NLS
FINNISH GEOSPATIAL
RESEARCH INSTITUTE
FGI

OSNMA in spoofing detection and positioning in practice

Toni Hammarberg

Finnish Geospatial Research Institute

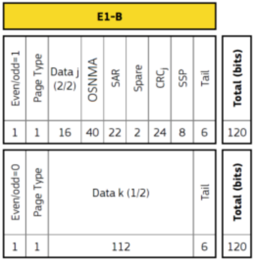
Department of Navigation and Positioning

14th March 2024

Open Service Navigation Message Authentication

Introduction

- OSNMA is a new/upcoming feature of the Galileo constellation
  - OS = Open Service
  - NMA = Navigation Message Authentication
- Detect if a navigation message has been tampered with
  - Can be used to detect spoofing
- First such service in the civilian sector
- The OSNMA data is is transmitted in the E1-B I/NAV pages, 40b per nominal page (2s)
  - Accumulated over 15 pages or one subframe (30s)



E1-B

Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC_j	SSP	Tail	Total (bits)
1	1	16	40	22	2	24	8	6	120

Even/odd=0	Page Type	Data k (1/2)	Tail	Total (bits)
1	1	112	6	120

OSNMA

More in detail

- Adapts the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol
- The receiver will compute a Message Authentication Code (MAC) using a navigation message and a cryptographic key
  - The MACs (or "tags") are also transmitted in the Signal-In-Space (SIS) and can be compared to the recomputed ones
  - This part is very similar to the typical digital signature scheme
- The cryptographic keys will be received also from the SIS, but with a 30s delay compared to the tags
- The cryptographic keys form a so-called hash chain, which allows the receiver to verify the authenticity of the keys
  - Verification of a new key requires a simple hash operation, forging a key is practically impossible

$$\ldots \overset{h}{\leftarrow} K_{i-1} \overset{h}{\leftarrow} K_i \overset{h}{\leftarrow} K_{i+1} \overset{h}{\leftarrow} \ldots$$

- Spoofer cannot forge/fake the keys $\implies$ cannot create tags to fool the receiver

Caveats in using OSNMA

Duality: NMA vs spoofing detection

- Many people see OSNMA as 'spoofing detector'
- Strictly speaking OSNMA is about navigation message authentication
  - Cryptographically verfying that the navigation message has not been altered (intentionally or unintentionally)
  - Spoofing mentioned exactly once in the official ICD and the OSNMA receiver guidelines combined
- Of course, NMA is linked to spoofing detection, however ...
  - OSNMA does not address all forms of spoofing
  - Failure to perform NMA is not the same as being under spoofing
- You can build a spoofing detector on top of OSNMA, or use OSNMA as a part of a spoofing detector

Caveats in using OSNMA

Duality: NMA vs spoofing detection

- Therefore, the "correct" way of interpreting OSNMA is:
  - "My NMA was successful, therefore, I know that my NM is authentic and I can perform positioning based on it"
  - ... and not "My NMA failed, therefore, I am under spoofing"
- Individual failures to perform NMA will happen here and there
  - Many sudden failures is still anomalous

Caveats in using OSNMA

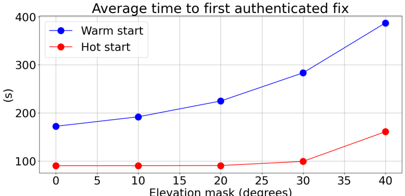
Using OSNMA in positioning

- OSNMA is about authenticating Galileo navigation messages
- How exactly OSNMA is incorporated into PVT computation is up to the users (or receiver manufacturers) and there are different security/performance trade-offs related to this
- Choices you need to make:
  - Are you using other constellations? OSNMA protects only the Galileo I/NAV
  - Are you using corrections? Often secure, but certainly they are not protected by OSNMA
  - What about authenticating/validating ranging information?
  - Maybe use all information available, but simply use OSNMA as a spoofing detector?
- Receivers (that support OSNMA) have made some of these choices and put them under different names (such as "OSNMA loose" or "OSNMA strict"), but these are not part of the OSNMA specification

Caveats in using OSNMA

Effects of using OSNMA in positioning

- The first 'authenticated' position fix will be delayed around 60-300s compared to a regular position solution
  - Certain cryptographic data needs to be received to initialize the authentication procedure
  - If there is signal blockage (e.g. urban canyons), this can get much worse
- Often not every visible satellite (or rather their navigation message) can be authenticated, especially in urban canyons
  - The PVT solution may be based on slightly fewer satellites
  - The availability of 'authenticated' PVT solutions is slightly less than the availability of general PVT solutions
- Or you might not be able to authenticate the most recent navigation message, and you need to rely on older navigation messages
  - PVT may be (partly) based on older navigation messages, and may be slightly less accurate



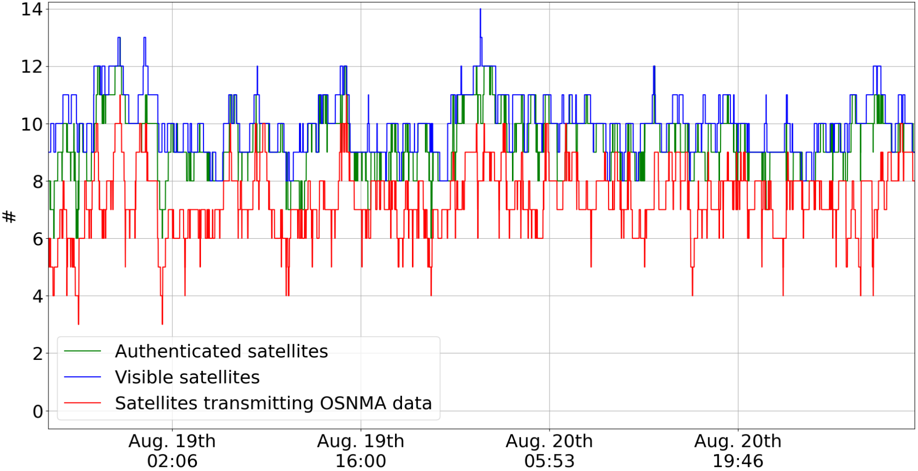
Caveats in using OSNMA

Cross-authentication and its implications

- OSNMA uses a cross-authentication scheme:
    - Not all satellites transmit OSNMA data, but those that do, transmit the required data also for the satellites that don't
- Saves bandwidth in the uplink
- Theoretically you can cross-authenticate messages from other constellations as well
    - There has been some talk of cross-authentication GPS navigation messages, not sure what the status is
- Cross-authentication has positive effects, but at the same time it can make OSNMA-based positioning slightly more vulnerable to signal blockage (for example, urban canyons)
    - If you lose track of one satellite transmitting OSNMA data, you might lose the possibility to authenticate several satellites
        - Typically not a problem, but in poor satellite visibility conditions can be

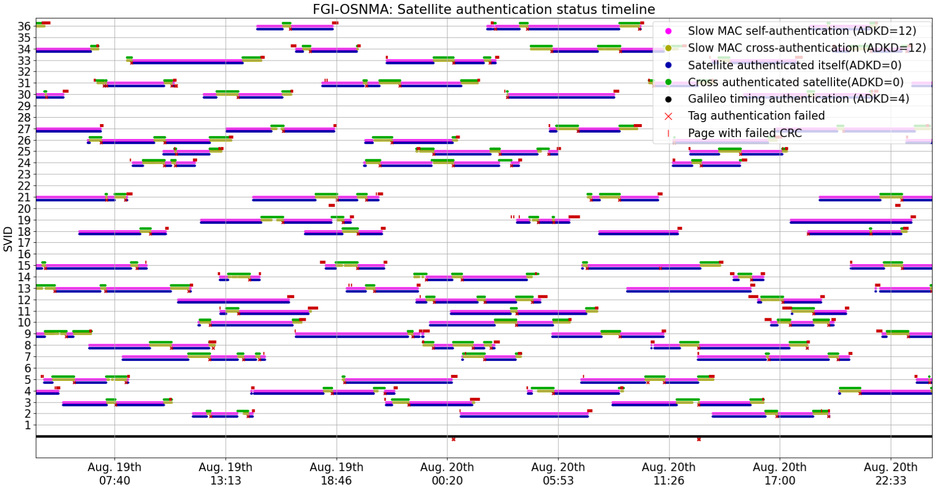
Effects of cross-authentication

Visible satellites vs OSNMA authenticated satellites vs satellites transmitting OSNMA data



Authentication events visualized

Rapid variance between self- and cross-authention modes



Spoofing detection with OSNMA

Case 1: GPS is being spoofed with fake navigation messages

- GPS is not protected by OSNMA, so you don't get cryptographic indication of spoofing
- However, one can perform authenticated Galileo-based positioning and check the consistency with the GPS positioning solution
  - Discrepancy should be noted, and spoofing should be detected

Spoofing detection with OSNMA

Case 2: Galileo being spoofed with fake navigation messages

- The navigation message alteration will be detected by OSNMA giving strong indication of spoofing
- This is exactly the situation to which OSNMA was designed for
- If the spoofer is transmitting valid data from the past (replay attack), the situation is still the same
  - The timing information is also verified by OSNMA, so if the receiver clock has even approximately correct time, this will be detected.

Spoofing detection with OSNMA

Case 2.5: Galileo being spoofed again with fake navigation messages

- The spoofing detection is based on the data contained in the I/NAV OSNMA bits
- However, the OSNMA bits might be empty (i.e. full of zeros) if the satellite is not transmitting OSNMA data
  - This is the case if the satellite is being cross-authenticated
- When the spoofer is transmitting the fake message, they can leave the OSNMA bits as zero
  - The OSNMA bits are cryptographically verified, so why should the attacker even try to replicate them, if the attacker can leave the bits as zero?

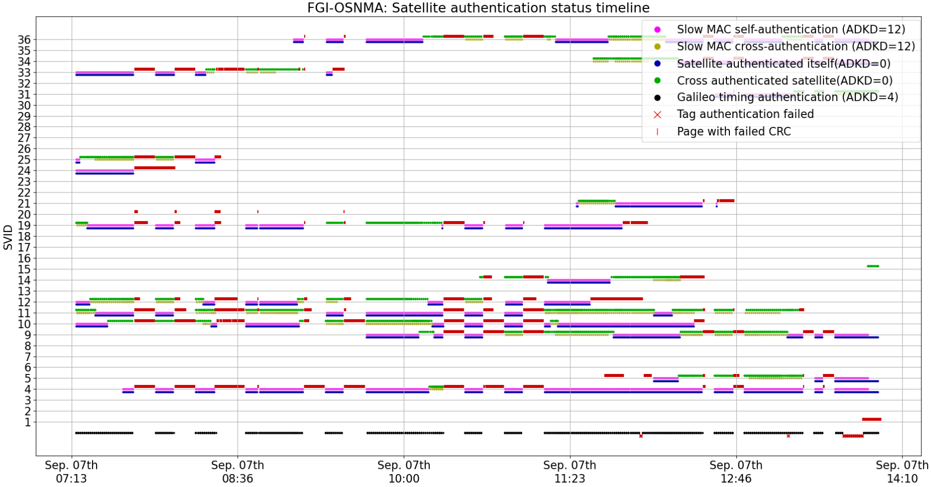
Spoofing detection with OSNMA

Case 2.5: Galileo being spoofed again with fake navigation messages

- When the attacker leaves the OSNMA bits as zero, the receiver will receive no cryptographic data, and can perform no cryptographic verification
- There will be no cryptographic indication of a spoofing, but the fact that no OSNMA data is received from any satellite is highly anomalous
- However, the receiver will still not get spoofed, as it will use an older verified navigation message until it can successfully authenticate newer navigation messages

Visualizing spoofing from OSNMA perspective

One day of data with multiple spoofing sessions. Can you guess when the spoofing is happening?



Spoofing detection with OSNMA

Case 3: Ranging information being spoofed

- The navigation message is not altered, therefore OSNMA does not detect anything invalid, and the receiver may get spoofed
- There are already works where OSNMA is successfully spoofed by focusing on the ranging information, rather than the navigation message
    - Motallebighomi, Maryam, et al. "Cryptography is not enough: Relay attacks on authenticated GNSS signals." arXiv preprint arXiv:2204.11641 (2022).

Future

Extending OSNMA

- OSNMA can be extended to address new types of attacks
- There has already been talk of Galileo Assisted Commercial Authentication Service (ACAS)
  - This is a Spreading Code Authentication (SCA) scheme, which utilizes the OSNMA key infrastructure
  - This will also protect the ranging information cryptographically

Conclusion

- OSNMA can increase the security of your PNT system
  - Even more so in the future
- However, it is not the solution for all problems
  - Users should be familiar with the caveats

Thank you for your interest!

- Questions or comments?

- Some of the visualization are done with our open-source OSNMA implementation, have a look if you are interested, and we are eager to hear any comments
  - `https://github.com/nlsfi/fgi-osnma`

Advancing together

NLS
FINNISH GEOSPATIAL
RESEARCH INSTITUTE
FGI