From: pnt-eo@list.nist.gov on behalf of Chris Huntley <c.huntley@ieee.org>
Sent: Monday, June 22, 2020 12:56 AM
To: pnt-eo@list.nist.gov
Subject: [pnt-eo] NIST's RFI about a profile toward the responsible use of PNT's

2020-06-21
This email is a response to the NIST RFI regarding technologies to provide resilient PNT.

First I would like to thank Hubert Kirrmann for his good contribution regarding time services.

The following comprises a few more thoughts, focused on the use of time by applications in power substations:

Holdover:
Holdover is a common name for the duration when a time clock has lost its time source, and is free-running using its internal oscillator.
PNT Profile Recommendation:

- While time is being distributed from a PRTC (Primary Reference Time Clock), the distribution chain of repeaters down to and including the end device should be continually running holdover simulations to capture the stabilities of their internal clock oscillators.
- Then, whenever any device in the time-distribution chain down to and including the end device loses all its PRTC time sources, it should continue to provide time along with a reasonable estimate of its likely worst-case time drift error.
- Finally, the end devices' applications should continually monitor this advertised worst-case time drift error in order to maintain their functions as long as possible.
  UTC applications must also be aware of any leap-second changes during this holdover period; see below.
  Note that for 60Hz power, even a 250us time error causes only a 10% TVE (Total Vector Error), and inexpensive TCXOs can now provide this for several days of holdover.

UTC support:
As Hubert mentioned, critical time applications should use TAI time; however such is not yet generally the case, and certainly not for power substation applications.
To keep its UTC time aligned with the earth's rotation, the IERS is mandated with making the decisions when to add or subtract a leap-second in the UTC offset from TAI; issuing a Bulletin-C when required (currently at 6 month intervals).
On the good side:

- The GPS GNSS service reliably supplies the IERS scheduled leap-second events with at least 6 weeks' notice.
- The IEEE C37.237-2018 Annex A.3 specifies how IRIG-B can distribute these events, with a days-to-expire validity field.
- The IEEE C37.2378a-2020 (pending) also specifies how IEEE 1588 can distribute these events, with a days-to-expire validity field.
- The required information is usually easily available from IERS (e.g. if their e-mail service is accessible from where needed).

On the not-good side:

- Other GNSS services need to be checked for their support.
- IEEE 1588-2008 does provide a mechanism (leap59 and leap61 flags) for advance notice of a leap-second, but only for 12 hours (or less) before an event.
- The ITU G.8275.1 WAN time-distribution 1588 profile does not include support.

PNT Profile Recommendation:
For any substation with critical applications requiring UTC time, its time gateway should:

- Either use GPS, or support an alternate way to obtain the Bulletin-C leap-second events from IERS.
- Distribute time to the substation IEDs using IRIG-B per IEEE C37.237-2018 Annex A.3, and/or IEEE C37.238a-2020.

GNSS time spoofing to fixed-targets (e.g. substations):
In reality (not a university lab bench), a spoofer will be outside the target's building, and hopefully with no knowledge of the location of the target's GNSS antenna; this makes it extremely unlikely that the target's GNSS receiver will continue to report the same location after being attacked.
PNT Profile Recommendation:

- All fixed-location GNSS time receivers should stop using the GNSS signal if the receiver's reported location changes by more than its location uncertainty.
- The GNSS antenna being used should be camouflaged.
- Another GNSS antenna, not camouflaged (and not used), should be placed in a visible location at least 20m away.

GNSS PNT spoofing to mobile-targets (e.g. boats)
Since any and all GNSS receivers with antennae exposed to the spoofer' s signal will report the same location; using multiple antennae should allow the detection of both location and time spoofing.
PNT Profile Recommendation:

- All mobile PNT applications should use multiple antenna/receiver pairs, with the antennae spaced by more than their location uncertainty.
- If the reported locations' geometric polygon dimensions (or line, if 2 antennae) differs from the actual polygon (the antenna positions), the reported time and location should be rejected.

Cybersecurity
Attacks on a GNSS's composite (all satellites) signal come under the spoofing discussed above.
Attacks on a GNSS's individual signals do not seem feasible.
Attacks on a GNSS antenna cable's signal should not be of concern, being a point-to-point cable within a substation.
Attacks on IRIG-B distribution signals should not be of concern, also being point-to-point cables within a substation.
Attacks on IEEE 1588 profile distribution signals, being on Ethernet networks, could be of concern.
PNT Profile Recommendation:

- All network devices supporting IEEE 1588 profile time-distribution should be chosen and configured to ensure that any traffic emulating IEEE 1588 messages and entering any untrusted Ethernet port cannot egress the Ethernet ports being used for the IEEE 1588 time distribution service.
  The use of secure VLANs (VLANs with IDs blocked on untrusted ports) may be useful for mitigating attacks.

Regards,
Chris Huntley
West Vancouver, B.C.

--