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

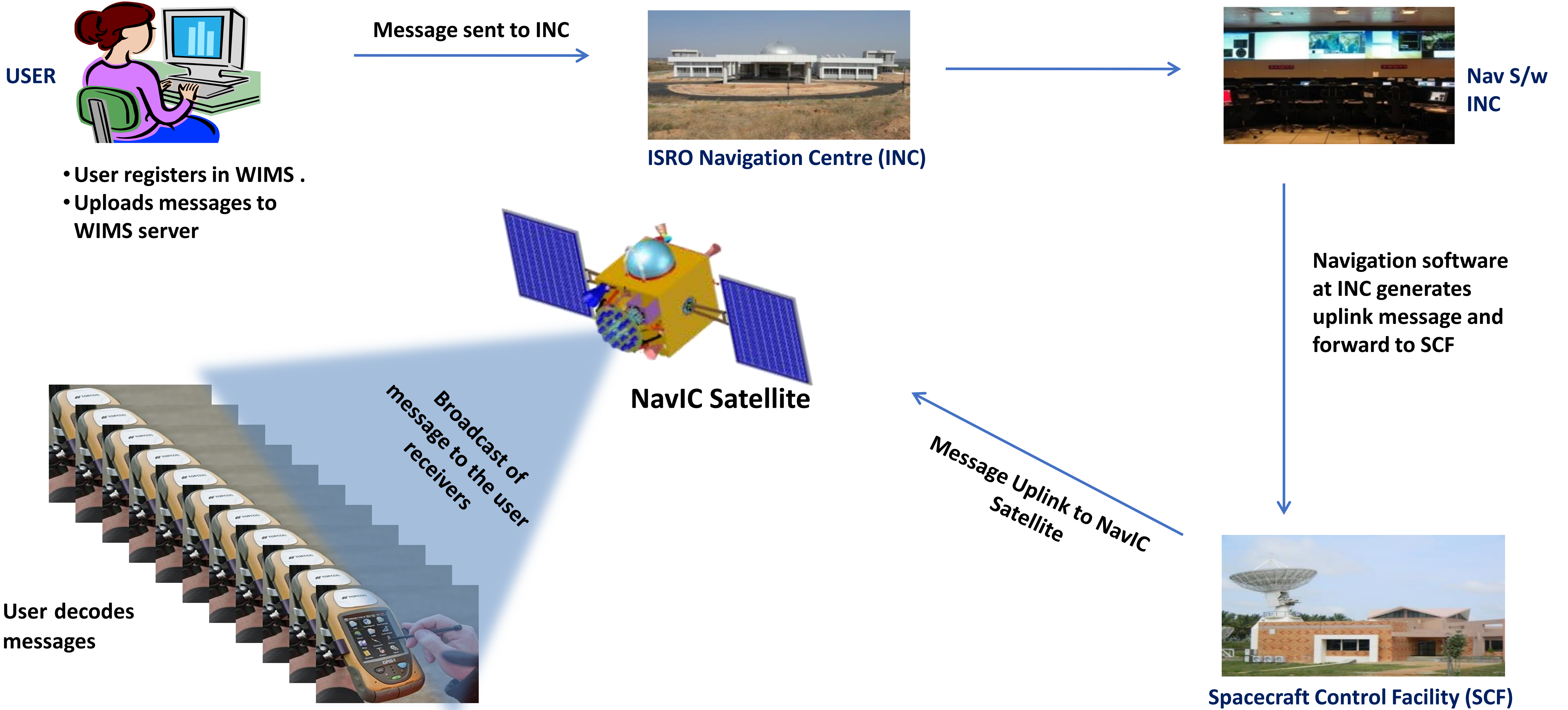
INDIAN SPACE RESEARCH ORGANIZATION (ISRO)

NavIC Messaging Service

- 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

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

Message sent to INC

ISRO Navigation Centre (INC)

Nav S/w INC

Navigation software at INC generates uplink message and forward to SCF

Spacecraft Control Facility (SCF)

Message Uplink to NavIC Satellite

NavIC Satellite

Broadcast of message to the user receivers

User decodes messages

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

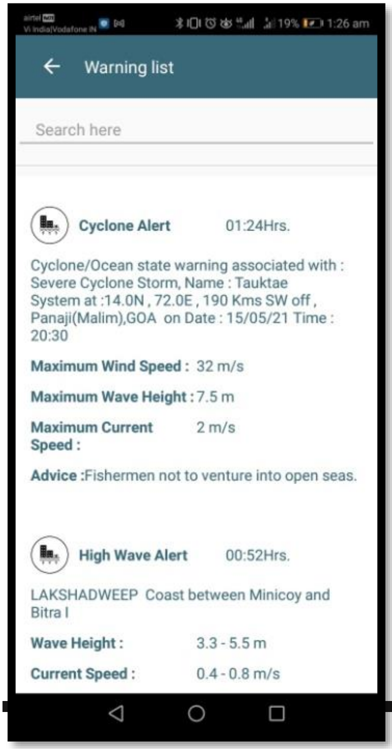
- Indian National Centre for Ocean Information Services (INCOIS) provides ocean information and advisory services. INCOIS generates bulletins for ocean state forecast like High Wave Alerts and Cyclone Alerts etc. and early warnings of Tsunami.

- 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)

S. No.	Name	Period	No. of Bulletins
1.	*Amphan Cyclone*	*13/05/2020 to 21/05/2020*	*42*
2.	*Nisarga Cyclone*	*29/05/2020 to 04/06/2020*	*30*
3.	*Depression_BOB*	*09/10/2020 to 15/10/2020*	*22*
4.	*Depression _AS*	*16/10/2020 to 19/10/2020*	*11*
5.	*Depression*	*21/10/2020 to 24/10/2020*	*11*
6.	*Tauktae*	*13/05/2021 to 18/05/2021*	*38*
7	*Yaas*	*22/05/2021 to 27/05/2021*	*30*

Alert Messages Received via NavIC Messaging Service



Cyclone Alert 01:24Hrs.

Cyclone/Ocean state warning associated with : Severe Cyclone Storm, Name : Tauktae System at :14.0N , 72.0E , 190 Kms SW off , Panaji(Malim),GOA on Date : 15/05/21 Time : 20:30

Maximum Wind Speed : 32 m/s

Maximum Wave Height : 7.5 m

Maximum Current Speed : 2 m/s

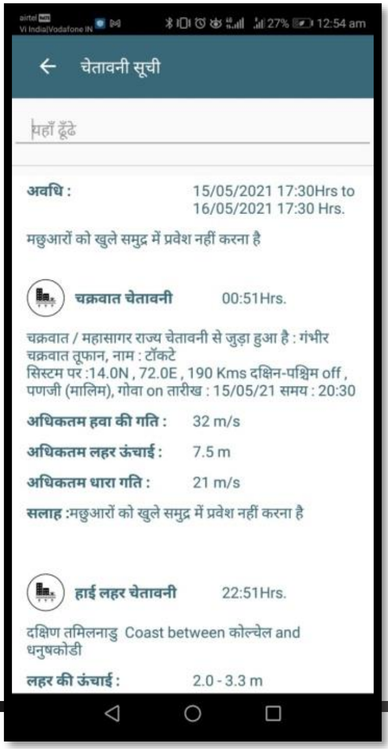
Advice : Fishermen not to venture into open seas.

High Wave Alert 00:52Hrs.

LAKSHADWEEP Coast between Minicoy and Bitra I

Wave Height : 3.3 - 5.5 m

Current Speed : 0.4 - 0.8 m/s



अवधि : 15/05/2021 17:30Hrs to 16/05/2021 17:30 Hrs.

मछुआरों को खुले समुद्र में प्रवेश नहीं करना है

चक्रवात चेतावनी 00:51Hrs.

चक्रवात / महासागर राज्य चेतावनी से जुड़ा हुआ है : गंभीर चक्रवात तूफान, नाम : टॉकटे
सिस्टम पर :14.0N , 72.0E , 190 Kms दक्षिन-पश्चिम off , पणजी (मालिम), गोवा on तारीख : 15/05/21 समय : 20:30

अधिकतम हवा की गति : 32 m/s

अधिकतम लहर ऊंचाई : 7.5 m

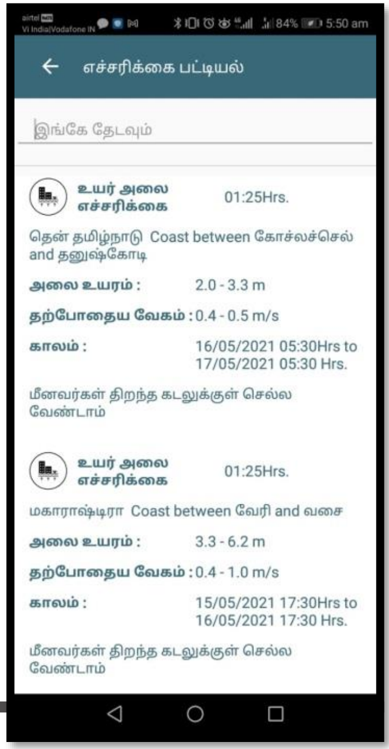
अधिकतम धारा गति : 21 m/s

सलाह :मछुआरों को खुले समुद्र में प्रवेश नहीं करना है

हाई लहर चेतावनी 22:51Hrs.

दक्षिण तमिलनाडु Coast between कोल्चेल and धनुषकोडी

लहर की ऊंचाई : 2.0 - 3.3 m



உயர் அலை எச்சரிக்கை 01:25Hrs.

தென் தமிழ்நாடு Coast between கோச்லச்செல் and தனுஷ்கோடி

அலை உயரம் : 2.0 - 3.3 m

தற்போதைய வேகம் : 0.4 - 0.5 m/s

காலம் : 16/05/2021 05:30Hrs to 17/05/2021 05:30 Hrs.

மீனவர்கள் திறந்த கடலுக்குள் செல்ல வேண்டாம்

உயர் அலை எச்சரிக்கை 01:25Hrs.

மகாராஷ்டிரா Coast between வேரி and வசை

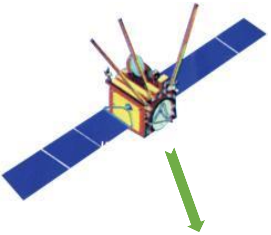
அலை உயரம் : 3.3 - 6.2 m

தற்போதைய வேகம் : 0.4 - 1.0 m/s

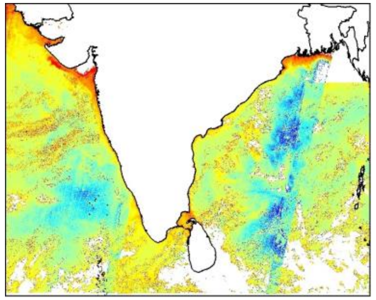
காலம் : 15/05/2021 17:30Hrs to 16/05/2021 17:30 Hrs.

மீனவர்கள் திறந்த கடலுக்குள் செல்ல வேண்டாம்

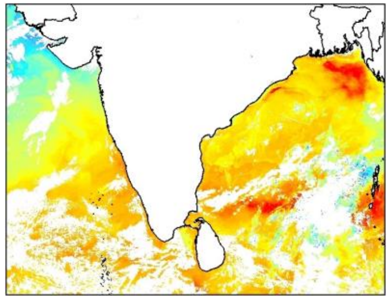
Potential Fishing Zone (PFZ) Information for Fishermen



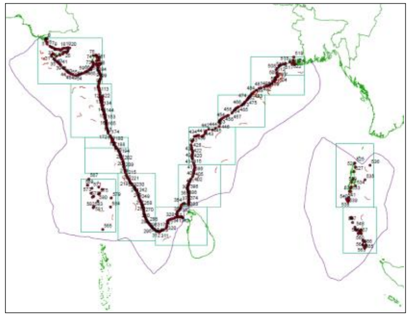
- INCOIS identifies location of fish aggregation by utilizing data from various remote sensing satellites.
- The PFZ advisories are generated in the form of PFZ maps and text.
- NavIC Messaging Service is used as one of the means to broadcast this information to the fishermen.



Chlorophyll Distribution from Oceansat-2

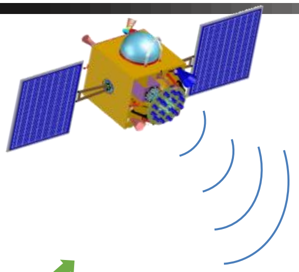


Sea-Surface Temperature from NOAA-AVHRR



PFZ map

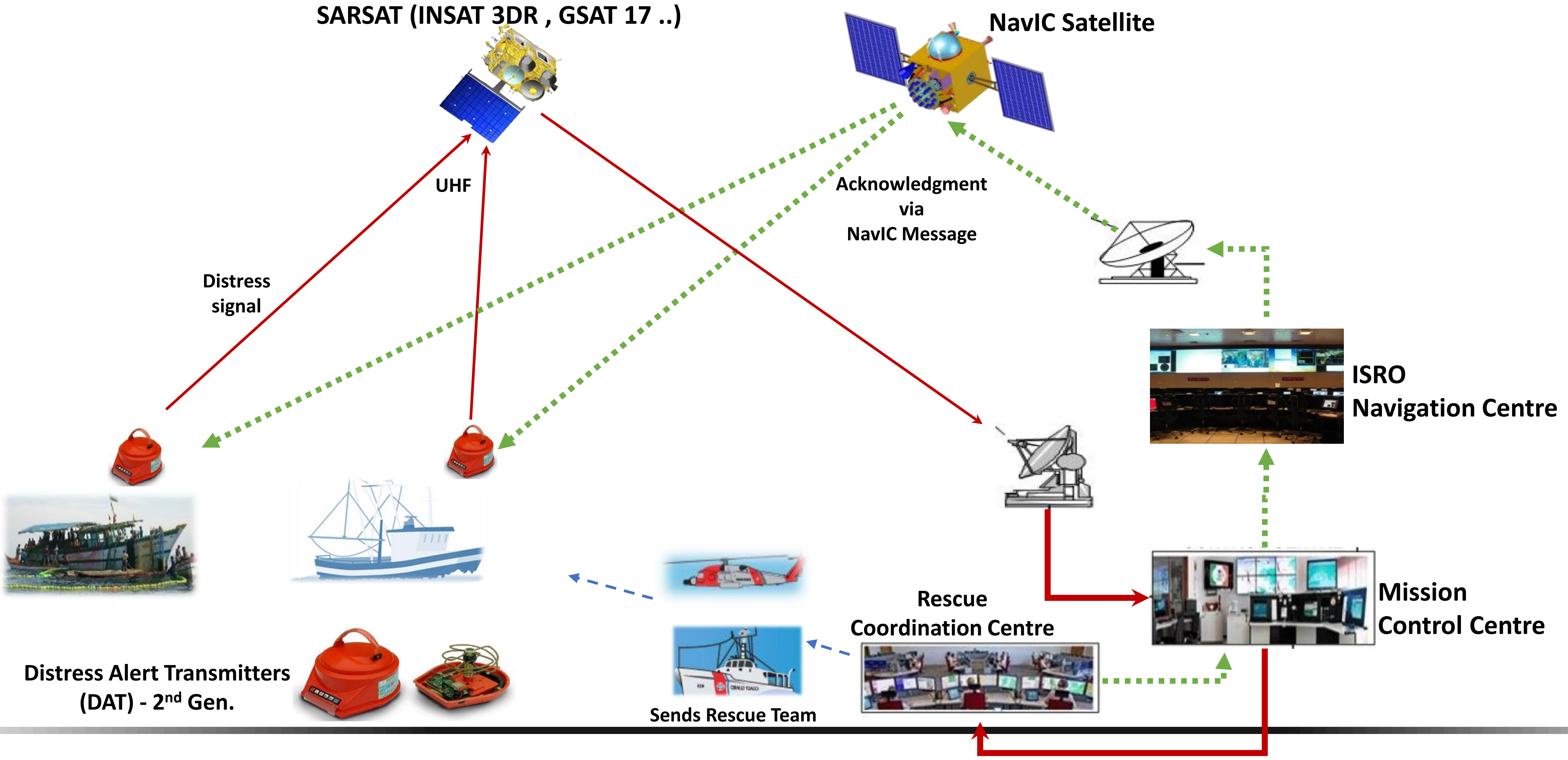
Message transmission to NavIC satellite



Dissemination

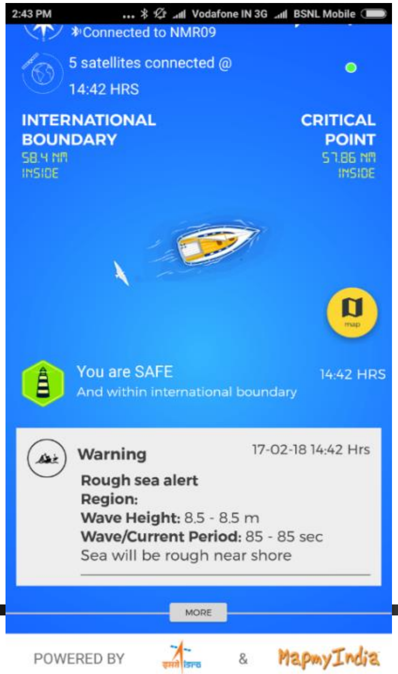
(Source: https://incois.gov.in)

Acknowledgment for Distress Alert Messages


SARSAT (INSAT 3DR , GSAT 17 ..)
NavIC Satellite
UHF
Distress signal
Acknowledgment via NavIC Message
ISRO Navigation Centre
Mission Control Centre
Rescue Coordination Centre
Sends Rescue Team
Distress Alert Transmitters (DAT) - 2nd Gen.

NavIC Messaging and Positioning Application

- ➢ 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.


2:43 PM ... Vodafone IN 3G BSNL Mobile

Connected to NMR09

5 satellites connected @
14:42 HRS

INTERNATIONAL BOUNDARY
58.4 NM
INSIDE

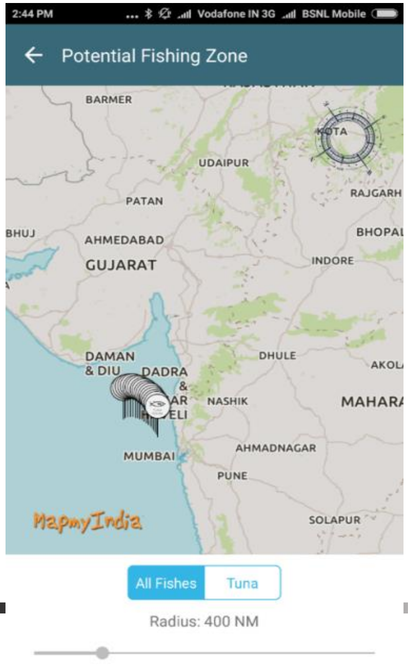
CRITICAL POINT
57.86 NM
INSIDE

You are SAFE 14:42 HRS
And within international boundary

Warning 17-02-18 14:42 Hrs
Rough sea alert
Region:
Wave Height: 8.5 - 8.5 m
Wave/Current Period: 85 - 85 sec
Sea will be rough near shore

MORE

POWERED BY & MapmyIndia


2:44 PM ... Vodafone IN 3G BSNL Mobile

← Potential Fishing Zone

All Fishes | Tuna

Radius: 400 NM

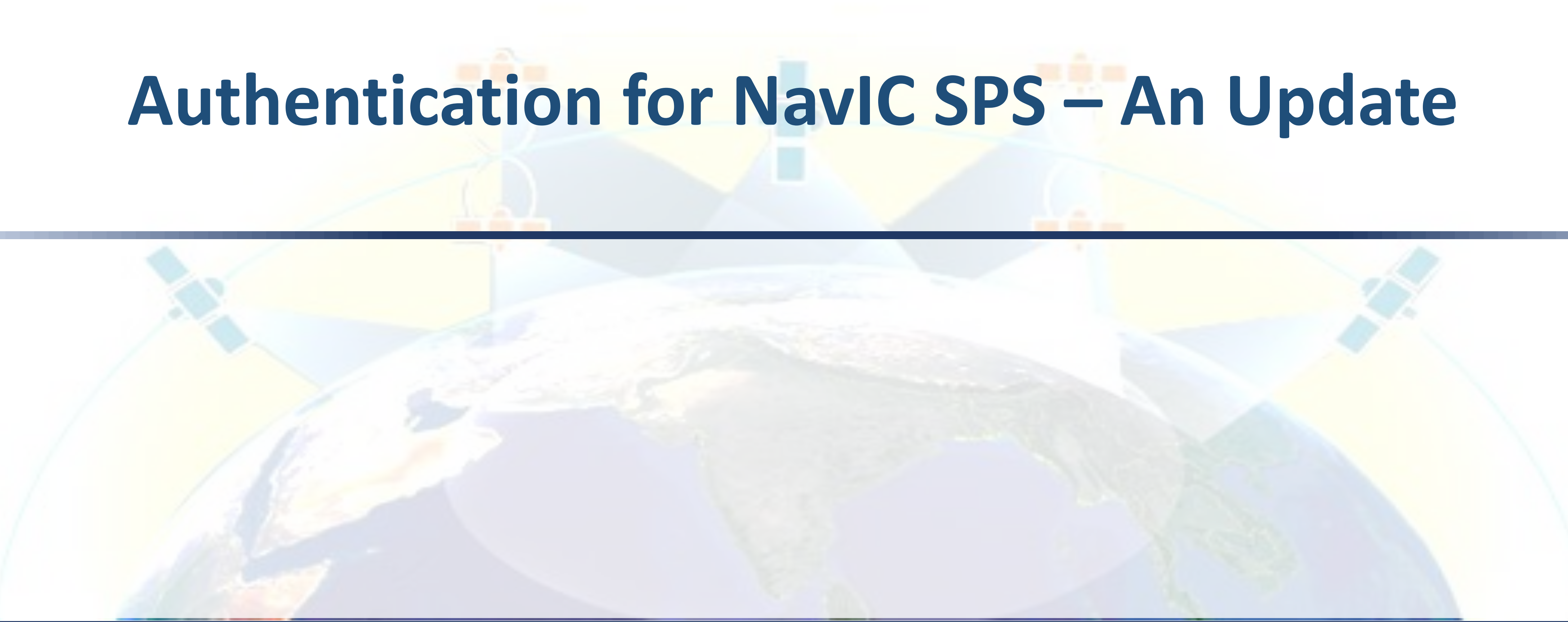
Future Activities

- 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



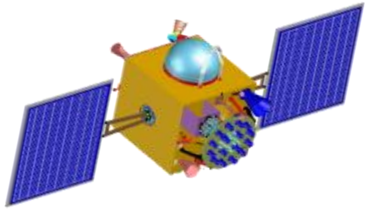
Overview of NMA for NavIC

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



NMA secondary message data uplink to satellite

NMA message in SPS downlink

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

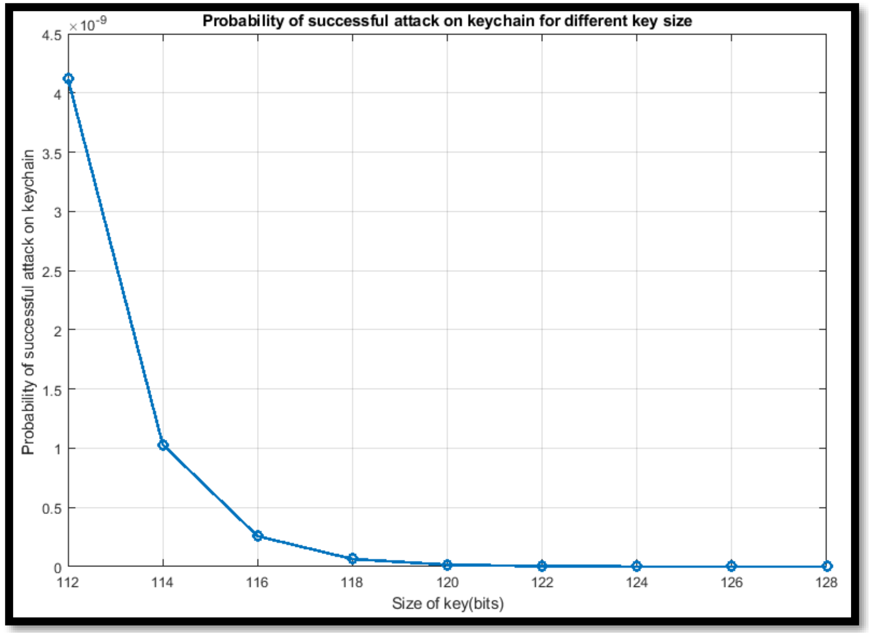
- Root key authentication using stored public key
- MAC Key verification using root key or earlier key
- Authentication of message by MAC verification

Key Disclosure Delay

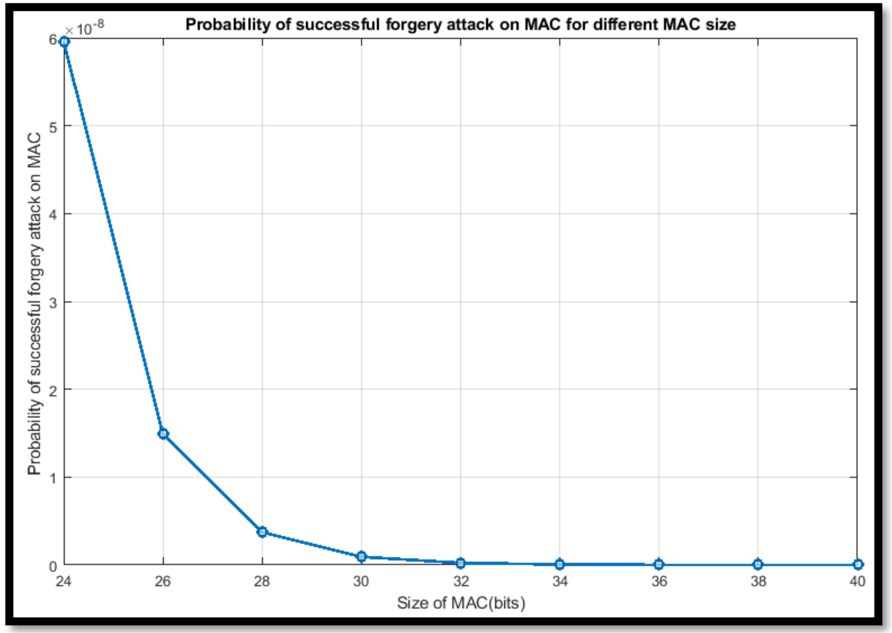
- Key disclosure delay governed by following considerations:
  - Throughput availability
  - Time between authentication (TBA)
  - Time synch requirements

- 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 $P_{MAC} \leq 10^{-9}$

Secondary sub frame occupancy one hour duration for one satellite

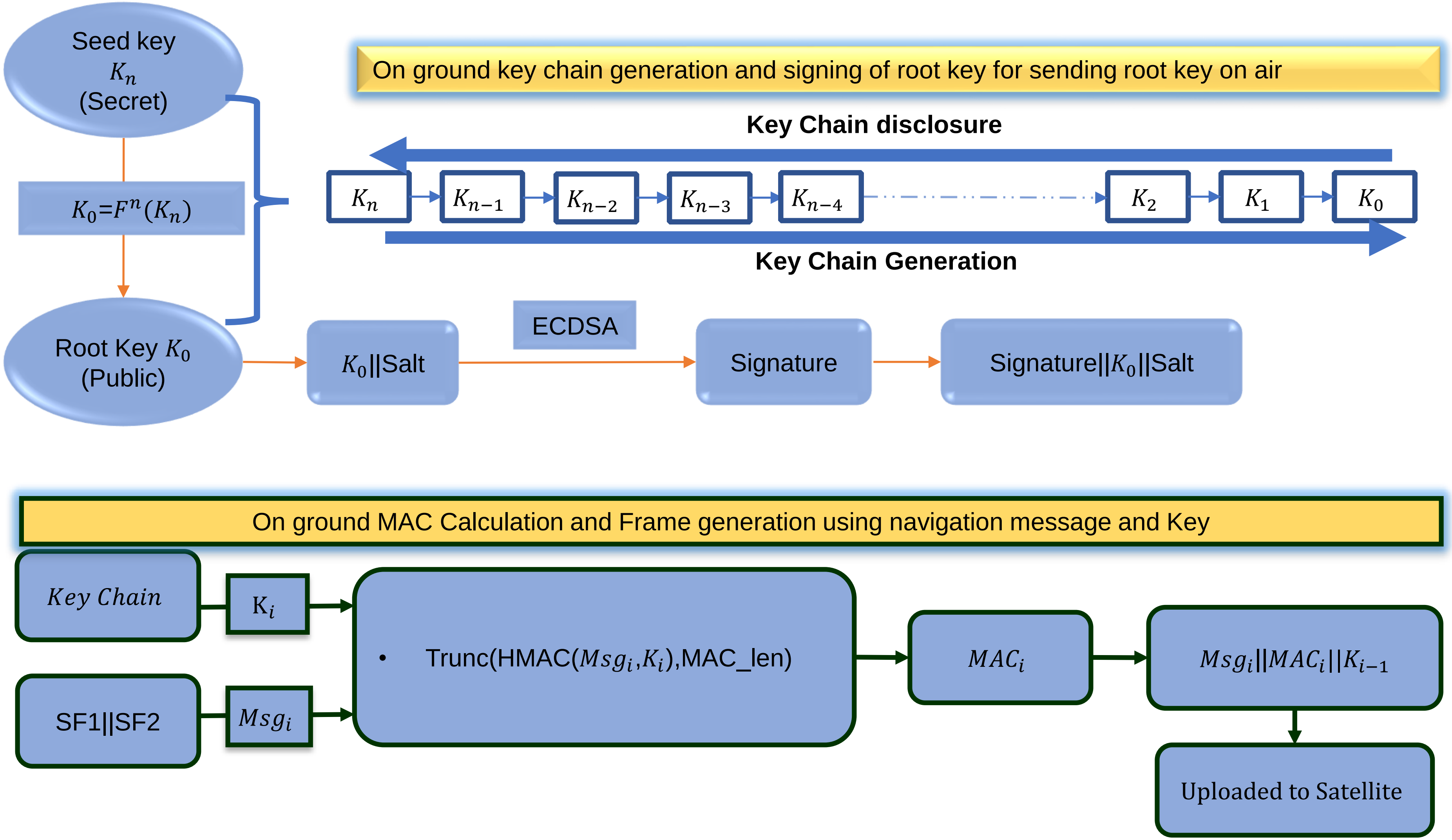
s|E	N|E	E|E	N|E	s|E
N|E	E|E	N|E	E|E	N|E
s|E	N|E	s|E	N|E	s|E
N|E	E|E	N|E	E|E	N|E
E|E	N|E	s|E	N|E	E|s
N|E	s|E	N|E	s|E	N|E
s|E	N|E	E|E	N|E	E|E
N|E	s|E	N|E	s|E	N|E
s|E	N|E	E|E	N|E	E|E
N|E	E|E	N|E	s|E	N|s
s|E	N|E	E|E	N|E	s|E
N|E	E|E	N|E	E|E	N|E
s|E	N|E	s|E	N|E	s|E
N|E	E|E	N|E	E|E	N|E
E|E	N|E	E|E	N|E	s|s

** NMA transmission possible in alternate frames*

N: NMA message
E: existing secondary messages
S: spare secondary sub frames

** Neish, Andrew, Walter, Todd, Enge, "Parameter Selection for the TESLA Keychain," in Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 2018.*

Role of Ground Station



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

Seed key K_n (Secret)

K_0=$F^n(K_n)$

Root Key K_0 (Public)

Key Chain disclosure

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

Key Chain Generation

K_0||Salt → ECDSA → Signature → Signature||K_0||Salt

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

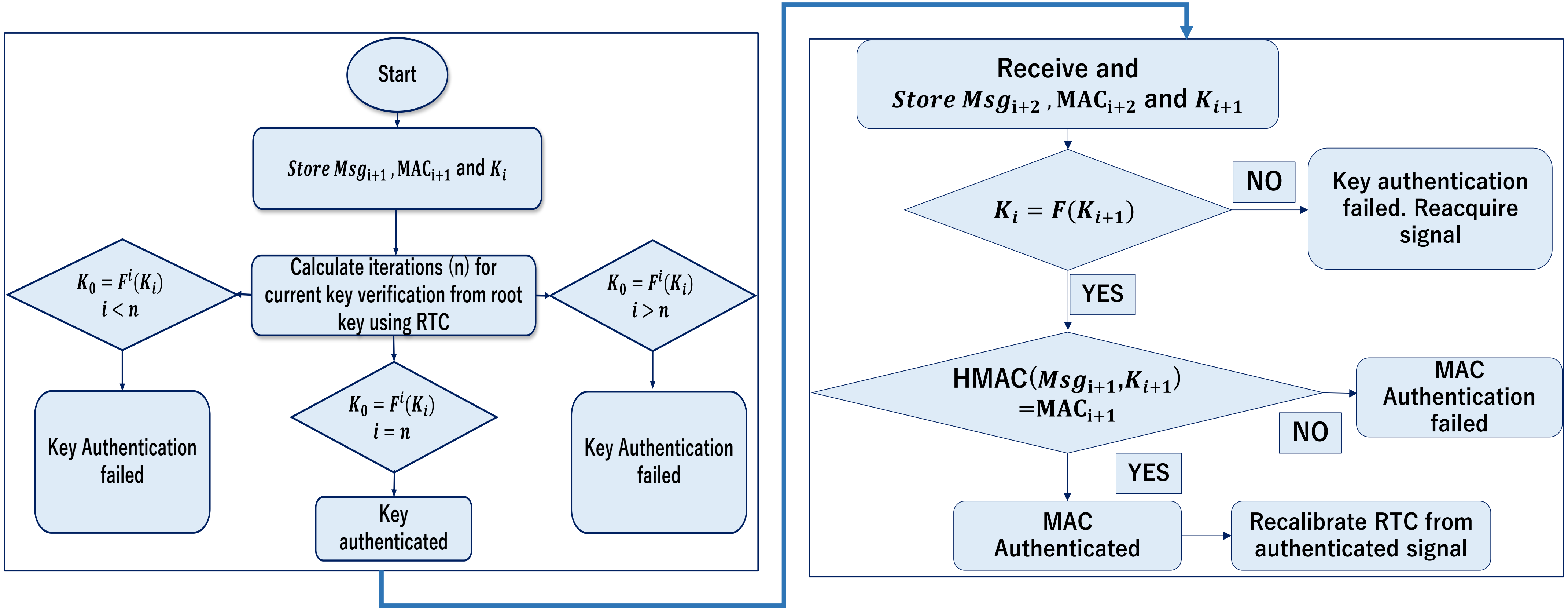
Key Chain → K_i

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


Start
Store Msg_{i+1} , MAC$_{i+1}$ and K_i
Calculate iterations (n) for current key verification from root key using RTC
$K_0 = F^i(K_i)$ $i < n$
$K_0 = F^i(K_i)$ $i > n$
$K_0 = F^i(K_i)$ $i = n$
Key Authentication failed
Key authenticated
Key Authentication failed
Receive and Store Msg_{i+2} , MAC$_{i+2}$ and K_{i+1}
$K_i = F(K_{i+1})$
NO
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

Key authentication process

MAC authentication process

NMA under different scenarios

Signal Source	Data Condition	Key	RTC Synchronization State				
			-96<offset<-48	-48<offset<0	offset=0	0<offset<48	48<offset<96
Spoofer	Data Manipulation	Old (1 index)	PASS	FAIL	FAIL	FAIL	FAIL
		Old (2 index)	FAIL	FAIL	FAIL	FAIL	FAIL
		current	FAIL	FAIL	FAIL	FAIL	FAIL
Satellite	Authentic	current	FAIL	PASS	PASS	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