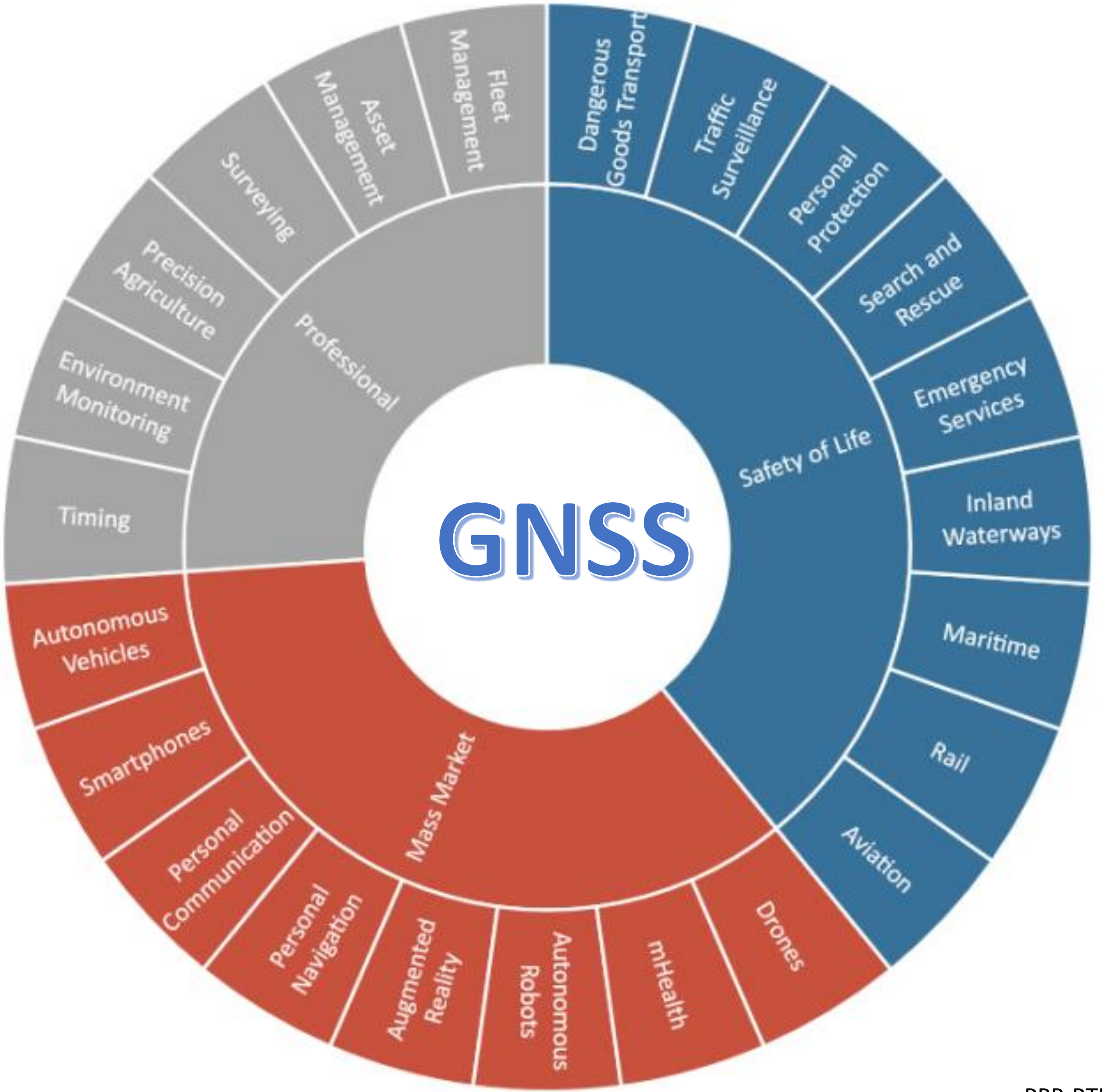
UN Mongolia Workshop on the Applications of GNSS
Ulaanbaatar, Mongolia, 25 - 29 October 2021

GNSS Signal Authentication Applications

Nishkam Jain and Hem Raj Shau
Space Applications Centre (SAC)
Indian Space Research Organisation (ISRO), India

GNSS Applications

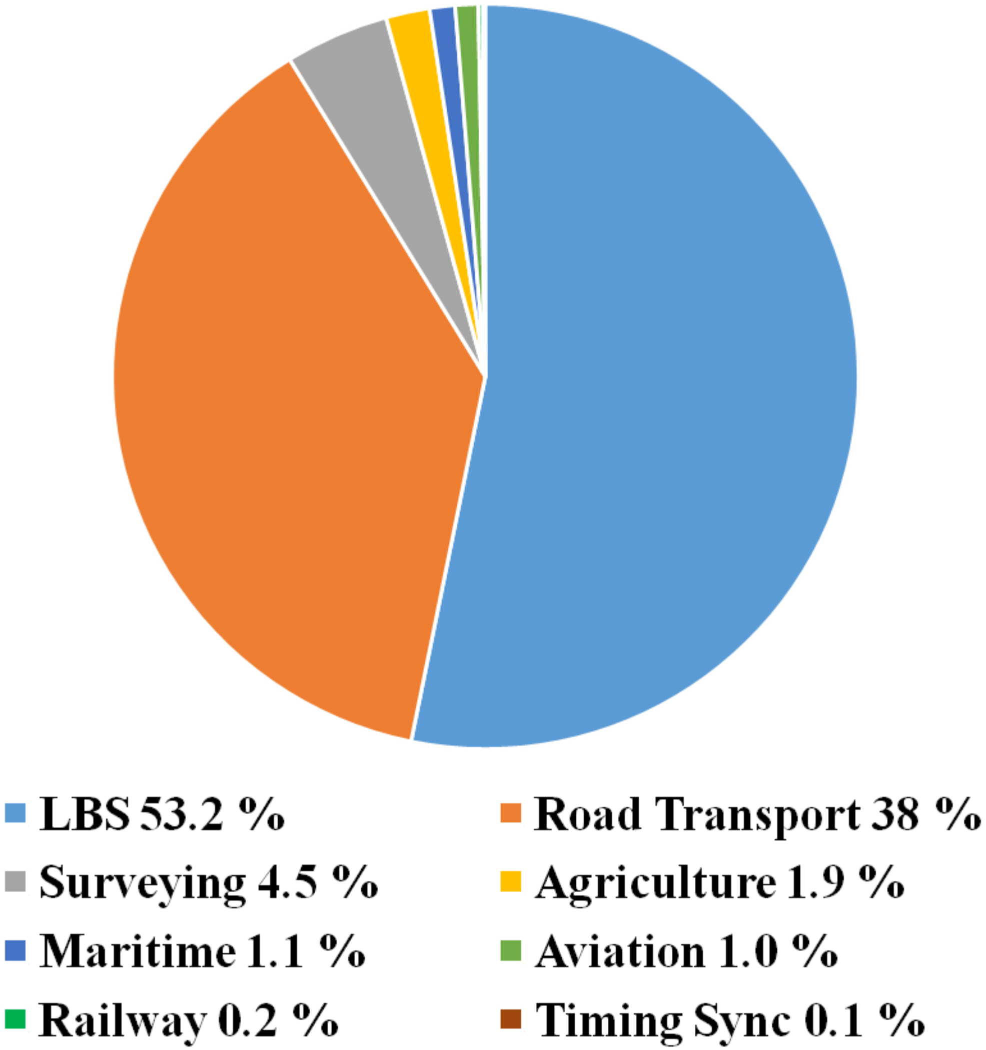


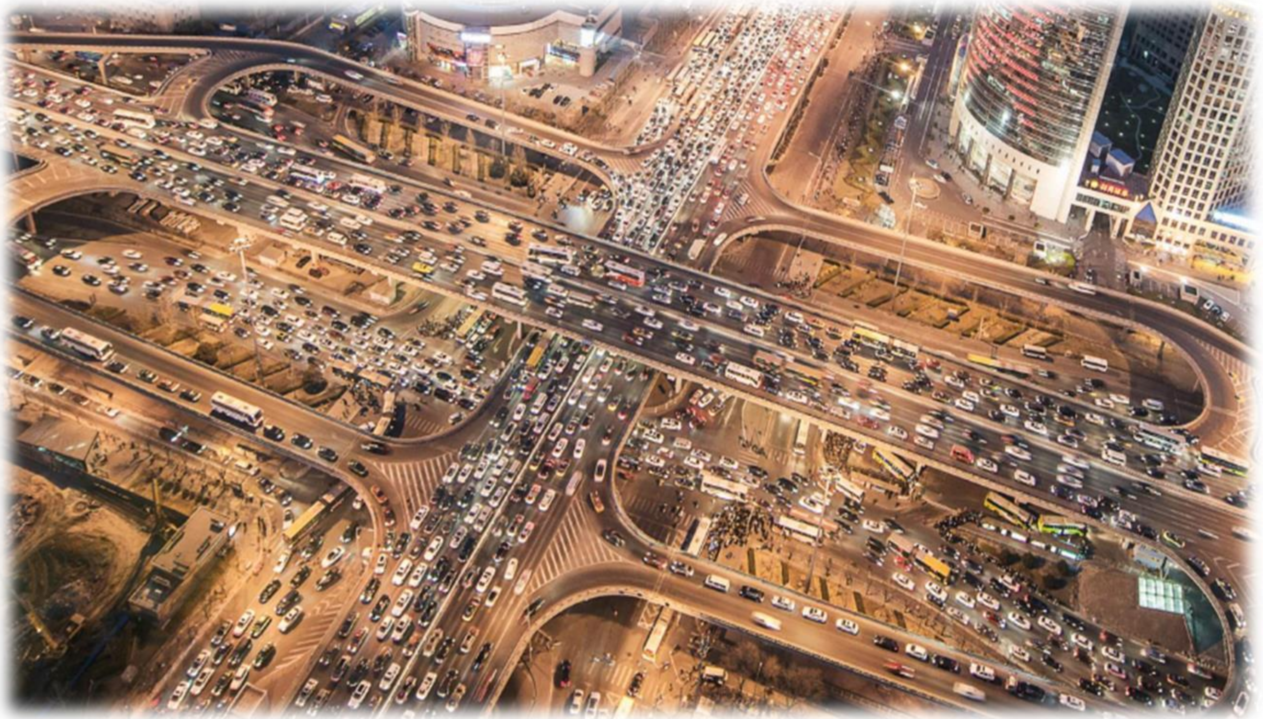
Our Economy is increasingly getting dependent on GNSS

PPP-RTK MARKET AND TECHNOLOGY REPORT EGSA

GNSS Market Potential by Applications

Cumulative Core Revenue forecast for 2013-2023
Growth 250 B€ per Annum

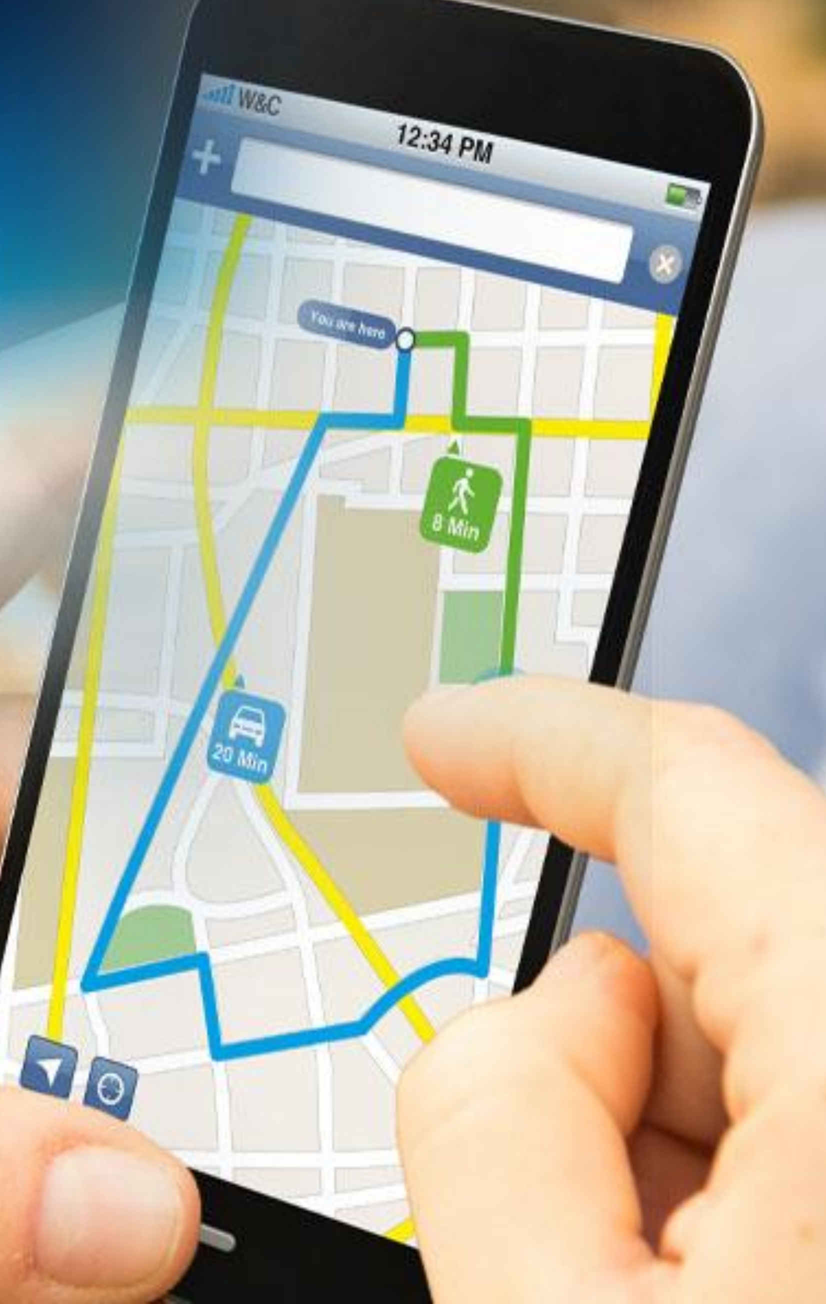




Our Economy is increasingly dependent on GNSS

GSA Market Report, www.mycoordinates.org

Need for GNSS Signal Authentication?



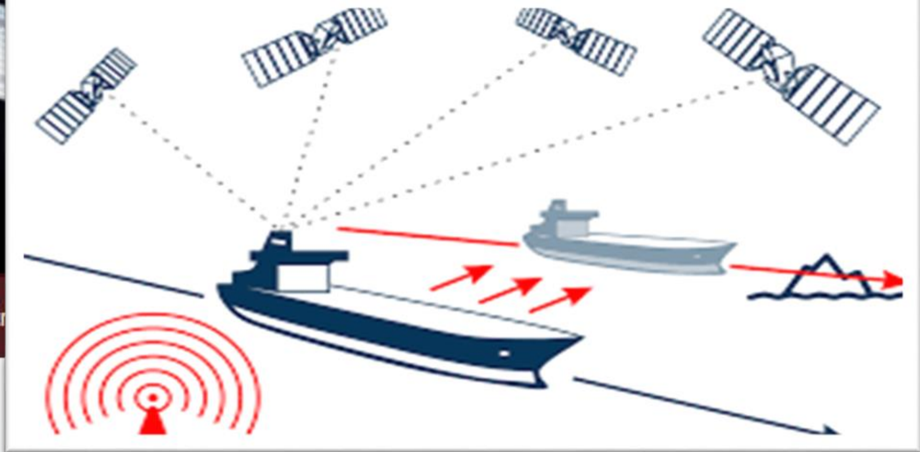
- Likelihood of spoofing attack on applications like personal car navigators is very low and its effects are negligible
- It will not require use of encrypted signals and with security module for authentication
- We expect a growing number of threats and attacks in future as billions of devices are enabled for GNSS

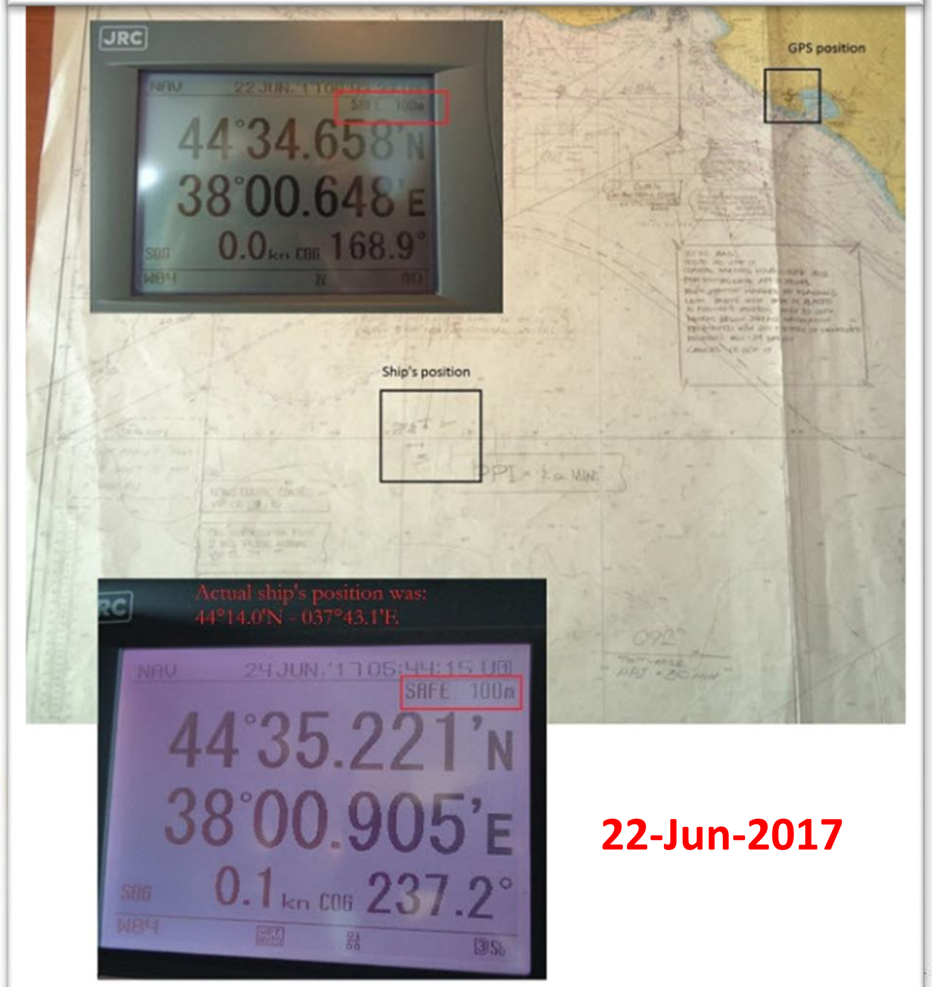
Growing Spoofing Threat

Spoofing in the Black Sea: What really happened?

October 11, 2017 - By Michael Jones   Est. reading time: 8:30

We've heard a lot in the news recently about GPS spoofing, mostly centred on the story of ship spoofing in the Black Sea. Between June 22-24, a number of ships in the Black Sea reported anomalies with their GPS-derived position, and found themselves apparently located at an airport.





22-Jun-2017

Growing Spoofing Threat

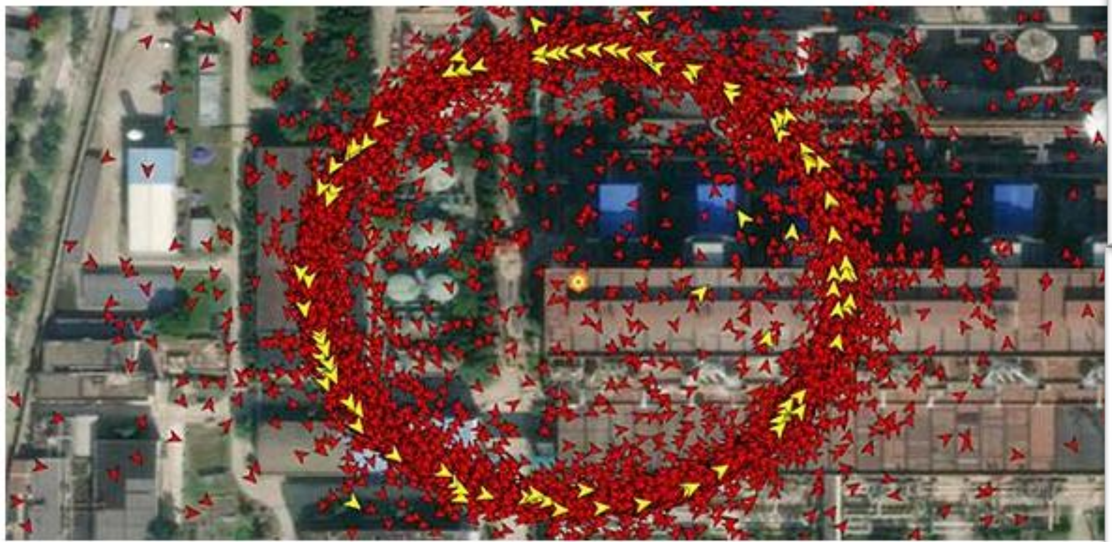
GPS WORLD
GNSS POSITIONING NAVIGATION TIMING

Follow Us

Search the Site...

subscr

GNSS | OEM | UAV | Survey | Mapping | Transportation | Defense | Mobile | Mac



Chinese GPS spoofing circles could hide Iran oil shipments

17-Dec-2019

December 17, 2019 - By Dana Goward

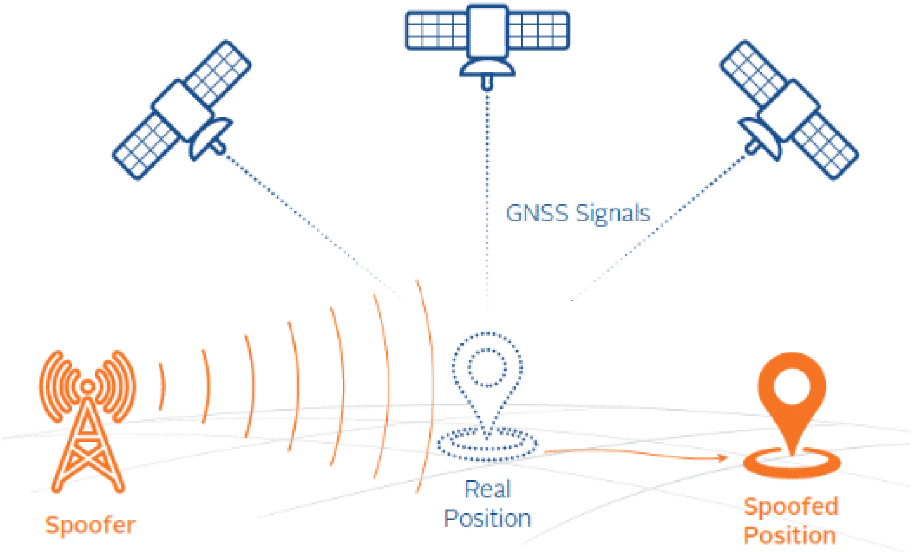
Est. reading time: 2 minutes

"GPS spoofing circles" have been discovered at 20 locations along the Chinese coast, according to the non-profit environmental group Skytruth. Of the locations observed, 16 were oil terminals; the others were corporate and government offices.

GPS spoofing in Shanghai that resulted in reported positions from ships

How to protect from Jamming and Spoofing Threat ?

- Use special Restricted GNSS services but that is reserved for special and strategic users
- Many Civilian users that cannot use Restricted services need some level of protection in civilian GNSS services



GNSS Authentication to detect Spoofing threats

Authentication can be broadly handled at two levels:

- System/Signal Level Authentication (Satellite Broadcast Service)
  - Galileo's Open Service Navigation Message Authentication (OSNMA)
  - Galileo's Commercial Augmentation Service (CAS)
  - SBAS Authentication

- User Level Authentication
  - Multi GNSS usage
  - Anti-Spoofing Algorithms, C/N_o or time bias checks

Types of Spoofing Attacks on Signals

- Data Level Attacks
  - Data forging or modification
  - Data replay of old data
- Ranging Level Attacks
  - Signal Forging
  - Signal Relay or meaconing

- Both Data level and Ranging Level Attacks

GNSS System/Signal Level Authentication

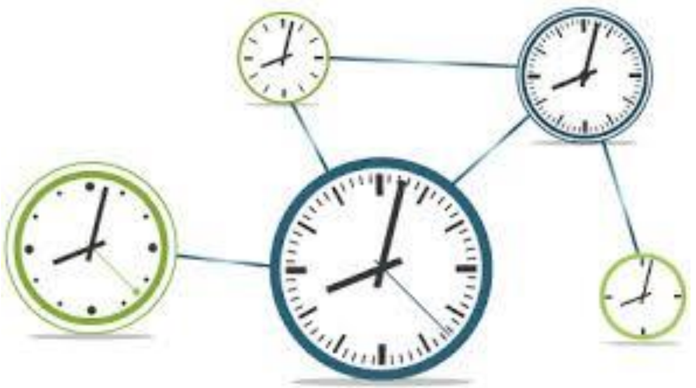
- Incorporating specific features that cannot be predicted or forged by malicious spoofers in the broadcast GNSS signals.
- Provide more robustness to GNSS users
- A receiver enabled for authentication can interpret these features in order to distinguish genuine signals from imitations.
- Data level - To authenticate the broadcast navigation messages
- Range level - To authenticate the measured ranges to the satellites
- Can protect against spoofing but not against jamming
- Cannot prevent spoofing but can detect it

Which GNSS applications require authentication ?

- Very appealing for civil users interested in an improved security but reluctant to deal with the crypto management constraints as well as additional GNSS receivers costs
- Applications requiring trust, involving financial transactions, or where reputation and privacy are at stake.
- Possible users could be road tolling, insurance telematics, smart mobility, logistics, smart digital tachographs, critical infrastructure network time synchronisation, rail operations, and autonomous vehicles in the coming years

GNSS Signal Authentication Applications

- ❖ Advanced Timing and Frequency synchronisation Services



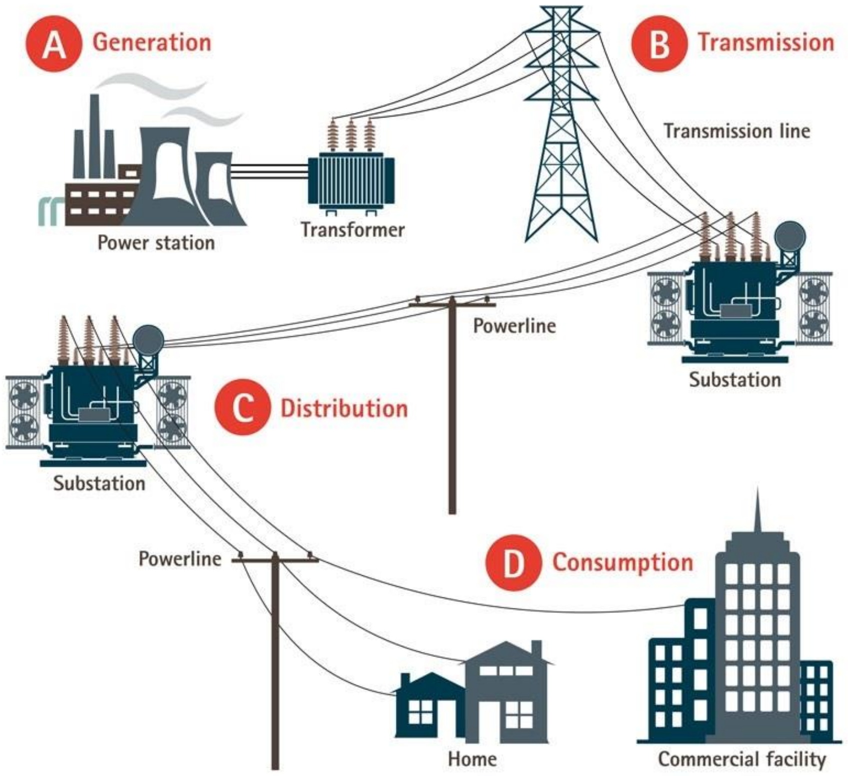
- ❖ Safety and Liability Critical Transport :
  - ❖ Aviation, Maritime, Rail and Road Transport
  - ❖ Road Transport: Insurance, car rental, taxi, and fleet-management or logistics services companies

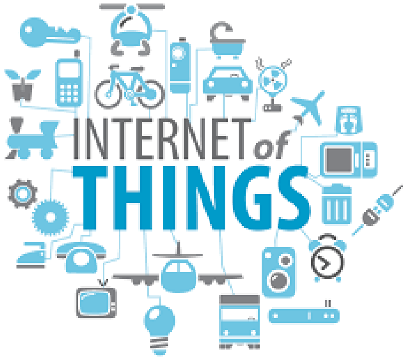
- ❖ Autonomous Cars

- ❖ Drones and Robots

GNSS Signal Authentication Applications

- Internet of Things
- Emergency Warning Services
- Energy Transmission and Distribution
- Financial Critical Services
- Telecommunications





Authentication scheme design considerations

- Broadcast nature of signals, protection at satellite end and test at receiver end
- Anti-Spoofing Capabilities
- Minimum changes to existing GNSS infrastructure
- Backward Compatibility to existing users
- Limited impact on User Receiver resources and Complexity
- Authenticate then use or use then authenticate ?

How to choose which Navigation Message Authentication (NMA) scheme

Need to achieve on optimal trade-off between following factors:

1. **Security** – size of keys, number of bits for authentication, security of algorithms, key management functions
2. **Communication overhead** – minimising the bandwidth requirement, key management messages, renewal of keys – crypto period, key revocation
3. **Robustness to channel errors** – maximising tolerance against errors in demodulation in challenging environments
4. **Tolerance for data loss** – minimising consequences of data loss, ability to recover from data loss
5. **Scalability** – distribution and management of keys
6. **Computation** and memory requirements on receiver
7. **Key Authentication performance indicators (KPI)** – Time to First Authenticated Fix (TTFAF), Authentication Error Rate (AER), Time to Authentication (TTA), Time between Authentication (TBA), Authentication Latency (AL)

Message Authentication schemes

- **Block Hashing** – star or tree based approaches
- **Hash Chaining** – forward or backward approaches
- **Digital Signatures** Algorithm (DSA)
- **Elliptical Curve Digital Signatures Algorithm (ECDSA)**
- **One time signature** schemes
  - Bins and Balls signature (BiBa)
  - Hash to obtain random subsets (HORS)
- **MAC based source authentication** with delayed key disclosure schemes
  - TESLA (Timed Efficient Stream Loss-tolerant Authentication) (symmetric cryptography)
- **Digital Signature Amortization** (SigAM) (Asymmetric Cryptography with non-repudiation)
  - Efficient Multi-chained stream signature (EMSS)
- **Supersonic GNSS authentication codes**

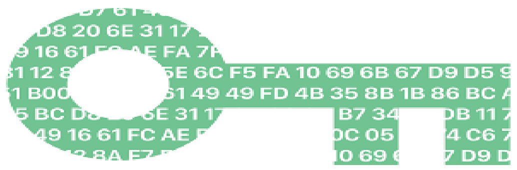
TESLA (Timed Efficient Stream Loss-tolerant Authentication)

- A Broadcast authentication protocol which enables the receivers to verify that a received packet was really sent by the claimed sender
- Low communication and computation overhead
- Scales to large numbers of receivers, and tolerates packet loss.
- Employs one way key chains (Easier to compute but hard to invert)

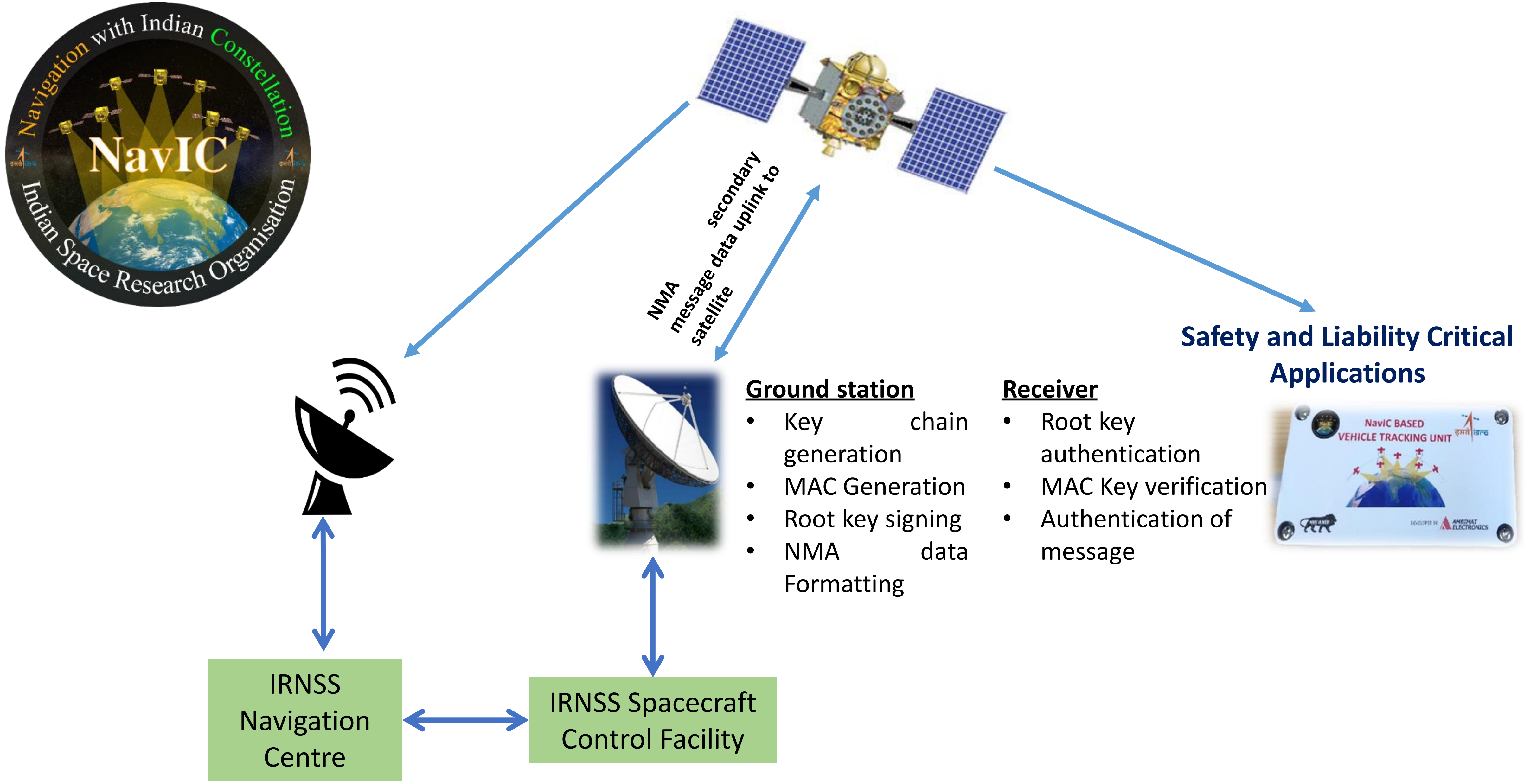
TESLA (Timed Efficient Stream Loss-tolerant Authentication)

- Sender attaches to each packet a Message Authentication code (MAC) computed with a key k known only to itself.
- The receiver buffers the received packet without being able to authenticate it.
- A short while later, the sender discloses k and the receiver is able to authenticate the packet.
- Consequently, a single MAC per packet suffices to provide broadcast authentication
- The receiver must loosely synchronized its clock with the sender.

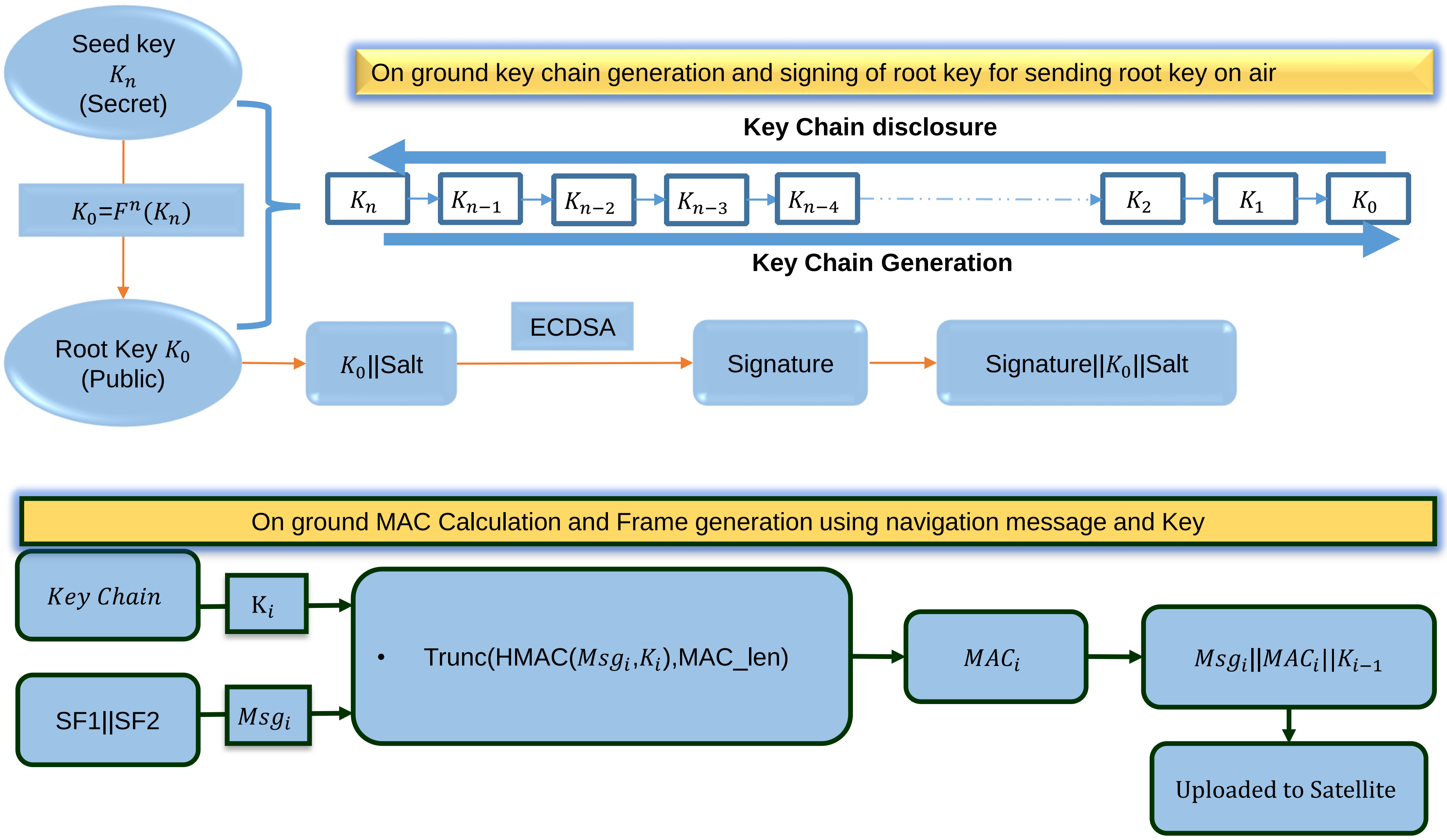
MAC



Navigation Message Authentication for NavIC


Navigation with Indian Constellation
NavIC
Indian Space Research Organisation
NMA message data uplink to secondary satellite
Safety and Liability Critical Applications
Ground station
• Key chain generation
• MAC Generation
• Root key signing
• NMA data Formatting
Receiver
• Root key authentication
• MAC Key verification
• Authentication of message
NavIC BASED VEHICLE TRACKING UNIT
IRNSS Navigation Centre
IRNSS Spacecraft Control Facility

Role of Ground Station



Design Parameters

- 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
- **<u>Simulated key disclosure delay: 96s</u>**

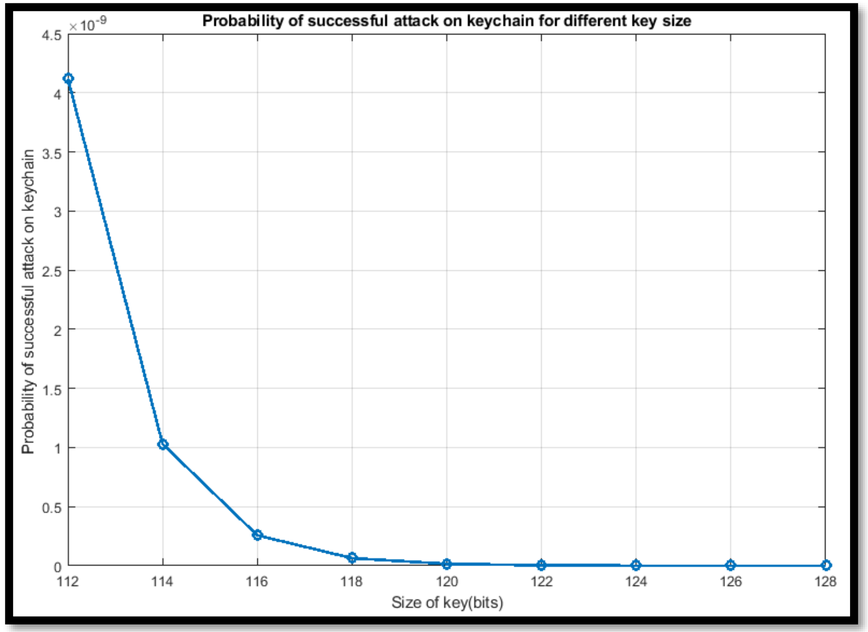
Secondary sub frame occupancy one hour duration for one satellite

<table>
<tr><td>S|E</td><td>N|E</td><td>E|E</td><td>N|E</td><td>S|E</td></tr>
<tr><td>N|E</td><td>E|E</td><td>N|E</td><td>E|E</td><td>N|E</td></tr>
<tr><td>S|E</td><td>N|E</td><td>S|E</td><td>N|E</td><td>S|E</td></tr>
<tr><td>N|E</td><td>E|E</td><td>N|E</td><td>E|E</td><td>N|E</td></tr>
<tr><td>E|E</td><td>N|E</td><td>S|E</td><td>N|E</td><td>E|S</td></tr>
<tr><td>N|E</td><td>S|E</td><td>N|E</td><td>S|E</td><td>N|E</td></tr>
<tr><td>S|E</td><td>N|E</td><td>E|E</td><td>N|E</td><td>E|E</td></tr>
<tr><td>N|E</td><td>S|E</td><td>N|E</td><td>S|E</td><td>N|E</td></tr>
<tr><td>S|E</td><td>N|E</td><td>E|E</td><td>N|E</td><td>E|E</td></tr>
<tr><td>N|E</td><td>E|E</td><td>N|E</td><td>S|E</td><td>N|S</td></tr>
<tr><td>S|E</td><td>N|E</td><td>E|E</td><td>N|E</td><td>S|E</td></tr>
<tr><td>N|E</td><td>E|E</td><td>N|E</td><td>E|E</td><td>N|E</td></tr>
<tr><td>S|E</td><td>N|E</td><td>S|E</td><td>N|E</td><td>S|E</td></tr>
<tr><td>N|E</td><td>E|E</td><td>N|E</td><td>E|E</td><td>N|E</td></tr>
<tr><td>E|E</td><td>N|E</td><td>E|E</td><td>N|E</td><td>S|S</td></tr>
</table>

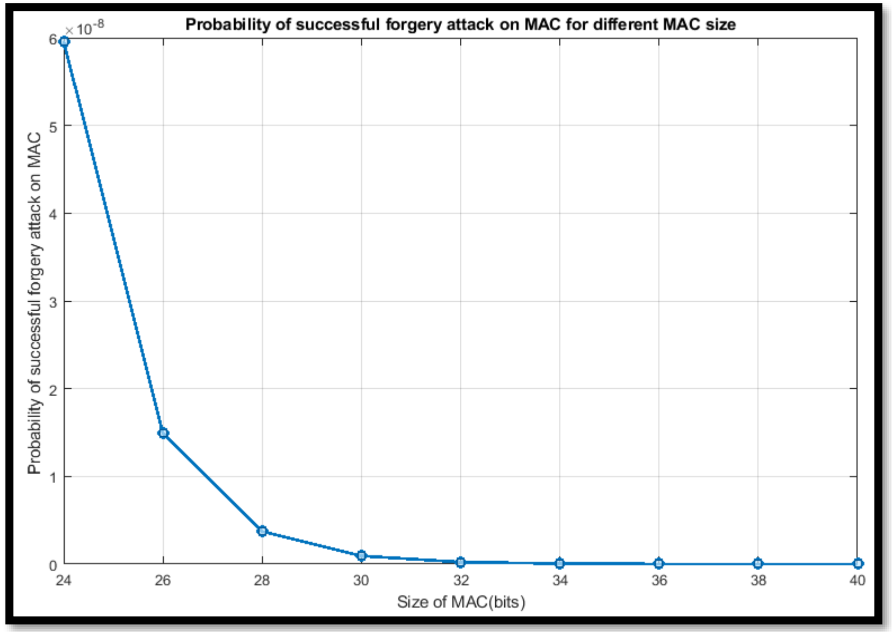
** NMA transmission possible in alternate frames*

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

<u>Size of MAC and Key</u>

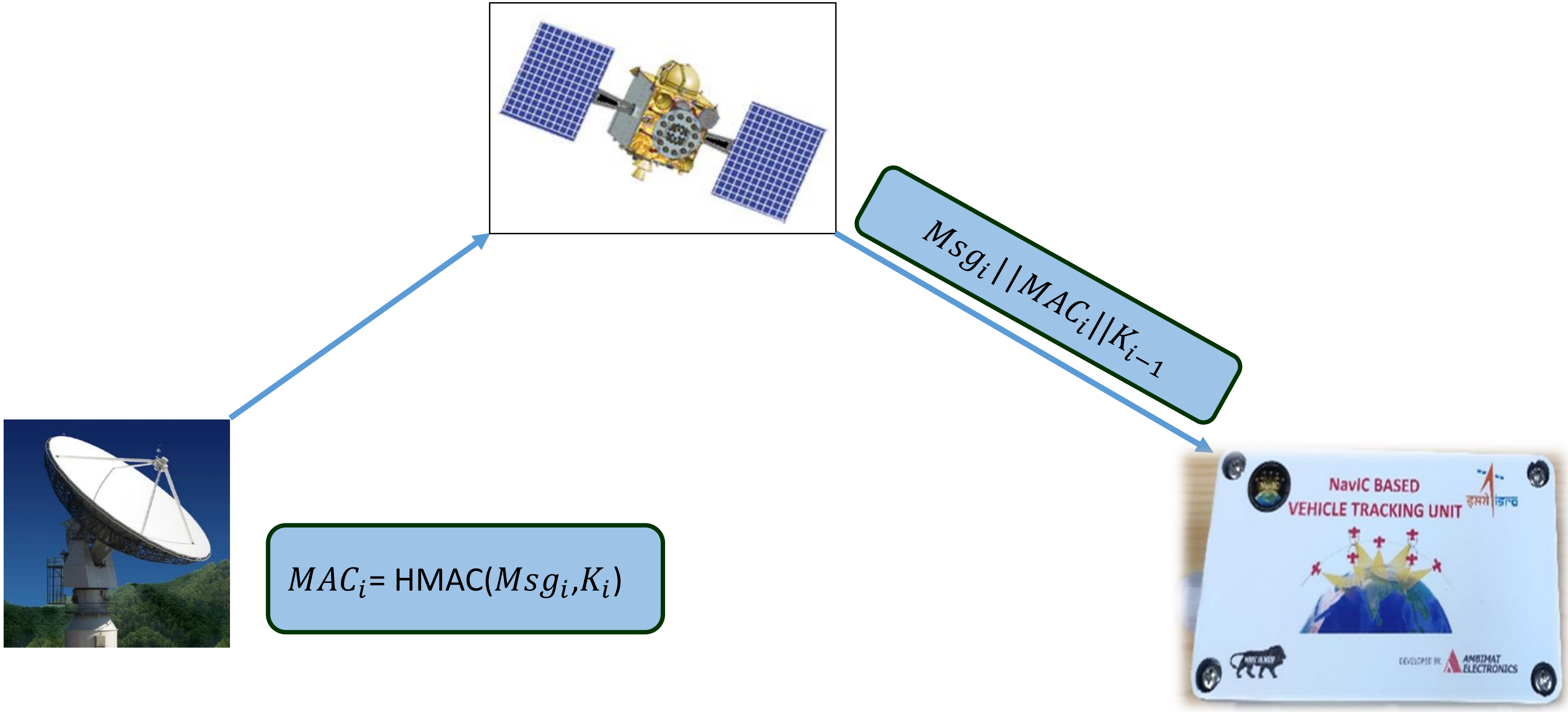


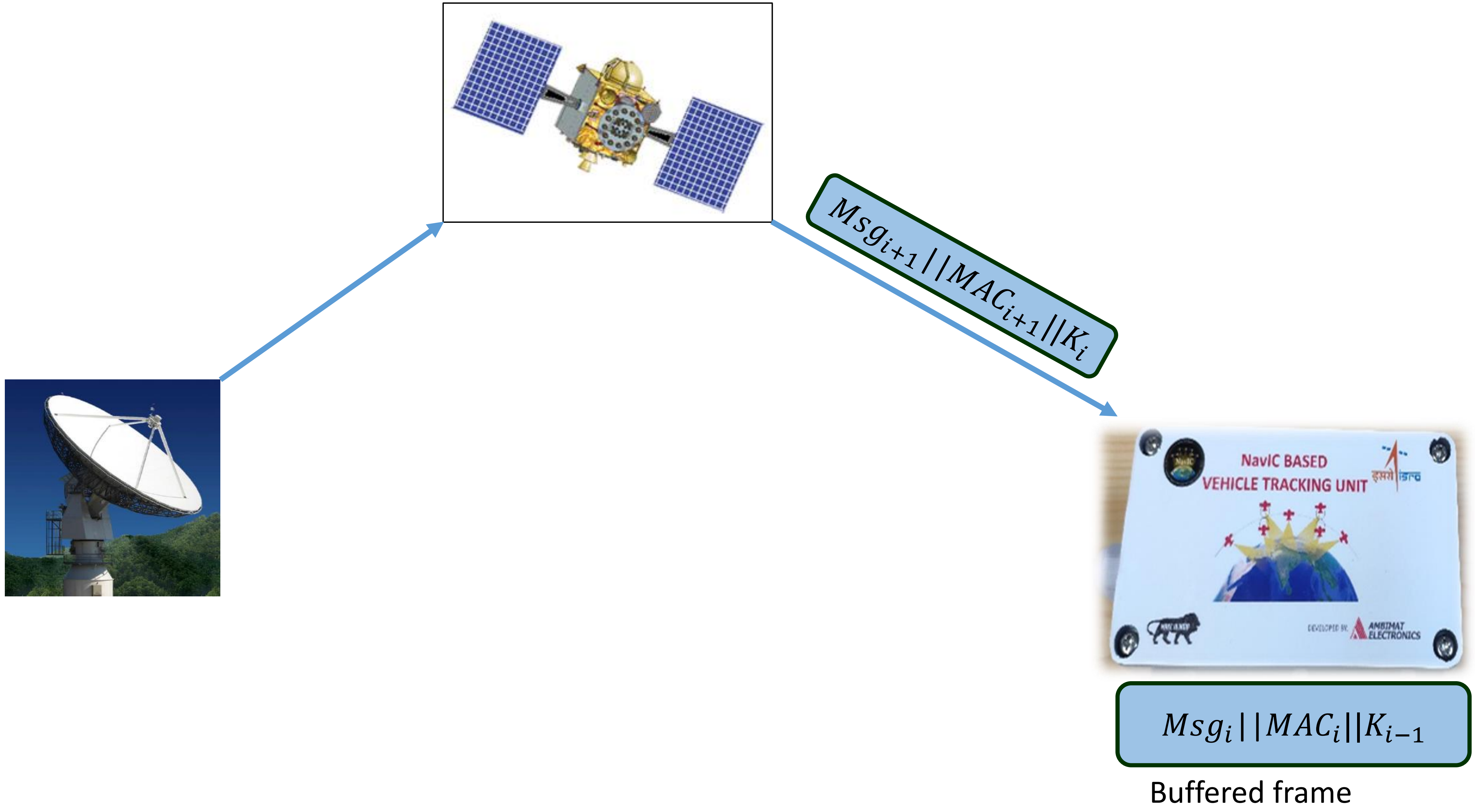
For TBA of 96s and length of key chain 30 days
116 bits required for $P_s \leq 10^{-9}$



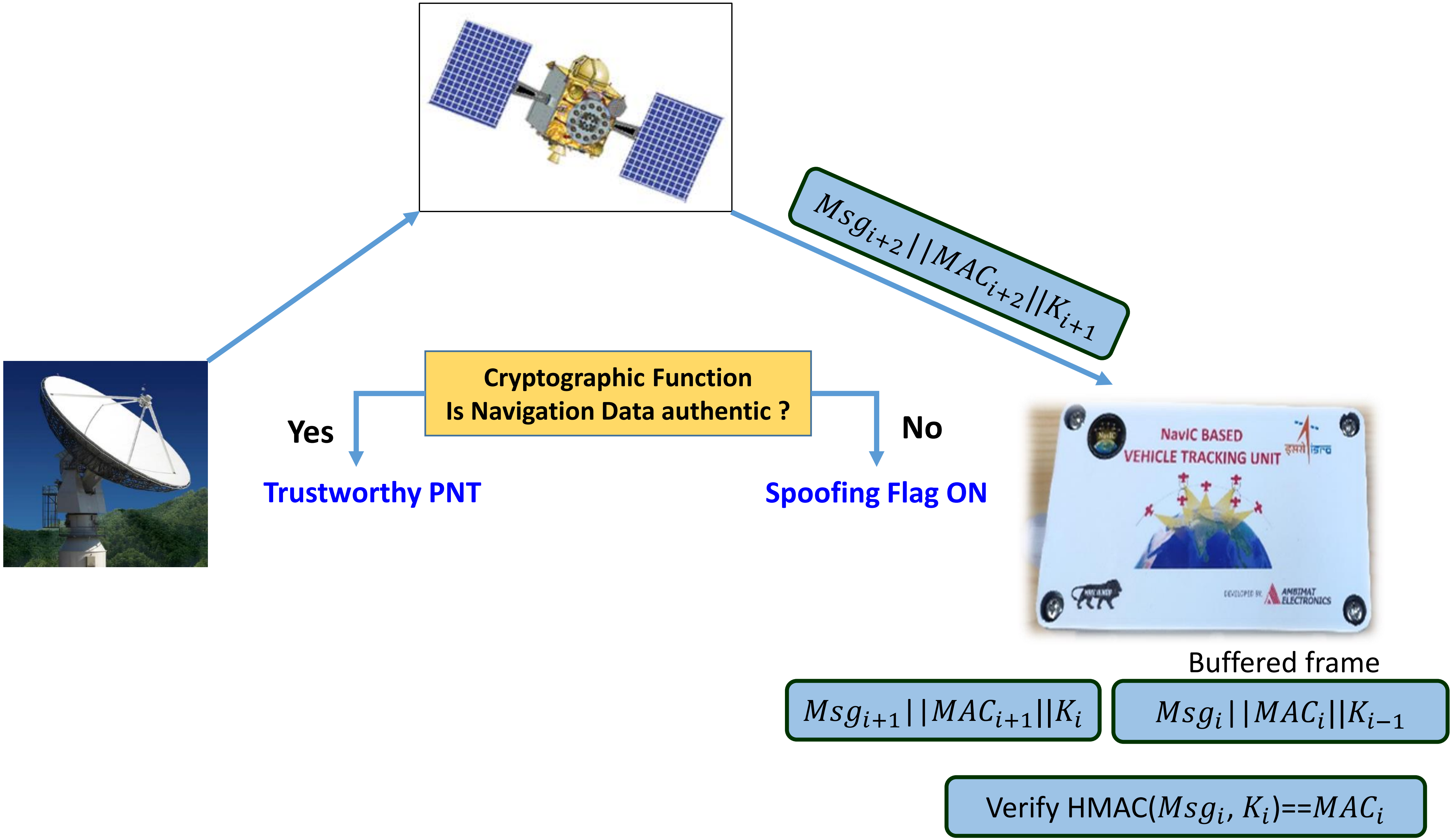
30 bits required for $P_{MAC} \leq 10^{-9}$

** 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.*


MAC_i= HMAC(Msg_i,K_i)
$Msg_i\,||\,MAC_i||K_{i-1}$
NavIC BASED
VEHICLE TRACKING UNIT
AMBIMAT ELECTRONICS

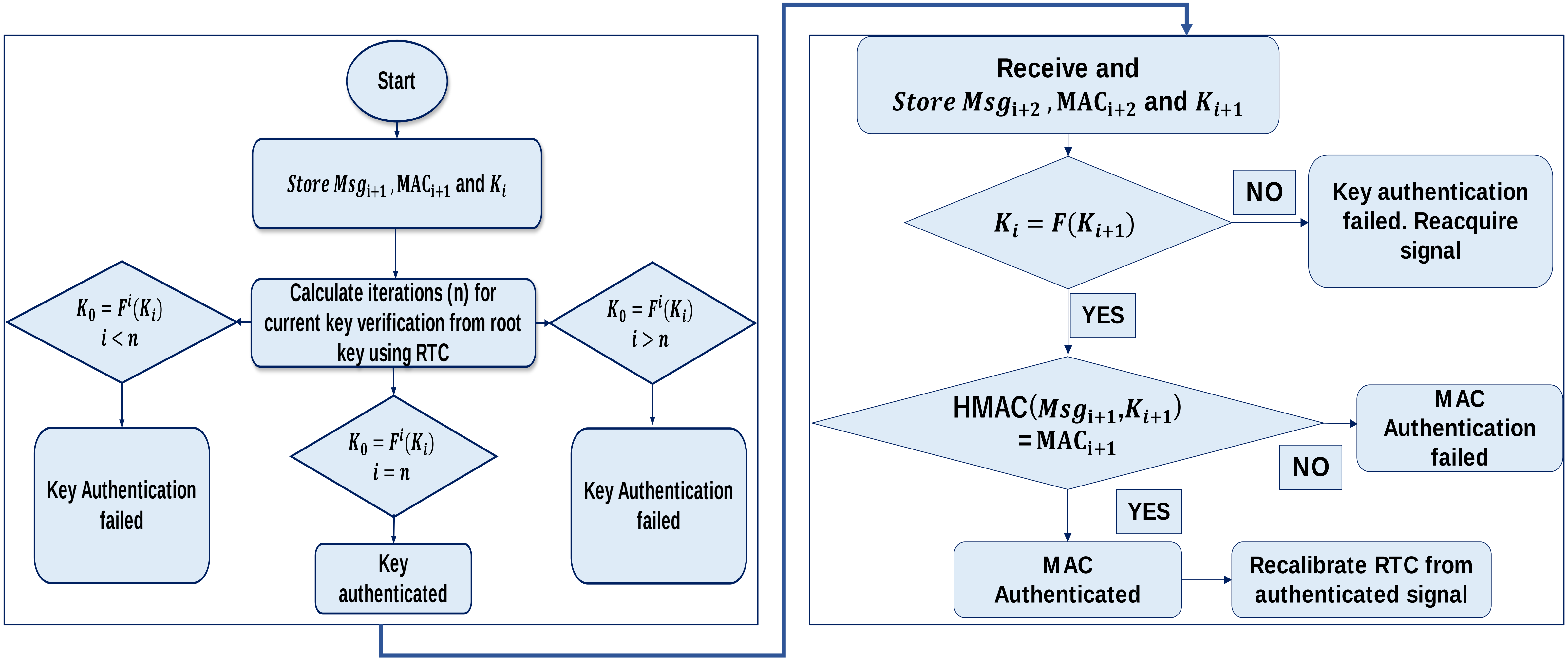


$Msg_{i+1}||MAC_{i+1}||K_i$
NavIC BASED
VEHICLE TRACKING UNIT
AMBIMAT ELECTRONICS
$Msg_i||MAC_i||K_{i-1}$
Buffered frame



$Msg_{i+2}||MAC_{i+2}||K_{i+1}$
Cryptographic Function
Is Navigation Data authentic ?
Yes
No
Trustworthy PNT
Spoofing Flag ON
NavIC BASED
VEHICLE TRACKING UNIT
Buffered frame
$Msg_{i+1}||MAC_{i+1}||K_i$
$Msg_i||MAC_i||K_{i-1}$
Verify HMAC(Msg_i, K_i)==MAC_i

NMA workflow at receiver



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 ($\pm$ 48s)*

Under Development……

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

Thank You