NavIC Messaging Service and Authentication for NavIC SPS – An Update

Ranjith V; Anand Dwivedi - U.R. Rao Satellite Centre
Hem Raj Shau – Space Application Centre

INDIAN SPACE RESEARCH ORGANIZATION (ISRO)
NavIC is offering short messaging service for the users in the Indian region.

End-users located at remote places where cellular or internet based communication are difficult to reach (eg. Open seas, remote terrains etc.) benefit from messaging service via NavIC satellites.

Message broadcasters are provided with a Web-Based Interface for Messaging Service (WIMS) portal for submitting message request through internet.

Messaging service is presently being used by INCOIS* for broadcasting Potential Fishing Zone (PFZ) messages, Cyclone & High wave alerts etc. to fishermen across the country.

Forward channel communication support to send acknowledgment to users in distress as part of Second Generation Distress Alert Transmitters (DAT-SG).

Tele-commanding of low earth orbit satellites has also been demonstrated by routing the commands through NavIC constellation (in GSO / IGSO) using the NavIC messaging service.

*INCOIS- Indian National Centre for Ocean Information Services
**NavIC messaging service flow**

- User registers in WIMS.
- Uploads messages to WIMS server.

**Message sent to INC**

- Navigation software at INC generates uplink message and forward to SCF.

**NavIC Satellite**

- Broadcast of message to the user receivers.
- User decodes messages.

**ISRO Navigation Centre (INC)**

**Spacecraft Control Facility (SCF)**
Messaging Service Broadcast

• The broadcast of messages is distributed among the NavIC satellites considering parameters like size of messages, priority of messages etc.

• Different message IDs shall be allotted to different broadcasters. The messaging channel is used in time-shared mode and preference is given users based on the priority of the applications.

• Priorities are allocated certain users based on applications like disaster warning, distress alerts etc. High priority messages shall be broadcast by multiple satellites so that requests are quickly serviced.

• Messages that broadcast a large amount of information (like the INCOIS PFZ messages) shall be staggered across multiple satellites to facilitate faster data collection.

• SIS ICD for Message service available in ISRO website: www.isro.gov.in/irnss-programme
INCOIS Ocean State Forecast and Tsunami Alert Messages

- Indian National Centre for Ocean Information Services (INCOIS) provides ocean information and advisory services. INCOIS generates bulletins for ocean state forecast like High Wave Alerts and Cyclone Alerts etc. and early warnings of Tsunami.

- NavIC Messaging Service is used as a means to broadcast these information to fishermen. The information is displayed in the regional languages for convenience.

**Major Cyclones / Depression Bulletins (2020-21)**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Name</th>
<th>Period</th>
<th>No. of Bulletins</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Amphan Cyclone</td>
<td>13/05/2020 to 21/05/2020</td>
<td>42</td>
</tr>
<tr>
<td>2.</td>
<td>Nisarga Cyclone</td>
<td>29/05/2020 to 04/06/2020</td>
<td>30</td>
</tr>
<tr>
<td>3.</td>
<td>Depression_BOB</td>
<td>09/10/2020 to 15/10/2020</td>
<td>22</td>
</tr>
<tr>
<td>4.</td>
<td>Depression _AS</td>
<td>16/10/2020 to 19/10/2020</td>
<td>11</td>
</tr>
<tr>
<td>5.</td>
<td>Depression</td>
<td>21/10/2020 to 24/10/2020</td>
<td>11</td>
</tr>
<tr>
<td>6.</td>
<td>Tauktae</td>
<td>13/05/2021 to 18/05/2021</td>
<td>38</td>
</tr>
<tr>
<td>7.</td>
<td>Yaas</td>
<td>22/05/2021 to 27/05/2021</td>
<td>30</td>
</tr>
</tbody>
</table>
Potential Fishing Zone (PFZ) Information for Fishermen

- INCOIS identifies location of fish aggregation by utilizing data from various remote sensing satellites.
- The PFZ advisories are generated in the form of PFZ maps and text.
- NavIC Messaging Service is used as one of the means to broadcast this information to the fishermen.

(Source: https://incois.gov.in)
Acknowledgment for Distress Alert Messages

SARSAT (INSAT 3DR, GSAT 17 ..)

NavIC Satellite

Distress signal

UHF

Acknowledgment via NavIC Message

ISRO Navigation Centre

Mission Control Centre

Rescue Coordination Centre

Sends Rescue Team

ISRO

Distress Alert Transmitters (DAT) - 2nd Gen.
- 600 units of NavIC Messaging Receiver (NMR) capable of receiving both the navigation signals and the messaging service signals delivered to fishermen.

- NMR also alerts fishermen from crossing international boundary.

- NavIC messaging receiver functionality integrated with second generation distress alert transmitters to provide two-way communication with NMR features.

- 50 units of second generation Distress Alert Terminals are ready to be deployed for trial.
Common Alerting Protocol (CAP) - Integrated alert system with NavIC Messaging. Disseminating alerts to geographically referenced audience, in vernacular language, about multi-hazards by different alert generating agencies like IMD\(^1\), CWC\(^2\), SASE\(^3\), INCOIS etc. in the ITU standard CAP format through National Disaster Management Agency.

International collaboration on unified Emergency Warning Services (EWS) messages, and Search & Rescue messages with Galileo and QZSS.

\(^1\)IMD- Indian Meterological Department; \(^2\)CWC- Cyclone Warning Centre; \(^3\)SASE- Snow and Avalanche Study Establishment
Authentication for NavIC SPS – An Update
Overview of NMA for NavIC

ICG -14

- Selected TESLA protocol based NMA scheme for NavIC
- Proposal of NMA for NavIC L5/S band signals with existing satellites

Updates

- Key disclosure delay for NavIC optimised
- Time synchronisation requirements
- Size of key chain, key and MAC
- Root key distribution mechanism

Satellite

- Broadcasting NMA messages in secondary sub frames
- Over the air root key distribution using additional secondary messages

Ground station

- Key chain generation
- MAC Generation
- Root key signing
- NMA data Formatting

Receiver

- Root key authentication using stored public key
- MAC Key verification using root key or earlier key
- Authentication of message by MAC verification

29-09-2021
Key Disclosure Delay

- Key disclosure delay governed by following considerations:
  - Throughput availability
  - Time between authentication (TBA)
  - Time synch requirements

- Obtained residual throughput after accounting for existing secondary messages
- **Best possible key disclosure delay: 96s**

### Size of MAC and Key

For TBA of 96s and length of key chain 30 days

116 bits required for \( P_s \leq 10^{-9} \)

30 bits required for \( P_{MAC} \leq 10^{-9} \)

Role of Ground Station

Seed key $K_n$ (Secret)

$K_0 = F^n(K_n)$

Root Key $K_0$ (Public)

On ground key chain generation and signing of root key for sending root key on air

Key Chain Generation

- $K_n$ → $K_{n-1}$ → $K_{n-2}$ → $K_{n-3}$ → $K_{n-4}$ → ... → $K_2$ → $K_1$ → $K_0$

Key Chain disclosure

- $K_0 || Salt$
- ECDSA
- Signature
- Signature || $K_0 || Salt$

On ground MAC Calculation and Frame generation using navigation message and Key

- $Key\ Chain$
- $K_i$
- $SF1||SF2$
- $Msg_i$

- $Trunc(HMAC(Msg_i, K_i), MAC\_len)$
- $MAC_i$
- $Msg_i || MAC_i || K_{i-1}$
- Uploaded to Satellite
NMA workflow at receiver

Key authentication process

- Start
- Store $Msg_{i+1}$, $MAC_{i+1}$ and $K_i$
- $K_0 = F^i(K_i)$  
  - $i < n$
  - Key Authentication failed
- Calculate iterations ($n$) for current key verification from root key using RTC
- $K_0 = F^i(K_i)$  
  - $i > n$
  - Key Authentication failed
- $K_0 = F^i(K_i)$  
  - $i = n$
  - Key authenticated

MAC authentication process

- Receive and 
  - Store $Msg_{i+2}$, $MAC_{i+2}$ and $K_{i+1}$
- $K_i = F^i(K_{i+1})$
- Key authentication failed. Reacquire signal
- YES
- HMAC($Msg_{i+1}, K_{i+1}$) = $MAC_{i+1}$
- NO
- MAC Authentication failed
- YES
- MAC Authenticated
- Recalibrate RTC from authenticated signal
- NO
- Key authentication failed
### NMA under different scenarios

<table>
<thead>
<tr>
<th>Signal Source</th>
<th>Data Condition</th>
<th>Key</th>
<th>RTC Synchronization State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite</td>
<td>Authentic</td>
<td>current</td>
<td>FAIL</td>
</tr>
<tr>
<td>Spoofer</td>
<td>Data Manipulation</td>
<td>Old (1 index)</td>
<td>PASS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Old (2 index)</td>
<td>FAIL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>current</td>
<td>FAIL</td>
</tr>
</tbody>
</table>

- **Key**
  - -96<offset<-48
  - -48<offset<0
  - offset=0
  - 0<offset<48
  - 48<offset<96

- **RTC Synchronization State**
  - PASS
  - FAIL

- It is absolutely necessary that the receiver RTC remains synchronised within the defined bounds (±48s)

### What Next......

- Hardware proof of concept of proposed NMA scheme
- Pilot test case for existing satellite
Thank You