Navigation Message Authentication for NavIC System

Authors: Durga Digdarsini, Deval Mehta
Indian Space Research Organization (ISRO)

10.10.2019
ICG-14, Bengaluru
Basics - NMA

- NMA uses cryptography to provide assurance of authenticity and integrity of the navigation message
- Harden the civil GNSS signals against spoofing attacks
- When the received message is authenticated the receiver can conclude that the received message are the same transmitted message
Two different ways to generate authentication signatures for Navigation Message

- Using symmetric key - Both transmitter and receiver share same secret key

- Using asymmetric key - Secret key split into two parts, a private key, known only to the transmitter and a public key which can be distributed to the receivers
Asymmetric NMA - ECDSA

- Operates on concept of private & public key
- Exa: Elliptic Curve Digital Signature Algorithm
- Generates & sends digital signature for each set of NAV data to be authenticated
- This needs to send the digital signature through several subframes/pages for single NAV data set
Symmetric NMA - TESLA

- Digital signatures, having large size of keys and/or signatures results impact on user authentication performances such as TTFAF and TBA
- Splitting digital signatures over multiple pages impose a high computational overhead on the receiver.
- Timed Efficient Stream Loss tolerant Authentication uses symmetric cryptography, minimizing the computational overhead of the receiver, and is flexible to meet a range of requirements in terms of authentication performances.
Basics of TESLA

- Based on loose time synchronization between the sender and the receivers
- Based on the transmission of a MAC to authenticate the Navigation message and delayed transmission of the key used to compute the MAC
- Sender attaches to each packet a Message Authentication Code (MAC) computed with a key K known only to the sender.
- The receiver buffers the received packet without being able to authenticate the packet
Basics of TESLA ...

- When the sender discloses Key K with a specific delay after MAC transmission then the receiver is able to authenticate the received packet.
- Consequently, a single MAC per packet suffices to provide broadcast authentication, provided that the receiver has synchronized its clock with the sender ahead of time.
Key Generation Method

- key belongs to a key chain generated through a one-way function. The chain starts with a random seed key $K_n$, which is secret, and ends with a root key $K_0$ that is public.
MAC Generation - Technique

- For each desired time interval $i$ the Navigation Message is authenticated by Key $K_i$. MAC generated with Key $K_i$ is known as $MACK_i$. In TESLA method the MAC is generated by HASH function called HMAC.
Important Parameters for NMA

- Time between authentication
- Length of Key chain
- Size of Key
- Size of MAC
- Root Key addressing method
NMA steps at Transmitting end

1. The Key generation chain starts with a random secret seed key $K_n$
2. One way function $F$ is operated $n$ times to generate root key $K_0$
3. Navigation message ($M_i$) & Key ($K_i$) are used to generate MACi
4. MACi is transmitted to the receiver
5. Keyi is transmitted to the receiver Without/with specific delay

$K_0 = F^n(K_n)$
NMA steps at Receiving end

start

Receiver receives & store the MAC\(_i\) for NAV data \(M_i\)

After zero/specific delay
Receiver receives key \(K_i\)

Receiver authenticates the received key from the previously stored authenticate Key

Receiver authenticates the received key from the stored root Key

\(K_{i-1} = F(K_i)\)

NO

YES

\(K_0 = F^i(K_i)\)

Key \(K_i\) not authenticated

YES

Received NAV data \(M_i\) authenticated in receiver

NO

Generated MAC\(_i\) = stored MAC\(_i\)

Receiver generates MAC\(_i\) from \(M_i\) & \(K_i\)

Received NAV data \(M_i\) is not authenticated in receiver
NMA scheme for L5/S band NavIC

- There is feasibility of Authentication scheme incorporation in L5/S of NavIC satellites
- Key generation & MAC generation can be operated at ground control station
- Only Ephemeris & Clock parameters can be taken as the NAV data to be authenticated
- MAC & key pair for the desired NAV set to be authenticated are upload from ground to onboard
- Authentication data can be defined with a message i.d which is not used is present messages structure
## Subframe Structure in NavIC

### Structure Sub Frame 3 & 4

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>9</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>30</th>
<th>31</th>
<th>37</th>
<th>263</th>
<th>287</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>A</td>
<td>A</td>
<td>S</td>
<td>S</td>
<td>M</td>
<td>D</td>
<td>C</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>O</td>
<td>U</td>
<td>T</td>
<td>U</td>
<td>P</td>
<td>E</td>
<td>A</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>W</td>
<td>B</td>
<td>F</td>
<td>A</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1Bit</th>
<th>1</th>
<th>2</th>
<th>6</th>
<th>226</th>
<th>24</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bits</td>
<td>Bit</td>
<td>Bits</td>
<td>Bits</td>
<td></td>
<td>Bits</td>
<td>Bits</td>
</tr>
</tbody>
</table>

- Subframe 1: T L M
- Subframe 2: A U T
- Subframe 3: S U B
- Subframe 4: A M E

2400 symbols @ 50 sps
Flexibility in Delays....

- Associated no of subframe delay between MAC & KEY is mentioned in the header information associated with each MAC

- Flexibility of transmitting Keyi for MACi with or without delay in subframe 3/4

- Possible combinations are:
  - MACi,Keyi - No delay
  - MACi,Keyi-1 - One subframe delay
  - MACi,Keyi-2 - Two subframe delay etc.
Topics Covered

- Basics of NMA
- TESLA Method for Authentication
- Authentication steps at Transmit & Receive end
- Feasibility of NMA in NavIC System
References


- SIGNAL IN SPACE ICD FOR STANDARD POSITIONING SERVICE, ISRO-IRNSS=ICD-SPS-1.1, AUGUST 2017