خود را (R_i) به‌صورت گمنام پخش همگانی می‌کند. مکان نادقیق، شامل نقاط بالا سمت چپ و پایین سمت راست، از مستطیلی با دست‌کم مساحت تعیین‌شدهٔ کاربر (یعنی $A_{i,min}$)، و حاوی مکان دقیق P_i است. مساحت R_i بزرگ‌تر یا مساوی $A_{i,min}$ است. اعضای گروه به‌منظور محاسبهٔ ناحیهٔ حاوی مرکز ثقل گروه، میانگین نقاط بالای سمت چپ و همچنین میانگین نقاط پایین سمت راست ناحیه‌های پنهانی اعضا را محاسبه می‌کنند؛ این دو میانگین بیان‌گر ناحیه میانگین حاوی مرکز ثقل گروه است. عضوی به‌طور تصادفی به‌عنوان نماینده انتخاب می‌شود؛ نماینده ناحیه مرکز ثقل گروه را به‌صورت گم‌نام برای فراهم‌کننده و فراهم‌کننده مجموعه‌ای از نزدیک‌ترین نقاط به ناحیه مرکزثقل گروه را در پاسخ ارسال می‌کند.

در مرحلهٔ دوم، اعضای گروه با انجام محاسبات چند سویهٔ امن، مرکز ثقل مکان گروه را به‌صورت مخفی محاسبه می‌کنند؛ به‌طوری‌که در پایان محاسبات تنها اعضای گروه از مرکز ثقل آگاهی دارند. بدین منظور، اعضا، از طریق پروتکل شبکه وتوی گم‌نام و پروتکل توافق کلید جلسه BD **[7]** مکان دقیق خود را به‌صورت رمزشده برای گروه ارسال می‌کنند. بنابراین هر عضو P_i دو مقدار تصادفی $a_i, e_i \in_R Z_q$ انتخاب و مقدار (g^{a_i}, g^{e_i}) را پخش‌همگانی می‌کند؛ سپس مقدار $t_i = (g^{e_{i+1}} / g^{e_{i-1}})^{e_i}$ را محاسبه و پخش همگانی می‌کند. حال هر عضو گروه قادر به محاسبهٔ $g^{b_i} = (\prod_{j=1}^{i-1} g^{a_j} / \prod_{j=i+1}^{n} g^{a_j})$ و کلید مشترک

[1] Location Cloaking
[2] Blind Centroid Computation

(k') است؛ سپس هر عضو P_i مختصات محور x خود را با انجام رابطه (۱۰) رمز و پخش همگانی می‌کند:

$$w_i = g^{a_i b_i} g^{e_{i-1} e_i} g^{x_i} \qquad (۱۰)$$

در این رابطه $g^{a_i b_i}$ ماسک شبکه و $g^{e_{i-1} e_i}$ سهم P_i از کلید مشترک $\boldsymbol{k'}$ است. با ضرب مقادیر w_i کل اعضای گروه ماسک شبکه از بین می‌رود و مجموع مختصات رمزشده گروه با کلید مشترک k' حاصل می‌شود که در رابطه (۱۱) نشان داده شده است.

$$\begin{aligned} \prod_{i=0}^{n-1} w_i &= \prod_{i=0}^{n-1} g^{a_i b_i} g^{e_{i-1} e_i} g^{x_i} \\ &= \prod_{i=0}^{n-1} g^{a_i b_i} \prod_{i=0}^{n-1} g^{e_{i-1} e_i} \prod_{i=0}^{n-1} g^{x_i} \\ &= 1 \times k' \times g^{\sum_i x_i} \end{aligned} \qquad (۱۱)$$

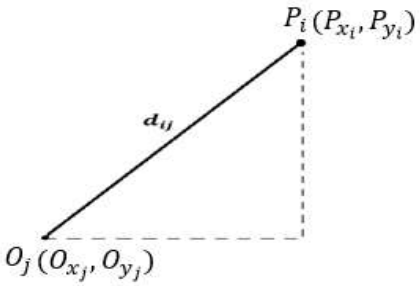
سپس حاصل‌ضرب رابطه (۱۱) بر کلید مشترک، تقسیم و مقدار $g^{\sum_i x_i}$ حاصل‌می‌شود و چون $\sum_i x_i$ مقدار کوچکی است با انجام لگاریتم گسسته می‌توان آن را محاسبه کرد و با انجام $(\frac{\sum_i x_i}{n})$ مرکز ثقل گروه محاسبه می‌شود؛ به‌دلیل مخفی‌بودن کلید جلسه، مرکز ثقل فقط توسط اعضای گروه قابل محاسبه است. مرحلهٔ دوم بر روی مختصات محور y گروه و محاسبه $\sum_i y_i$ نیز تکرار می‌شود؛ سپس، اعضا از بین مجموعه پاسخ، نزدیک‌ترین مکان به مرکز ثقل را به‌دست می‌آورند. این راه‌کار، از طریق اثبات صفر دانش، مانع دخالت مهاجم بدخواه می‌شود؛ مختصات دقیق کاربر به‌کمک مقادیر شبکه وتوی گم‌نام و کلید از دید افراد داخل و خارج گروه پنهان می‌ماند و به‌دلیل استفاده از کلید مشترک فقط اعضای گروه قادر به آگاهی از مکان جلسه انتخابی هستند؛ به‌علاوه در مقابل حملهٔ تبانی تا سطح $n-2$ نفر امن است؛ اما در این راه‌کار مکان جلسه انتخابی ممکن است پاسخ دقیق نباشد و هزینه محاسباتی $O(n)$ نمارسانی است.

رحمان‌خان[1] به‌همراه همکاران در مقاله [5] حمله MPAD[2] و دو الگوریتم LOOP[3] و H − LOOP[4] را معرفی کرده است. اعضای گروه P_1، P_2، ... ، P_n و مجموعه پاسخ O_1، O_2، ... ، O_n هستند. مختصات دقیق کاربر P_i را با $(\boldsymbol{P_{x_i}}, \boldsymbol{P_{y_i}})$ و مختصات نقطه O_j را با (O_{x_j}, O_{y_j}) و مجموع فاصله گروه از نقطه O_j با D_j نشان داده می‌شود.

درحمله MPAD با دراختیارداشتن مجموع فاصلهٔ کاربران از نقاط مجموع پاسخ، می‌توان مکان دقیق کاربران را، البته بدون امکان انتساب مقدار محاسبه‌شده به مالک آن، محاسبه کرد. MPAD براین اساس است که مجموع فاصله محاسبه‌شده برای یک نقطهٔ $O_j \in O$ برابر مجموع فاصله هر یک از اعضای گروه P_1، P_2، ... ، P_n از آن نقطه است:

$$D_j = d_{1j} + d_{2j} + \cdots + d_{nj} \qquad (۱۲)$$

فاصلهٔ کاربر P_i از نقطهٔ O_j با d_{ij} نشان داده شده است. هر d_{ij} در فاصله اقلیدسی برابر طول یک خط مستقیم از مختصات مکان دقیق کاربر P_i تا مختصات نقطه O_j است که در شکل (۴) نشان داده شده است. طول این خط را طبق قضیه فیثاغورث با استفاده از رابطه‌ی $d_{ij} = \sqrt{(O_{x_j} - P_{x_i})^2 + (O_{y_j} - P_{y_i})^2}$ می‌توان محاسبه و به‌ازای n کاربر در مقادیر رابطه (۱۲) جایگزین کرد.



(شکل-۴): رسم خط مستقیم مابین مکان دقیق کاربر P_i و نقطه O_j

بنابراین D_j از رابطه‌ی (۱۳) به‌دست می‌آید:

$$D_j = \sqrt{(O_{x_j} - P_{x_1})^2 + (O_{y_j} - P_{y_1})^2} + \ldots + \sqrt{(O_{x_j} - P_{x_2})^2 + (O_{y_n} - P_{y_n})^2} \qquad (۱۳)$$

در این معادله مختصات دقیق نقطه O_j (O_{x_j}, O_{y_j}) و مجموع فواصل کاربران از آن (D_j) آشکار است و به‌ازای هر کاربر P_i دو مجهول (P_{x_i}, P_{y_i}) وجود دارد، بنابراین برای n کاربر، با آشکارشدن مجموع فاصله گروه از $2n$ نقطه نامزد می‌توان $2n$ معادله و $2n$ مجهول ساخت و حل کرد و حمله MPAD موفق به محاسبه مکان دقیق اعضای گروه می‌شود (در شبکهٔ راه‌ها چون همیشه نمی‌توان بین کاربر و نقطه، خط راست رسم کرد نمی‌توان به‌طور قطع حمله MPAD را اعمال کرد).

[1] Rahman Khan
[2] Multi-Point Aggregate Distance (MPAD)
[3] Location Oblivious Private
[4] Heuristic LOOP

راه‌کار [5] در مدل مهاجم شبه‌درستکار، به‌منظور مقابله با MPAD، مانع از آشکارسازی مجموع فاصله گروه، از نقاط مجموع پاسخ می‌شود.

در الگوریتم LOOP، فراهم‌کننده، مجموعه نقاط پاسخ را محاسبه و به تعداد مساوی در بین اعضا توزیع می‌کند. هر عضو، نماینده نقاط دریافتی از فراهم‌کننده است و با روش جمع چندسویه امن مقاله [10] مجموع فاصله از نقاط دریافتی را محاسبه و نزد خود نگه‌می‌دارد و از بین مجموعه نقاط، نقطه با کمینه مجموع فاصله را انتخاب و حاصل‌جمع آن را برای فراهم‌کننده ارسال می‌کند. بنابراین فراهم‌کننده از n کاربر n حاصل‌جمع را دریافت می‌کند و از بین آن‌ها، کم‌ترین حاصل‌جمع را انتخاب و برای نمایندهٔ آن نقطه، درخواست ارسال نقطه را می‌فرستد و نماینده مختصات نقطه را برای فراهم‌کننده ارسال می‌کند تا فراهم کننده آن را به عنوان پاسخ پخش همگانی کند.

الگوریتم LOOP مانع حمله MPAD توسط فراهم‌کننده می‌شود. برای مقاومت در برابر تبانی در الگوریتم LOOP باید شرط رابطهٔ (۱۴) برقرار باشد که در آن n تعداد اعضای گروه و x تعداد اعضای تبانی‌کننده است و N_{max} برابر بیشینه نقاط مجموعه پاسخ است.

$$N_{max} = \begin{cases} n \times \lfloor \frac{2(n-x)-1}{x} \rfloor & \text{اگر } 2(n-x)-1 \geq x \\ 2(n-x)-1 & \text{در غیر این صورت} \end{cases} \quad (۱۴)$$

در الگوریتم $H-LOOP$، هدف محدودکردن تعداد نقاط ارسالی برای هر نماینده است؛ بنابراین اعضای گروه با توجه به سطح امنیتی درخواستی یک آستانه β را که برابر N_{max} است، برای فراهم‌کننده ارسال می‌کنند و فراهم‌کننده، اگر تعداد نقاط مجموعه پاسخ، بیش از β باشد، پیش از تقسیم و ارسال آن‌ها برای گروه، ناحیهٔ حاوی مجموعه پاسخ را به تعدادی نواحی مساوی تقسیم می‌کند (γناحیه) و مرکز نواحی را برای گروه می‌فرستد؛ سپس گروه مجموع فاصله خود را از مرکز هر ناحیه محاسبه می‌کند؛ و ناحیهٔ حاوی مرکز با کمینه فاصله از گروه، انتخاب می‌شود؛ این روال تا زمان کمترشدن نقاط از آستانه β ادامه می‌یابد؛ سپس، برای مجموعه نقاط ناحیه نهایی الگوریتم LOOP اجرا می‌شود.

مزیت اصلی این راه‌کار عدم انجام محاسبات سنگین رمزنگاری و هزینه محاسباتی برای m نقطه و nکاربر $O(n \times m)$ جمع است. درصورت مقاومت در برابر حمله MPAD، مکان دقیق اعضای گروه افشا نمی‌شود؛ اما با بزرگ‌ترشدن مجموعه پاسخ، به‌دلیل تقسیم کردن مجموعه و ارسال مراکز نواحی، احتمال حمله افزایش می‌یابد؛ و راهکار به‌طور قطع در برابر تبانی امن نیست.

۳- راه‌کارهای حفظ حریم مکانی فردی

در راه‌کارهای حفظ حریم مکانی فردی، سه روش وجود دارد[13]:

۱) کاربر به‌طورمستقیم با فراهم‌کنندهٔ خدمات ارتباط داشته باشد[1]؛ به‌عنوان مثال مکان نادقیق خود را برای فراهم‌کننده خدمات ارسال کند. ارسال مکان نادقیق باعث کاهش کیفیت خدمات می‌شود.

۲) کاربر به منظور حفظ حریم مکانی، ابتدا با طرف سوم معتمد ارتباط برقرار می‌کند. در این سناریو طرف سوم در بین کاربر و فراهم‌کننده قرار می‌گیرد و عمدتاً به آن گم‌نام‌کننده[2] گفته می‌شود. طرف سوم به دو روش حریم مکانی فرد را در برابر فراهم‌کننده حفظ می‌کند: ۱. کاربر درخواست و مکان دقیق خود را برای گمنام‌کننده ارسال می‌کند $\{ID_u, query, x_u, y_u\}$ و گمنام‌کننده اطلاعات کاربر را از پرس‌وجو حذف می‌کند و سپس آن را برای فراهم‌کننده ارسال می‌کند $\{pseud_u, query, x_u, y_u\}$. فراهم‌کننده پاسخ را برای گمنام‌کننده و گمنام‌کننده برای کاربر ارسال می‌کند. ۲. گمنام‌کننده مکان دقیق کاربر را در ناحیه شامل $k-1$ کاربر دیگر پنهان می‌کند. در این راهکار کاربران ترجیحات خود را در رابطه با کمینه تعداد کاربران در ناحیه پنهانی[3]، کمینه و بیشینه اندازه ناحیه پنهانی تعیین می‌کنند. کاربر درخواست خود را برای گمنام‌کننده ارسال می‌کند و گم‌نام‌کننده باید ناحیهٔ پنهانی دارای خصوصیات موردنیاز k کاربر را ایجاد کند و ممکن است از این ناحیه یک مکان پوشانده‌شده[4] مانند مرکز ثقل k کاربر را محاسبه و مکان پوشانده‌شده را برای کاربر اولیه ارسال کند و کاربر پرس‌وجو را همراه این مکان برای فراهم‌کننده ارسال کند.

۳) کاربر با کاربران نظیر و مجاورخود، در راستای ایجاد مکان مبهم، همکاری می‌کند؛ سپس، مکان مبهم برای فراهم‌کننده ارسال می‌شود.

در این مقاله راه‌کارهای روش سوم بررسی می‌شوند.

[1] Client-Server
[2] Anonymizer
[3] Cloaked Region
[4] Masked Location

چاو[1] و همکاران [11] نخستین راه‌کار در حیطهٔ حفظ حریم مکانی فرد با همکاری گروهی از کاربران را ارائه دادند. نواحی به سلول‌هایی[2] تقسیم می‌شود و هر کاربر، کمینه تعداد کاربران به منظور ایجاد گمنامی[3] (k) و کمینه تعداد سلول‌های ناحیه پنهانی A_{min} را تعیین می‌کند. کاربر با همکاری دیگر کاربران به صورت نظیربه‌نظیر[4] ناحیه پنهانی با کمینه نیازمندی‌های کاربر را ایجاد و برای فراهم‌کننده ارسال می‌کنند. هر کاربر از طریق یک کارت شبکه، با سایر اعضا و به‌وسیلهٔ کارت دیگری، با فراهم‌کننده ارتباط برقرار می‌کند. این راه‌کار شامل سه مرحلهٔ جست‌وجوی کاربران نظیر، مرحلهٔ تنظیم مکان و مرحلهٔ پنهان‌سازی مکانی است.

در مرحلهٔ جست‌وجوی کاربران نظیر، هر کاربر u پیش از ارسال پرس‌وجو به فراهم‌کنندهٔ خدمات، درخواست همکاری را به کاربران مجاور خود در فاصله h (یک hop) ارسال می‌کند و منتظر دریافت پاسخ از کاربران مجاور می‌ماند. اگر کاربر مجاور (p) نخستین‌بار است که درخواست به او می‌رسد، مکان دقیق خود(x_p, y_p) و بیشینه سرعت حرکت خود (v_{max_p}) و زمان فعلی (t_p) را برای u ارسال می‌کند، درغیر این‌صورت، تکراری‌بودن را اطلاع می‌دهد. اگر تعداد کاربران مجاور u از حد نصاب کمتر باشد، u از کاربران همسایهٔ خود می‌خواهد که درخواست همکاری او را به کاربران مجاور خود ارسال کنند. روال تا زمانی ادامه می‌یابد که u از $k-1$ کاربر پاسخ دریافت کند.

در مرحلهٔ تنظیم مکان، u بیشینه فاصلهٔ خود از کاربر مجاور p را مطابق رابطه (۱۵) محاسبه می‌کند.

$$|up'| = |up| + (t_c - t_p)v_{max_p} \qquad (۱۵)$$

در این رابطه t_c برابر زمان فعلی است و $|up|$ برابر فاصله اقلیدسی u و p است که به‌صورت رابطه (۱۶) محاسبه می‌شود.

$$|\boldsymbol{up}| = \sqrt{(\boldsymbol{x_u} - \boldsymbol{x_p})^2 + (\boldsymbol{y_u} - \boldsymbol{y_p})^2} \qquad (۱۶)$$

پس از محاسبهٔ بیشینه فاصله برای همهٔ کاربران مجاور، وارد مرحلهٔ بعدی می‌شود. در مرحلهٔ پنهان‌سازی مکانی، $\boldsymbol{u}$ همراه $k-1$ عضو دیگر و در بیشینه فاصله محاسبه‌شده، یک گروه می‌سازد؛ بدین صورت که حداقل ناحیهٔ شامل کل گروه را مشخص می‌کند. این ناحیه به اندازه‌ای گسترش داده می‌شود که A_{min} کل گروه تأمین شود؛ سپس به‌طور تصادفی یکی از اعضای گروه را انتخاب و درخواست خود را به‌همراه ناحیهٔ پنهانی برای او ارسال و عضو انتخابی آن را برای فراهم‌کننده ارسال می‌کند. فراهم‌کنندهٔ مجموعه پاسخ را برای عضو انتخابی و عضو انتخابی برای $\boldsymbol{u}$ می‌فرستد. در این راه‌کار، اعضا به‌صورت درستکار در نظرگرفته شده‌اند؛ و راه‌کار در برابر عضو بدخواه و شنود امن نیست.

بائو[5] و همکاران در مقاله [12] روش PROS را ارائه داده‌اند، که توسعه‌یافتهٔ روش چاو و همکاران [11] در شبکه جاده‌ای است. ناحیه‌های پنهانی براساس سلول‌ها قابلیت حفظ حریم مکانی در شبکه جاده‌ای را ندارند؛ بنابراین در اینجا هر کاربر باید ضمن تعیین کمینه تعداد کاربران به‌منظور ایجاد گم‌نامی (k)، مقادیر کمینه تعداد قطعات جاده‌ای (N_{min}) و کمینه طول کل قطعات جاده‌ای مورد نیاز (L_{min}) را به‌منظور پنهان‌سازی تعیین کند؛ سپس مابقی روال مانند قبل طی می‌شود. ناحیهٔ پنهانی ایجادشده باید تنظیمات موردنیاز کل گروه را تأمین کند.

سولاناس[6] و همکاران در مقاله [13] چند سطح امنیتی در نظر گرفته‌اند. کاربر p پیش از ارسال درخواست به فراهم‌کننده باید $k-1$ کاربر دیگر را بیابد. بنابراین، با جستجو در فاصلهٔ معین L، کاربران مجاور را می‌یابد. درصورتی‌که تعداد به حد نصاب نرسد، کابران مجاور برای یافتن تعداد مجاور بیشتر، جستجو می‌کنند. در این مقاله یک نقطه برابر مرکز ثقل k عضو برای فراهم‌کنندهٔ خدمات ارسال می‌شود. به‌منظور محاسبهٔ مرکز ثقل k عضو، در پایین‌ترین سطح امنیتی، $k-1$ عضو مکان خود را به‌طور آشکار برای کاربر p ارسال می‌کنند و او مرکز ثقل را محاسبه و برای سایر اعضا و فراهم‌کننده ارسال می‌کند؛ بنابراین کاربر p به جای مکان دقیق خود، مکانی جعلی را ارسال می‌کند؛ در این سطح حریم مکانی $k-1$ عضو در برابر p حفظ نمی‌شود.

در سطح امنیتی بالاتر، اعضا به مقادیر ارسالی مکان خود، نوفه گاوسی اضافه می‌کنند؛ به‌طوری‌که هنگام محاسبهٔ مرکز ثقل، اثر آن از بین می‌رود. پس از محاسبه مرکز ثقل، کاربر p مرکز ثقل را برای فراهم‌کننده و سایر اعضا ارسال

[1] Chow
[2] Grid
[3] K-Anonymous
[4] Peer-To-Peer (P2P)
[5] Bao
[6] Solanas

می‌کند. هر کاربر p_i مقادیر $(x'_i, y'_i) = (x_i, y_i) + (N^x{}_i, N^y{}_i)$ را ارسال می‌کند که (x_i, y_i) برابر مختصات مکان کاربر و $(N^x{}_i, N^y{}_i)$ برابر نوفه اضافه شده است. نحوهٔ محاسبهٔ مرکز ثقل $\bar{P}$ در رابطه (۱۷) نشان داده شده است. در این سطح اگر کاربر p_i بدون تغییر مکان، چندین بار مکان جمع‌شده با نوفه گاوسی را ارسال کند، می‌توان مکان دقیق او را به‌دست آورد؛ درنتیجه حریم مکانی اعضا به‌طور کامل حفظ نمی‌شود.

$$\begin{aligned}\bar{P} &= \left(\frac{\sum_{i=1}^{k} x'_i}{k}, \frac{\sum_{i=1}^{k} y'_i}{k}\right)\\ &= \left(\frac{\sum_{i=1}^{k}(x_i + N^x{}_i)}{k}, \frac{\sum_{i=1}^{k}(y_i + N^y{}_i)}{k}\right)\\ &= \left(\frac{\sum_{i=1}^{k} x_i}{k}, \frac{\sum_{i=1}^{k} y_i}{k}\right)\\ &+ \left(\frac{\sum_{i=1}^{k} N^x{}_i}{k}, \frac{\sum_{i=1}^{k} N^y{}_i}{k}\right)\\ &= \left(\frac{\sum_{i=1}^{k} x_i}{k}, \frac{\sum_{i=1}^{k} y_i}{k}\right) + (\bar{N}^x, \bar{N}^y)\\ &\approx \left(\frac{\sum_{i=1}^{k} x_i}{k}, \frac{\sum_{i=1}^{k} y_i}{k}\right) + (0,0)\end{aligned} \tag{۱۷}$$

در سطح امنیتی بالاتر، از رمزنگاری هم‌ریخت[1] استفاده می‌شود. $k-1$ کاربر مکان خود را با کلید عمومی فراهم‌کننده رمز و برای کاربر p ارسال می‌کنند، کاربر p از رمزنگاری هم‌ریخت برای محاسبه مرکز ثقل استفاده می‌کند؛ و پس از محاسبه مجموع مختصات رمزشده، آن را به‌همراه k برای فراهم‌کننده ارسال و فراهم‌کننده آن را رمزگشایی و مرکز ثقل را محاسبه می‌کند. این روش در برابر تبانی کاربر p و فراهم‌کنندهٔ خدمات، امن نیست.

در بالاترین سطح امنیتی روال از محوریت کاربر اولیه p خارج می‌شود، او یک زنجیره تصادفی از اعضا ایجاد می‌کند و مکان دقیق خود را با کلید عمومی فراهم‌کننده رمز و از $k-1$ عضو به‌طور تصادفی عضوی را انتخاب می‌کند و مقدار رمزشده را برای او می‌فرستد؛ عضو بعدی مکان خود را از طریق رمزنگاری هم‌ریخت، به مقدار دریافتی اضافه می‌کند و از $k-2$ عضو باقی‌مانده عضو دیگری را انتخاب و مقدار رمزشده را برای او ارسال می‌کند. روال تا انتخاب کل اعضا و محاسبهٔ مجموع مختصات رمزشده ادامه می‌یابد. کاربر نهایی مجموع نهایی را برای p ارسال و p آن را همراه k برای فراهم‌کننده ارسال می‌کند. فراهم‌کننده پس از رمزگشایی مجموع رمزشده مرکز ثقل را محاسبه و به درخواست p پاسخ می‌دهد. راهکار این مقاله در برابر تبانی جزئی امن نیست؛ و امکان تبانی کاربر دوم با فراهم کننده و آشکارشدن مکان کاربر اولیه وجود دارد.

هو[2] و همکاران [14] روش دیگری ارائه می‌کنند که در آن اعضای مجاور کاربر درستکار فرض نشده‌اند. این راه‌کار شامل دو مرحله است؛ در مرحلهٔ نخست، کاربران مجاور کاربر اولیه، تعیین می‌شوند؛ از پایگاه داده حاوی گراف مجاورت کاربران استفاده می‌شود، درواقع این پایگاه‌داده حاوی اطلاعات مجاوربودن کاربران مانند طول سیگنال دریافتی[3]، تفاوت زمان ورود[4] است، این اطلاعات مجاورتی به گراف مجاورت مدل می‌شوند در گراف مجاورت، رئوس بیان‌گر کاربران و هر یال (u,v) بیان‌گر مجاوربودن دو کاربر u و v و وزن یال (u,v) نشان‌دهندهٔ فاصلهٔ تقریبی دو کاربر u و v است؛ سپس برروی گراف تشکیل‌شده خوشه‌بندی جزئی با تضمین کمینه k عضو در خوشه انجام می‌شود؛ بیشینه وزن یال (MEW)[5] در خوشه‌بندی تعیین می‌شود. برای کنترل MEW از ویژگی t-connected استفاده می‌شود. دو رأس a, b، t-connected هستند اگر مسیر $a, v_1, v_2, \dots, b$ وجود داشته باشد که در آن وزن هیچ یالی از t بیش‌تر نباشد. مقدار t برابر MEW است. با انجام خوشه‌بندی، مجاوران هر گروه از کاربران، صرف‌نظر از کاربر درخواست کننده خدمات، اعضای ثابتی است.

در مرحلهٔ دوم، برای تعیین محدودهٔ ناحیه پنهانی، اعضای هر خوشه، از طریق محاسبات چندسویه امن کوچک‌ترین ناحیه پنهانی شامل همه کاربران را به‌دست می‌آورند. در این مرحله محدودهٔ بالا و پایین مختصات کاربران بدون افشای مختصات آن‌ها تعیین می‌شود که به آن محدودسازی امن[6] گویند. در این راستا محدوده به‌تدریج تا زمان توافق k کاربر افزایش می‌یابد. پس از آن، کاربر اولیه درخواست خود را به همراه ناحیه پنهانی شامل k کاربر، برای فراهم‌کننده ارسال می‌کند.

۴- مقایسه

راه‌کارهای هاشم و همکاران [1] و هوانگ و همکاران [2] و رحمان‌خان و همکاران [5] در مدل شبه درست‌کار بوده و به‌طور قطع در برابر تبانی جزئی نیز امن نیستند. راه‌کار

[1] Public-Key Privacy Homomorphism

[2] Hu
[3] Received Signal Strength (RSS)
[4] Time Difference Of Arrival (TDOA)
[5] Maximum Edge Weight (MEW)
[6] Secure Bounding

هوانگ و همکاران به‌دلیل استفاده از مدارهای آشفته دارای هزینه ارتباطی بالایی است از این‌رو سایر راه‌کارها کاربردی‌تر هستند. راه‌کارهای هاشم و همکاران و رحمان‌خان و همکاران از لحاظ محاسباتی کارا هستند و فقط به عملیات جمع نیاز دارند. راه‌کار هاشم و همکاران [1] از راه‌کار رحمان‌خان و همکاران [5] کاراتر است؛ اما در برابر تبانی جزئی فراهم‌کننده و دو کاربر امن نیست؛ امنیت راه‌کار رحمان‌خان و همکاران [5]در برابر تبانی جزئی مشروط به بزرگی فضای مجموعه پاسخ و اعمال حملهٔ MPAD است. به‌علاوه راه‌کارهای هاشم و همکاران [1] و رحمان‌خان و همکاران [5] کانال ارتباطی بین اعضای گروه را امن فرض کرده‌اند. راه‌کارهای مدل شبه درست‌کار در برابر حملهٔ MPAD امن نیستند؛ زیرا مجموع فاصلهٔ کاربران از نقاط به‌طور آشکار محاسبه می‌شود؛ به علاوه در برابر تبانی جزئی تا سطح $n-2$ نفر امن نیستند.

راه‌کارهای GLP، GLP-2 و cloaked centroid در مدل بدخواه ارائه شده‌اند و با وجود عدم نیاز به کانال امن کارا هستند و هزینهٔ محاسباتی آن‌ها از مرتبهٔ $O(n)$ نمارسانی است. راه‌کار cloaked centroid محرمانگی مکان جلسه را حفظ می‌کند؛ اما در این سه راه‌کار نزدیک‌ترین مکان جلسه به مرکز ثقل انتخاب می‌شود و امکان دارد این مکان نزدیک‌ترین همسایه با کم‌ترین مجموع فاصلهٔ گروه نباشد. درصورتی‌که در این سه راه‌کار قصد داشته باشیم، نزدیک‌ترین همسایهٔ گروه با کم‌ترین مجموع فاصله گروه یافت شود باید دو پروتکل را به‌ازای نقاط مجموعه پاسخ (m) تکرار کرد و از این‌رو هزینهٔ محاسباتی از مرتبهٔ $O(nm)$ نمارسانی می‌شود؛ حتی درصورتی‌که مدل مهاجم شبه‌درست‌کار باشد، این هزینه اعمال می‌شود.

(جدول-۱): مقایسه روش‌های یافتن نزدیک‌ترین مکان به گروه.m تعداد نقاط کاندید، n تعداد کاربران و l تعداد بیت

		امنیت برون گروهی	امنیت درون گروهی	مدل تهدید	فاصله	امنیت در برابر تبانی	هزینه ارتباطی	هزینه محاسباتی	مکان جلسه	پاسخ بهینه
راه‌کارهای حفظ حریم مکانی گروهی	راه‌کار هاشم و همکاران[۱]	✗	✗	شبه درست کار	اقلیدسی	×	$O(nm)$	$O(nm)$ جمع	آشکار	✓
	راه‌کار هوانگ و همکاران[۲]	✓	✗	شبه درست کار	اقلیدسی	×	$O(2^l nm)$	هزینه ساخت و ارزیابی مدار	آشکار	✓
	راه‌کار عاشوری و همکاران(GLP)[۳]	✓	✓	بدخواه	اقلیدسی	$n-2$	$O(n)$	$O(n)$نمارسانی	آشکار	×
	راه‌کار عاشوری و همکاران(GLP-2)[۳]	✓	✓	بدخواه	اقلیدسی	$n-2$	$O(n)$	$O(n)$نمارسانی	آشکار	×
	راه‌کار عاشوری و همکاران(Cloaked-Centroid)[۴]	✓	✓	بدخواه	اقلیدسی	$n-2$	$O(n)$	$O(n)$نمارسانی	پنهان	×
	راه‌کار رحمان‌خان و همکاران(H-LOOP)[۵]	✗	✗	شبه درست کار	اقلیدسی	مشروط	$O(n^2m)$	$O(nm)$ جمع	آشکار	×

راه‌کارهای حفظ حریم مکانی فرد با همکاری گروه	راه‌کار چاو و همکاران [۱۱]	×	×	درست کار	اقلیدسی	-	$O(n)$	$O(n)$جمع	
	راهکار سولاناس و همکاران [۱۳]	×	×	شبه درست کار	اقلیدسی	×	$O(n)$	$O(n)$نمارساز ی	
	راه‌کار هو و همکاران [۱۴]	✓	✓	شبه درست کار	اقلیدسی	$n-1$	$O(n^2)$	هزینه خوشه‌بندی گراف + $O(n^2)$ مقایسه	
	راه‌کار بائو و همکاران [۱۲]	×	×	درست کار	شبکه راه‌ها	-	$O(n)$	$O(n)$جمع	

از این‌رو ارائهٔ راه‌کاری که در مدل شبه‌درست‌کار در برابر تبانی جزئی تا سطح $n-2$ نفر امن باشد، به علاوه کانال ارتباطی اعضا را نیز نا امن در نظر بگیرد و پاسخ دقیق با کم‌ترین مجموع فاصلهٔ گروه را بیابد، حائز اهمیت است.

در راه‌کار چاو و همکاران تنها امنیت کاربر در برابر فراهم‌کننده حفظ می‌شود و کاربران مجاور درست‌کار فرض شده‌اند. راهکار بائو و همکاران شبکه‌راه‌ها را نیز درنظر گرفته است، اما در این راه‌کار کابران مجاور درست‌کار فرض شده‌اند. در راه‌کار سولاناس و همکاران، کاربران مجاور شبه‌درست‌کار هستند و با وجود درنظرگرفتن چندین سطح امنیتی، این راه‌کار در برابر تبانی جزئی کاربر و فراهم‌کننده امن نیست. راه‌کار هو و همکاران در مدل مهاجم شبه‌درست‌کار در برابر تبانی جزئی تا سطح $n-2$ نفر امن است؛ این راه‌کار به طرف سوم غیر معتمد نیاز دارد. بنابراین ارائهٔ راه‌کاری که در مدل شبه‌درستکار و یا حتی مدل بدخواه در برابر تبانی جزئی تا سطح $n-2$ نفر امن باشد و نیازی به ارتباط با طرف سوم (معتمد یا غیر معتمد) نداشته باشد بهبود مناسبی محسوب می‌شود.

در راه‌کارهای [11-14] هدف یافتن کاربران مجاور کابر اولیه به‌طور امن است و کاربر اولیه با کاربران مجاور خود ارتباط برقرار می‌کند و قصد دارد با همکاری مجاوران، ناحیهٔ پنهانی را برای خود پیدا کند و به مسئلهٔ یافتن نزدیک‌ترین همسایهٔ گروه پرداخته نشده است. در مسئلهٔ نزدیک‌ترین همسایهٔ گروه اعضای گروه لزوماً مجاور یکدیگر نیستند؛ اما از ایده‌های موجود در این راه‌کارها می‌توان جهت یافتن نزدیک‌ترین همسایهٔ گروهی استفاده کرد. خلاصه‌ای از توضیحات ذکرشده در جدول (۱) نشان داده شده است.

۵- جمع‌بندی

در این مقاله راه‌کارهای حفظ حریم مکانی کاربران در خدمات مبتنی بر مکان در دو دستهٔ یافتن نزدیک‌ترین همسایهٔ گروهی و حفظ حریم مکانی فرد با همکاری کاربران مجاور مرور شدند. راه‌کارهای ارائه‌شده در این حیطه در سال‌های ۲۰۰۶ تا ۲۰۱۴ بوده‌اند. راه‌کارهای گروهی از لحاظ امنیت در برابر تبانی و حملهٔ MPAD و کارایی و محرمانگی مکان جلسه در دو مدل شبه‌درست‌کار و مخرب و راه‌کارهای حفظ حریم مکانی با همکاری کاربران مجاور نیز از لحاظ حفظ حریم مکانی فرد در برابر تبانی کاربران مجاور او نیز مقایسه و بررسی شدند.

۶- مراجع

[1] Hashem, T., Kulik, L., and Zhang, R. Privacy Preserving Group Nearest Neighbor Queries. 13th ACM International Conference Proceeding Series. 2010.

[2] Huang, Y., and Vishwanathan, R., Privacy Preserving Group Nearest Neighbour Queries in Location-based Services using Cryptographic Techniques. IEEE GLOBECOM, pp. 1-5, 2010.

[3] Ashouri-Talouki , M., Baraani-Dastjerdi, A., and Selçuk, A. A. GLP: A cryptographic approach for group location privacy, Computer Communications, vol. 35, no. 12, pp. 1527–1533, 2012.

[4] Ashouri-Talouki, M., Baraani-Dastjerdi, A., and Selçuk, A. A. The Cloaked-Centroid protocol: location privacy protection for a group of users of location-based services, Knowledge and Information Systems, vol. 45, pp. 589-615, 2015.

[5] Rahman Khan, A. M., Hashem, .T., Tanin, E., and Kulik, L., Location oblivious privacy protection for group nearest neighbor queries. In Geographic Information Science, Springer, pp. 301-317, 2014.

[6] Hao, F., and Zielinski, P., A 2-Round Anonymous Veto Protocol. In Security Protocols, In Transactions on Computational Science IV, LNCS 5430, pp. 202-211, 2009.

[7] Burmester, M., and Desmedt, Y., A secure and efficient conference key distribution system. In Proceedings of Advances in Cryptology (EUROCRYPT'94), pp. 275-286, 1994.

[8] Paillier, P., and Pointcheval, D., Effcient Public-Key Cryptosystems Provably Secure Against Active Adversaries, Advances in Cryptology (ASIACRYPT), 1999.

[9] Schnorr, C. P., Efficient Signature Generation by Smart Cards. Journal of Cryptology, vol 4, pp. 161-174, 1991.

[10] Sheikh, R., Kumar, B., and Mishra, D. K., A Distributed k-Secure Sum Protocol for Secure Multi-Party Computations. Journal of Computing, vol. 2, no. 3, 2010.

[11] Chow, C. Y., Mokbel, M. F., and Liu, X., A Peer to Peer Spatial Cloaking Algorithm for Anonymous Location based Services. In 14th annual ACM international symposium on Advances in geographic information systems (GIS'06). pp. 171-178, 2006.

[12] Bao, J., Chen, H., and Ku, W. S., PROS: A Peer-to-Peer System for Location Privacy Protection on Road Networks. In 17th annual ACM international symposium on Advances in geographic information systems (GIS'09), pp. 552-553, 2009.

[13] Solanas, A., and Balleste, A. M., A TTP-free protocol for location privacy in location-based services. Computer Communications, vol. 31, pp. 1181-1191, 2008.

[14] Hu, H., and Xu, J., Non-Exposure Location Anonymity. IEEE International Conference on Data Engineering, pp. 1120–1131, 2009.

[15] Roth, J., Tummala, M., McEachen, J., &Scrofani, J., Location Privacy in LTE: A Case Study on Exploiting the Cellular Signaling Plane's Timing Advance, In 50th Hawaii International Conference on System Sciences, pp. 6285-6292, 2017.

[16] Zhou, T., Understanding location-based services users' privacy concern: an elaboration likelihood model perspective, Internet Research, vol. 27 no. 3, 2017.

[17] Ashouri-Talouki, M., Baraani-Dastjerdi A., Homomorphic encryption to preserve location privacy, International Journal of Security and Its Applications, vol. 6, pp. 183-189, 2012.

[18] Ashouri-Talouki, M., Baraani-Dastjerdi, A., Selcuk, A.A., Preserving location privacy for a group of users, Turkish Journal of Electrical Engineering & Computer Science, vol. 21, pp. 1857-1870, 2013.

شادیه عزیزی. ایشان مدرک کارشناسی مهندسی فناوری اطلاعات را در سال ۱۳۹۱ از دانشگاه کردستان اخذ کرد و از سال ۱۳۹۳ دانشجوی کارشناسی ارشد دانشگاه اصفهان در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات است. زمینه‌های پژوهشی مورد علاقهٔ ایشان: استخراج قوانین انجمنی از پایگاه داده‌ها، حفظ حریم مکانی در خدمات مبتنی بر مکان، کنترل دسترسی و پروتکل‌های امنیتی.

رایانامهٔ ایشان:

sh.azizi93@eng.ui.ac.ir

مائده تلوکی عاشوری ایشان مدرک کارشناسی مهندسی کامپیوتر را در سال ۱۳۸۲ و مدرک کارشناسی ارشد را در سال ۱۳۸۵ و مدرک دکترا را نیز در سال ۱۳۹۱ از دانشگاه اصفهان اخذ کرده است و در حال حاضر عضو هیئت علمی و استادیار دانشکده کامپیوتر دانشگاه اصفهان نیز است؛ زمینه‌های پژوهشی مورد علاقهٔ ایشان: امنیت

شبکه‌های موبایل، گم‌نامی و حریم خصوصی کاربران، پروتکل‌های امنیتی، پروتکل‌های رمزنگاری توزیع‌شده و امنیت شبکه.

رایانامهٔ ایشان:

m.ashouri@eng.ui.ac.ir

حمید ملا ایشان مدرک کارشناسی مهندسی کامپیوتر را در سال ۱۳۸۲ و مدرک کارشناسی ارشد را درسال ۱۳۸۴ و مدرک دکترا را نیز در سال ۱۳۸۹ از دانشگاه صنعتی اصفهان اخذ کرده است و در حال حاضر عضو هیئت علمی و استادیار دانشکده کامپیوتر دانشگاه اصفهان هستند. زمینه‌های پژوهشی مورد علاقهٔ ایشان: طراحی و تحلیل رمزهای قالبی، امضای دیجیتال و پروتکل‌های امنیتی.

رایانامهٔ ایشان:

h.mala@eng.ui.ac