A Control-Theoretic Approach for Location Privacy in Mobile Applications

Sophie Cerf, Bogdan Robu, Nicolas Marchand, Sonia Ben Mokhtar, Sara Bouchenak

A Control-Theoretic Approach for Location Privacy in Mobile Applications

Sophie Cerf[1], Bogdan Robu[1], Nicolas Marchand[1], Sonia Ben Mokhtar[2] and Sara Bouchenak[2]

***Abstract*— The prevalent use of mobile applications using location information to improve the quality of their service has arisen privacy issues, particularly regarding the extraction of user's points on interest. Many studies in the literature focus on presenting algorithms that allow to protect the user of such applications. However, these solutions often require a high level of expertise to be understood and tuned properly. In this paper, the first control-based approach of this problem is presented. The protection algorithm is considered as the "physical" plant and its parameters as control signals that enable to guarantee privacy despite user's mobility pattern. The following of the paper presents the first control formulation of POI-related privacy measure, as well as dynamic modeling and a simple yet efficient PI control strategy. The evaluation using simulated mobility records shows the relevance and efficiency of the presented approach.**

I. Introduction

Last years have seen the rise of Location Based Services (LBS) i.e. applications running on mobile devices that use the location data of a user to create or simply improve their service. In spite of their valuable gain in terms of utility for the user, they are a source of reluctance for privacy-aware persons. A large variety of threats exists for a user to whom the location information has been revealed to a malicious attacker. Sensitive information can be extracted such as the user points of interest (home, work place, etc.), familial and social relationships, and even religious beliefs or political convictions. Re-identification or mobility prediction attacks can also be performed. A wildly used notion is a Point Of Interest (POI) which is a place, characterized by its size in meters, where a user spends a significant amount of time. POIs are often used as basis for more elaborated attacks. For instance, the set home-work places is in most of the cases enough to re-identify persons. In the following of this article, the notion of privacy will be centered on protection of points of interests.

The dedicated literature proposes many solutions to protect users' privacy through what is commonly called Location Privacy Protection Mechanism (LPPM). The mechanism applied to the location data can be of many types: addition, removal, modification, etc. and mostly depends on the privacy property that should to be ensured. Among the well known privacy guarantees are k-anonymity that hides a user among $k-1$ other people [9] and ϵ-differential privacy that limits the amount of data revealed to an attacker by ϵ [5], one can also see Geo-Indistinguishability [2] for the location privacy application of the latter concept. Despite the flourishing works, most LPPMs still suffer from lack of feasibility. Two main challenges regarding nowadays protection mechanisms can be highlighted:

1) LPPMs are configurable in order to refine the provided protection according to the users' needs (k-anonymity, ϵ-differential privacy, etc.). Even though it is of prime importance to be able to leverage LPPMs action, it is not straightforward to know *how* to do it, even for experts. Indeed, most of the time, a direct link between the LPPMs' parameters and the privacy (and utility) of the obfuscated data is lacking. This translates into a reduced usability of the algorithm for the user who does not necessary know - and neither wants to know - the inner behavior of the protection mechanism under use.
2) The protection needs of users depend on their mobility characteristics. The level of protection provided by a LPPM varies for each user over time. When a user is not moving the mechanism should be ON to protect the POIs, while when the user moves, data obfuscation can be limited to enable more utility. Therefore, protection action of LPPMs should be leveraged over time.

In this paper, a control-theoretic approach to these issues is presented. The first challenge identified previously translates into a problem of sensing privacy (being able to have a privacy metrics that is relevant for users) and as reference tracking problem (leverage LPPM's configuration to achieve the user's privacy target). The second challenge can be seen as a regulation problem, where the privacy objective should be kept constant no matter the mobility characteristics of the user (seen here as a disturbance). Regarding these challenges, this paper makes the following contributions:

- Definition of a privacy measure that can be computed online. The metric is POI-oriented (i.e. reflects stops in the mobility trace) and enables linear control. This is further developed in Section II.
- First control-oriented modeling of the impact of a LPPM (Geo-Indistinguishability) on POI-oriented privacy. The model is a first order one with saturation. (Section III)
- Development of a control strategy to guarantee privacy & utility for location data. (Section IV)
- Evaluation of the measure, modeling and control using simulation data representative of LBS users' mobility. (Section V)

II. System Definition

The system under study is a Location Privacy Protection Mechanism (LPPM), that obfuscates a user location data before sending it to the Location Based Service (LBS). This section

[1]Univ. Grenoble Alpes, CNRS, Grenoble INP*, GIPSA-lab, 38000 Grenoble, France firstname.lastname@gipsa-lab.fr
[2]INSA Lyon - LIRIS - CNRS, Distributed Systems Research Group, Lyon, France firstname.lastname@insa-lyon.fr
*Institute of Engineering Univ. Grenoble Alpes

details and formulates in a control-theoretic way the concepts of protection mechanism (plant), LPPM parameter (controllable input), raw location data (latitude and longitude over time, seen as an uncontrollable input) and privacy and utility of the resulting obfuscated data (outputs). These concepts are schematically represented in Fig. 1.

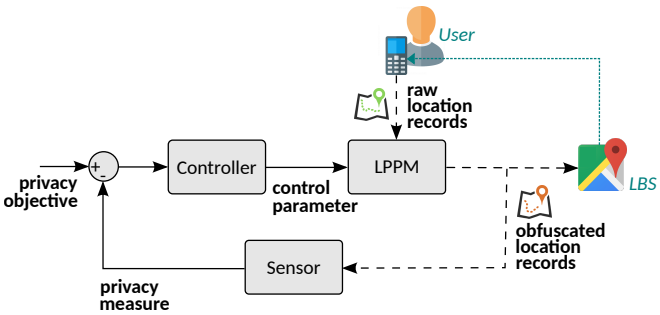

Fig. 1. Classic control schema applied for Location Privacy Protection of a mobile service user.

A. Process

Location Privacy Protection Mechanisms (LPPMs) are algorithms that aim at increasing privacy of location data. They are parametrized algorithms that take as input raw mobility data and output the obfuscated ones. These algorithms can be of many kinds: real-time or offline, requiring a trusted server or at local level, etc. and realize various transformation to data: blurring [8], [2], cloaking [6], [11], [7], merging [4], [1], etc. Some LPPM are off-line processes that require the entire mobility record, such as Promesse [8] that smoothen spatial data to remove the users' POIs. For a control approach, only LPPMs that can work in real-time are considered, as they enable on-line tuning to adapt privacy level of data.

Geo-Indistinguishability [2] (Geo-I for short), the chosen LPPM for this paper, is a well known LPPM from the state of the art that can work on-line. Its quite simple yet efficient principle is to add spatial noise to the location data. Each new obfuscated location is computed using a Laplacian distribution centered in the raw location record with parameterizable variance. Geo-I's parameter is noted ϵ and is inversely proportional to the amount of noise added: the lower ϵ is, the more noise is added and the better the location is obfuscated. An illustration of the application of Geo-I on a real mobility trace for various parametrization is done in Fig. 2. All points of the traces have been obfuscated with the same configuration of Geo-I in this case.

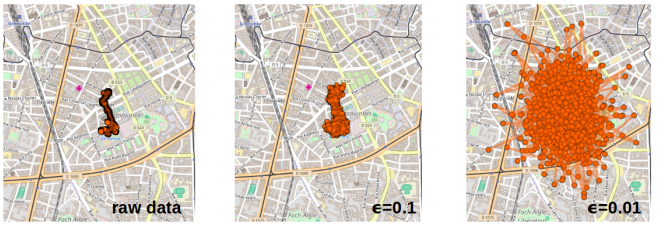

Fig. 2. Application of Geo-I on a mobility trace for various configurations: (a) raw mobility data, (b) obfuscation with low noise ($\epsilon = 0.1\ m^{-1}$), (c) obfuscation with high noise ($\epsilon = 0.01\ m^{-1}$)

B. Input signals

Geo-I protection mechanism has two inputs: the location record of the user and its own parameter ϵ. Their control-oriented presentation is provided in the next paragraphs.

Geo-I's parameter ϵ can be changed at each iteration and impacts the POI-oriented privacy and utility of the obfuscated data. Indeed, as can been seen in Fig. 2, the lower ϵ is, the more noise is added to the data and the more difficult it becomes to extract the real points of interest of the user - or even to realize that the user has stopped. ϵ usually takes its values in the range $[10^{-4}; 1]m^{-1}$. A low ϵ (i.e. high obfuscation) also alter utility of the data. When the location record sent to the service is far from the real one, the quality of service can be significantly reduced. Then, ϵ will be chosen in the following as the control signal.

Another factor impacting the level of privacy, even when using a LPPM is the properties of the raw mobility data to be obfuscated. For instance if a user is in a train, the continuous move naturally prevents from extracting any POI. Whereas if she is home, the location data require obfuscation to protect the extractable POIs. This highlights the dependency of the privacy on the raw mobility data itself. Indeed some cases are not as trivial regarding whether it requires obfuscation of not (and how much), for instance when driving a car and stopping at traffic lights or to grab groceries at self-driving. In the following, raw data will be considered as an uncontrollable but measurable input.

The movement is assumed unidirectional - this assumption will be discussed in the evaluation section. The mobility data has then two main properties: speed of the user and the changes in the speed values, which can be seen as a frequency. By varying the speed of a user at different paces, the simulated data can fairly represent a human mobility trace.

C. Output signals

After defining the algorithm considered as the plant and its input signals, the system's outputs are presented. In the context of location privacy, there are two goals to be achieved: the protection of a user and the guarantee of the usability of the revealed data. As a consequence, two performance signals are considered, that will be called privacy and utility. The next sections formally define these output signals.

1) Measuring Privacy: This work takes as assumption that the objective of a user in terms of privacy is to prevent an attacker from retrieving the points of interest. A point of interest (POI) is formally defined as a circular zone of a given diameter in meters where the user spent a significant amount of time. The ability to have one's POIs hidden is defined as being privacy. The POI diameter and minimal duration are parameters that allow to refine the POI definition to better fit a user's point of view about her own privacy. For instance, if a user considers that work place and home are sensitive information but do not really care about other people knowing where she has lunch, the minimal duration of the user's POI should be set quite large. Moreover, if a user does not mind others to know the neighborhood where she lives but still want to keep the exact address private, the POI diameter should be set quite small. In the following, the POIs are considered parametrized by users.

For the addressed problem, one should have an *online* measure of privacy. The privacy signal should represent how likely the user is to reveal a POI, i.e. if she is spending a significant time in a restricted area. Regarding the control-theoretic approach, the privacy signal should also enable a control as simple as possible, for instance by ensuring its linearity. Consequently, the following requirements for the privacy signal are used: (i) reflect a user stop, (ii) being controllable.

The privacy definition is based on dispersion of the obfuscated data over a past time window. Indeed a small dispersion represents a concentration in space and in time (due to the time window calculation) of location records, which matches with the definition of a POI. Formally, the privacy signal is defined as being the maximum distance between any location record of the time window to the centroid of these points. The location $l(k)$ is considered as being the vector of the latitude and longitude of the user at time k. Then, the centroid $l_c(k)$ of the locations over the past window of length T is defined by eq. (1)

$$l_c(k) = \frac{1}{T} \sum_{t=k-T}^{k} l(t) \tag{1}$$

and the privacy signal is defined as

$$priv(k) = \max_{t \in [k-T;k]} dist[l(t), l_c(k)] \tag{2}$$

with $dist[x, y]$ being the euclidean distance between two points x and y at the surface of the earth.

The privacy signal is expressed in meters and is to be related with the POI diameter. Thus, its reference value is to be set by the user as previously explained for the offline case. The length of the time window T is again chosen by the user to fit her conception of privacy.

2) Measuring Utility: The best way to ensure privacy is to prevent any information from being revealed, that is to say not to use the service. However if one still wants to use a LBS, a compromise has to be done between privacy and utility. In this work, utility is considered as being instantaneous and spacial. The closer the location sent to the LBS is to the user's real one, the better the service will be. Moreover, the location information used by the LBS is assumed to be only the current one, which is the case for many applications (recommendation systems, navigators, etc.). Higher priority is set to privacy over utility: utility should be as high as possible, as long as the privacy requirements are respected, with a limit set by a minimal threshold on utility.

The notion of utility in this paper is related to the dispersion the obfuscated data around the original one, which is precisely Geo-I's parameter ϵ. Then, the objectives for utility translates into minimizing ϵ (which for reminder is inversely proportional to the amount of noise added) whenever it does not detriment privacy objective, however with an upper limit on ϵ.

III. Modeling Location Privacy

Based on this system formulation, a dynamical model of the LPPM is derived in a two steps process: a static characterization and a dynamic step response. Beforehand, the experimental protocol (particularly regarding input scenario) is explained.

A. Input Scenario

The control signal (i.e. LPPM parameter ϵ) is first varied in its whole definition range for the static characterization. In a second time, a step will be applied where the values of the initial and final level will be chosen in the linear working range of the system, derived from the static characterization. The dynamics of the system is expected to come only from the time window calculation of the privacy signal, which motivates the time analysis over the frequency one.

As for the disturbance scenario, its two parameter are varied: the user speed and the frequency of speed changes. These parameters are discretized: speed can be high (50 km/h), low (5 km/h) or null (the user is stopped); and the period of changes can be high (every 15 minutes), low (every 5 minutes) or null (no changes). Therefore, static studies are realized with five disturbance scenarios: constant high, low and no speed; and high and low frequency changes between null and high speed.

In order to deal with the stochasticity of the LPPM, each simulation is run 100 times, only the means of the outputs are presented.

B. Static Characteristic

Results are reported in Fig. 3, where each curve is a different disturbance condition. The following statements can be formulated: (i) the logarithm of privacy is linear with respect to the logarithm of Geo-I parameter for low values of ϵ (high noise) and (ii) for high values of ϵ (low noise) there is a saturation, and the level of this saturation depends on the disturbance.

The saturation reflects that there are some conditions, for instance if the user is moving fast, for which adding a few noise has no impact on the privacy as the user is already protected (i.e. only POI with large diameters can be extracted from the raw trace). The linear part of the curve means that, at some point, the more noise is added to the data, the larger the diameter of the extracted POI is.

The linear part of the static characteristic has the same equation in all cases:

$$log(priv) = a\, log(\epsilon) + b \tag{3}$$

with $a = -1$ and $b = 0.85$.

Due to the presence of this offset, the model is linearized around a working point ϵ_0 and its corresponding privacy level

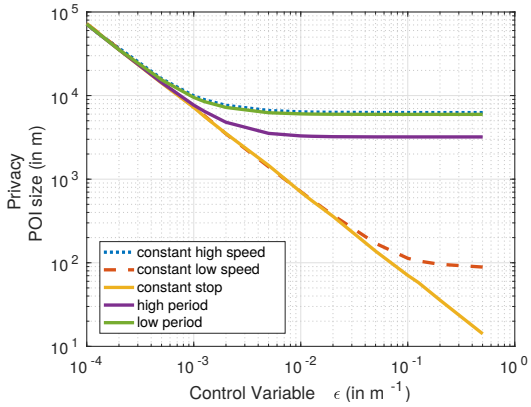

Fig. 3. Static characteristics for various disturbance (raw location data) scenario.

$priv_0$. Thus the control signal is defined as

$$\Delta\epsilon = log(\epsilon) - log(\epsilon_0) \tag{4}$$

and the performance signal as

$$\Delta priv = log(priv) - log(priv_0). \tag{5}$$

The schema of Fig. 4 illustrates these notations on the control loop.

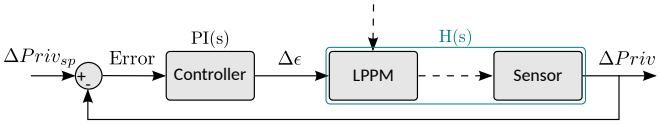

Fig. 4. Feedback loop with signal and transfer functions notations

The saturation level corresponds to the privacy of the mobility data when $\epsilon \to +\infty$, i.e. no noise is added. It is the privacy of the raw trace, that can be measured in real time. This value is denoted $priv_{raw}$.

The modeling of the static characteristic is the following:

$$K = \begin{cases} a & \text{if } a\ log(\epsilon) + b > log(priv_{raw}) \\ 0 & \text{otherwise.} \end{cases}$$

where no smooth transition between the saturation level and the linear behavior is considered.

C. Dynamic modeling

Fig. 3 highlighted the zones in which the behavior from the LPPM parameter to the privacy measure is linear ($\epsilon < \epsilon_0$). Hence for the dynamic analysis, the step variation of Geo-I's parameter will be chosen as being part of this linearity zone (from $\epsilon = 1$ to $\epsilon = 0.1\ m^{-1}$), otherwise ϵ has no impact on privacy. The disturbance is set to constant null speed (i.e. the user is stopped). Results are reported in Fig. 5. The shape of the step response can be approximated by a first order transfer function given its exponential form with non null tangent at the origin.

The transfer function relating the LPPM parameter to privacy is then:

$$H(s) = \frac{\Delta Priv(s)}{\Delta\epsilon(s)} = \frac{K}{1+\tau s} \tag{6}$$

with $\tau = 3$ min.

IV. A Simple Control Strategy

This section presents the Location Privacy controller. The user's objective is defined as a minimal threshold on the privacy value no matter the mobility pattern. Indeed as privacy and utility are contradictory objectives, in order to maximize utility the control signal should be high (i.e. low noise), but still enabling the reference privacy to be met. Concerning the rejection time of disturbances, it can vary according to the user requirements. In our case, we chose a value of 5 minutes. It corresponds to a constrained objective where every small stops (in a shop, at a bus stop, etc.) and all larger ones should be hidden.

To sum up, the specifications are: follow the reference and reject the perturbation with (i) zero steady state error, (ii) no overshoot and in approximately 5 minutes and (iv) increase the utility whenever privacy constraints are met.

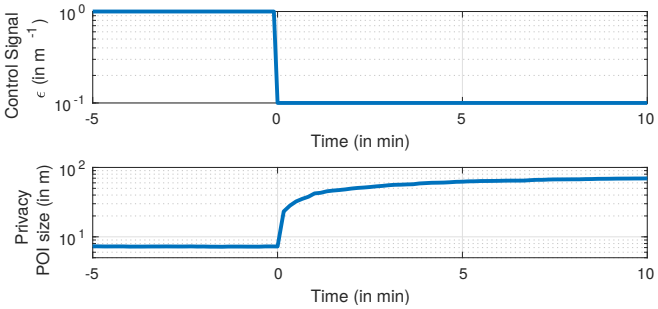

Fig. 5. System step response. Input from $\epsilon = 1\ m^{-1}$ to $\epsilon = 10^{-1}\ m^{-1}$, during a stop (constant disturbance). Mean over 100 experiments.

In order to meet these specifications, a simple PI controller is selected. Its integral action enables zero steady state and its tuning allows to avoid overshoot and reach a desired response time. The controller has the following expression:

$$PI(s) = \frac{\Delta\epsilon(s)}{Error(s)} = \frac{K_I}{s} + K_P. \tag{7}$$

The parameters are tuned using pole placement as detailed in [3]: $K_I = \frac{\tau}{K.\tau_{obj}}$ and $K_P = \frac{1}{K.\tau_{obj}}$, with τ_{obj} the pole of the objective closed loop.

In this control formulation, the gain K is assumed to be linear, always equal to a. As such, the controller is not aware of the saturated effect on privacy (flat zones of Fig. 3). If the privacy objective is overshooted naturally thanks to the user mobility pattern, the controller will keep decreasing ϵ as it will not see any impact on privacy. This is a behavior that interest us, as decreasing the control signal without impacting privacy actually means increasing utility without privacy loss. However, if the user stops or slows down, the controller should not take too much time to react and decrease the control signal. In order to ensure such behavior, an anti wind-up strategy is added, in the form of an actuator saturation, as described in [10]. Threshold are chosen according to Geo-I's common range of variations $[\epsilon_{min}; \epsilon_{max}] = [10^{-4}; 1]\ m^{-1}$.

V. Evaluations

This section presents the evaluation of the privacy metric of eq. (2), LPPM modeling and the control using a PI controller.

A. Disturbance scenario

The objectives of the metric, model and control are to capture and monitor the privacy of users *no matter their mobility pattern*. This notion of disturbance being essential in this work, the contributions should be evaluated with the best representative mobility scenario. As explained in Section II-B, two key properties of a mobility trace are the speed of the user and the frequency of variation of this speed.

The synthetic trace is sampled every 10 seconds and has varying speeds (0, 5, 50, 150 km/h) representing various transportation means (stop, walk, car, train, etc.). The periods between two changes range from 30 seconds (e.g. stop at a traffic light) to one hour (e.g. medical visit), including medium values as 5 minutes (e.g. stop in a coffee shop). The synthetic mobility trace is illustrated in Fig. 6 (speed over time). The total

trace is 18 hours long. Other mobility properties are included, such as turns (between hour 1 and hour 2), acceleration and decelerations (hours 8 to 9) and local movements (hours 10 to 18, user's speed is almost zero). However, due to space restrictions, these properties are hardly visible when plotting only speed over time as in Fig. 6.

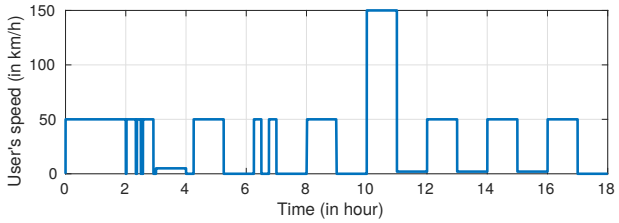

Fig. 6. Disturbance scenario: changes of user's speed over time

B. Privacy Metric Evaluation

As stated previously in Section II-C.1, the two requirements of the privacy metric are to reflect a user's stops and to enable easy control.

To ensure the first point, the privacy sensor is applied to the mobility trace described just before (Section V-A) without any obfuscation ($\epsilon = \infty$). Results are illustrated in Fig. 7, which shows privacy measure over time, where dark blue dots are during the user movement and light gray ones during a stop. The privacy signal reflects the user's stop by having low (almost null) values. Privacy tends to zero with some dynamics which is due to the time-window calculation of the metric. The first requirement is then satisfied.

Regarding the second point, experiments of Section III have shown a linear static characteristic with saturation and a 1^{st} order-like step response. This classic behavior validates the simplicity of the presented metric regarding control.

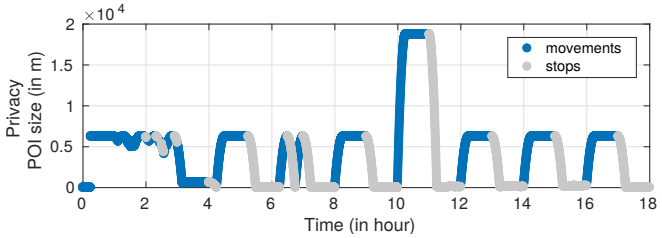

Fig. 7. Metric evaluation: stops are correctly captured. Mean over 100 experiments.

C. Modeling Evaluation

The accuracy of the saturated model presented in Section III is now investigated, with the disturbance scenario of Fig. 6. The model input scenario is illustrated in Fig. 8 (top plot): ϵ is taken to vary in its whole range of values with changes at various frequencies (randomly chosen between 10 sec and 1h). The comparison of the measured data and the model prediction are in Fig. 8 (bottom plot). The two curves are almost overlaid, indicating a good model accuracy most of the time. At some instants (around 3h, 6h, etc.) the model fails to perfectly match the reality. These moments corresponds to situations where the LPPM configuration raises with a large amplitude and for a long time. In these cases, the model predicts a decrease of privacy which is faster than the reality. However, the steady state value achieved is correct. Note that the modeling is always underestimating the privacy, which is more valuable that overestimating. The model accuracy could then be improved but with a cost in complexity. This would also mean increasing the control complexity, which would not be necessary beneficial considering the intended implementation of this control algorithm on a smartphone. An extended analysis of this point will be done in a future work. Nevertheless, the model is still able to successfully capture the influence of the LPPM Geo-I configuration (control signal) and user's mobility (disturbance) on the privacy.

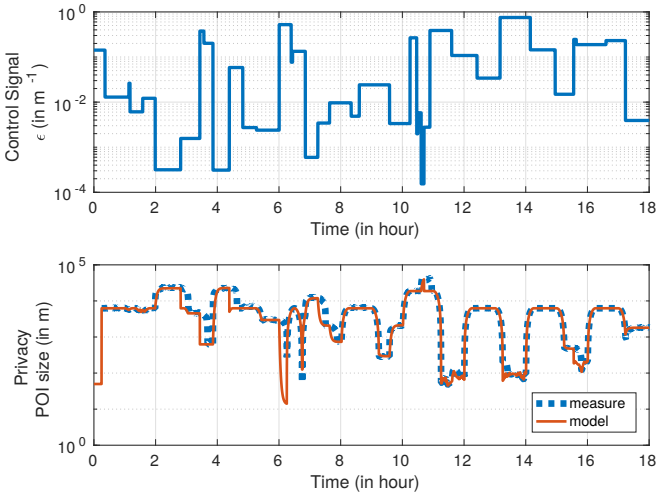

Fig. 8. Model evaluation: input signal scenario (top plot) and the comparison of measured privacy and modeled one (bottom plot). Mean over 100 experiments.

D. Control Evaluation

1) Privacy: Firstly, the controller performances are illustrated and commented for two simple scenario, where a comprehensive analysis can be done. First a step in the reference is realized while the user is stopped (speed is null, see Fig. 9), then a step in the disturbance is applied (i.e. the user was moving and suddenly stops, see Fig. 10).

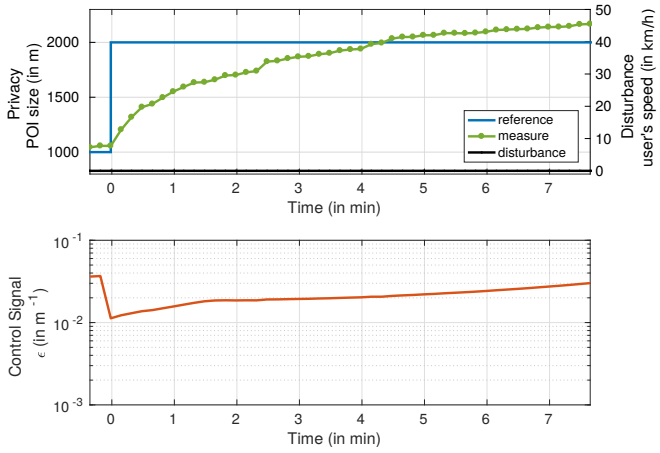

Fig. 9. Control validation with a step in the objective. Mean over 100 experiments.

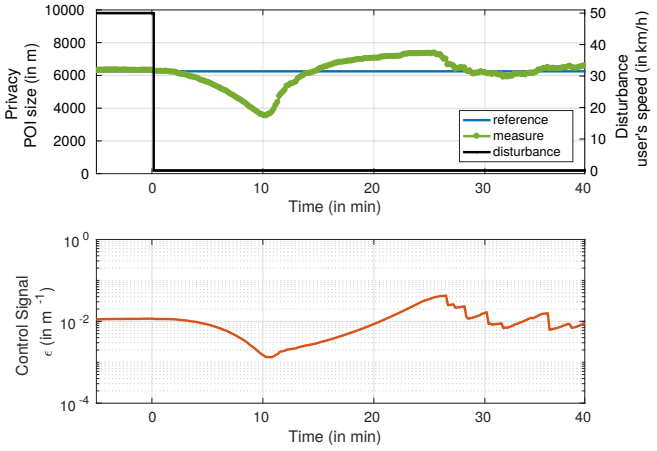

Fig. 10. Control validation with a step in the disturbance. Mean over 100 experiments.

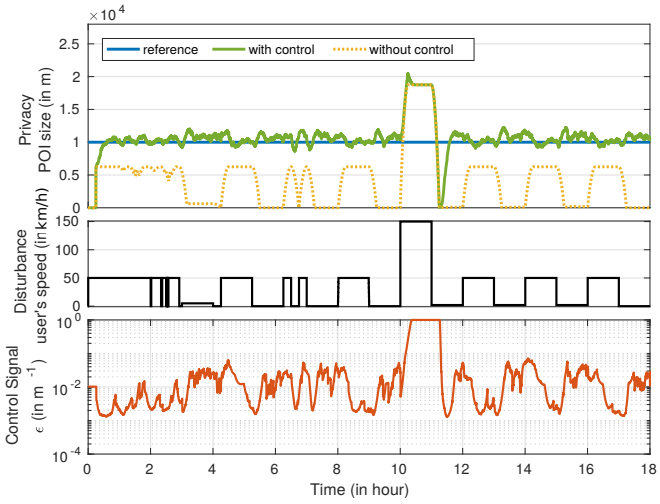

Fig. 11. Control evaluation with the complete disturbance scenario. Mean over 100 experiments.

For reference tracking (Fig. 9), steady state error is non-null but quite low (+20%). The response shows no overshoot and a rise time of around 5 min. During regulation (Fig. 10), steady state error is almost null, while maximal amplification is of -50% and rejection time is of 15 min (if rejection is considered as having a privacy above the reference). These results validate the specifications in these specific conditions, even though the steady state is not completely equal to zero, and the rejection time is relatively long.

The control key specifications are regulation related. Hence, for the complete controller evaluation, the objective POI size is fixed to $Priv_{ref} = 10\ 000$m and the trace properties are varied as in Fig. 6. Results of applying control is illustrated in Fig. 11. The controller is able to follow the reference, even though with some oscillations. The only exception is around 10 to 11 hours, when the user has high speed (150 km/h). This naturally protects the user from POI extraction, which explains why the privacy is high even with a high ϵ (i.e. low noise). The anti-windup saturates the control signal, and thus enables the controller to react fast when the users stops and require protection (at 11 hours). Indeed, there still is a transient phase at this time, which explains why privacy decreases sharply before rising again.

2) Utility: As defined in Section II-C.2, the utility of the obfuscated data is illustrated by looking at the control signal. The higher ϵ, the better the utility. The preservation of utility is well illustrated between hours 10 and 11, where the user is intrinsically protected due to the high speed. The controller then tends to increase the control signal (i.e. decrease the noise), thus increasing utility for the user.

VI. Conclusion

Users of Location-Based Services are particularly sensible to privacy attacks. Location Privacy Protection Mechanisms (LPPMs) have been developed to tackle this issue. Yet, two issues remain open with state of the art LPPMs: (i) usability by a non expert, especially regarding LPPMs' configuration (ii) robustness to users' specificities. In this paper a control-based approach is proposed, that enables users to control their privacy and utility when using such protection mechanisms, regardless of their mobility behavior. Contributions are on the novel problem formulation and particularly a definition of real-time Points of Interest oriented privacy metric, on the modeling of the system and on a first PI control strategy. Evaluation carried out in simulation highlight the relevance of the formulation from a control point of view and the efficiency of the controller to meet its privacy and utility objectives, with the restriction oscillations in the achieved privacy, and slow reaction to large changes in the user speed. The future of this work will be its evaluation using data collected from real users, as well as more advanced control techniques that could be able to tackle the PI limitations.

References

[1] Osman Abul, Francesco Bonchi, and Mirco Nanni. Never walk alone: Uncertainty for anonymity in moving objects databases. In *ICDE*, pages 376–385, 2008.

[2] Miguel E. Andrés, Nicolás E. Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Geo-indistinguishability: Differential Privacy for Location-based Systems. In *CCS*, pages 901–914, 2013.

[3] Karl Johan Åström and Tore Hägglund. *PID controllers: theory, design, and tuning*, volume 2. Instrument society of America Research Triangle Park, NC, 1995.

[4] Kai Dong, Tao Gu, Xianping Tao, and Jian Lu. Complete bipartite anonymity: Confusing anonymous mobility traces for location privacy. In *Parallel and Distributed Systems (ICPADS), 2012 IEEE 18th International Conference on*, pages 205–212. IEEE, 2012.

[5] Cynthia Dwork. Differential Privacy. In *Automata, Languages and Programming*, volume 4052 of *Lecture Notes in Computer Science*, pages 1–12. Springer Berlin Heidelberg, 2006.

[6] Bugra Gedik and Ling Liu. A customizable k-anonymity model for protecting location privacy. Technical report, Georgia Institute of Technology, 2004.

[7] Mohamed F Mokbel, Chi-Yin Chow, and Walid G Aref. The new casper: Query processing for location services without compromising privacy. In *Proceedings of the 32nd international conference on Very large data bases*, pages 763–774. VLDB Endowment, 2006.

[8] Vincent Primault, Sonia Ben Mokhtar, Cédric Lauradoux, and Lionel Brunie. Time distortion anonymization for the publication of mobility data with high utility. In *TrustCom*, pages 539–546, 2015.

[9] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[10] D Vrancic. *Design of anti-windup and bumpless transfer protection.* PhD thesis, University of Ljubljana, J. Stefan Institute, 1996.

[11] Yi-Chin Wu, Karthik Abinav Sankararaman, and Stéphane Lafortune. Ensuring privacy in location-based services: An approach based on opacity enforcement. *IFAC Proceedings Volumes*, 47(2):33–38, 2014.