Probabilistic Models for Assured Position, Navigation, and Timing

Andrés Molina-Markham

Trust and Assurance Cyber Tech | The MITRE Corporation

Problem

Position, navigation, and timing (PNT) are fundamental for critical infrastructure, ranging from air traffic control, emergency services, telecom, financial markets, personal navigation, power grids, space applications, etc. However, the problem of estimating how much to trust a position, velocity, and time (PVT) solution in the presence of adversaries is open.

Threats

Some of the important threats that we are concerned about include:

- **Jamming:** Efforts by an adversary to disrupt the availability of sources.
- **Spoofing:** Efforts by an adversary to pass manipulated information as legitimate.

Challenges

We need to design assurance metrics for position, velocity, and time (PVT) estimates when:

- The **availability** of the sources is **unknown**.
- Different sources are **trusted differently**.
- There is **uncertainty** about how **adversaries influence** the sources.
- Conditions **vary over time**. For example, trust of inputs and outputs, situational awareness, and SW/HW concerns.

Probabilistic Programming as Foundation for Assurance Models

To overcome these challenges, we need a formal framework for designing assurance metrics that adequately model *object uncertainty* and *relational uncertainty.* We argue that probabilistic programs with *possible worlds semantics* [1] enable the definition of richer models than those traditionally used to define PVT estimators (see Figure 1).

Need for Richer Representation

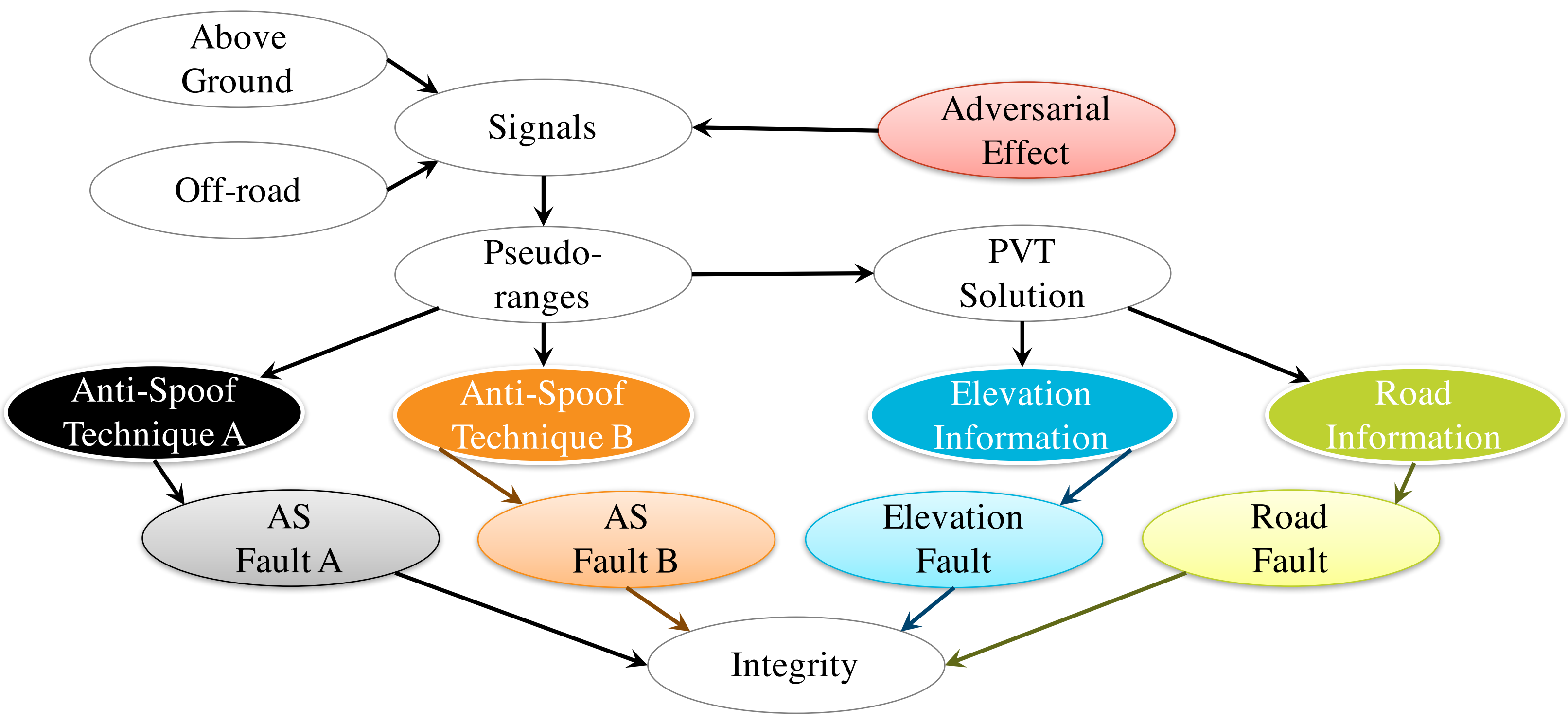

Figure 1: Bayesian Networks have rigid structure.

Today's PVT estimators can be described using probabilistic graphical models such as Bayesian Networks or Dynamic Bayesian Networks. However, the rigid structure of such probabilistic models is not suitable to model object uncertainty and relational uncertainty.

Assurance Metrics for GPS

We give examples of PVT assurance metrics and use them 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 [2], 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.

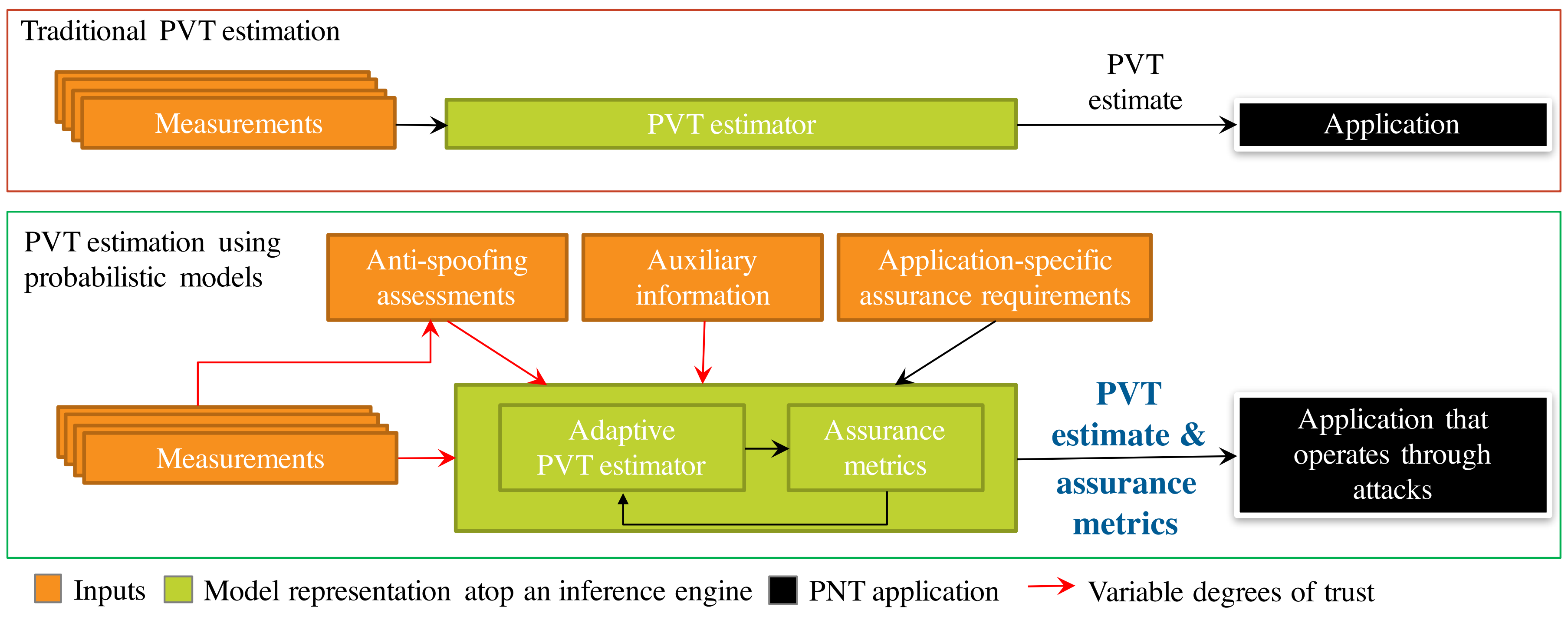
Traditional PVT estimation
Measurements
PVT estimator
PVT estimate
Application
PVT estimation using probabilistic models
Anti-spoofing assessments
Auxiliary information
Application-specific assurance requirements
Measurements
Adaptive PVT estimator
Assurance metrics
PVT estimate & assurance metrics
Application that operates through attacks
Inputs
Model representation atop an inference engine
PNT application
Variable degrees of trust

Figure 2: In contrast to traditional PVT estimators (top), adaptive PVT estimators (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 metrics meaningful in the context of an application.

Key Concepts Supported by Probabilistic Programming

- **Open-Universe Probability Models.** OUPMs 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) [3].
- **Foundation for Model Scrutiny and Verification.** Probabilistic programs can encode trust and adversarial models, as well as assurance requirements (e.g., related to accuracy, availability, and continuity). The integration of these assumptions is often done in an opaque manner that does not facilitate expert verification.

Beyond Sensor Fusion

- Increasingly, PVT estimators integrate anti-spoofing (A/S) techniques that aim to detect spoofed signals. However, multiple A/S signals are integrated in ad hoc ways.
- We argue that probabilistic programming can provide a foundation for rigorously defining how to integrate multiple A/S techniques (e.g., relations among A/S assessments and relations between A/S assessments and PVT solutions).

Conclusion

Our work demonstrates that probabilisitc programs provide a powerful way to define assurance models with strong foundations.

While our work is motivated by the need to define PNT assurance metrics, 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.

References

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

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

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

Additional Information

Andrés Molina-Markham
a.mm@mitre.org