Input paper: [[1]](#footnote-2) ENAV28-5.1.3.1

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP **x** Input

**X** ENAV **□** VTS **□** Information

Agenda item [[2]](#footnote-3) n.n

Technical Domain / Task Number 2 …………………………………

Author(s) / Submitter(s) Francisco Lázaro, Ronald Raulefs, DLR, Institute of Commun. & Nav.

An Authentication Concept for VDES R-Mode

# Summary

VDES R-Mode is designed as a contingency maritime positioning and navigation system in case the operation Global Navigation Satellite Systems (GNSS) is disrupted due to a malfunctioning or an intentional attack. However, VDES R-Mode itself can also be subject to attacks, such as jamming or spoofing. Systems like GPS and Galileo plan currently the introduction of some hardening techniques to improve its resilience against such attacks. Unfortunately, the techniques used to mitigate attacks on GNSS, if directly applied to VDES R-mode do not provide a satisfactory level of security. In this input paper, we propose an authentication scheme that can be used to strongly mitigate the effects of attacks on VDES R-mode. In particular, we advocate for the use of navigation message authentication (NMA) relying on the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol, together with the introduction of a novel technique to protect the ranging sequences. The introduction of these techniques would elevate the resilience of VDES R-mode on par with that of GPS and Galileo.

## Purpose of the document

Inform the committee about the vulnerabilities of VDES R-mode and about the existence of countermeasures to protect it.

## Related documents

1. IALA . Guideline 1158: VDES R-Mode. tech. rep., IALA; 2020.

# Background

## VDES R-Mode Overview

The VDES R-Mode System intends to provide a contingency Positioning, Navigation and Timing (PNT) system for maritime shipping. The operational concept foresees using VDES R-Mode when a disruption to Global Navigation Satellite System (GNSS) services on-board a ship occurs. Furthermore, when both GNSS and VDES R-Mode are available, it is possible to assess the PNT integrity by comparing the estimates obtained through both systems.

VDES R-Mode is offered as a navigation service within VDES. In particular, VDES R-Mode requires sending two different messages over VDES. The first type is a so-called navigation message. This message contains different navigation data, such as information about the location of the VHF antenna of the VDES shore stations to determine the distance, information about the (atomic) clocks of each shore station to track the changes in the timing between multiple transmissions of each station, and it also indicates which ranging sequence out of multiple predefined ones will be transmitted by the different stations. The second message type is a ranging sequence, i.e., a packet containing a known sequence. This sequence is used by the vessels to estimate their position. VDES R-Mode supports different ranging sequences, see IALA guideline G1158 for more details[1].

Each VDE-TER shore station allocates the data resources by time-division multiplexing access (TDMA) using a frame length of 1s. Each shore station transmits navigation messages with a periodicity of 60 s and ranging sequences with a periodicity of 1 s. In order to provide a good positioning accuracy, VDES R-Mode requires neighbouring shore stations to coordinate so that a shore station is silent in slots in which neighbouring shore stations are transmitting their ranging sequence, see Figure 1.

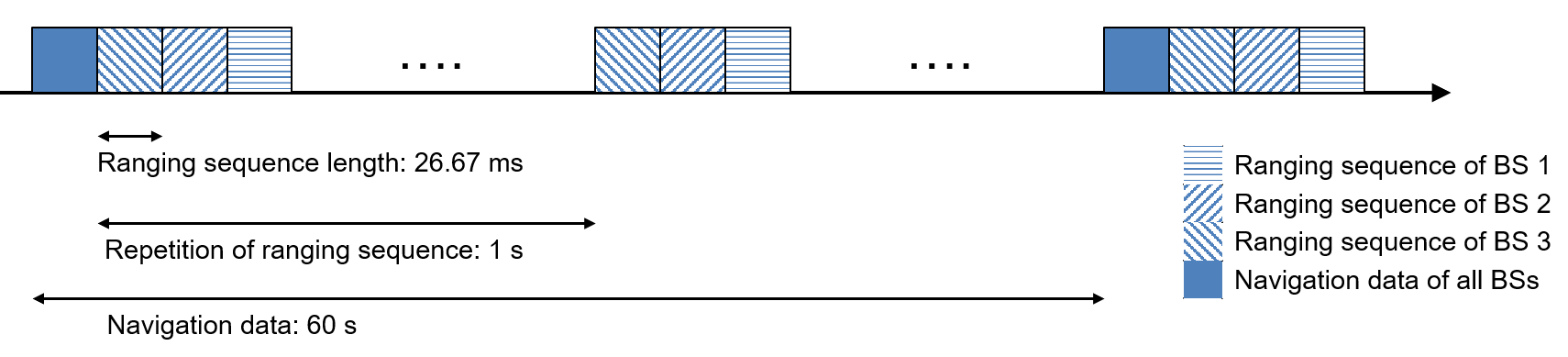


Figure 1. Time slot allocation of the ranging sequences of three different base stations and the navigation data from either one base station or a VDE satellite.

Shore stations are planned primarily considering their communication coverage in order to provide a continuous coverage in waters close to the shore, while preventing too much overlap between neighbouring shore stations. However, the ranging coverage of a shore station is considerably larger than its communication coverage, since ranging boils doing to detecting he presence of a known sequence in the received signal, which is an easier task than recovering unknown data from the received signal (i.e, it can be achieved at a lower signal to noise ratio). In order to be able to access the VDES R-Mode service, a vessel needs up-to-date navigation data, and must thus receive the navigation messages error free with high probability. Thus, the vessel must be within the communication coverage of at least one VDE-TER shore station or alternatively within the communication coverage of a VDE-SAT satellite. Furthermore, the vessel must be within the ranging-coverage of at least 3 VDE-TER shore stations or VDE-SAT satellites, since it needs to compute its distance to at least 3 transmitters in order to be able to estimate its position. Figure 2 depicts a scenario of one vessel that is receiving navigation data by a VDE-SAT link and is in range of multiple base stations to estimate its position. As shown in the figure, the satellite coverage area is significantly larger than that of the shore stations. Hence, VDE-SAT can be used to increase the service area of VDES R-Mode.

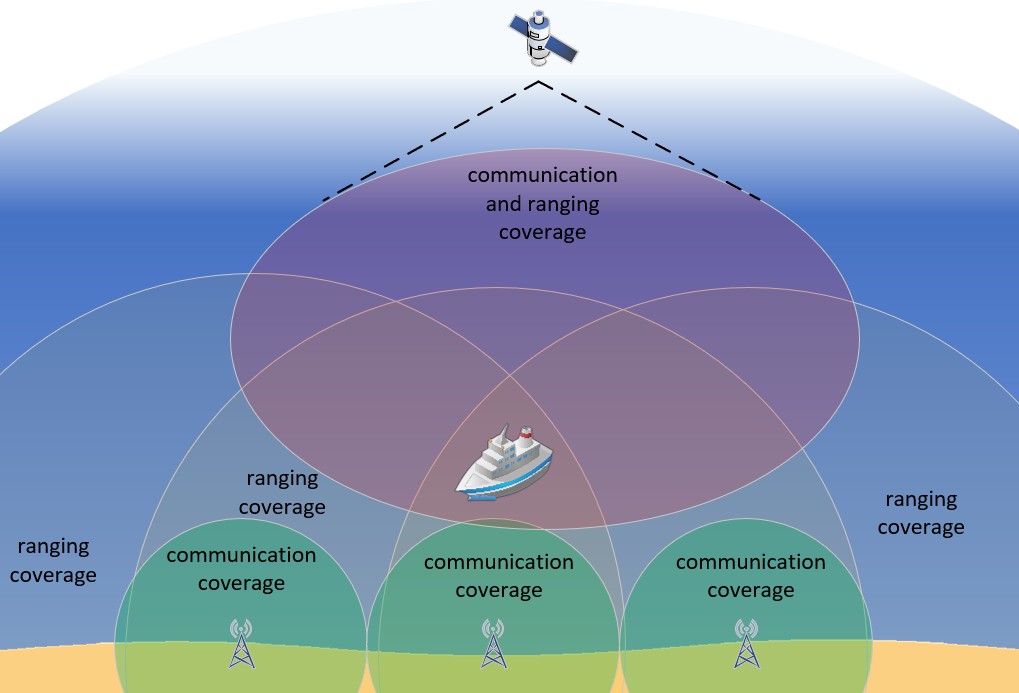


Figure 2. R-Mode diagram. The communication coverage of shore stations is considerably smaller than its ranging coverage. In this example the vessel is within the ranging coverage but outside the communication coverage of the shore stations. However, the vessel is within the communication and coverage radius of the VDE satellite, and this allows him to position itself.

## Attacks on PNT Systems

Positioning, Navigation and Timing (PNT) systems can be subject to different attacks:

* Jamming attacks, broadly speaking, consist of the transmission of undesired signals (interference) in a given part of the radio frequency spectrum. Thus, jamming results in a reduction of the signal of the SNIR and thereby in a reduction of the service quality. In the case of a PNT system, the SNIR decrease results in an increased positioning error.
* Spoofing attacks, in which an attacker generates bogus signals which are interpreted by the receiver as valid, but which contain fake information. This causes the system and receiver to malfunction by providing significantly different positioning estimates, or by making the receiver believe he is located somewhere else.
* Meaconing attacks lie halfway between jamming and spoofing. They involve intercepting the transmission of the navigation signals, storing them, and replaying them at a later point in time. Meaconing lies halfway between jamming and spoofing, because it does not imply sending random-like interference, as it is the case for jamming, but it also does not require mimicking the potentially complex logic of the transmitter in order create an attack, as it is the case for spoofing.

## Existing countermeasures

The different countermeasures can be categorized in two different classes: cryptographic and non-cryptographic. Cryptographic countermeasures are based on the use of cryptographic protocols and can be used to protect the confidentiality and authenticity of the navigation signals transmitted by the shore stations / satellites. Non-cryptographic countermeasures encompass signal processing (e.g., zero forcing techniques against jammers using multiple antennas or using SNIR measurements to estimate the positioning accuracy) as well as relying on a local clock and/or an inertial system to authenticate the navigation signals by checking its plausibility.

In the near future, GPS and Galileo will introduce a cryptographic countermeasure known as Navigation Message Authentication (NMA). This technique aims at protecting the authenticity of the navigation message by applying a digital signature or using a hash-chain based protocol such as Timed Efficient Stream Loss-Tolerant Authentication (TESLA) [3]. This technique adds an additional tag to every navigation message (either a digital signature or a Message Authentication Code). This tag allows receivers to verify the authenticity of the navigation message, but is (computationally) hard to forge for an attacker. NMA schemes rely on the existence of a public key infrastructure (PKI), that allows to link identities to public cryptographic keys.

GNSS receivers will complement NMA with several non-cryptographic countermeasures applied at the receiver. At a high level of abstraction, these countermeasures are used to ensure that the PNT signals belong to the same continuous stream. When these non-cryptographic countermeasures are used together with NMA, they allow the receiver to determine if the PNT signals belong to the same continuous transmission as the navigation message that has been successfully authenticated relying on NMA. If this is the case, the receiver can treat the PNT signals as authentic, and operate normally. However, if an attacker tries to create a falsified PNT signal, the receiver, with very high probability, will be able to detect the attack and modify its behavior accordingly (e.g., by ignoring the signal it has determined to be falsified). A simple example is that the receiver monitors the instantaneous frequency, phase and amplitude of the received signal. If at a given point in time an attacker tries to inject a false signal, the receiver will immediately detect a variation in the signal parameters (amplitude, phase or frequency) and flag the transmission not authentic.

In [4] it was proposed to introduce NMA in order to protect the navigation messages in VDES R-mode. However, as already stated in [4], this only protects the navigation messages and not the ranging sequences. Unfortunately, the approach followed in GPS and Galileo cannot be applied to R-Mode because the navigation messages and the ranging sequences do not belong to the same continuous transmission. Although NMA does protect successfully the authenticity of navigation messages, an attack in which only the ranging sequences are spoofed is not detected by NMA. Hence, the security of VDES R-Mode when NMA is applied is inferior to that of GPS and Galileo.

## A Novel Countermeasure to Protect VDES R-Mode

In the following we describe a variant of NMA patented in [5] which allows to authenticate not only the navigation messages, but also the ranging sequences. The main idea behind this novel scheme is the following.

1. Instead of transmitting deterministically known ranging sequences, as it is usually always the case in a PNT system, legitimate transmitters choose the ranging sequence they want to transmit from a pool of multiple ranging sequences. For simplicity we will assume the pool is just of size 2, so that a legitimate transmitter always chooses among 2 possible ranging sequences. Note that by choosing uniformly among 2 different sequences, the transmitter is actually conveying 1 bit of information.
2. An attacker wanting to impersonate a legitimate transmitter, not knowing which ranging sequence to choose from the multiple ones in the pool, is forced to choose at random one of the ranging sequences from the pool. If there are 2 sequences in the pool, his choice will be wrong with probability ½.
3. In a standard PNT setting the receiver knows deterministically the ranging sequence and uses this knowledge to determine the pseudo ranges, usually by correlating the received signal with the ranging sequence. However, in this setting the receiver must first estimate which of the 2 ranging sequences was transmitted. After doing that the receiver computes the pseudo ranges to estimate its position. Note that while estimating which of the 2 sequences was transmitted, the receiver is “decoding” 1 bit of information.
4. At a later point in time, the legitimate PNT transmitters reveal which ranging sequences were transmitted. This information is conveyed in a navigation message, which is protected using NMA.
5. After receiving a successfully authenticated navigation messages, a receiver gains knowledge about which ranging sequences were transmitted. If ranging sequences have been actually sent, this equivalent to revealing a vector of length bits, where the -th bit is associated to the choice of the -th ranging sequence. The receiver, who has kept track of which ranging sequences he estimated, has derived an estimate of vector , which we denote by . The receiver now compares and,if they are similar the receiver concludes that the ranging sequences were authentic, otherwise (if and are very different) the receiver concludes that the ranging sequences were forged.

One should note that in VDES R-mode, the navigation message must contain the navigation data for all the transmitters in its vicinity. Hence, it must also contain information about the ranging sequences transmitted by all the transmitters in the vicinity. At first sight, one may conclude that the scheme in [5] requires a large amount of overhead. However, it is actually possible to convey which ranging sequences were transmitted without any additional overhead compared to standard NMA. This is achieved by deriving from the same one-way chain of TESLA which is used to secure the navigation messages, i.e., for NMA. More details can be found in [5] and in the Annex of this paper.

# Discussion

In view of the facts. The authors of this paper believe that implementing the security mechanism from [5] would be beneficial for R-Mode since this would achieve a security level comparable to that of GPS and Galileo (after NMA is introduced). Furthermore, this can be achieved with a very limited overhead.

At this point we would like to remark that a necessary condition to secure VDES R-mode, be it through NMA or through the scheme proposed in [5], is the existence of a public key infrastructure. Implementing a PKI in the maritime domain may prove challenging, mainly due to the limited bandwidth available and the intermittent connectivity between vessels and shore stations. However, several concepts have been proposed to realize it, see [6], [7]. We would like to remark that the hardening of VDES R-mode by means of NMA and or the method in [5] can in principle work with any of these PKI concepts.

# References

1. IALA . G1139 – THE TECHNICAL SPECIFICATION OF VDES. tech. rep., IALA; 2019
2. Perrig A, Canetti R, Tygar J, Song D. The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes* Summer/Fall 2002; 5: 2-13.
3. F. Lázaro, R. Raulefs, H. Bartz, T. Jerkovits “VDES R-mode: Vulnerability Analysis and Mitigation Concepts”, International Journal of Satellite Communications and Networking, 2021
4. F. Lázaro, R. Raulefs, M. Wirsing, “Verfahren zur Authentifizierung einer Sendeeinheit durch eine Empfängereinheit“, German Patent Application DE 10 2021 119 891.7, 2021
5. Frøystad C, Bernsmed K, Meland PH, Rødseth OJ, Nesheim DA. Using digital signatures in the maritime domain. *CySiMS Project Technical Report D2.2* 2017
6. Maritime Identity Register, Maritime Connectivity Platform, available online <https://docs.maritimeconnectivity.net/en/latest/MIR.html>

# Action requested of the Committee

The Committee is requested to:

1. Note the information provided
2. Consider the inclusion of the described security mechanism in order to protect R-Mode against attacks.
3. ANNEX.
   1. Timed Efficient Stream Loss-Tolerant Authentication

The Timed Efficient Stream Loss-Resilient Authentication (TESLA) protocol is an efficient, low-computing broadcast authentication protocol that extends to many receivers and tolerates the loss of packets [6]. Since insertion of malicious packets in many broadcast networks can pose a risk, the receivers want to ensure that their received packets originate from a trusted source. When dealing with point-to-point communication, the authenticity (and integrity) of a message is usually protected using a so-called Message Authentication Code (MAC), which is a (hard to forge) tag that gets appended to the exchanged messages. MACs are generated using a secret key which is shared by the two communication endpoints. Employing MACs in broadcast communications does not provide secure source authentication, since it requires that all the receivers have access to the secret key, and having access to the secret key makes it possible to generate valid MACs. Thus, anyone in possession of the secret key can forge the MAC of a message. Obviously, applying a digital signature to each data packet provides secure broadcast authentication, but it comes with a high overhead, both in terms of bandwidth and signing and verification time. The core idea of TESLA is that the sender attaches a MAC to each packet, which is computed using a (secret) key known only to itself. The receivers in turn buffer the received messages, without being able to authenticate them. Shortly afterwards, the sender discloses the (secret) key and the recipients are able to authenticate the packet. This way, a single MAC appended to every message suffices to provide broadcast authentication, resulting in lower overhead and less computation time when compared to the use of digital signatures. One requirement of the TESLA protocol is a loose time synchronization of the receiver with the senders clock. In particular, the receiver needs to know an upper bound on the local time of the sender. Furthermore, TESLA requires receivers to buffer a number of packets, which results in an authentication delay, which is commonly in the order of one round trip delay between the sender and receiver.

The authentication in the TESLA protocol is based on a one-way key chain. A one-way key chain is built by using a one-way function such that a key is computed from another key as . Each key is associated with a time interval of uniform duration, indexed by . Furthermore, using another one-way function a key is derived from as . If a message is sent during the -th time frame, the sender uses the key to compute a MAC, of the packet . Additionally, the packet contains the key from time intervals in the past. The parameter is called the *packet disclosure delay* and is specified beforehand along with the duration of the time intervals and the maximum length of the one-way key chain. The packet is then given as

TESLA receivers operate as follows:

When a receiver receives a packet the key can be used to determine . Assuming a loosely synchronized clock with the sender, the receiver can check the latest possible time interval that the sender could currently be in. If , then the packet is considered to be safe.

The receiver has to reject all packets that are not safe, i.e., those that contain keys that already have been disclosed and are publicly known. Packets for which contain keys that, at this moment, can only be known by the sender.

When receiving a packet sent in the time interval , the receiver cannot yet verify the authenticity and needs to add the collected information to a buffer until it learns the key , which is only disclosed after time intervals.

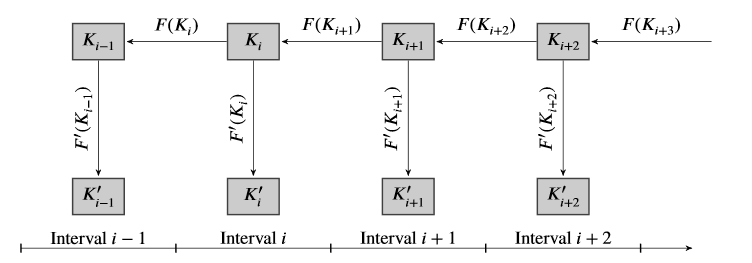


Figure 3. Illustration of the key-chain used in the TESLA protocol.

* 1. Proposal to use TESLA to protect VDES R-Mode

This implementation relies on using a single TESLA chain for a group of VDES R-Mode transmitters, which are in the vicinity of each other.

For simplicity we shall assume that the navigation messages sent by all transmitters of the group are identical. Let us denote by the -th navigation message. Let us denote by the number of ranging sequences transmitted by the -th transmitter between the -th and the -th navigation messages ( and ), and let us assume that each ranging sequence conveys information bits (it is chosen uniformly at random from a pool of ranging sequences). Hence, a total of bits are conveyed by the ranging sequences transmitted between and . Let us denote by the bits long bitstring that is conveyed by the ranging messages transmitted by the -th transmitter between and . This bitstring identifies which ranging sequences where transmitted by the -th transmitter between the -th and the -th navigation messages. We will say that in the n-th TESLA interval starts right after the transmission of and end right before the transmission of . Thus the packet disclosure delay of TELSA will correspond to the time between two consecutive navigation messages.

According to a standard TESLA procedure, a one-way key chain is built by using a one-way function such that a key is computed from another key as . Each key is associated with a time interval of uniform duration, indexed by . Furthermore, using another one-way function a key is derived from as . During the time -th time interval, all transmitters use key to compute the MAC for the packets they transmit. Thus, if a navigation message is sent during the -th time interval, the sender uses the key to compute a MAC, of the packet . Additionally, the packet contains the key from time intervals in the past. The parameter is called the *packet disclosure delay* and is specified beforehand along with the duration of the time intervals and the maximum length of the one-way key chain. The packet is then given as

Up to this point, this represents a standard TESLA one-way chain and contains no novelty. According to [5], the standard TESLA procedure can be modified as follows in order to protect as well the ranging sequences.

An additional key-derivation function is used in order to derive multiple keys from which are associated to the different transmitters in the group. In particular, let us consider a group of transmitters and let be the (distinct) identifiers of the transmitters.

The key associated to transmitter in the -th time is obtained by applying the key derivation function to and as

As an alternative, in some situations it might be advantageous to include an additional parameter to derive . In this case the key is obtained as:

According to [5], the j-th transmitter, whose id is , does not freely choose the ranging sequences he transmits. Instead, the ranging sequences are determined by , which is directly derived from In particular,

* We can have
* Alternatively, can be obtained by truncating , in case the length of is larger than that of .

This way, after a receiver obtains , it can generate for all the transmitters in the group, i.e., for any . Thus, without sending any additional data, the TESLA chain can be used to obtain .

Note that the functions , and can be chosen to be identical, although they can also be different.

Note also that the transmitters need not have knowledge of the complete TESLA chain. In particular, it is sufficient that the -th transmitter, who has id , has knowledge of before the -th TESLA interval starts. In fact, it is actually possible to delay the delivery of to the transmitters. In this case one has to provide after the i-th TESLA interval has ended, provided that the transmitter with id had knowledge of , or equivalently , before the -th TESLA interval started. This could increase security, by avoiding that the -th transmitter reveals the information related to (the ranging sequences used by the -th transmitter).

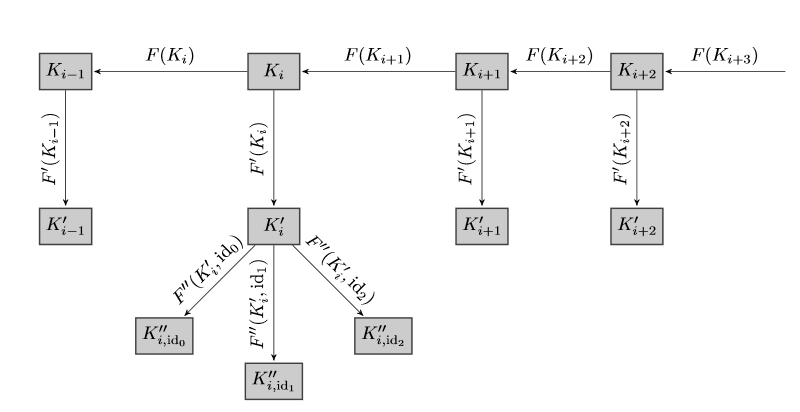


Figure 4. Illustration of TESLA with a single chain used to convey .

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-2)
2. Leave open if uncertain [↑](#footnote-ref-3)