Robust and Secure GPS-based Timing for Power Systems

Website: http://cred-c.org/researchactivity/robustgps

Researchers (Illinois): Grace Xingxin Gao, Sriramya Bhamidipati, Enyu Luo, and Shubhendra Chauhan

Industry Collaboration:

- Currently seeking collaborators from industry, power utilities, or national labs, as well as energy sector research institutes and consortia. Contact Grace Gao or Sriramya Bhamidipati for more information.

Description of research activity: The GPS time-synchronized readings of Phasor Measurement Units (PMUs) provide assistance with real-time operations and off-line analysis to improve the reliability and efficiency of the bulk electric system. Unfortunately, the GPS signal is weak and vulnerable to jamming, meaconing and spoofing. As such, there is a concern that the GPS-based time synchronization of PMUs may be a potential point of entry for attacks on the power system. To address this concern, we propose a multi-layer scheme for the reliable, robust and secure GPS-based time transfer to PMUs. We investigate eight countermeasures in three layers: GPS raw signals layer; semi-processed layer; and fully processed layer. We also develop at GPS simulator/ receiver testbed capable of investigating spoofing attacks and mitigation schemes specific to the use-case of PMUs.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
Our research activity addresses the strategy framework representing "Develop and Implement New Protective Measures to Reduce Risk" of the Roadmap. Our work outlines new protective measures that are essential to improve the resilience of phasor measurement units (PMUs) against external GPS timing attacks. Implementation of our multi-layer scheme will provide synchronized phasor measurements up to an accuracy of 100ns, reduce the system risks against external timing attacks and ensure continued robust performance even in degraded scenarios. The results of the activity also enable WAMS to operate through jamming and spoofing attacks.

If successful, we believe that adoption of our results will elevate the maturity of WAMS, along the risk, threat, and dependencies domains as described in the Es-C2m2 [8], to maturity indicator level (MIL) between 2 and 3.

Summary of EDS gap analysis: The application of GPS/GNSS in the power sector can potentially have significant impact on the bulk electric system through its integration into synchronization devices, such as Phasor Measurement Units (PMUs). Given that PMU technology is expected to transition to control applications in the future and that the primary wide area time synchronization mechanism used by PMUs (today) is GPS, there is growing concern that a dependency on GPS will introduce a built-in vulnerability into the infrastructure. This activity addresses that vulnerability by investigating spoofing vectors that can adversely affect PMU accuracy, and devising mitigation schemes to counteract these attacks, thereby enabling the adoption of GPS/GNSS synchronized PMUs while advancing EDS resiliency.

Full EDS gap analysis: Wide Area Measurement Systems (WAMS) depend on synchronized phasor measurements obtained from distributed Phasor Measurement Units (PMUs). These precise measurements are required for high-resolution grid state estimation and potential early-stage detection of destabilizing conditions.

Given that the power community is transitioning to smart grid in future, synchronized phasor measurements from PMUs are extremely essential for automated control and stability monitoring. The precise operation of PMUs greatly reply on highly accurate time keeping sources like GPS for its time synchronization. GPS can provide up to microsecond level accuracy and is freely available to all the users. In addition to this, the GPS constellation has global coverage, which enables network-wide stability monitoring of power grid. However, given the unencrypted nature and low signal power, GPS/GNSS signals are vulnerable to external interference, either natural or man-made. The susceptibility of GPS/GNSS signals to jamming and spoofing leads to potential vulnerabilities in WAMS. The NESCOR failure scenarios address this attack as failure scenario WAMPAC.12 [1].

Our research is focused on developing robust GPS/GNSS algorithms to improve the robustness of the power grid against the external timing attacks and corresponding mitigation schemes. Our multi-layer protection scheme enables higher tolerance levels for WAMS, thereby allowing continued operation in the presence of attack. Previously, our lab has published relevant papers on robust GPS timing using position-information-aided vector tracking approach [2, 3, 4]. Presently, we designed a novel GPS signal processing technique known as Direct Time Estimation (DTE) that tracks the authentic signals in the event of spoofing and low signal-to-noise ratio (SNR) environments with an accuracy of up to 100ns [5].

GPS/GNSS background: The Global Positioning System (GPS) is the most widely used example of what is more broadly known as Global Navigation Satellite Systems (GNSS). GPS provides precise location and time information to any receiver capable of receiving and decoding the timing signals from at least four satellites in the GPS constellation. The civilian GPS signal does not come with any authenticators and, given the relatively low signal strength, is vulnerable to intentional or malicious spoofing and jamming.

Direct Time Estimation (DTE) synopsis: The concept of DTE involves vector correlating the incoming signal with cumulative satellite signal replica and then evaluating the maximum likely clock parameters for a pre-generated sets of clock candidates considered [6].

Timing attacks background: As mentioned above, the external timing attacks of high threat include Jamming and Spoofing [7]. Jamming involves broadcasting a high-power noise signal near the GPS frequency range, thereby making the timing signals unavailable for the PMUs. Meaconing (also termed as record and replay) is a type of spoofing. In this type of timing attack, spurious look-alike GPS signals are generated with a high power thereby misleading the PMUs with wrong time.

Bibliography:

[1] Electric Sector Failure Scenarios and Impact Analyses, National Electric Sector Cybersecurity Organization Resource (NESCOR)

[2] Daniel Chou, Liang Heng, and Grace Xingxin Gao, Robust GPS-Based Timing for Phasor Measurement Units: A Position-Information-Aided Vector Tracking Approach, in Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2014), Tampa FL, Sep 2014

[3] Daniel Chou, Yuting Ng, and Grace Xingxin Gao, Robust GPS-Based Timing for PMUs Based on Multi-Receiver Position-Information-Aided Vector Tracking, ION International Technical Meeting 2015, Dana Point, California, January 2015

[4] Yuting Ng and Grace Xingxin Gao, Advanced Multi-Receiver Position-Information-Aided Vector Tracking for Robust GPS Time Transfer to PMUs, in Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2015), Tampa FL, Sep 2015

[5] Yuting Ng and Grace Xingxin Gao, Robust GPS-Based Direct Time Estimation for PMUs, in Proceedings of the IEEE/ION PLANS conference, Savanah GA, Apr 2016

[6] Sriramya Bhamidipati, Yuting Ng and Grace Xingxin Gao, Multi-Receiver GPS-based Direct Time Estimation for PMUs, in Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2016), Portland OR, Sep 2016

[7] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, “Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks,” International Journal of Critical Infrastructure Protection, vol. 5, no. 3-4, pp. 146–153, 2012

[8] Electricity Subsector Cybersecurity Capability Maturity Model (Es-C2m2), Us Department of Homeland Security

[9] Roadmap to Achieve Energy Delivery Systems Cybersecurity, Energy Sector Control Systems Working Group