Um Framework de Multi-Ataques de Re-identificação de Trajetórias em Dados Abertos de Smart Cities

Guilherme S. Tristacci[1], Ekler P. de Mattos[1], Heitor S. R. Filho[2], Antonio A. F. Loureiro[2] *

[1]Universidade Federal de Mato Grosso do Sul - Campus de Coxim – Coxim, MS

[2]Departamento de Ciência da Computação - Universidade Federal de Minas Gerais Belo Horizonte, MG

{guilherme.tristacci,ekler.mattos}@ufms.br, {ramosh,loureiro}@dcc.ufmg.br

Abstract. *Open mobility data is vital for the development of smart cities, but it poses privacy risks to users even when anonymized. A promising approach to improve the development of Location Privacy Protection Mechanisms (LPPMs) is the application of sophisticated re-identification attacks. In this work, we propose a multi-trajectory re-identification attack framework based on spatiotemporal constraints and kinetic profiles, such as acceleration and velocity, to evaluate the robustness of LPPMs, specifically mix-zones. We validated the proposed solution using a collection of real data, comparing its performance with that of single-modal attacks. The results demonstrate that the approach achieved accuracies of 84.2% and 76.3% in the re-identification task, using sets of 500 and 1000 trajectories, respectively, and also provided a better balance between accuracy and sensitivity than single-modal methods.*

Resumo. *Dados abertos de mobilidade são vitais para o desenvolvimento das cidades inteligentes, mas trazem riscos de privacidade dos usuários mesmo quando anonimizados. Uma abordagem promissora para aprimorar o desenvolvimento de Mecanismos de Proteção à Privacidade de Localização (LPPMs) é a aplicação de sofisticados ataques de re-identificação. Neste trabalho propomos um framework de Multi-Ataque de re-identificação de trajetórias baseado nas restrições espaço-temporais e perfis cinéticos, como a aceleração e velocidade, para avaliar a robustez de LPPMs, especificamente as mix-zones. Validamos a solução proposta utilizando uma coleção de dados reais, comparando seu desempenho com o de ataques monomodais. Os resultados demonstram que a abordagem alcançou precisão de 84,2% e 76,3% na tarefa de reidentificação, considerando conjuntos com 500 e 1000 trajetórias, respectivamente, além de apresentar maior equilíbrio entre precisão e sensibilidade em relação aos métodos monomodais.*

1. Introdução

O avanço das Cidades Inteligentes é impulsionado pela disponibilidade massiva de dados de mobilidade urbana, cuja publicação impõe graves riscos à privacidade. Mesmo

*O presente trabalho foi realizado com apoio da Universidade Federal de Mato Grosso do Sul – UFMS/MEC – Brasil e Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

quando anonimizados pela remoção de identificadores diretos, as trajetórias mantêm padrões comportamentais altamente discriminativos, sendo passíveis de serem re-identificadas, processo que busca restabelecer o vínculo entre os dados anônimos e a identidade real do usuário [De Montjoye et al. 2013]. Estudos demonstram que apenas quatro pontos espaço-temporais bastam para re-identificar a grande maioria dos indivíduos [De Montjoye et al. 2013]. Um adversário pode ir além da inferência de pontos de interesse [Freudiger et al. 2011] e explorar características cinemáticas implícitas como aceleração e velocidade [Lestyán et al. 2019] para restabelecer o vínculo entre motorista e trajetória anonimizada.

As *mix-zones* operam como regiões delimitadas onde múltiplos veículos interrompem a transmissão de localização e trocam pseudônimos simultaneamente. O objetivo desse LPPM é criar um conjunto de anonimato k, onde k representa o número mínimo de veículos presentes simultaneamente na zona, garantindo teoricamente que um adversário tenha no máximo $1/k$ de probabilidade de acerto ao tentar associar uma saída à sua respectiva entrada.

Este trabalho propõe um *framework* de *Multi-Ataque* para a re-identificação de trajetórias em dados abertos, baseado na combinação de duas abordagens: restrições espaço-temporais e análise de perfis cinéticos. A abordagem não requer dados de treinamento e opera em modo online. Para validar sua robustez, utilizamos dados reais e comparamos os resultados com uma *baseline*, um ataque monomodal fundamentado na média aritmética das saídas da *mix-zone*. Particularmente, o *framework* de Multi-Ataque adota uma metodologia de "prova e contra-prova", onde a intersecção de vetores eleva a confiança da inferência. Os resultados demonstram a eficácia do método, que manteve 84,2% e 76,3% de precisão em cenários de baixa e alta densidade de veículos, respectivamente, superando a baseline com valor 25% e 14,7% para os respectivos cenários. Além de apresentar maior equilíbrio entre precisão e sensibilidade em relação aos métodos monomodais. Assim, as contribuições deste trabalho são:

- **Ataque espaço-temporal:** Filtragem de candidatos por distância geodésica e restrição temporal, validando a coerência física do deslocamento.
- **Ataque cinético:** Modelagem do perfil de condução via histograma de acelerações com suavização Gaussiana, permitindo re-identificação por similaridade vetorial independente da posição geográfica.
- **Framework de Multi-Ataque:** Validação híbrida por interseção dos dois ataques, maximizando a precisão e mitigando falsos positivos.

O restante deste trabalho está organizado conforme segue. Na Seção 2, apresentamos os trabalhos relacionados sobre re-identificação de trajetórias. Na Seção 3, detalhamos a metodologia proposta, formalizando a modelagem dos ataques baseados em restrições físicas e comportamentais do condutor, bem como o algoritmo de interseção lógica e a definição da *baseline*. A Seção 4 apresenta a avaliação experimental utilizando dados reais de mobilidade, discutindo a eficácia do Multi-Ataque frente aos métodos de referência. Por fim, a Seção 5 sintetiza as considerações finais e aponta perspectivas para trabalhos futuros.

2. Trabalhos Relacionados

Nos últimos anos, podemos observar significativa evolução na frequência e na sofisticação dos ataques de inferência e identidade em dados de mobilidade.

Tabela 1. Comparação entre abordagens de re-identificação de trajetórias.

Autor	Abordagem	Features / Características usadas no ataque	Qtd. de features	Tipo de Ataque
Mattos et al. (2019)	Unicidade de trajetórias	Pontos georreferenciados; preferências de rotas; padrões espaciais individuais	3	Monomodal
Zhou et al. (2019)	Double Mix-Zone	Tempo; localização; velocidade; ruído espacial; ruído cinético	5	Monomodal
Lestyán et al. (2019)	Assinaturas cinéticas de condução	Séries temporais de aceleração; desaceleração; perfis de condução; vetores de características	4	Monomodal
Mattos et al. (2022)	Impacto da mobilidade em mix-zones	*Stay Points*; padrões de parada; modo de transporte	3	Monomodal
Eshun et al. (2022)	Modelos probabilísticos de re-identificação	Padrões espaço-temporais; HMM; DBSCAN; divergência Kullback–Leibler	4	Monomodal
Li et al. (2024)	Ataque por Preenchimento de Matriz	Dados de localização incompletos; RSUs; matriz de amostragem; agrupamento hierárquico	4	Monomodal
Schestakov et al. (2024)	Re-Trace	Similaridade espacial; similaridade temporal; correlação de fragmentos	3	Monomodal
Este trabalho	Framework de multi-ataque	Restrições espaciais; restrições temporais; velocidade; aceleração; perfis cinéticos	5	**Multimodal**

Existem diversas limitações nas abordagens de privacidade, inclusive nas técnicas de anonimização baseadas em troca de pseudônimos, como nas *mix-zones*. Foi evidenciado que devido à singularidade das trajetórias humanas, um adversário necessita de apenas dois pontos georreferenciados para re-identificar a grande maioria das trajetórias de um conjunto de dados de táxis [de Mattos et al. 2019]. O estudo explora o comportamento dos motoristas (como preferências de rotas) como uma assinatura digital, evidenciando que a simples supressão de identificadores ou o recorte de trajetórias por *mix-zones* é insuficiente contra ataques que exploram o conhecimento de contexto.

De Mattos et al. [de Mattos et al. 2022] investiga como a própria natureza do transporte urbano afeta a eficácia da privacidade. Ao analisar métricas de *Stay Points* (pontos de parada) em dados multimodais (ônibus, táxis, pedestres), concluindo que não existe uma configuração de privacidade universal que atenda todos os perfis de mobilidade. Eles demonstraram que parâmetros estáticos de *mix-zones* falham em proteger diferentes perfis de mobilidade, sugerindo que a privacidade é altamente dependente do nível de detalhe e do modo de transporte.

Eshun e Palmieri [Eshun and Palmieri 2022] propuseram dois modelos de re-identificação, um algoritmo probabilístico baseado em observações e outro baseado na divergência Kullback-Leibler. Ambos utilizam Modelos Ocultos de Markov (HMM) e o algoritmo de clusterização (DBSCAN) para serem correlacionadas com usuários reais a partir de padrões espaço-temporais de mobilidade. No entanto, as técnicas propostas são dependentes de dados de treinamento para a construção dos perfis de mobilidade.

Li e Li [Li and Li 2024] propuseram um ataque de rastreamento de trajetórias baseado em Preenchimento de Matriz, que explora dados de localização incompletos de infraestruturas de comunicação para redes veiculares, como as *Roadside Units* (RSUs), para reconstruir os movimentos dos usuários. A abordagem modela as posições dos veículos

em uma matriz de amostragem e recupera trajetórias com alta precisão usando técnicas de agrupamento hierárquico, que reduz o número de RSUs necessárias para o ataque. Os resultados de simulação demonstram que a abordagem proposta apresenta elevada precisão, boa adaptabilidade a variações e desempenho consistente sob diferentes taxas de amostragem.

Schestakov et al. [Schestakov et al. 2024] apresentaram o *Re-Trace*, um *framework* de re-identificação de trajetórias que, por meio da correlação de padrões espaço-temporais, permitem a reconstrução e associação de fragmentos de trajetórias aos seus respectivos usuários. Apesar de a abordagem apresentar altas taxas de re-identificação, esta assume regularidade nos padrões de mobilidade, de modo que o seu desempenho pode ser comprometido em cenários dinâmicos.

Além das abordagens baseadas exclusivamente em correlação espaço-temporal, alguns estudos demonstram que características cinéticas também podem atuar como fortes identificadores de mobilidade. Lestyan et al. [Lestyán et al. 2019] demonstraram que padrões de aceleração e desaceleração veicular constituem assinaturas comportamentais altamente discriminativas, permitindo a identificação de condutores independentemente da informação espacial explícita. Os autores extraíram séries temporais de aceleração dos veículos e as transformam em vetores de características, os quais são comparados por meio de métricas de similaridade para distinguir perfis individuais de condução. Os resultados evidenciam que atributos cinéticos carregam forte poder identificador, mesmo na ausência de coordenadas geográficas precisas.

Existem na literatura diversas propostas de re-identificação de trajetórias que estudam isoladamente características da mobilidade, como aspectos espaciais ou temporais. Contudo, abordagens monomodais apresentam uma limitação crítica: quando o único vetor de ataque falha o método perde poder discriminativo. A combinação sistemática de múltiplos vetores de ataque permanece pouco explorada na literatura, representando uma lacuna que este trabalho busca preencher. Diferente das abordagens anteriores, este trabalho avança o estado-da-arte ao propor um *framework* de Multi-Ataque de re-identificação de trajetórias para dados abertos de mobilidade, baseado na integração de restrições espaço-temporais com a análise de perfis cinéticos, como velocidade e aceleração. Essa combinação permite correlacionar diferentes estratégias de ataque de forma conjunta, resultando em maior precisão e elevadas taxas de re-identificação. Esta discussão está sumarizada na Tabela 1.

3. Metodologia

Nesta seção apresentamos a metodologia do *framework* de re-identificação. Inicialmente, formalizamos o conceito de *Mix zone* e o modelo de ameaça do adversário. Em seguida, descrevemos a *baseline* adotada, os modelos de ataques monomodais isolados e o funcionamento do *framework*. Por fim, definimos as métricas de avaliação do trabalho.

3.1. Mix-zones

O mecanismo de privacidade adotado para a anonimização dos dados são as *mix-Zones* [Beresford and Stajano 2003]. A *mix-zone* é uma região espacial deliberada onde nenhum usuário envia atualizações de localização para os serviços conectados. O funcionamento básico consiste em três etapas para garantir a desvinculação de identidade entre os usuários e suas trajetórias:

1. **Entrada:** Ao ingressar na *mix-zone* MZ_x, o veículo v utiliza um pseudônimo $ID_{in,v}$ e cessa a transmissão de suas coordenadas de GPS.
2. **Troca de Pseudônimos:** Ocorre quando o número de veículos dentro de MZ_x atinge pelo menos o nível mínimo de privacidade k. Ou seja, k representa o número mínimo de veículos simultâneos na *mix-zone* para gerar privacidade, garantindo que o adversário não tenha probabilidade de re-identificação superior a $1/k$. Durante a travessia da MZ_x, o veículo v permanece incomunicável. O sistema encerra o uso do pseudônimo antigo $ID_{in,v}$.
3. **Saída:** Ao deixar MZ_x, o veículo v retoma a comunicação utilizando um novo pseudônimo não-correlacionado $ID_{out,v}$.

O objetivo de uma *mix-zone* é formar um conjunto de anonimato A, com cardinalidade igual ou superior a k, de modo que um adversário, ao observar k veículos entrando e k saindo, não consiga associar, com probabilidade superior a $1/k$, cada saída à respectiva entrada. Entretanto, a eficácia desse modelo está condicionada à suposição de que os movimentos no interior da *mix-zone* sejam imprevisíveis. Este trabalho questiona essa premissa ao considerar que propriedades cinéticas, como velocidade e aceleração, bem como restrições físicas inerentes à mobilidade, tendem a ser preservadas mesmo durante o período de silêncio de uma *mix-zone*.

3.2. Modelo do Adversário

O modelo de adversário é uma entidade passiva que possui acesso global ao conjunto de trajetórias anonimizadas a partir de uma função de proteção sobre trajetórias originais. O adversário busca correlacionar os usuários e suas respectivas trajetórias, explorando a correlação de informações latentes com o objetivo de re-identificar os titulares dos dados. Particularmente, o atacante obtém acesso a um conjunto de trajetórias anonimizadas por *mix-zone*, disponibilizadas em um repositório público de dados ($\mathcal{D}'$). No contexto das *mix-zones*, o adversário observa todos os segmentos de entrada e saída das *mix-zones*, mas desconhece o mapeamento entre tais segmentos devido à troca de pseudônimos [de Mattos et al. 2022]. Além dos dados observáveis, o conhecimento prévio do adversário, denotado por $\mathcal{B}$, é formado por informações relacionadas às leis da cinemática, que incluem restrições de velocidade e aceleração, as quais são exploradas para extrair padrões comportamentais de velocidade e aceleração dos condutores.

Considere um conjunto de ataques de rastreamento $\mathcal{Z} = \{Z_1, \ldots, Z_n\}$. Um ataque Z_i é representado pela função $T_{u,i} \leftarrow Z_i(\mathcal{D}', B_{u,i})$, onde o adversário utiliza os dados $\mathcal{D}'$ e o conhecimento a priori $B_{u,i}$ para reconstruir as trajetórias $T_{u,i}$ do usuário u [de Mattos et al. 2022]. Seja $\mathcal{T}_u = \{T_{u,1}, \ldots, T_{u,n}\}$ o conjunto de trajetórias obtidas. Um Multi-Ataque é modelado pela agregação Ω, em que $\Theta \leftarrow \Omega(T_{u,1} \cap \cdots \cap T_{u,n})$. Nessa formulação, a interseção assegura que a re-identificação exija consenso simultâneo dos modelos. Assim, Ω correlaciona os resultados para maximizar a acurácia da associação, e Θ representa as hipóteses finais.

3.3. Framework Multi-Ataques

A fim de avaliar a vulnerabilidade de dados abertos de mobilidade, foi desenvolvido um *framework* de simulação de ataques que opera nas seguintes etapas: (1) Leitura do Banco de Dados de trajetórias; (2) Pré-processamento e extração de características; (3) Execução

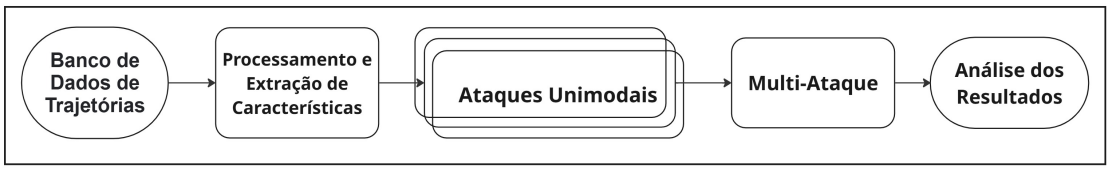


Figura 1. Fluxo do *framework*

de ataques unimodais e de um *baseline* comparativo; (4) Multi-Ataque e (5) a análise dos resultados.

Na Figura 1, o fluxo inicia-se com a entrada do banco de dados de trajetórias brutas, submetido a um processamento e extração de características para a remoção de ruídos, separando os dados em marcos de fronteira espaço-temporal e vetores de aceleração. Esses insumos estruturados alimentam a etapa de ataques unimodais, onde as abordagens baseadas em física (Espaço-Temporal) e comportamento (Cinético) são executadas isoladamente para estabelecer as métricas de desempenho individuais. Na sequência, a partir dos resultados obtidos pelos ataques, implementa-se o Multi-Ataque, que realiza a intersecção estratégica das técnicas, utilizando o filtro espacial para delimitar o conjunto de candidatos e a assinatura cinética do condutor para seu refinamento. O ciclo encerra-se com a análise de resultados, onde a eficácia da re-identificação é validada e comparada quantitativamente, mensurando-se a precisão e a robustez do sistema frente aos desafios de escalabilidade e privacidade. Vale ressaltar que o Multi-Ataque é capaz de combinar ataques de re-identificação distintos, porém neste trabalho, utilizamos os dois enfatizados anteriormente.

3.4. Modelagem dos Ataques

Neste trabalho propomos um framework de Multi-Ataque composto pela combinação de dois ataques derivados de abordagens já consolidadas na literatura, adaptados ao contexto específico de *mix-zones* com dados GPS. O primeiro é uma adaptação da proposta de Hoh et al. [Hoh et al. 2006] que é baseada nas restrições de distância física. Adaptamos este algoritmo para considerar apenas segmentos de entrada/saída que atravessam a região da *mix-zone* com distância geodésica (Haversine) ao invés de métricas euclidianas. O segundo ataque é chamado de Ataque Cinético, que consiste em uma adaptação da abordagem de Lestyan et al. [Lestyán et al. 2019] para o contexto de coordenadas GPS, representando o comportamento do condutor através de um vetor de aceleração e comparando por distância do cosseno, permitindo a re-identificação independentemente da posição geográfica.

► **Ataque Espaço-Temporal:** busca relacionar o ponto final de uma trajetória T_{out} e o ponto inicial de T_{in}. A associação é válida se, e somente se: $0 < \Delta t_{ij} \leq \Delta t_{max}$ e $d_{\text{geo}}(T_i^{out}, T_j^{in}) \leq \Delta d_{max}$ onde d_{geo} é a distância geodésica calculada pela fórmula de Haversine. Os valores de $\Delta t_{max} = 60\,\text{s}$ e $\Delta d_{max} = 300\,\text{m}$ foram definidos empiricamente com base nas características do conjunto de dados e são discutidos na Seção 4. Os candidatos elegíveis formam o conjunto $\mathcal{C}_i^{ST}$, cuja cardinalidade define o nível de anonimato espacial k_i^{ST}, ordenados por proximidade geodésica para fins de priorização. O Ataque Espaço-Temporal é representado pelo Algoritmo 1.

► **Ataque Cinético:** implementado conforme o Algoritmo 2, fundamenta-se na

hipótese de que padrões de aceleração e desaceleração constituem assinaturas comportamentais distintivas do condutor [Lestyán et al. 2019]. Cada segmento é representado por um histograma de acelerações $\mathbf{h}$ com 15 *bins* no intervalo $[-5, 5]$ m/s^2, suavizado por filtro Gaussiano ($\sigma = 1$) e normalizado para que $\sum_b h_b = 1$. A similaridade entre dois segmentos é calculada pela distância do cosseno entre seus histogramas: $\text{score}(j) = 1 - \frac{\mathbf{h}_i \cdot \mathbf{h}_j}{\|\mathbf{h}_i\| \cdot \|\mathbf{h}_j\|}$ onde $\mathbf{h}_i, \mathbf{h}_j \in \mathbb{R}^{15}$ são os vetores de histograma dos segmentos i e j. Valores próximos a zero indicam maior similaridade comportamental. O ataque opera com raio ampliado ($\Delta d_{max} = 2000\,\text{m}$) para capturar candidatos além do vizinho espacialmente mais próximo, priorizando a afinidade de perfil de condução sobre a proximidade geográfica.

▶ **Média Aritmética (Baseline):** o ataque baseado na média aritmética utiliza a posição média dos veículos pertencentes a um mesmo conjunto anônimo ao saírem da *mix-zone* para inferir o vínculo entre pseudônimos antigos e novos [Zhou and Zhang 2019]. Nesse modelo, o atacante explora o fato de que os mecanismos de anonimização baseados em média espacial produzem posições virtualizadas concentradas em torno de um ponto médio comum, calculado a partir das localizações observadas dos veículos no conjunto anônimo. Dessa forma, a informação espacial disponível após a anonimização apresenta distribuição aproximadamente uniforme entre os possíveis mapeamentos, fazendo com que cada novo pseudônimo possua probabilidade equivalente de associação a qualquer pseudônimo antigo do conjunto. Por não empregar restrições espaço–temporais nem atributos comportamentais, esse método atua exclusivamente como *baseline*, servindo como referência inferior de desempenho para a avaliação comparativa dos ataques propostos.

Algorithm 1: Ataque Espaço–Temporal

Data: segmento alvo i;
matriz temporal ΔT;
matriz espacial D;
limiar temporal Δt_{max};
limiar espacial Δd_{max}
Result: conjunto de candidatos espaço–temporais $\mathcal{C}_i^{ST}$;
nível de anonimato espacial k_i^{ST}

$\mathcal{C}_i^{ST} \leftarrow \emptyset$
foreach *segmento* $j \neq i$ **do**
  if $0 < \Delta T_{ij} \leq \Delta t_{max}$ ***and*** $D_{ij} \leq \Delta d_{max}$ **then**
    $\mathcal{C}_i^{ST} \leftarrow \mathcal{C}_i^{ST} \cup \{j\}$
  end
end
$k_i^{ST} \leftarrow |\mathcal{C}_i^{ST}|$
Ordenar $\mathcal{C}_i^{ST}$ em ordem crescente de D_{ij}
return $\mathcal{C}_i^{ST}$, k_i^{ST}

Algorithm 2: Ataque Cinético

Data: segmento alvo i;
matriz cinética K; matriz espacial D; limiar relaxado $d_{max} \leftarrow 2000m$
Result: conjunto cinético $\mathcal{C}_i^{Kin}$;
nível de anonimato cinético k_i^{Kin}

$\mathcal{C}_i^{Kin} \leftarrow \emptyset$
foreach $j \neq i$ **do**
  // Busca independente em raio ampliado
  if $D_{ij} \leq d_{max}$ **then**
    $dist_{cos} \leftarrow K_{ij}$;
    $\mathcal{C}_i^{Kin} \leftarrow \mathcal{C}_i^{Kin} \cup \{(j, dist_{cos})\}$
  end
end
$k_i^{Kin} \leftarrow |\mathcal{C}_i^{Kin}|$
Ordenar $\mathcal{C}_i^{Kin}$ em ordem **crescente** de $dist_{cos}$
return $\mathcal{C}_i^{Kin}$, k_i^{Kin}

3.5. Multi-Ataque de Re-identificação de Trajetórias

A abordagem proposta neste trabalho fundamenta-se em um modelo de adversário composto, operando sob uma lógica de **Multi-Ataque**. Diferente de abordagens que utilizam somas ponderadas (onde um score alto em uma métrica pode compensar um score baixo em outra), nessa proposta é feito um critério de consenso entre ambos ataques.

O método explora dois comportamentos distintos para obter a alta confiabilidade no ataque: o ataque Espaço-Temporal avalia a viabilidade física (cinemática externa), enquanto o ataque Cinético avalia a forma de condução (comportamento interno). Sob a estratégia de interseção, uma re-identificação só é considerada válida se houver uma dupla confirmação independente:

$$Resultado_{EspacoTemporal}(u) \equiv Resultado_{Cinetico}(u) \tag{1}$$

Neste modelo, o sistema atua como um mecanismo de validação cruzada. Por exemplo, se a análise de distância sugere o candidato A, mas a análise de aceleração aponta para o candidato B, o sistema descarta a tentativa, assumindo a ambiguidade. Essa decisão sacrifica a quantidade de identificações (Recall) em prol da confiabilidade (Precision), atuando como um filtro contra falsos positivos. Ou seja, a identidade do usuário só é inferida quando a proximidade física e a assinatura comportamental apontam, independentemente, para o mesmo indivíduo candidato. A implementação lógica desta decisão, que atua como um filtro de falsos positivos, é detalhada no Algoritmo 3.

Algorithm 3: Framework do Multi-Ataque

Data: Segmento alvo i;
Conjunto espaço–temporal $\mathcal{C}_i^{ST}$ (candidatos ordenados por D_{ij} crescente);
Conjunto cinético $\mathcal{C}_i^{Kin}$ (candidatos ordenados por $score_j$ crescente)
Result: Lista ordenada de candidatos $\mathcal{C}_i$;
Nível de anonimato residual k_i

1 $\mathcal{C}_i \leftarrow \emptyset$;
2 **foreach** $j \in \mathcal{C}_i^{ST}$ **do**
3 **if** $\exists\,(j,\, score_j) \in \mathcal{C}_i^{Kin}$ **then**
4 $\mathcal{C}_i \leftarrow \mathcal{C}_i \cup \{(j,\, score_j)\}$;
5 **end**
6 **end**
7 **if** $|\mathcal{C}_i| > 0$ **then**
8 Ordenar $\mathcal{C}_i$ em ordem **crescente** de $score_j$; `// menor cosseno = maior similaridade`
9 **else**
  `// Sem concordância: tentativa descartada`
10 **return** $\emptyset$, 0;
11 **end**
12 $k_i \leftarrow |\mathcal{C}_i|$;
13 **return** $\mathcal{C}_i$, k_i;

O algoritmo recebe o segmento i e os conjuntos candidatos $\mathcal{C}_i^{ST}$ e $\mathcal{C}_i^{Kin}$ (parâmetros de entrada). Para cada candidato j do filtro espaço-temporal (linha 2),

verifica-se a presença no perfil cinético **(linha 3)**. Apenas confirmados em ambos integram $\mathcal{C}_i$, ordenados por similaridade. Sem concordância (linha 10), a tentativa é descartada, priorizando precisão à cobertura.

3.6. Métricas de Avaliação

A validação dos resultados consiste em confrontar os pares de trajetórias inferidos pelo algoritmo com o gabarito original da coleção de dados. Para quantificar o desempenho, adotou-se a métrica **Precisão**, definida pela razão entre o número de re-identificações corretas ($N_{acertos}$) e o volume total de associações propostas pelo modelo ($N_{tentativas}$). Esta métrica reflete a confiabilidade do ataque, indicando a probabilidade de uma ligação sugerida pelo adversário ser verdadeira: $Precisao = \frac{N_{acertos}}{N_{tentativas}}$

F1-Score — indicador de equilíbrio entre a precisão e a sensibilidade (*Recall*), sendo especialmente relevante para o Multi-Ataque, cujo critério de interseção reduz a cobertura em prol da confiabilidade: $\text{F1} = \frac{2 \cdot \text{Precisão} \cdot \text{Recall}}{\text{Precisão} + \text{Recall}}$

Mean Reciprocal Rank (MRR) — avalia a qualidade do ranqueamento, medindo a posição média do segmento correto na lista ordenada de candidatos: $\text{MRR} = \frac{1}{|Q|} \sum_{i=1}^{|Q|} \frac{1}{\text{rank}_i}$,onde rank_i é a posição do segmento correto para o segmento i, e $\text{rank}_i^{-1} = 0$ quando o alvo não é recuperado. O MRR captura nuances que a precisão isolada omite: um ataque que sistematicamente coloca o alvo em segundo lugar é substancialmente melhor do que um que o coloca em décimo, mesmo que ambos tenham a mesma precisão.

4. Resultados e Discussão

Nesta seção apresentamos os resultados e a discussão deste trabalho. Inicialmente detalharemos o conjunto de dados e cenários usados na validação do Multi-Ataque. Em seguida, apresentaremos a análise e discussão dos resultados dos métodos convencionais e o Multi-Ataque em termos das métricas de precisão, *Mean Reciprocal Rank* e F1-score.

4.1. Conjunto de Dados

Neste trabalho, utilizamos um conjunto de dados reais de mobilidade urbana composto por aproximadamente 500 táxis, coletado na cidade de São Francisco, EUA, ao longo de 25 dias. O conjunto de dados, denominado Cabspotting [Piorkowski et al. 2009], foi coletado em 2008 e contém informações de localização dos veículos, obtidas periodicamente por meio de sensores GPS embarcados. O Cabspotting reúne cerca de 440.000 viagens, com média diária de 17.600 viagens, cobrindo mais de 70% da malha viária da cidade, além de registrar aproximadamente 400.000 contatos entre veículos por dia, o que evidencia seu elevado potencial para análises de mobilidade. Em particular, selecionamos uma amostra referente ao dia 19 de maio de 2008 (segunda-feira), caracterizado por condições de tráfego intenso. Essa amostra é composta por 417.781 registros, 454 usuários distintos e 2.036 viagens. Em seguida, os dados foram anonimizados por meio da aplicação de quatro *mix-zones* distribuídas pela área urbana, considerando níveis de privacidade k iguais a 2, 3 e 5. Por fim, foi aplicado o processo de re-identificação das trajetórias.

A fim de verificar a escalabilidade e a robustez da proposta frente às flutuações de tráfego, os dados foram segregados em dois cenários experimentais:

- **Cenário A (Média Densidade):** Um recorte contendo 500 arquivos de trajetórias (aprox. 1992 segmentos).

- **Cenário B (Alta Densidade):** Um recorte expandido com 1000 arquivos (aprox. 3908 segmentos).

Neste trabalho, foram utilizadas quatro *mix-zones* posicionadas na área urbana da cidade São Francisco, priorizando regiões com maior densidade de tráfego e maior concentração de trajetórias veiculares, típicas de períodos de fluxo intenso (vide Tabela 2). Esse critério visa maximizar a sobreposição entre trajetórias no interior das zonas, favorecendo a formação de conjuntos de anonimato com diferentes valores de k. Basicamente produzimos três versões anonimizadas para cada cenário do conjunto de dados (A e B), que foi protegido por *mix-zones* previamente configuradas com três níveis distintos de privacidade $k = 2, 3,$ e 5 e com raio de 300 m.

Tabela 2. Coordenadas das Mix-Zones Distribuídas

Mix-Zone	Latitude	Longitude
Mix-Zone 1	37.7984	-122.4240
Mix-Zone 2	37.7884	-122.4220
Mix-Zone 3	37.6557	-122.4068
Mix-Zone 4	37.6139	-122.3956

O ataque ocorre através de uma varredura iterativa de todo o conjunto de dados. O algoritmo processa cada ponto de descontinuidade mapeado, que representa a localização de uma *mix-zone* (vide Tabela 2), como um gatilho independente para o processo de reidentificação. Para cada uma dessas *mix-zones*, o sistema examina o entorno espaço-temporal em busca de trajetórias candidatas, aplicando os vetores de ataque para tentar restabelecer o vínculo entre o segmento interrompido e sua continuação correspondente. Dessa forma, a validação do método não se restringe a casos isolados, mas reflete a média de sucesso ao tentar quebrar a anonimização em todas as oportunidades de desconexão presentes nas trajetórias.

4.2. Análise dos Métodos Convencionais

A análise comparativa revela uma degradação severa do método trivial (Baseline) com o aumento do volume de dados. Conforme observado nas Figuras 2 e 3, a confiabilidade da Baseline caiu de 25,0% para apenas 14,7% no cenário mais denso, evidenciando que métodos baseados puramente em estatísticas simples perdem utilidade prática em ambientes de *Big Data*. Em contrapartida, destaca-se a alta eficiência do ataque Espaço-Temporal como o componente de maior impacto global. Em condições de média densidade ($k \geq 2$), essa abordagem atingiu 85,22% de precisão, demonstrando que as restrições físicas de deslocamento (distância e tempo) constituem o filtro mais discriminante para a maioria das conexões. Esse desempenho se mantém elevado mesmo no cenário de alta densidade (76,73%), reforçando que a coerência cinemática é a principal barreira que a anonimização deve superar.

Ainda assim, o ataque Cinético (Aceleração) apresentou bom desempenho à medida que a exigência de privacidade aumenta. No cenário de 500 trajetórias com alto nível de anonimato ($k \geq 5$), em que pelo menos cinco veículos coexistem na mesma *mix-zone* e a restrição espacial perde poder discriminatório, o ataque Cinético atingiu 37,62% de precisão, superando a Baseline (19,80%) e também o método Espaço-Temporal (25,00%). Esses resultados indicam que, quando a ambiguidade física é elevada, o estilo de condução

passa a desempenhar um papel central no desempate entre candidatos, atuando como um discriminador eficaz nos casos em que a localização isoladamente falha.

4.3. Robustez do Multi-Ataque

Figura 2. Comparativo de Resultados por K-Anonymity (Cenário 500 trajetórias)

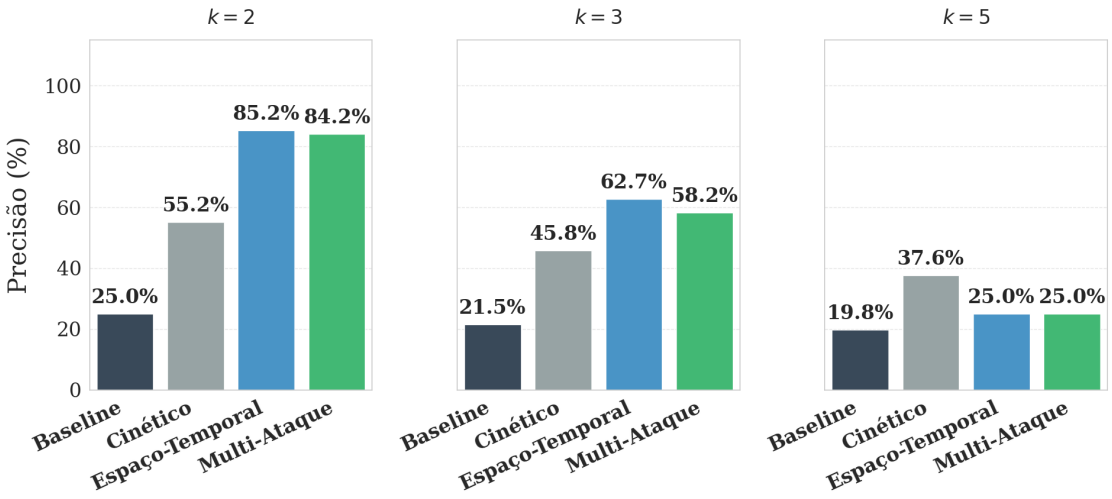
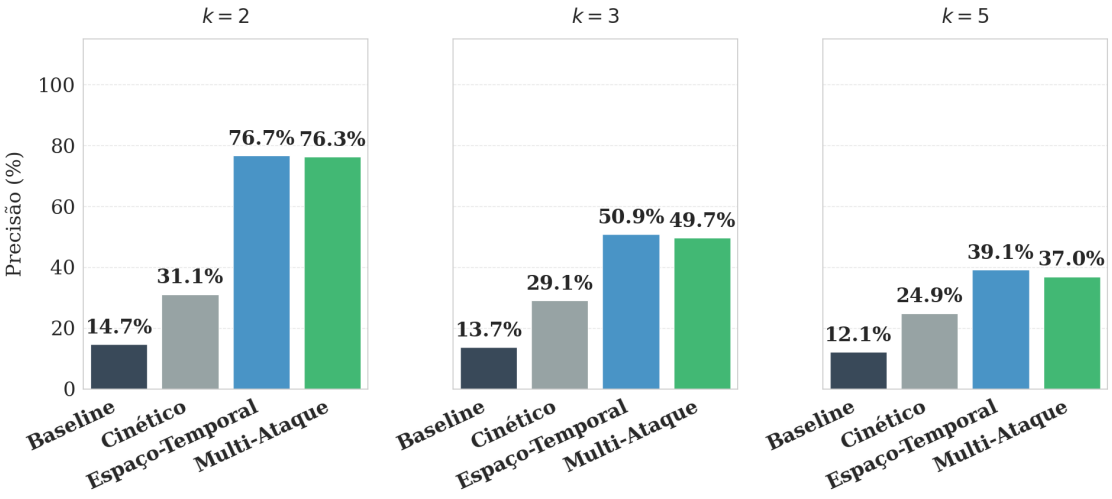


Figura 3. Comparativo de Resultados por K-Anonymity (Cenário 1000 trajetórias)



Em contraste com as abordagens isoladas, a proposta de **Multi-Ataque** demonstrou alta resiliência, especialmente em cenários onde a privacidade foi preservada (onde $k \geq 2, 3, 5$). Conforme evidenciado nas Figuras 2 e 3, observa-se que a eficácia do ataque Espaço-Temporal diminui à medida que múltiplos veículos passam a satisfazer simultaneamente as mesmas restrições espaço-temporais, resultando em conjunto de anonimato com tamanho $k \geq 2$. Nessas situações, o Multi-Ataque recupera parte da capacidade de

re-identificação ao empregar o ataque cinético como mecanismo de refinamento, promovendo o ranqueamento dos candidatos espacialmente viáveis com base na similaridade de seus perfis comportamentais. Por exemplo, no cenário contendo 500 trajetórias, mesmo sob um nível elevado de anonimato ($k = 5$), o método proposto manteve uma taxa de recuperação de 25%, superando a Baseline, que obteve 19,80%. Esse resultado sugere a integração de informações espaciais e cinéticas, contribuindo para diferenciar trajetórias semelhantes, diminuindo a quantidade de candidatos possíveis para o ataque, mesmo com o aumento da quantidade de veículos.

O desempenho intermediário do Multi-Ataque em relação aos ataques isolados está diretamente ligado à sua natureza híbrida. Quando comparado ao ataque espaço-temporal, o Multi-Ataque tende a apresentar resultados ligeiramente inferiores, pois as restrições físicas de espaço e tempo já são bastante eficazes para eliminar candidatos inviáveis. Nesse caso, o perfil cinético entra apenas como um critério de ordenação dos candidatos restantes, sem conseguir recuperar trajetórias que já foram descartadas pelo filtro espacial. Por outro lado, o Multi-Ataque supera o ataque puramente cinético, que opera em janelas mais amplas e acaba sofrendo com maior ambiguidade entre motoristas com comportamentos semelhantes. Ao combinar filtros físicos mais restritivos com a análise comportamental, o método consegue reduzir o conjunto de candidatos e tornar a re-identificação mais precisa, reduzindo significativamente a ocorrência de falsos positivos.

Os experimentos revelaram uma fragilidade crítica na abordagem tradicional (Baseline) frente ao aumento da densidade de dados, degradando sua precisão de 25% para 14,7% ao dobrar o volume de tráfego. Em contraste, a proposta de Multi-Ataque demonstrou alta robustez e escalabilidade. Mesmo no cenário de alta densidade (1000 trajetórias), o conjunto de restrições físicas integrado ao comportamento cinético sustentou uma precisão de 76,3%. Apesar de atuar como um discriminador poderoso em ambiguidades espaciais, as falhas do framework concentram-se na convergência de perfis de aceleração em vias lentas ou no descarte prematuro por limites físicos marginais. Nesses conflitos, o critério de interseção intencionalmente aborta a tentativa (retorna $\emptyset$), priorizando a precisão sobre a cobertura.

Contudo, a verdadeira vantagem do Multi-Ataque se revela na sua capacidade de ranqueamento, medida pelo *Mean Reciprocal Rank* (MRR) e pelo F1-Score (Tabela 3). Mesmo no cenário de alta densidade (1000 trajetórias), o conjunto de restrições sustentou um MRR de 66,94% e um F1-Score de 57,21%. Este resultado evidencia que, embora o alvo possa não figurar exatamente na primeira posição em 100% dos casos devido às variações naturais de condução, a combinação espaço-temporal e cinética isola a vítima sistematicamente no topo da lista de suspeitos, reduzindo o nível de incerteza probabilística ($1/k$) das *mix-zones*.

Um fator importante é que o Multi-Ataque obteve maior estabilidade em termos de precisão e sensibilidade em relação aos ataque monomodais diante da variação do volume de dados dos cenários A e B. Ou seja, para as respectivas configurações de *mix-zones* nos dois cenários o Multi-Ataque obteve menor variação da precisão, MRR e F1-Score apresentando maior robustez. Por exemplo, para o $k = 2$, a diferença de precisão entre os cenários A e B, o Multi-Ataque obteve uma diferença de 7,9 pontos contra 8,5 pontos da abordagem Espaço-Temporal (vide Figuras 2 e 3). Esta baixa variação do Multi-

Tabela 3. Comparativo de Desempenho (MRR e F1-Score) variando o Nível de Privacidade (k)

Cenário	Privacidade	Método	MRR	F1-Score
A (500 traj.)	$k \geq 2$	Baseline	47,30%	36,50%
		Espaço-Temporal	71,90%	61,44%
		Cinético	50,88%	40,01%
		Multi-Ataque	**70,93%**	**61,00%**
	$k \geq 3$	Baseline	43,56%	30,99%
		Espaço-Temporal	61,37%	48,08%
		Cinético	47,50%	35,45%
		Multi-Ataque	**56,56%**	**46,15%**
	$k \geq 5$	Baseline	39,40%	23,95%
		Espaço-Temporal	46,67%	37,50%
		Cinético	42,37%	29,66%
		Multi-Ataque	**44,58%**	**25,00%**
B (1000 traj.)	$k \geq 2$	Baseline	33,57%	22,10%
		Espaço-Temporal	68,64%	57,47%
		Cinético	36,71%	25,11%
		Multi-Ataque	**66,94%**	**57,21%**
	$k \geq 3$	Baseline	32,12%	19,93%
		Espaço-Temporal	55,92%	43,27%
		Cinético	35,27%	23,22%
		Multi-Ataque	**54,86%**	**42,46%**
	$k \geq 5$	Baseline	29,06%	15,89%
		Espaço-Temporal	46,30%	30,12%
		Cinético	32,56%	19,79%
		Multi-Ataque	**45,16%**	**29,82%**

Ataque também pode ser observada para as métricas MRR e F1-Score (vide Tabela 3). Particularmente, em $k \geq 3$, o Multi-Ataque registrou uma diferença de 1,70 pontos no MRR contra 5,5 do Espaço-Temporal. Em $k \geq 5$, o ataque Espaço-Temporal apresenta a diferença de 7,38 pontos no F1-Score, já o Multi-Ataque mantém o valor de 4,82 pontos evidenciando a robustez do Multi-Ataque diante do volume de dados.

5. Conclusão

Neste trabalho propomos um *framework* de Multi-Ataque de re-identificação de trajetórias baseado nas restrições espaço-temporais e perfis cinéticos, como a aceleração e velocidade, para avaliar a robustez de LPPMs, especificamente as *mix-zones*. Validamos a solução proposta utilizando uma coleção de dados reais, comparando seu desempenho com os de ataques monomodais. Os resultados demonstraram que a abordagem alcançou precisão de 84,2% e 76,3% na tarefa de re-identificação, e apresentou maior robustez do que as abordagens monomodais, demonstrando maior equilíbrio entre precisão e sensibilidade, com variação inferior a 4 pontos percentuais no F1-Score entre os cenários de 500 e 1000 trajetórias, contra até 7,38 pontos do ataque Espaço-Temporal, diante da variação

do volume de dados.

Como trabalhos futuros, planejamos estender a avaliação a conjuntos de dados de maior escala e incorporar estratégias adicionais de re-identificação, como Modelos Ocultos de Markov (HMM), para ampliar o poder discriminativo do *framework*. Além disso, propomos o desenvolvimento de defesas focadas na anonimização de dados cinéticos, visando mitigar as vulnerabilidades multimodais expostas e garantir a privacidade dos usuários em ambientes urbanos.

Referências

Beresford, A. R. and Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive computing*, 2(1):46–55.

de Mattos, E. P., Domingues, A. C., and Loureiro, A. A. (2019). Give me two points and i'll tell you who you are. In *2019 IEEE Intelligent Vehicles Symposium (IV)*, pages 1081–1087. IEEE.

de Mattos, E. P., Domingues, A. C. S. A., Santos, B. P., Ramos, H. S., and Loureiro, A. A. F. (2022). The impact of mobility on location privacy: A perspective on smart mobility. *IEEE Systems Journal*, 14(8).

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. In *Scientific reports*, volume 3, pages 1–5. Nature Publishing Group.

Eshun, S. N. and Palmieri, P. (2022). Two de-anonymization attacks on real-world location data based on a hidden Markov model. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 01–09. IEEE.

Freudiger, J., Shokri, R., and Hubaux, J.-P. (2011). Evaluating the privacy risk of location-based services. In *International conference on financial cryptography and data security*, pages 31–46. Springer.

Hoh, B., Gruteser, M., Xiong, H., and Alrabady, A. (2006). Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*, 5(4):38–46.

Lestyán, S., Acs, G., Biczók, G., and Szalay, Z. (2019). Extracting vehicle sensor signals from can logs for driver re-identification. *arXiv preprint arXiv:1902.08956*.

Li, C. and Li, Z. (2024). Trajectory tracking attack for vehicular ad-hoc networks. *Security and Privacy*, 7(6):e433.

Piorkowski, M., Sarafijanovic-Djukic, N., and Grossglauser, M. (2009). CRAWDAD dataset epfl/mobility (v. 2009-02-24). Downloaded from `http://crawdad.org/epfl/mobility/20090224`. Acesso em: 24 de abril de 2026.

Schestakov, S., Gottschalk, S., Funke, T., and Demidova, E. (2024). RE-Trace: Re-identification of modified GPS trajectories. *ACM Transactions on Spatial Algorithms and Systems*, 10(4):1–28.

Zhou, Y. and Zhang, D. (2019). Double mix-zone for location privacy in vanet. In *Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City*, pages 322–327.