



# Update on Navigation Message Authentication (NMA) for NavIC SPS

*Pravin Patidar*

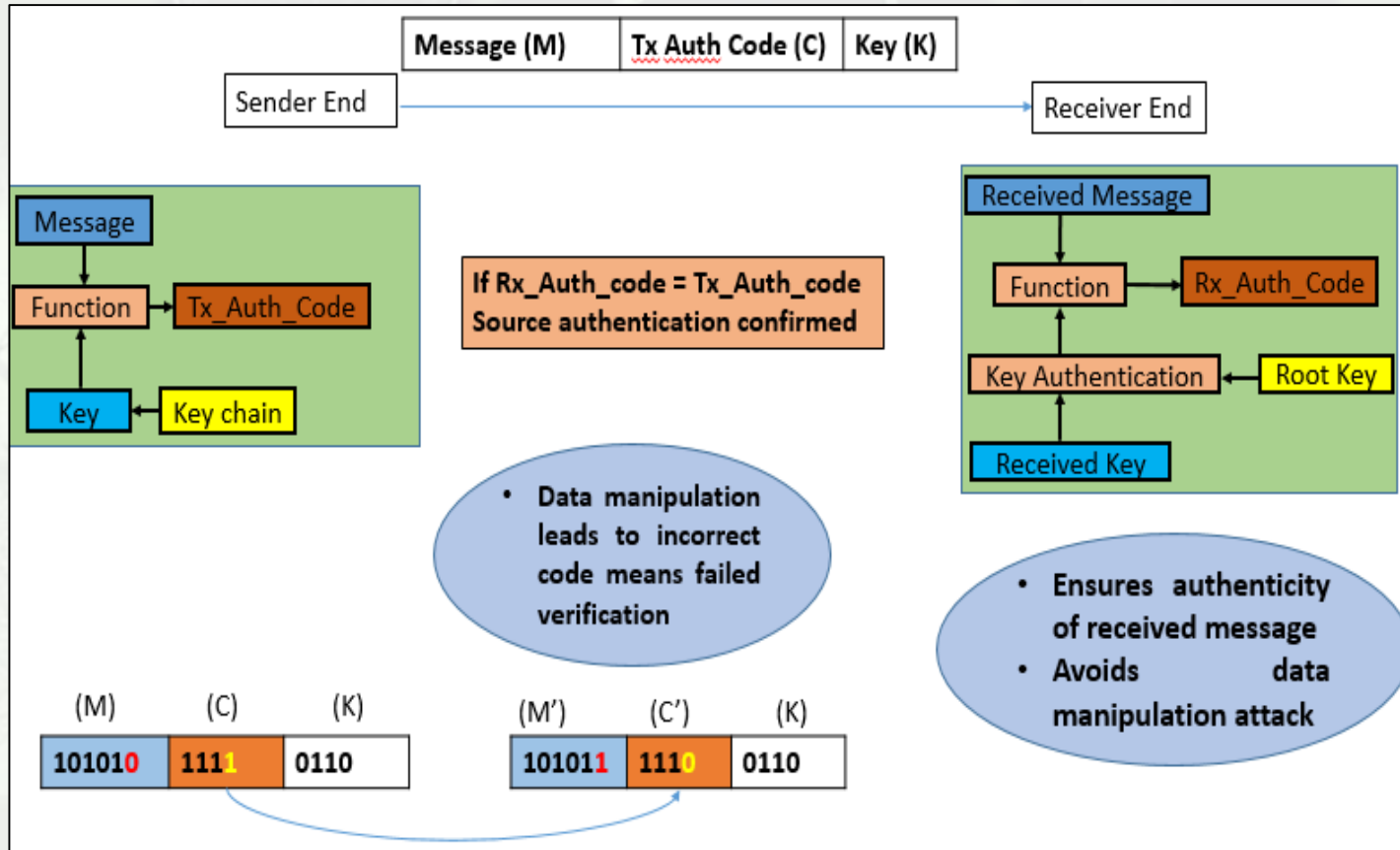
*Space Applications Centre*

*Indian Space Research Organisation*

*Ahmedabad, India*

- The ***Navigation Message Authentication (NMA) in NavIC SPS*** proposes to provide data authentication as value added provision.
- The NMA shall provide NavIC receivers with the assurance that the received navigation message is coming from the system itself and has not been modified.

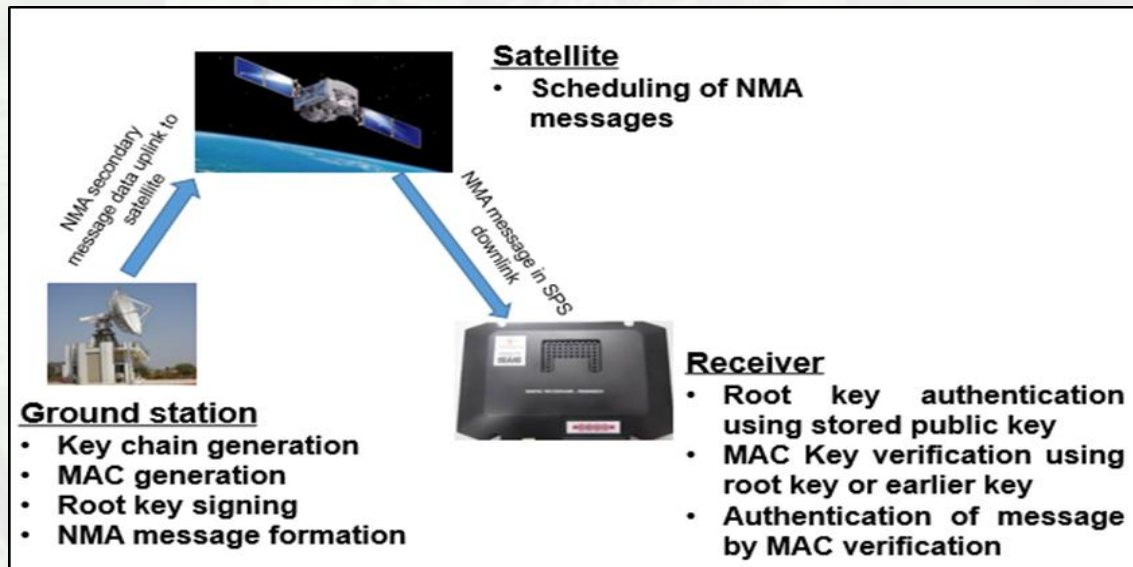
# TESLA based NMA Concept



The receiver and sender should be in *loose synchronization*.

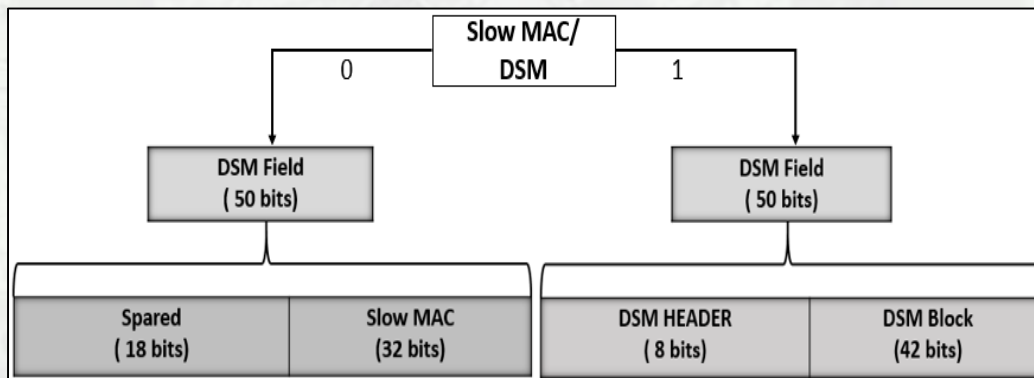
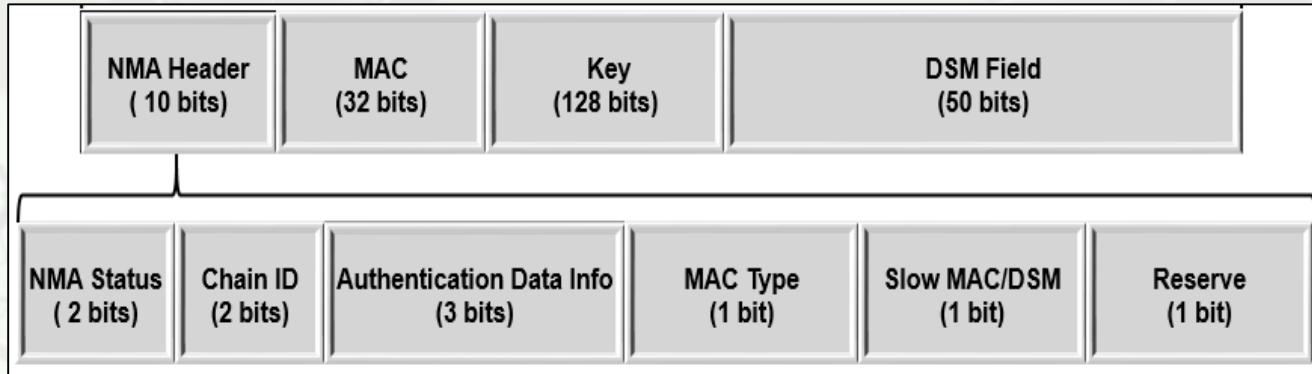
# NMA for NavIC SPS

- The NMA in NavIC SPS (L5, S & L1) is proposed to be offered by defining a new secondary message.
  - Utilizing the flexibility of NavIC SPS data structure
- Two approaches for implementation:
  - For existing satellites: Ground based message generation and uplink
  - For future satellites: On-board message generation



## Ground based Implementation

# NavIC NMA Message



# Root Key Distribution

- The root key distribution will be done through slow rate data embedded into the NMA message.
- For Root Key Distribution , the EdDSA digital signature algorithm has been chosen:
  - Approved in NIST document for Digital Signature Standard
    - FIPS 186-5, Ed25519 curve
  - Faster signature generation and verification and is easier to implement.
  - Better security against side channel attacks

| Attribute  | Separate Keychain for L5/S & L1 | Shared Keychain for L5/S & L1 |
|--|---------------------------------|-------------------------------|
| Minimum Key Disclosure Delay (KDD)               | L5/S: 96 sec<br>L1: 36 sec      | 144 sec                       |
| Typical Time To First Authenticated Fix (TTF AF) | L5/S: 144 sec<br>L1: 54 sec     | 162-192 sec                   |
| Minimum Time between Authentication (TBA)        | L5/S: 96 sec<br>L1: 36 sec      | 144 sec                       |
| Size of MAC                                      | 32 bits                         | 32 bits                       |
| Size of key                                      | 128 bits                        | 128 bits                      |
| Typical Time Synchronisation Requirement         | L5/S: <48 sec<br>L1: <18 sec    | <72 sec                       |

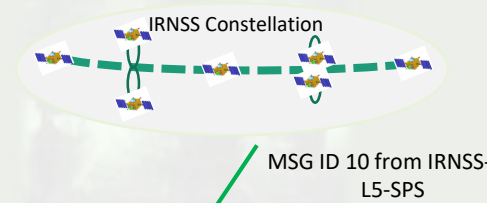
# NavIC NMA Testing

- NavIC NMA scheme is currently under test phase.
- Test transmission using *IRNSS-1D* and *IRNSS-1I* satellites carried out.
- Following test were done:
  - Functional Test
  - Test under spoofed scenario



# NMA Functional Test

- NavIC receiver with NMA capability was tested using live NavIC signal from IRNSS-1D & 1I satellite.
- The NMA message is transmitted as secondary message in SF4 with message ID 10.
- Following functionalities were tested
  - The key and MAC extraction from secondary message
  - The key verification from Root key.
  - MAC authentication using the authenticated key.
  - Root key collection from DSM blocks.
  - Time synchrony error test



**Navigation Message Authentication Status Window**

| DSM Type | Msg ID | Pub Key ID | TOA | Key | KDD | Key Root |   |   |   |   |   |   |   |       |                                |   |   |                      |
|----------|--------|------------|-----|-----|-----|----------|---|---|---|---|---|---|---|-------|--------------------------------|---|---|----------------------|
| 1        | 2      | 3          | 4   | 5   | 6   | 7        | 8 | 9 | 1 | 1 | 0 | 0 | 0 | 34464 | 059906F82244D0904E25B044A1F507 | 1 | 1 | 15/03/23 09:05:02 AM |

**Current Root Key Info**

| TOA(s)    | Chain | KD | Key                            |
|-----------|-------|----|--------------------------------|
| 124276800 | 0     | 1  | 0BC42CA686AFEB4D4958CB231D03EE |

**Update Root Key Info**

| Msg ID | SF | Mag ID | Rel | MAC | TOA Key(s) | Key       | ChainID                        | Key Authorization Status | NMA Authorization Status |
|--------|----|--------|-----|-----|------------|-----------|--------------------------------|--------------------------|--------------------------|
| 1      | 40 | 0      | 0   | 00  | 0          |           | 0                              | KEYAUTH_STS_NA           | NOT AUTHENTICATED        |
| 2      | 47 | 1      | 0   | 00  | 0          |           | 0                              | KEYAUTH_STS_NA           | NOT AUTHENTICATED        |
| 3      | 46 | 1      | 0   | 00  | 0          |           | 0                              | KEYAUTH_STS_NA           | NOT AUTHENTICATED        |
| 4      | 46 | 2      | 0   | 1   | 33C20407   | 124276800 | 0BC42CA686AFEB4D4958CB231D03EE | VALID KEY                | AUTHORIZED               |

**Position Details**

| Date and Time           | Temp | Fix  | TOWC(s) | TTF |
|-------------------------|------|------|---------|-----|
| 15/03/2023 . 09:25:12 . | 201  | 1200 | 293112  | 45  |

**CHANNEL LOCK STATUS**

| SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK | SATSLOCK |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 1        | 1        | 1        | 1        | 1        | 1        | 1        | 1        | 1        | 1        |
| 2        | 1        | 1        | 1        | 1        | 1        | 1        | 1        | 1        | 1        |

**POSITION INFORMATION AUTHORIZED**

| SOL TYPE  | Mode | PRN | PRN | PRN | PRN | PRN | PRN | PRN | PRN |
|-----------|------|-----|-----|-----|-----|-----|-----|-----|-----|
| SATS USED | D    | L   | S   | G   | G   | G   | G   | G   | G   |
|           | 0    | 4   | 0   | 0   | 0   | 0   | 0   | 0   | 0   |

**Tropo ON**

| SF | Iono | Grd | Off | Or | Of |
|----|------|-----|-----|----|----|
| 1  | 1    | 1   | 1   | 1  | 1  |

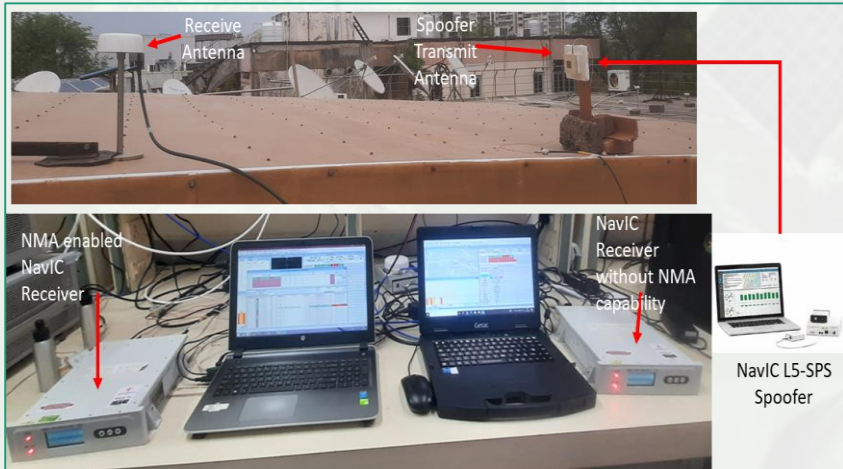
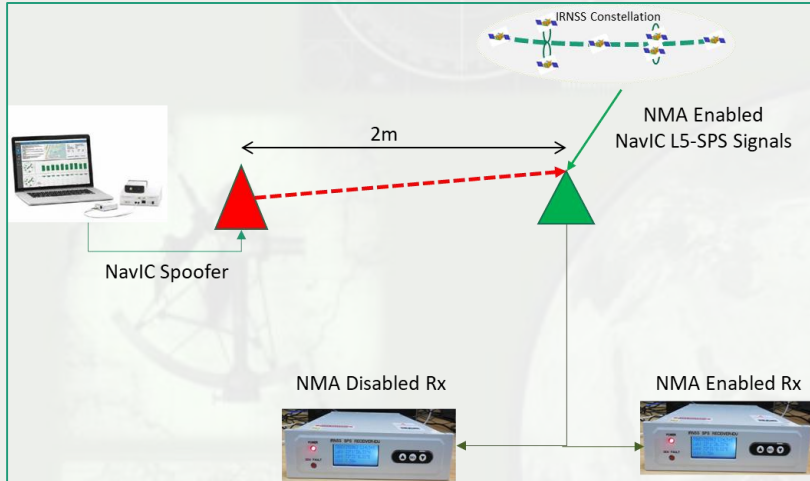
**Position Information**

| Latitude      | Longitude     | Altitude(m) | ECEF X     | ECEF Y     | ECEF Z     | PDOP  | GDOP  | Velocity | ClockBias | Sec Clock Bias(m) |
|---------------|---------------|-------------|------------|------------|------------|-------|-------|----------|-----------|-------------------|
| 23°1' 28.75"N | 72°31' 6.13"E | 168.34      | 1764308.17 | 5601938.72 | 2479298.16 | 35.81 | 47.25 | 0.7      | 978003.89 | 0                 |

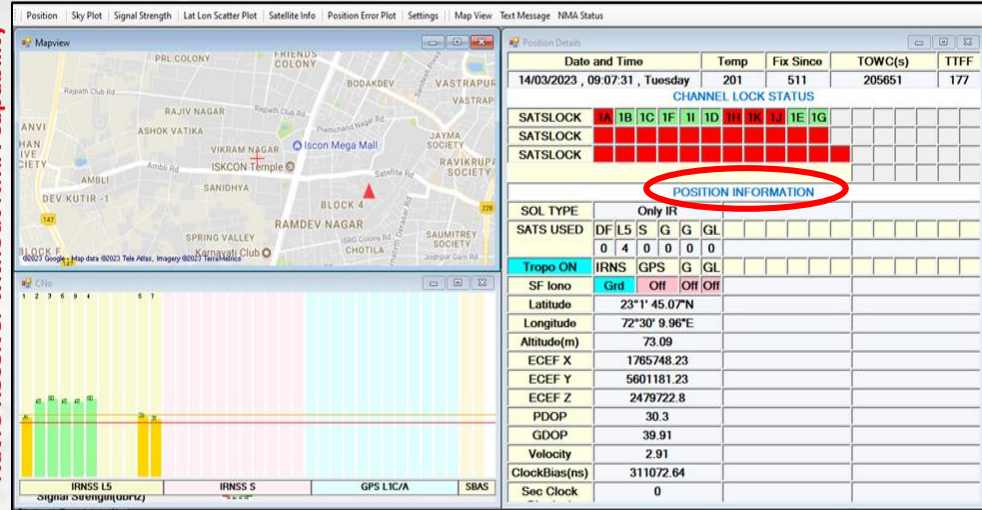


NMA Enabled Receiver

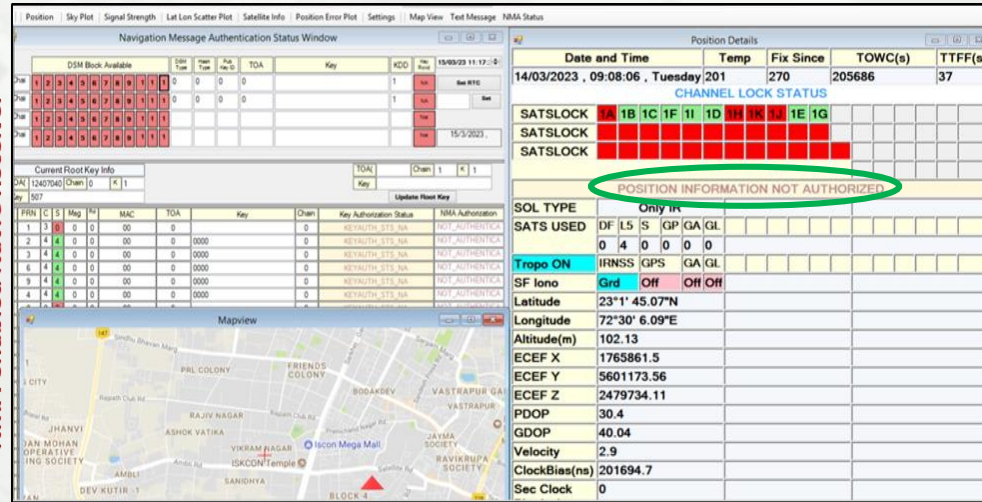
# NMA test Under Spoofing scenario



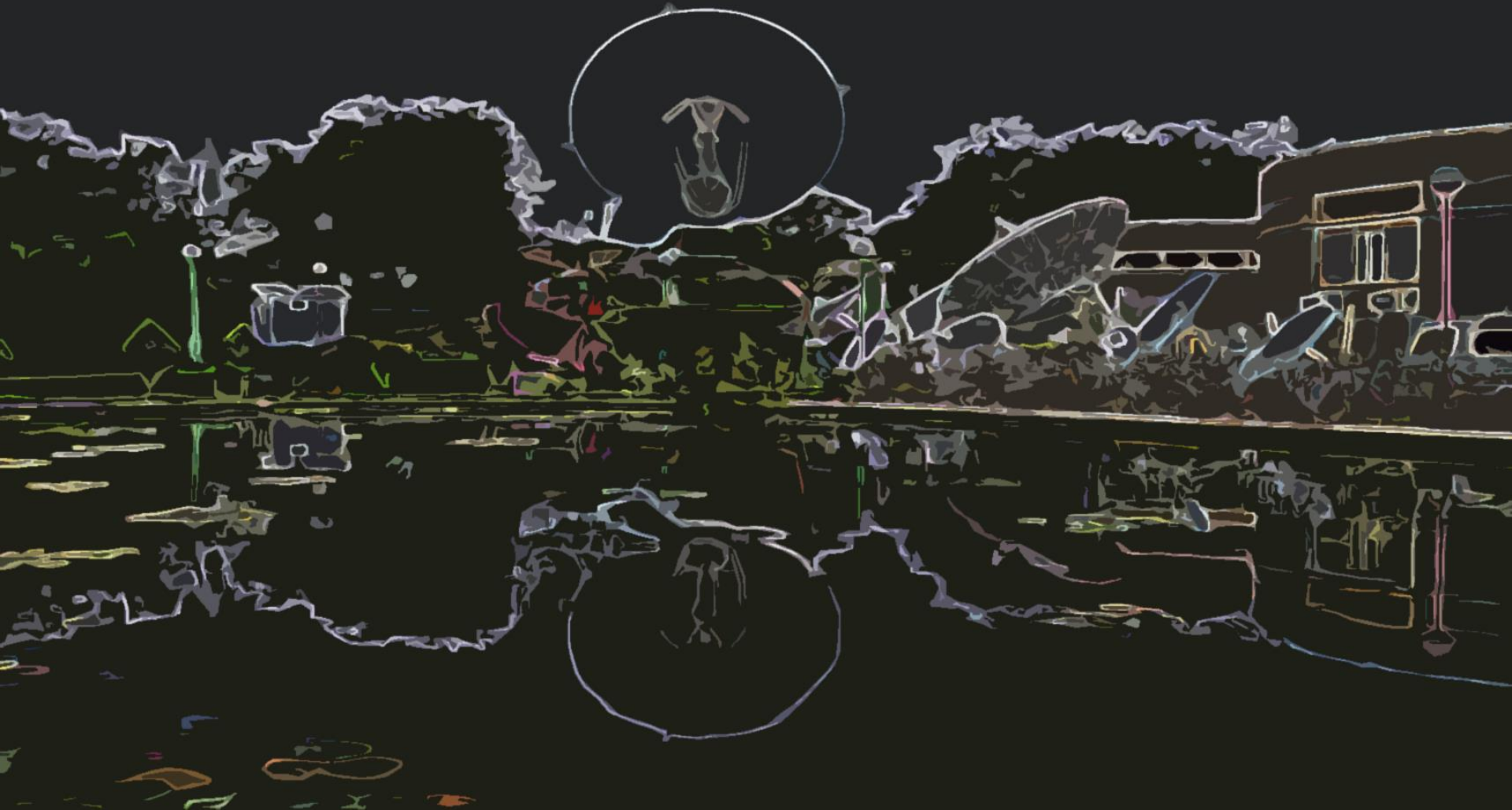
NavIC Receiver without NMA capability



NMA enabled NavIC Receiver



- NMA for NavIC SPS users have been proposed as value added service.
- NavIC shall be able to support the civil signal authentication within the existing SPS signals and with existing satellites.
- The SIS experiments for NavIC SPS NMA are currently in progress.
  - Preliminary tests with IRNSS-1D and IRNSS-1I L5&S SPS signals carried out.
  - New NavIC L1-SPS shall also provide similar NMA provision.



**Thank You for Your Kind Attention**

[\*pravinpatidar@sac.isro.gov.in\*](mailto:pravinpatidar@sac.isro.gov.in)