ANÁLISE E AVALIAÇÃO DE MIX ZONES COMO MECANISMO DE PRIVACIDADE DE REDES MÓVEIS EM AMBIENTES UNIVERSITÁRIOS

Matheus Cenerini Jacomini (PIC/UEM), Alisson Renan Svaigen (Orientador). E-mail: arsvaigen@uem.br.

Universidade Estadual de Maringá, Centro de Tecnologia, Maringá, PR.

Área e subárea do conhecimento: Ciência da Computação / Sistemas de Computação.

Palavras-chave: privacidade de localização; segurança cibernética; mix zones.

RESUMO

A coleta contínua de dados de localização por dispositivos móveis é fundamental para diversos serviços digitais (como a sugestão de melhores rotas), mas também habilita a inferência de informações dos usuários por parte de uma entidade maliciosa por meio da inferência de trajetórias. O impacto da coleta de dados de localização em ambiente universitário é ainda pouco investigado na literatura. Este trabalho avalia o emprego de Mix Zones, um mecanismo de proteção de privacidade de dados contra ataques de inferência de localização, para mitigar a inferência de trajetórias em um ambiente universitário. Foi implementado um aplicativo experimental de coleta de localização, que coletou dados reais ao longo de 30 dias. Foi definido um protocolo de aplicação de Mix Zones frente aos registros coletados para anonimização e proteção dos dados. Para avaliar o nível de privacidade fornecido pelo mecanismo, foram aplicados dois ataques de inferência de trajetórias. No cenário mais crítico, os ataques conseguiram reconstruir mais de 50% das trajetórias. Os resultados indicam que as Mix Zones rompem a associação direta entre pseudônimos, mas padrões espaço-temporais ainda permitem recuperar parte relevante das trajetórias, evidenciando a necessidade de propor mecanismos mais robustos e avaliar o mecanismo contra adversários mais sofisticados.

INTRODUÇÃO

Serviços baseados em localização coletam continuamente coordenadas de dispositivos móveis, permitindo reconstruir trajetórias e inferir hábitos dos usuários, mesmo quando identificadores reais não estão disponíveis (LE et al., 2011). Como mecanismo de proteção, as Mix Zones promovem a troca de pseudônimos em regiões específicas, dificultando a associação entre os trechos anterior e posterior da trajetória, especialmente quando há pelo menos *k* usuários simultaneamente na região (BERESFORD; STAJANO, 2004; DOMINGUES et al., 2021). A eficácia do mecanismo depende do posicionamento das Mix Zones e do fluxo de usuários, além de poder ser reduzida por ataques que exploram características espaciais e temporais das trajetórias (ZHANG et al., 2018). Embora seja um campo de pesquisa

amplamente estudado na literatura, o impacto em ambientes universitários, que possui um padrão especial de mobilidade, é pouco investigado (JADLIWALA et al., 2013).

Assim, o objetivo deste trabalho é avaliar experimentalmente o uso de Mix Zones sobre dados reais de mobilidade em um ambiente universitário, analisando a eficácia de ataques de inferência de localização na reconstrução de trajetórias.

MATERIAIS E MÉTODOS

Inicialmente, foi conduzida uma revisão sistemática da literatura, considerando a base Scopus, sobre trabalhos relacionados à privacidade de localização, Mix Zones e ataques de inferência de localização. A busca retornou 29 estudos, dos quais 7 foram selecionados após a aplicação dos critérios definidos. A sumarização está disponível em um anexo online[1]. Baseado no conhecimento obtido com a revisão, foi estabelecido um protocolo metodológico, listado a seguir:

- **Desenvolvimento de aplicativo:** foi desenvolvido um aplicativo experimental para coleta de dados de localização no campus sede da UEM, resultando em 150.653 registros de 12 dispositivos, distribuídos em 30 dias, contendo identificador, coordenadas geográficas e instante de coleta.
- **Processamento dos dados coletados:** os dados coletados foram organizados por dia e ordenados cronologicamente pelo instante de medição, permitindo reconstruir a trajetória de cada participante.
- **Simulação experimental da aplicação de Mix Zones:** a partir dos dados processados, a trajetória dos usuários foi reproduzida via simulação, utilizando um ambiente na linguagem Python 3. Para o protocolo de aplicação das Mix Zones, foram distribuídas quatro zonas no mapa do *campus* sede da UEM, considerando as regiões de maior concentração dos registros de localização. Como parâmetros, utilizou-se k = 2: quando dois ou mais usuários permanecem simultaneamente em uma região, tornam-se elegíveis à pseudonimização e recebem um novo pseudônimo ao sair. Os registros internos às Mix Zones são omitidos, resultando na divisão das trajetórias em subtrajetórias identificadas por pseudônimos distintos (MATTOS et al., 2023).
- **Aplicação de ataques de inferência de localização**: Para avaliar a possibilidade de reconstrução dessas associações, foram implementados os ataques FIFO - baseado na ordem temporal de entrada e saída - e DTW - baseado na similaridade espaço-temporal das subtrajetórias. As inferências foram comparadas com as associações reais registradas pelo simulador, utilizando-se as métricas de acurácia e recall.

RESULTADOS E DISCUSSÃO

[1] Disponível em: https://tinyurl.com/jacominisvaigen2026

Ao longo dos 30 dias foram registrados 1.069 eventos de entrada nas quatro Mix Zones, sendo 980 na região 1, 25 na região 2, 54 na região 3 e 10 na região 4. Apesar dos 150.653 registros coletados, a amostra ainda apresentou limitações quanto ao número de participantes e à continuidade das trajetórias, o que pode ter reduzido a ocorrência de encontros nas regiões. A Figura 1 (a) apresenta um exemplo ilustrativo do processo de troca de pseudônimos em uma Mix Zone, enquanto a Figura 1 (b) ilustra a distribuição espacial dos registros de um dos dias de coleta.



Figura 1 – (a) Exemplo ilustrativo da troca de pseudônimos em uma Mix Zone; (b) registros de localização coletados em 22/04/2026 no campus da UEM.

Embora todas as regiões tenham registrado passagem de usuários, apenas as Mix Zones 1 e 3 atingiram o requisito k = 2 e produziram anonimização. Foram realizadas 850 trocas de pseudônimos, sendo 826 na Mix Zone 1 e 24 na Mix Zone 3.

Os resultados dos ataques são apresentados na Tabela 1.

Tabela 1: Resultados dos ataques de associação

Ataque	Associações	Acertos	Acurácia	Recall
FIFO	721	161	22,33%	18,94%
DTW	538	302	56,13%	35,53%

O ataque FIFO apresentou uma acurácia menor do que 25%, demonstrando ser um ataque pouco efetivo. Já o DTW conseguiu reconstruir mais de 50% das trajetórias, demonstrando que a exploração das características espaço-temporais aumenta significativamente a capacidade de rastreamento. Ainda assim, a efetividade do DTW, quando comparado a efetividade de ataques na literatura, não demonstra ser suficientemente efetivo, indicando que as Mix Zones introduzem incerteza relevante na associação entre pseudônimos no ambiente universitário, mesmo considerando as limitações encontradas na coleta de dados. Os resultados apontam, portanto, para uma proteção parcial: a troca de identificadores dificulta o rastreamento direto, mas não elimina a possibilidade de correlação quando o adversário explora padrões de mobilidade (BERESFORD; STAJANO, 2004; ZHANG et al., 2018).

CONCLUSÕES

Este trabalho avaliou experimentalmente o uso de Mix Zones sobre dados reais de mobilidade em um ambiente universitário, analisando a eficácia de ataques de inferência. Os experimentos indicam que as Mix Zones oferecem proteção parcial contra ataques de rastreamento em um ambiente universitário, com eficácia dependente do posicionamento das regiões e dos padrões de circulação dos usuários no campus. Das quatro Mix Zones avaliadas, apenas duas produziram anonimização, sendo uma delas responsável por 97,2% das trocas de pseudônimos.

O DTW apresentou maior capacidade de reconstrução, embora a maioria das trocas tenha permanecido sem identificação correta. Assim, no cenário universitário analisado, a troca de pseudônimos dificulta o rastreamento direto, mas não elimina totalmente a possibilidade de associação quando o adversário explora padrões de mobilidade. Para trabalhos futuros, espera-se propor mecanismos mais robustos e avaliar o mecanismo contra adversários mais sofisticados.

REFERÊNCIAS

BERESFORD, A. R.; STAJANO, F. **Mix zones: user privacy in location-aware services.** In: IEEE ANNUAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, 2., 2004. *Proceedings [...]*. IEEE, 2004.

DOMINGUES, A. C. S. A. et al. **Social Mix-zones: anonymizing personal information on contact tracing data.** In: ACM INTERNATIONAL SYMPOSIUM ON PERFORMANCE EVALUATION OF WIRELESS AD HOC, SENSOR, & UBIQUITOUS NETWORKS, 18., 2021. *Proceedings [...]*. ACM, 2021. DOI: 10.1145/3479240.3488533.

JADLIWALA, M.; BILOGREVIC, I.; HUBAUX, J.-P. **Optimizing mix-zone coverage in pervasive wireless networks.** *Journal of Computer Security*, v. 21, p. 317-346, 2013.

LE, Z.; OUYANG, Y.; CHEN, G.; MAKEDON, F. **Dynamic mix zone: location data sanitizing in assisted environments.** *Universal Access in the Information Society*, v. 10, p. 195-205, 2011.

MATTOS, E. P. de et al. **Protect your data and I'll show its utility: a practical view about mix-zones impacts on mobility data for smart city applications.** In: ACM INTERNATIONAL SYMPOSIUM ON PERFORMANCE EVALUATION OF WIRELESS AD HOC, SENSOR, & UBIQUITOUS NETWORKS, 2023. *Proceedings [...]*. ACM, 2023.

ZHANG, L.; MA, C.-G.; YANG, S.-T.; ZHENG, X.-D. **Users collaborative mix-zone to resist the query content and time interval correlation attacks.** *Technical Gazette*, v. 25, n. 4, p. 962-969, 2018.