Probabilistic Models for Assured Position, Navigation, and Timing

Extended Abstract

Andrés Molina-Markham
The MITRE Corporation
a.mm@mitre.org

ABSTRACT

Position, navigation, and timing (PNT) user equipment produces position, velocity, and time (PVT) estimates by combining measurements from multiple Global Navigation Satellite Systems (GNSS) and from additional sensors. PVT estimates are computed using linear estimators or Bayesian filters. However, because linear estimators and Bayesian filters are susceptible to adversarial manipulation, it is challenging to assess the trust of PVT estimates that rely on them.

We investigate the suitability of open-universe probabilistic models OUPMs—introduced by Milch and Russell—as a foundation to design PVT estimators that output PVT information together with trust assessments of PVT inputs and outputs. OUPMs model structural uncertainty (object uncertainty and relational uncertainty) necessary to measure assurance where the availability of sensors and the absence of adversaries cannot be guaranteed.

We evaluate two novel adaptive PVT estimators designed to operate through attacks: (1) an adaptive estimator to compute PVT from GNSS; and (2) an adversarial Bayesian filter for location tracking from multiple sensors. Adaptive PVT estimators reduce the influence of inputs that are probably manipulated by an adversary and return PVT with trust assessments. Our results highlight the strengths of probabilistic programming to model trust and adversarial models, as well as assurance requirements for PNT applications.

CCS CONCEPTS

• **Mathematics of computing → Probabilistic representations**; *Probabilistic algorithms*; • **Security and privacy → Trust frameworks**;

KEYWORDS

Probabilistic programming, assurance models, position, navigation and timing

Position, Navigation, and Timing (PNT) platforms provide fundamental support for critical infrastructure, ranging from air traffic control, emergency services, telecom, financial markets, personal navigation, power grids, space applications, etc. However, it remains an open problem to assess the extent to which PNT information can be trusted when there is uncertainty about the sources or the adversaries that may be present.

PVT estimates are computed using Bayesian filters [5], such as Kalman filters [8] and particle filters [2], or linear estimators [1]. However, none of these take into account that the inputs of PVT estimators can be strategically manipulated by adversaries in order to influence their outputs [16].

A fundamental problem of designing PVT estimators suitable for adversarial settings is that these need to infer the state of a system and also infer assurance information in order to allow the user to quantitatively measure the trustworthiness of the state estimation.

This work evaluates an approach that uses probabilistic programming for designing PVT assurance metrics and adaptive PVT estimators that process inputs according to corresponding assurance assessments (see Figure 1). The *possible worlds semantics* developed in the field of Statistical Relational Learning [4] provides a formal framework that can serve as the basis for defining rigorous assurance models for PVT.

Probabilistic programming allows us to define open-universe probabilistic models (OUPMs) [12], which have richer semantics than other commonly used probabilistic models (i.e., Bayesian filters). Concretely, OUPMs allow us to model structural uncertainty that corresponds to the uncertain availability of sensors (satellites, inertial sensors, clocks, etc.) and the presence of an adversary. Additionally, OUPMs allow us to model relational uncertainty (e.g., how adversaries influence observations). Probabilistic programs, in addition to encoding trust and adversarial models, allow us to specify assurance requirements (e.g., related to accuracy, availability, and continuity).

Uncertainty about the availability, continuity, and integrity of a PVT solution can arise from noise or incomplete information. Therefore, robust probabilistic models, particularly those suitable for adversarial environments, must be able to model uncertainty about which objects exist (or may be present), and uncertainty about the relations among these objects. Adversaries can be represented as objects that influence other objects in the world, including sensors (their availability and their measurements), the physical behavior of vehicles, etc. It is possible to describe the behavior of some adversaries very accurately, based on prior knowledge about how various adversaries behave (e.g., encoding knowledge from GPS spoofing taxonomies [13]). However, we can also describe adversaries with uncertain behavior.

To demonstrate that probabilistic programming is a powerful approach to define assurance metrics, we give examples of PVT assurance metrics. We also use these metrics to assess solutions computed from GPS signals with a traditional approach, as well as with an adaptive PVT estimator. To do this, we use the Texas Spoofing Test Battery [6], which contains several recorded spoofing scenarios, proposed in 2012 as part of an effort to define a notion of *spoof resistance* for commercial GPS receivers.

Prior work has largely tried to design PVT estimators to be tolerant to specific types of faults (e.g., [9–11, 17]). However, there has been insufficient work related to developing a framework to

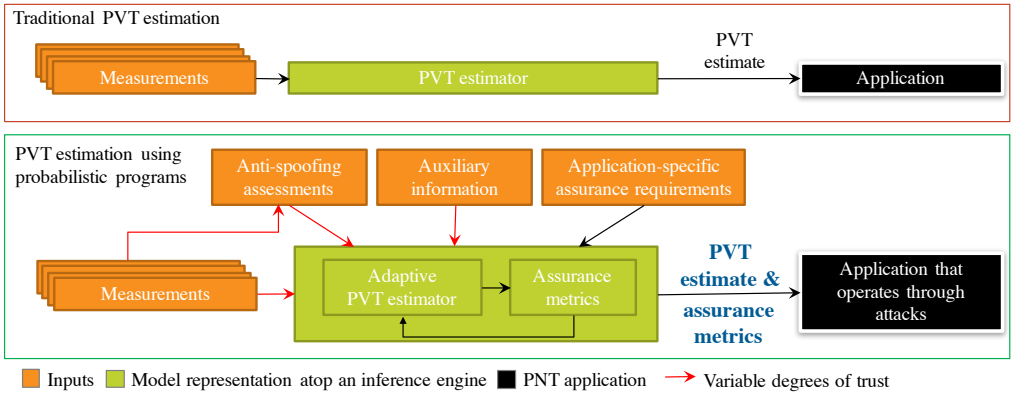

Figure 1: In contrast to traditional PVT estimators (top), adaptive PVT estimators, designed as probabilistic programs (bottom), can model uncertainty about sensor availability and the presence of potential adversaries. Adaptive PVT estimators also output trust assessments that, together with application specific requirements, can be used to compute assurance scores that are meaningful in the context of an application.

systematically model adversaries and to define assurance of PVT estimators. The closest prior work led by Urbina et al., in collaboration with the National Institute of Standards and Technology [14, 15], proposes an advanced adversary—one that is stealthy and adaptive—in the context of physics-based attack detection for control systems. Their work introduces a metric to measure the impact of such stealthy attacks on industrial control systems. Our approach differs in several respects: First, their work seeks to unify metrics and adversary models. In contrast, we propose to leverage advancements in probabilistic programming to facilitate the design of PVT estimators and trust metrics for specific PNT applications under concrete assumptions. In addition, their general metric aims to measure the performance of anomaly detection algorithms. Our goal is to assess the trust in the output of a PVT estimator. While these concepts may be related, we argue that assurance depends on the adversary that we model, the application, and other concrete assumptions. This does not require us to know all the details about all possible adversaries beforehand. Rather, probabilistic programming provides a framework to integrate new information (e.g. from new Anti-spoofing techniques) to infer assurance as we learn about new threats.

Our work is motivated by the need to reason about PNT assurance. However, our ideas apply more generally to other applications of Bayesian filters that require high levels of assurance. For example, autonomous vehicles use Bayesian filters to identify other vehicles or obstacles on the road [7]. Ultimately, vehicles will share such critical information with other vehicles, e.g., through the use of V2X communication to directly impact their behavior [3].

REFERENCES

[1] John W Betz. 2015. *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers.* John Wiley & Sons.

[2] J. Carpenter, P. Clifford, and P. Fearnhead. 1999. Improved particle filter for nonlinear problems. *Sonar and Navigation IEE Proceedings - Radar* 146, 1 (Feb. 1999), 2–7. https://doi.org/10.1049/ip-rsn:19990255

[3] Naveen Chilamkurti. 2016. *Emerging Innovations in Wireless Networks and Broadband Technologies.* IGI Global.

[4] Lise Getoor and Ben Taskar. 2007. *Introduction to Statistical Relational Learning.* MIT Press.

[5] Y. Ho and R. Lee. 1964. A Bayesian approach to problems in stochastic estimation and control. *IEEE Trans. Automat. Control* 9, 4 (Oct. 1964), 333–339. https://doi.org/10.1109/TAC.1964.1105763

[6] Todd E Humphreys, Jahshan A Bhatti, Daniel P Shepard, and Kyle D Wesson. 2012. The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques. In *Proceedings of the ION GNSS Meeting.*

[7] R. Kaestner, J. Maye, Y. Pilat, and R. Siegwart. 2012. Generative object detection and tracking in 3D range data. In *2012 IEEE International Conference on Robotics and Automation.* 3075–3081. https://doi.org/10.1109/ICRA.2012.6224585

[8] Rudolph Emil Kalman and others. 1960. A new approach to linear filtering and prediction problems. *Journal of basic Engineering* 82, 1 (1960), 35–45.

[9] J. Kramer and A. Kandel. 2011. Robust Small Robot Localization From Highly Uncertain Sensors. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 41, 4 (July 2011), 509–519. https://doi.org/10.1109/TSMCC.2010.2068545

[10] X. Li, C. Y. Chan, and Y. Wang. 2016. A Reliable Fusion Methodology for Simultaneous Estimation of Vehicle Sideslip and Yaw Angles. *IEEE Transactions on Vehicular Technology* 65, 6 (June 2016), 4440–4458. https://doi.org/10.1109/TVT.2015.2496969

[11] C. B. Medeiros and M. M. Wanderley. 2014. Multiple-Model Linear Kalman Filter Framework for Unpredictable Signals. *IEEE Sensors Journal* 14, 4 (April 2014), 979–991. https://doi.org/10.1109/JSEN.2013.2291683

[12] Brian Milch and Stuart Russell. 2010. Extending Bayesian networks to the open-universe case. *Heuristics, Probability and Causality: A Tribute to Judea Pearl. College Publications* (2010).

[13] Mark L Psiaki and Todd E Humphreys. 2016. GNSS spoofing and detection. *Proc. IEEE* 104, 6 (2016), 1258–1270.

[14] David I Urbina, Jairo Giraldo, Alvaro A Cardenas, Junia Valente, Mustafa Faisal, Nils Ole Tippenhauer, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Survey and New Directions for Physics-Based Attack Detection in Control Systems. (2016). NIST GCR 16-010.

[15] David I. Urbina, Jairo A. Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Limiting the Impact of Stealthy Attacks on Industrial Control Systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.* ACM, New York, NY, USA, 1092–1105. https://doi.org/10.1145/2976749.2978388

[16] Kyle D Wesson, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. 2011. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *ION GNSS.*

[17] M. Zhong, J. Guo, and Q. Cao. 2015. On Designing PMI Kalman Filter for INS/GPS Integrated Systems With Unknown Sensor Errors. *IEEE Sensors Journal* 15, 1 (Jan. 2015), 535–544. https://doi.org/10.1109/JSEN.2014.2334698