International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

Classical Ciphers Techniques to protect the privacy of Mobility Traces

Mr. D. Kalyan Kumar [1] Dr. V.S.Giridhar Akula[2]

[1] Assistant Professor, Department of computer science and Engineering, Mallareddy institute of engineering and technology, Hyderabad, India,

[2] Professor and principal,Mallareddy Institute of Engineering and Technology, Hyderabad, India

Abstract

The proposed work presents "classical cipher" techniques applied to the spatial and/or temporal domains to give a useful tradeoff between the two antagonistic requirements. Driven by real-world mobility traces, diverse simulation results illustrate the performance of the proposed *location cipher* and *time-zero cipher*. This work targets the problem of balancing between *secrecy* for privacy protection and *transparency.*

Key Words: Protection ciphers, Bayesian inference, Maximum likelihood estimator, Gaussian noise, A+B cipher

Introduction:

For strong protection of secrets, standard cryptography based on one-way functions could be used. For mobility traces, however, privacy must be protected against attacks by even a legitimate user of the traces. Hence, on the one hand, the user, may not be given a key to unlock the secret. On the other hand, the unavailability of the key implies that the traces in "encrypted" form must preserve sufficient original information to remain useful to the user. The last requirement rules out strong cryptography as a protection strategy.

This work targets the problem of balancing between *secrecy* for privacy protection and *transparency* for functional effectiveness by introducing a prudently chosen puzzle (or a "cipher") to encrypt (or "transform") the trace beyond the introduction of commonly applied statistical noise. The chosen cipher Serves one key purpose based on important features of the mobility problem domain – it aims to reduce the linkability between recorded trace data points and any side information obtained by the adversary.

The contributions of the proposed work are (i) To propose a set of protection ciphers for the privacy of mobility traces. Importantly, these ciphers preserve information needed by various real-world applications *by design*, and hence can increase privacy without compromising usefulness. (ii) To design adversary strategies that aim to solve the ciphers in conjunction with Bayesian techniques to infer a victim's trace under noise, while considering all available information in diverse forms. It is assumed that a set of traces, each recording intermittently the time and corresponding location of a mobile node, are published to the public.

It is also assumed that each trace entry is given in the format of *{id, time, location}*, where *id* is a random and unique ID replacing consistently the true identity of the mobile node, *time* is the sampling time of the node's location, and *location* is that recorded location. Another assumption is that *spatial cloaking* of the location information has been applied to the traces before publication, for increased privacy protection. Specifically, the traced area is divided into a grid of cells, each of size $S \times S$, and *location* is published as the cell ID instead of a more precise point within the cell. Further to the spatial cloaking, for privacy protection, it is proposed by two cipher techniques that may be applied to

transform the original traces before publication

Material and Methods:

Good research was conducted on Privacy protection of mobile nodes. In one approach, the method used is to reduce the spatial/temporal granularity of the location information made available to the service provider, while achieving satisfactory service effectiveness. Hoh *et al.* devise a protection strategy to release user data only when certain privacy constraints are met. Meyerowitz and Choudhury suggest sending fake requests with the real ones to reduce the ability of an eavesdropper to trace a mobile node over time.
Sweeney pro-poses a protection model named k-anonymity, as well as a set of accompanying policies for the privacy protection. When k-anonymity is satisfied, each individual is indistinguishable from k − 1 other individuals.

Classical ciphers:

In location cipher, each real-world location in the original trace is replaced consistently by a unique and random ID in the published traces. The random IDs are not correlated in any way with the real locations.

In time-zero cipher, the sampling times of locations in a trace are not published in absolute values, but they are all relative to a start time, t0, whose true value is not released.
We assume that the adversary has general world knowledge about the relative popularity of locations in the traced area and the patterns of movements between adjacent locations.

Protection method	Location Cipher (A)	Time Zero Cipher (B)
Effect on traces	Temporal domain & Sequence of contacts are not altered	Inter contact times of sequence of contacts are not altered
Effects on attacks	No direct usage of mobility models	Mobility models can be used with traces

Fig 1: Comparison of proposed ciphers

Bayesian inference is used to overcome the noise in the spatial domain of the snapshots and/or the traces, and return a robust answer of the victim's trace to the adversary. Maximum likelihood estimator method is a robust and effective attack strategy, when information is noisy but the adversary could have some estimation about the model of the noise perturbing the traces and/or snapshots.
In the attack, the adversary first computes, from the published trace set, the statistics of location popularity and the transition probabilities from one location to the next. After that, she compares the computed statistics from the traces with her general knowledge of the real-world statistics.
The maximum likelihood estimator method is a robust and effective attack strategy, when information is noisy but the adversary could have some estimation about the model of the noise perturbing the traces and/or snapshots. The Bayesian inferencing makes use of all available snapshots, whether they are collected at popular locations to which relevant encrypted locations can be resolved with high confidence, or at unpopular locations to which the encrypted locations can only be resolved to uncertain likelihood distributions.

Output:

If the traces are protected with the location cipher, we assume that the adversary has already deciphered the random location IDs, even though the cipher attack may not be complete or correct. We assume that the adversary then uses the maximum likelihood estimator inference strategy. We study the special case where the snapshots of the victim collected by the adversary coincide with the sampling times of the traces.

We quantify the performance of the strategies with the following metrics, (i) Correct conclusion percentage. A conclusion is correct if the victim is uniquely identified by the adversary according to the criterion of highest compatibility metric; (ii) Incorrect conclusion percentage. A conclusion is incorrect when the victim is not among the set of candidates having the highest compatibility metric.

In the simulations, we assume that the spatial granularity is of 0.001° in latitude and longitude, the snapshots are perturbed with zero-mean Gaussian noise with $\sigma = 4.6$, and a randomized/real-world location is unpopular if its popularity is less than 0.001% of the total length of visit duration.

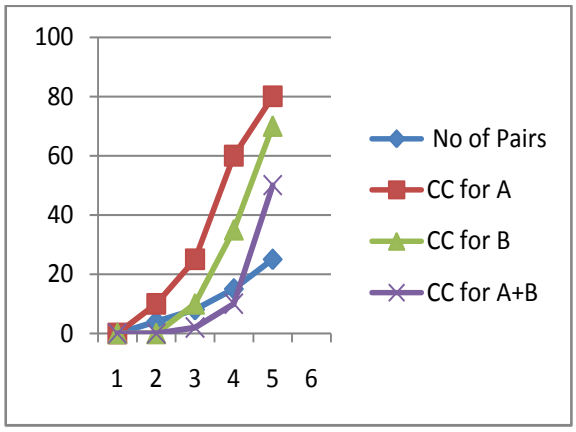

Fig 2: Graph showing the results of A , B and A+B

Conclusion:

In this paper we have observed (a) the location cipher A clearly mitigates the privacy attack in all the experiments, compared with the baseline of no cipher protection. (b) In general, the time-zero cipher B is more effective than A.
However, since the cipher B attack is based on subsequence matching, it can benefit a lot from a longer sequence of snapshots. (c) The combined A+B cipher performs the best

References:

[1] Sweeney, L.: k-anonymity: a Model for Protecting Privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems **10**(5) (2002)

[2]. Xiao, X., Tao, Y.: M-invariance: Towards Privacy Preserving Re-publication of Dynamic Datasets. In: ACM SIGMOD, Beijing, China (June 2007)

[3] Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. In: ACM MobiSys, San Francisco, CA (May 2003)

[4] Hoh, B., Gruteser, M., Xiong, H., Alrabady, A.: Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking. In: ACM CCS, Alexandria, VA (October 2007)

[5] Meyerowitz, J., Choudhury, R.R.: Hiding Stars with Fireworks: Location Privacy through Camouflage. In: ACM MobiCom, Beijing, China (September 2009)

[6] Nergiz, M.E., Atzori, M., Saygin, Y., Guc, B.: Towards Trajectory Anonymization: a Generalization-Based Approach. Transactions on Data Privacy **2**(1) (2009)

[7] Abul, O., Bonchi, F., Nanni, M.: Never Walk Alone: Uncertainty for Anonymity in Moving Objects Database. In: IEEE ICDE, Cancun, Mexico (April 2008)

[8] Faloutsos, C., Ranganathan, M., Manolopoulos, Y.: Fast Subsequence Matching in Time-Series Databases. In: ACM SIGMOD, Minneapolis, MN (May 1994)
[9] Piorkowski, M., Sarafijanovic-Djukic, N., Grossglauser, M.: CRAW-DAD data set epfl/mobility (v. 2009-02-24). Downloaded fromhttp://crawdad.cs.dartmouth.edu/epfl/mobility (February 2009)
[10] Jonsson, J., Kaliski, B.: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. RFC 3447, Internet Engineering Task Force (February 2003)