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

Generation Technique - NMA

- 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

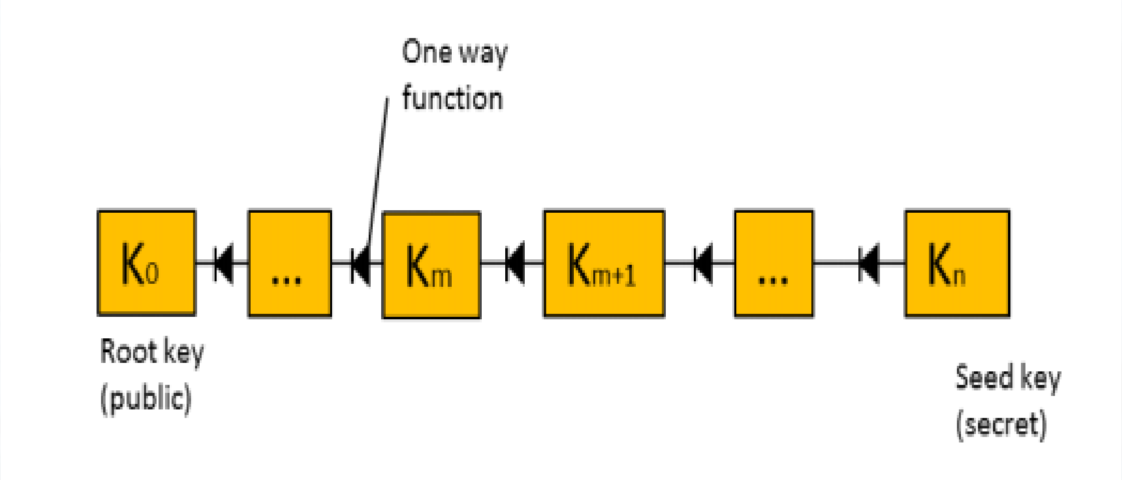
- Based on loose time synchronization between the sender and the receivers
- Based on the transmission of a MAC to authenticate the Navigation message and delayed transmission of the key used to compute the MAC
- Sender attaches to each packet a Massage Authentication Code (MAC) computed with a key K 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

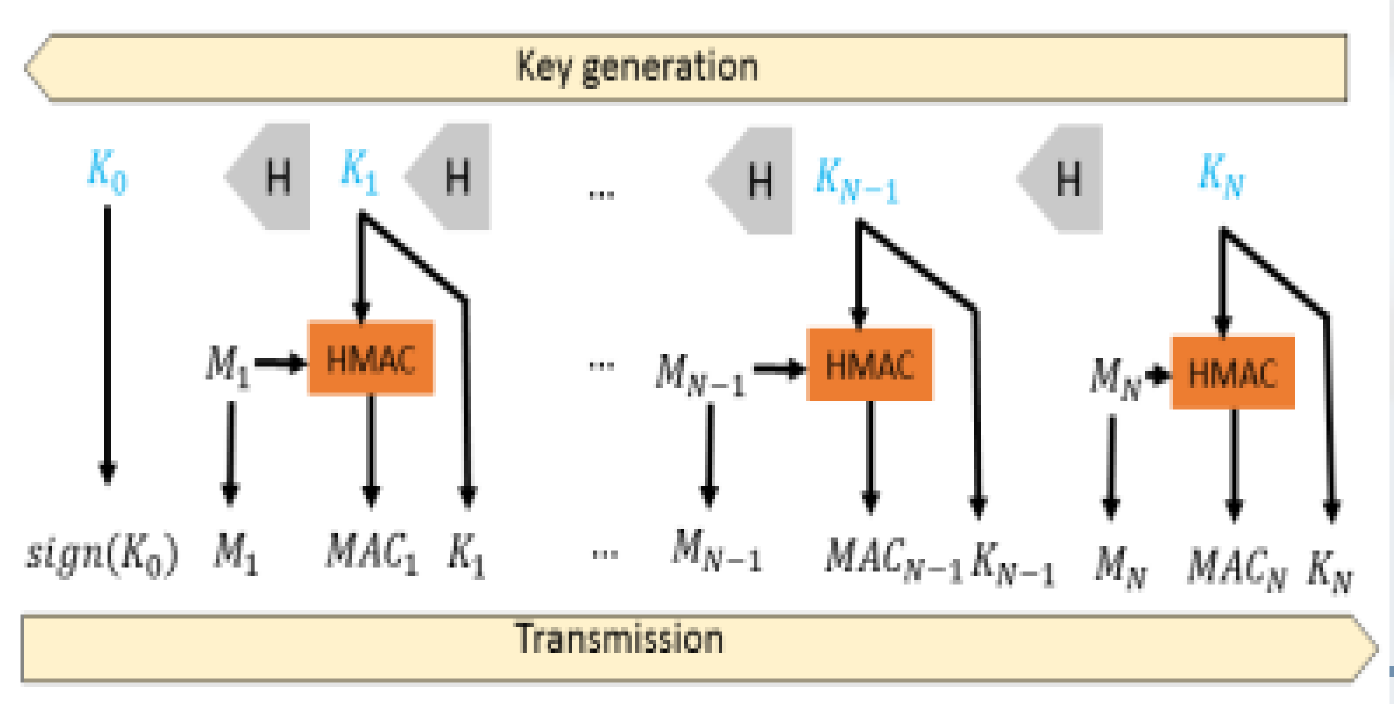
- key belongs to a key chain generated through a one-way function. The chain starts with a random seed key K_n, which is secret, and ends with a root key K_0 that is public



$$K_0 = F^n(K_n)$$

MAC Generation - Technique

- For each desired time interval i the Navigation Message is authenticated by Key K_i. MAC generated with Key_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

start

The Key generation chain starts with a random secret seed key K_n

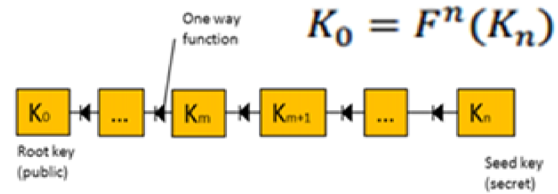
One way function F is operated n times to generate root key K_0

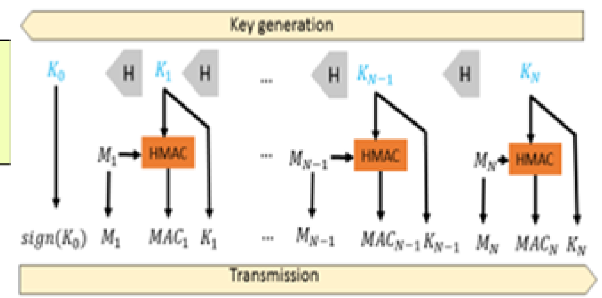
Navigation message (M_i) & Key (K_i) are used to generate MACi

MAC_i is trasmitted to the receiver

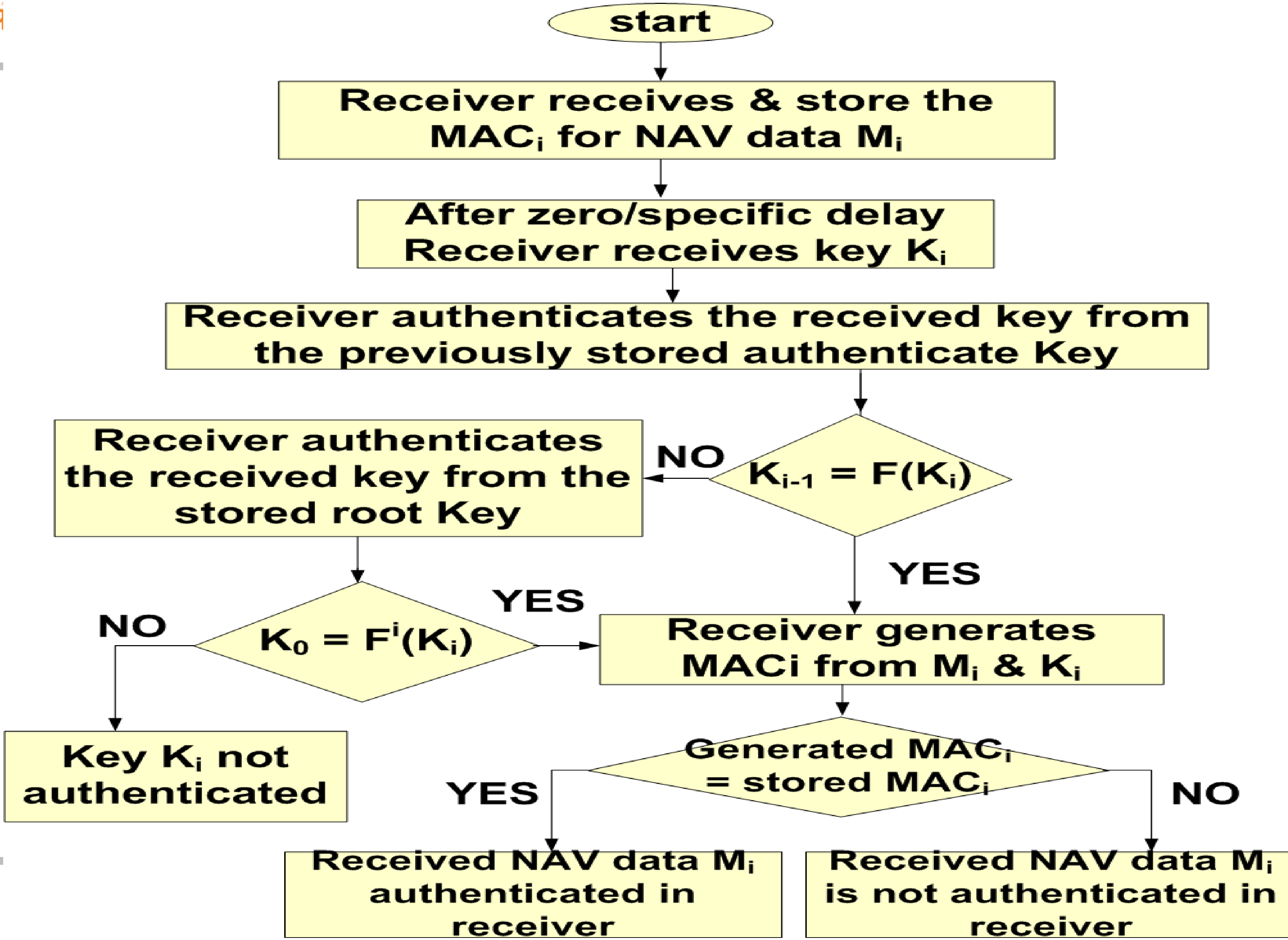
Key_i is trasmitted to the receiver Without/with specific delay

end





NMA steps at Receiving end



NMA scheme for L5/S band NavIC

- There is feasibility of Authentication scheme incorporation in in L5/S of NavIC satellites
- Key generation & MAC generation can 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

Sub frame1	Sub frame2	Sub frame3	Sub frame4

2400 symbols @ 50 sps

Structure Sub Frame 3 & 4

1	9	26	27	28	30	31	37	263	287
TLM	TOW	ALERT	AUTONAV	SUBFRAME ID	SPARE	MESSAGE ID	DATA	CRC	Tail
8 Bits	17 Bits	1 Bit	1Bit	2 Bits	1 Bit	6 Bits	226 Bits	24 Bits	6 Bits

Flexibility in Delays….

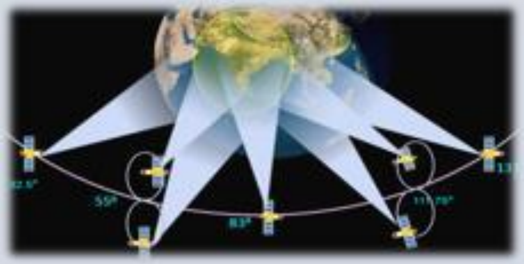
- Associated no of subframe delay between MAC & KEY is mentioned in the header information associated with each MAC
- Flexibility of transmitting Keyi for MACi with or without delay in subframe 3/4
- Possible combinations are:
  - MACi,Keyi - No delay
  - MACi,Keyi-1 - One subframe delay
  - MACi,Keyi-2 - 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

- Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Song. The TESLA Broadcast Authentication Protocol. In CryptoBytes, 5:2, Summer/Fall 2002, pp. 2-13
- IGNACIO FERNÁNDEZ et.al. A Navigation Message Authentication Proposal for the Galileo Open Service. NAVIGATION: Journal of The Institute of Navigation Vol. 63, No. 1, Spring 2016
- SIGNAL IN SPACE ICD FOR STANDARD POSITIONING SERVICE, ISRO-IRNSS=ICD-SPS-1.1, AUGUST 2017




Thank You