Journal of Marine Science and Engineering

MDPI

Article

A Credibility Monitoring Approach and Software Monitoring System for VHF Data Exchange System Data Link Based on a Combined Detection Method

Xiaoye Wang *, Leyun Fu, Weichen Wang and Qing Hu

College of Information Science and Technology, Dalian Maritime University, Dalian 116026, China; fly020900@163.com (L.F.); 15235200898@163.com (W.W.); hq0518@dlmu.edu.cn (Q.H.)
* Correspondence: wangxiaoye@dlmu.edu.cn

Abstract: Due to VDES's higher data transmission speed and complex communication protocols, vulnerabilities within its data link infrastructure are more pronounced. To ensure the reliability of VDES data transmission, this manuscript proposes a credibility monitoring approach based on the combined detection method of radio interference detection and spoofing source identification and localization, focusing on key data link vulnerabilities outlined in the IALA G1181 VDES VDL Integrity Guide. Automated monitoring is achieved through VDES data link monitoring software, which is based on a three-tier architecture and a Client/Server (C/S) model. The software validates monitoring techniques and software against various interference scenarios. Visualization of monitoring results, alarm notifications, and relevant data through the front-end interface enhances understanding of VDES data link credibility. This framework supports effective surveillance and detection of vulnerabilities, such as radio interference and spoofing sources.

Keywords: VDES; data link; credibility; monitoring approach; monitoring system

Citation: Wang, X.; Fu, L.; Wang, W.; Hu, Q. A Credibility Monitoring Approach and Software Monitoring System for VHF Data Exchange System Data Link Based on a Combined Detection Method. *J. Mar. Sci. Eng.* **2024**, *12*, 1751. https://doi.org/10.3390/jmse12101751

Academic Editor: Xinqiang Chen

Received: 3 September 2024
Revised: 29 September 2024
Accepted: 30 September 2024
Published: 3 October 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

To ensure maritime traffic safety and address the increasing demands of maritime communication, the International Organization for Marine Aids to Navigation (IALA), previously designated as The International Association of Marine Aids to Navigation and Lighthouse Authorities, as of 22 August 2024, officially transformed its status from a Non-governmental Organization (NGO) to an Intergovernmental Organization (IGO) based on a convention that has been ratified or acceded to by 34 states to date. The new organization is named The International Organization for Marine Aids to Navigation, and the International Telecommunication Union (ITU) introduced the Very-High-Frequency Data Exchange System (VDES) into maritime mobile communication in 2013 [1]. Building upon the foundational functionalities of the Automatic Identification System (AIS), VDES integrates Application Specific Messages (ASM) and Wideband Very-High-Frequency Data Exchange (VDE) capabilities. Consequently, VDES mitigates the data communication burden on AIS, enhancing the capacity and efficiency of data exchange processes. In October 2015, IALA led the formulation of international standards for VDES, culminating in the release of the initial standard, ITU-RM.2092-0. This standard has since undergone iterative enhancements and refinements [2]. Currently, with the maturation of VDES technical standards, the international procedural progression of VDES has transitioned into the acknowledgment phase within the International Maritime Organization (IMO). During the 11th session of the IMO Sub-Committee on Navigation, Communications, and Search and Rescue (NCSR11), held in June of this year, discussions focused on proposed amendments to the Safety of Life at Sea (SOLAS) Convention related to VDES and its performance standards. Subsequently, a correspondence group was established to advance these

amendments to Chapter V of SOLAS, aiming to comprehensively introduce VDES as a replacement for AIS and as the inheritor of AIS's international legal standing. This development positions VDES as the foundational maritime digital infrastructure for advancing global E-navigation [3]. As the transition from AIS to VDES within the SOLAS Convention progresses, nations worldwide are expected to seize this opportunity to enhance research efforts regarding the performance and systemic evolution of VDES [4].

Nevertheless, notwithstanding the considerable potential of VDES to enhance the effectiveness of maritime communication, it also confronts certain drawbacks and challenges [5]. Currently, the maritime communication network mainly encompasses satellite-based maritime communication systems, land-based maritime communication systems, island-based maritime communication systems and other systems that respond to diverse service requirements. A schematic diagram of the maritime wireless communication system is presented in Figure 1 [6].

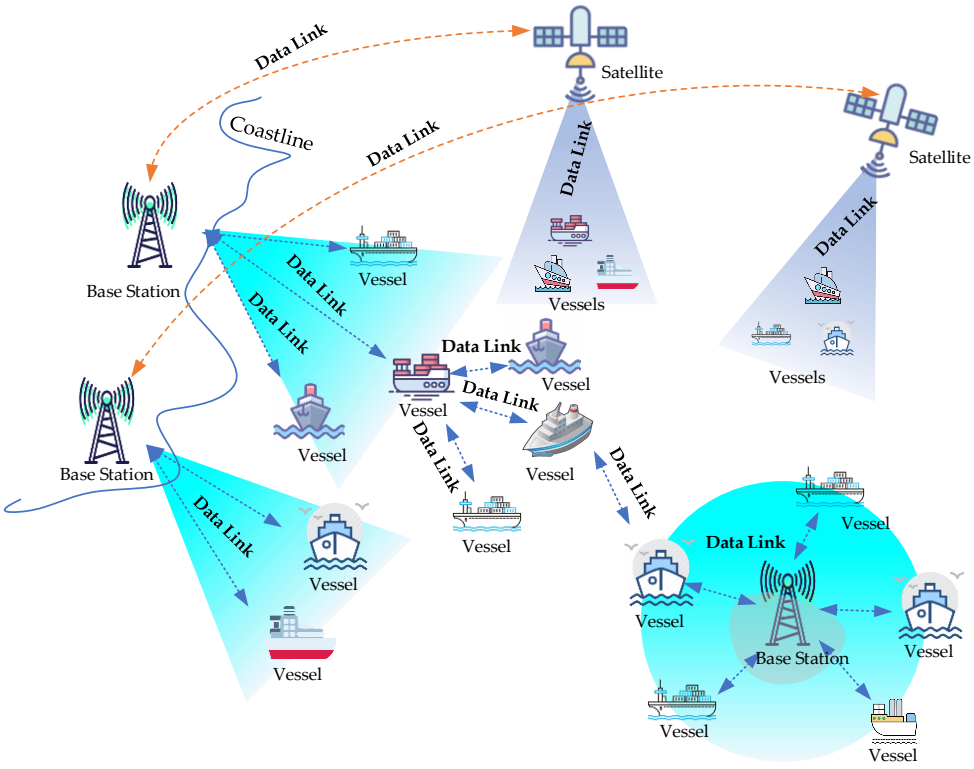


Figure 1. Schematic illustration of the maritime wireless communication system.

However, as each system is relatively independent and lacks unified resource management and operational coordination, the overall utilization efficiency is extremely low, which restricts the development of maritime communications. Realizing the effective system integration of the existing maritime communication system can facilitate the efficient operation of the maritime network system and provide an effective guarantee for the scope of network coverage, real-time information transmission and reliability. In recent years, as maritime data communication requirements have continuously evolved, AIS, originally designed for automatic ship identification and collision avoidance, has increasingly assumed the role of ship-to-shore data communication. Intelligent processing of AIS data is used to predict ship positions in real time and can assist in decision making, thus enhancing maritime transportation safety and efficiency [7,8]. The escalating communication demands placed on the AIS system within the VHF band have resulted in a highly congested frequency band. IALA has indicated that when AIS data link loads exceed 50%, it can give rise to severe problems such as information congestion, affecting navigation safety. The performance of the AIS system is directly influenced by factors such as link

load. As the link load increases, the time slot multiplexing ratio rises, along with the time slot conflict rate. When the conflict rate reaches a certain level, the communication reliability of the system is compromised. The AIS system is of crucial importance for ensuring safe navigation, and its effectiveness is of paramount significance [9]. Moreover, the increasing demand for data exchange is a key driver that necessitates an upgrade of the AIS system. As the demand for maritime data communication keeps rising, designing and managing efficient wireless communication networks becomes indispensable [10,11]. To address AIS frequency band congestion, multi-band communication technologies can be utilized to optimize spectrum usage. Additionally, enhancing the network's adaptive capabilities to monitor and adjust communication parameters in real time can help alleviate the risk of information blockages [12]. Furthermore, implementing a cloud-based management system that leverages big data analytics to optimize data flow and resource allocation can significantly enhance overall communication efficiency. Through these measures, the ultimate aim is to achieve a more secure and efficient maritime wireless communication network to meet the growing demand [13,14]. To alleviate the strain on AIS channels caused by this increased occupancy, VDES leverages the existing AIS infrastructure by introducing ASM and VDE to enhance data transmission capabilities comprehensively. The risk of AIS link overload necessitates the adoption of VDES, which offers improved data transmission rates and advanced protocols, as recommended in ITU-RM.2092-1. However, the increased complexity of VDES, particularly its Very-High-Frequency Data Link (VDL), makes it more susceptible to various issues. Consequently, diligent monitoring of the VDL is crucial to mitigate potential impacts and ensure the reliability and resilience of VDES operations [15]. Notably, on 14 December 2023, the "Guidelines for Integrity Monitoring of Very-High-Frequency Data Exchange System Data Links (G1181)", led by China, were approved by the IALA Council and officially released [16]. These guidelines emphasize that the wireless nature of VDES introduces inherent vulnerabilities in its VDL, including factors such as radio interference and spoofing messages, as illustrated in Figure 2. Radio interference affecting the VDES data link includes co-channel interference from non-VDES services, adjacent channel interference from other maritime operations, and spurious emissions from high-power devices [17,18]. Additionally, interference in the VDES domain may stem from VDES base station slot collisions and atmospheric disturbances [19]. Such interference can compromise the capacity of VDES equipment to accurately demodulate signals, thus jeopardizing navigational safety by propagating errors in message transmission [20,21]. Furthermore, VDES base stations transmit various messages to facilitate navigation, including safety-related and hydro-meteorological messages. However, because the messages broadcast by VDES base stations lack encryption and the system does not incorporate an authentication mechanism [22], malicious actors can exploit genuine base station information for identity spoofing, spreading false information to vessels, misguiding navigational decisions, and endangering safety [23]. Consequently, if vulnerabilities compromise the VDES data link—leading to information loss, content errors, or the dissemination of false messages—the confidentiality, integrity, and availability of wireless communication are severely impacted. These vulnerabilities not only threaten the credibility and security of maritime communication but also create significant navigational safety risks. Therefore, to protect the authenticity and effectiveness of information disseminated by VDES base stations, proactive measures must be implemented to monitor vulnerabilities in the VDES data link, with a particular focus on ensuring the credibility of the data link [24].

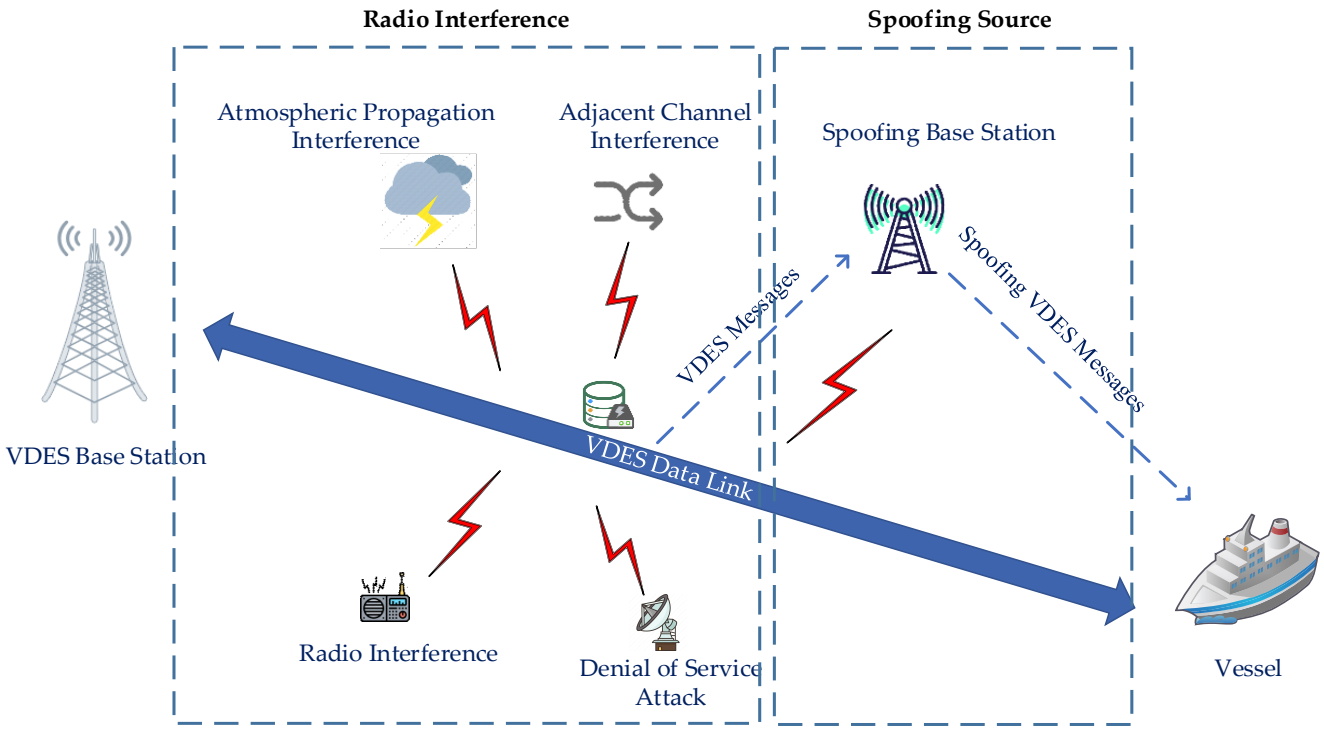


Figure 2. Two types of VDES data link interference scenarios mentioned in the IALA G1181 guidelines.

Research on the credibility of the VDES data link remains nascent and exploratory. Zhu et al. significantly enhanced the data transmission credibility of the VDES ground subsystem in complex multipath interference scenarios by integrating OFDM technology. This advancement not only improved the credibility of long-range maritime transmissions within the VDES framework but also provided practical technical solutions and theoretical foundations for assessing the credibility of the VDES base station data link. However, this study failed to fully mirror the long-term stability and large-scale application effects of the VDES system integrated with OFDM technology in complex real marine circumstances [25]. In a related effort, Li et al. introduced the concept of virtual beacons based on VDE-SAT, developed a message framework for disseminating long-distance virtual beacon data, and validated the coherence of this framework through illustrative examples, thereby offering a new perspective on long-range navigational support. This initiative also strengthened the data transmission integrity and security of the VDES infrastructure. However, the acceptance and integration of any new technology within the industry typically entail time, rendering promotion and adoption potentially challenging [26]. Moreover, Wang et al. thoroughly examined the system architecture and spectrum allocation strategy of VDES, offering a detailed overview of key technologies and developmental milestones within the VDES domain. Their comprehensive investigation into the architectural framework and critical technologies of the space–air–ground–sea communication network based on VDES provided technical support and theoretical rationale for the secure and efficient operation of intelligent maritime communication systems, while also enriching discussions on the stability and credibility of the VDES base station data link. Additionally, the study fails to investigate the specific challenges that VDES might encounter during actual deployment [27]. Furthermore, Jiang et al. proposed an ultra-low-power RF fingerprint recognition system using pulse neural networks (SNN) combined with an attention mechanism for authenticating satellite components within the VDES framework. By integrating these features, they enhanced the precision and resilience of the system. Moreover, some technical challenges must be overcome before the SNN-based RFFI system can be applied practically [28]. Concurrently, Jamal et al. explored advanced

very-high-frequency data link (A-VDL) technology relevant to aviation VHF communication. Their design of a filter significantly reduced out-of-band power emissions in A-VDL, mitigating adjacent channel interference and improving the system's spectral efficiency, thus enhancing communication quality within the VDES spectrum. The study also lacks performance verification under non-ideal circumstances [29]. In parallel, Hu et al. proposed a Feedback based Time Division Multiple Access (FBTDMA) protocol to prevent transmission conflicts among vessels. Their findings showed a marked reduction in transmission conflict rates among vessels using VDES for communication, along with an increase in the system's throughput, thereby paving the way for further exploration of channel utilization within the VDES data link. While augmenting the throughput of the VDES system, it concurrently increases communication complexity and potential latency [30]. Lastly, Zeng et al. designed and implemented a circularly polarized rotatable gate antenna specifically for satellite VDES, significantly expanding the coverage angle of satellite communication. This antenna design met EIRP requirements and link budget constraints, helping to mitigate interference from other communication systems and strengthening the integrity of the VDES data link. The applicability of this study might be restricted to specific types of satellites [31]. Zheng et al. also proposed a maritime autonomous surface vessel local communication area protocol based on VDES, analyzing ship domain models to identify critical avoidance zones and delineate routing request regions accordingly. Within these designated areas, data transmission is facilitated using the ad hoc on-demand distance vector (AODV) routing protocol. This methodology considers vessel positional data, fostering robust communication links with vessels in the routing request area. As a result, it significantly enhances VDES communication credibility while mitigating burdens on the VDES link. For different types of vessels with diverse speeds, this research method might call for further discussion [32]. Moreover, Ma et al. introduced a VDES signal frequency offset estimation algorithm based on cross-correlation techniques. This algorithm constructs localized sequences using character sequences and distinct Doppler frequency offsets, deriving preliminary estimates through cross-correlation analysis with the received signal. These estimates are then reintegrated into the received signal to rectify phase ambiguities, culminating in the application of the Fitz algorithm for precise estimation of the VDES signal frequency offset. This strategic approach effectively addresses various frequency offset challenges in the VDE-SAT downlink, markedly improving VDES data transmission quality and reducing communication discrepancies caused by frequency deviations. Although the algorithm performs well in estimating frequency offset within a broad range, its suitability for all types of VDES signals and other communication systems demands further investigation [33]. Furthermore, Shim et al. advanced maritime Automatic Rate Fallback (mARF) technology to optimize the adaptive capacity of the Modulation and Coding Scheme (MCS) within the VDES link. Experimental findings highlight the significant effectiveness of this approach in increasing VDES data link transmission rates and enhancing link control capabilities. Finally, the performance of the system in practical applications calls for additional verification [34]. Additionally, Zhang et al. introduced an enhanced Self-Organizing Time Division Multiple Access (SOTDMA) protocol to address the performance limitations of conventional SOTDMA protocols amid increasing VDL loads within the VDES framework. By reducing slot reservation conflict rates, this protocol significantly improves the efficiency and credibility of data transmission in VDES operations. While the paper defines the reporting frequency and corresponding probability parameters for ships under different motion states, these parameters might require adjustment based on the actual application environment to more accurately reflect real-world conditions [35].

In conclusion, existing studies have enhanced the resilience of VDES data transmission through the examination of data structures and system architecture. However, a comprehensive assessment of the vulnerability landscape within VDES data links is still lacking. Vigilant monitoring of VDES data link reliability can expedite the prompt detection and precise localization of vulnerabilities, enabling alerts regarding these vulnerabilities

to be sent to vessels or operational hubs. This proactive approach effectively mitigates security risks while ensuring the integrity of VDES communications received by maritime entities, thereby strengthening navigational safety. Consequently, this study addresses the vulnerability challenges facing VDES data links, particularly those arising from distinct interference scenarios outlined in the G1181 guidelines. It advocates for the combined detection method of radio interference detection and spoofing source identification and localization to maintain the credibility of VDES data links. To accomplish this overall goal, the following research objectives were established:

1. To detect radio interference in the VDES data link, a radio interference detection approach based on message characteristics is put forward. By examining adherence to message formats, parameter validity, content integrity, and transmission coherence, it is determined whether radio interference will impact the correct transmission of VDES messages.
2. Due to the lack of encryption in the messages broadcast by VDES base stations and the absence of an identity verification mechanism within VDES itself, malicious entities could deceive vessels within the signal coverage area by illicitly sending false VDES messages using the MMSI code stolen from a legitimate base station. This deceptive practice can mislead vessel navigation decisions, posing a significant threat to maritime safety. This paper employs a method for spoofing source detection based on distance matching analysis. Specifically, the VHF signal propagation loss model in the complex sea environment is employed to calculate the propagation distance of the VDES signal, and the position information in the ship position report is utilized to calculate the ship-to-shore distance. The matching degree analysis of the two distances is adopted to effectively identify the spoofing source, and the spoofing source position and range are then located by using the spoofing source positioning algorithm.
3. To automatically monitor the credibility of the VDES data link and issue timely warnings of vulnerabilities to vessels or management centers, this study develops monitoring software based on a tripartite data architecture supported by a client/server (C/S) model, using the front-end interface to display the monitoring results, warning information, and related data visually, facilitating a direct understanding of the credibility of the VDES data link.
4. The credibility monitoring approach and monitoring software for the VDES data link proposed in this paper are verified based on various interference scenarios, and the results indicate that the proposed approach and the developed software system can effectively monitor and identify the vulnerability threats such as radio interference and spoofing sources existing in the VDES data link.

The findings of this study provide a foundation for developing high-trust services for VHF data links within a comprehensive maritime navigation support system.

2. VDES Data Link Credibility Monitoring Approach

This paper examines two primary categories of vulnerability threats, as delineated in Figure 2, and proposes a collaborative monitoring strategy based on radio interference detection and spoofing source identification and localization to oversee the credibility status of data links within the outlined threat scenarios, as depicted in Figure 3. Radio interference threats targeting VDES data links originate from various sources, including atmospheric interference, adjacent channel interference, electromagnetic radiation interference, and pseudo-transmission interference from high-power devices. Detection of these interferences can be effectively carried out through several methodologies, including telegram format compliance verification, telegram parameter legitimacy verification, telegram content integrity verification, and verification of transmission and reception consistency. To elaborate, the process of telegram format compliance verification involves

parsing received VDES messages. Successful parsing indicates compliance with the format; conversely, a failure to parse suggests the presence of radio interference, thereby compromising the credibility of the VDES data link. Additionally, telegram parameter legitimacy verification can utilize an AIS/VDES telegram distributed database, meticulously curated by the author's research team in collaboration with relevant maritime administrative entities following extensive research and consultations. This database contains all legitimate telegrams previously dispatched by each shore station. Ensuring that the parameters within the VDES message align with those of legitimate telegrams from the specific shore station in the database is essential for passing the parameter legitimacy check; any misalignment signals potential radio interference, jeopardizing the credibility of the VDES data link. For a comprehensive understanding of the implementation methodologies related to these aspects, readers are referred to reference [36]. Furthermore, telegram content integrity verification employs the MD5 algorithm to assess the integrity of received VDES messages against legitimate telegrams stored in the original VDES telegram database. A match in the hash values of both messages indicates successful passage of the content integrity check; conversely, a mismatch signifies radio interference, thereby impacting the credibility of the VDES data link. VDES shore stations disseminate link management telegrams through TDB statements, which VDES ship stations then relay using VEM statements upon reception. After receiving this relayed message, VDES shore stations use the HMAC algorithm to validate the consistency between transmitted and received telegrams. If the HMAC values of both telegrams align, the transmission and reception consistency check is passed; any disparity indicates radio interference, casting doubt on the credibility of the VDES data link. Upon completing radio interference detection procedures, the VDES messages transition to the spoofing source identification and localization algorithm. Spoofing source interference targeting VDES data links originates from "Spoofing" base stations that threaten maritime safety by propagating false VDES messages to vessels within their signal coverage, often by misappropriating the Maritime Mobile Service Identity (MMSI) of genuine VDES shore stations. Detecting such interferences requires a comprehensive analysis of ship-to-shore distances and propagation distances to ascertain the presence of spoofing sources. VDES ship-based stations compute the ship-to-shore distance by comparing the vessel's position, relayed by the VDES ship-based station, with the base station's position, using a VHF signal propagation loss model and received power calculations to determine VDES signal propagation distances in complex maritime environments. Subsequent analysis evaluates whether the ship-to-shore distance falls within the acceptable propagation distance tolerance range. Any deviation beyond this range indicates a potential spoofing source, prompting further scrutiny through the spoofing source identification algorithm to pinpoint the position or range of the spoofing source. Conversely, compliance with the tolerance range affirms the absence of a spoofing source, thereby confirming the credibility of the VDES data link.

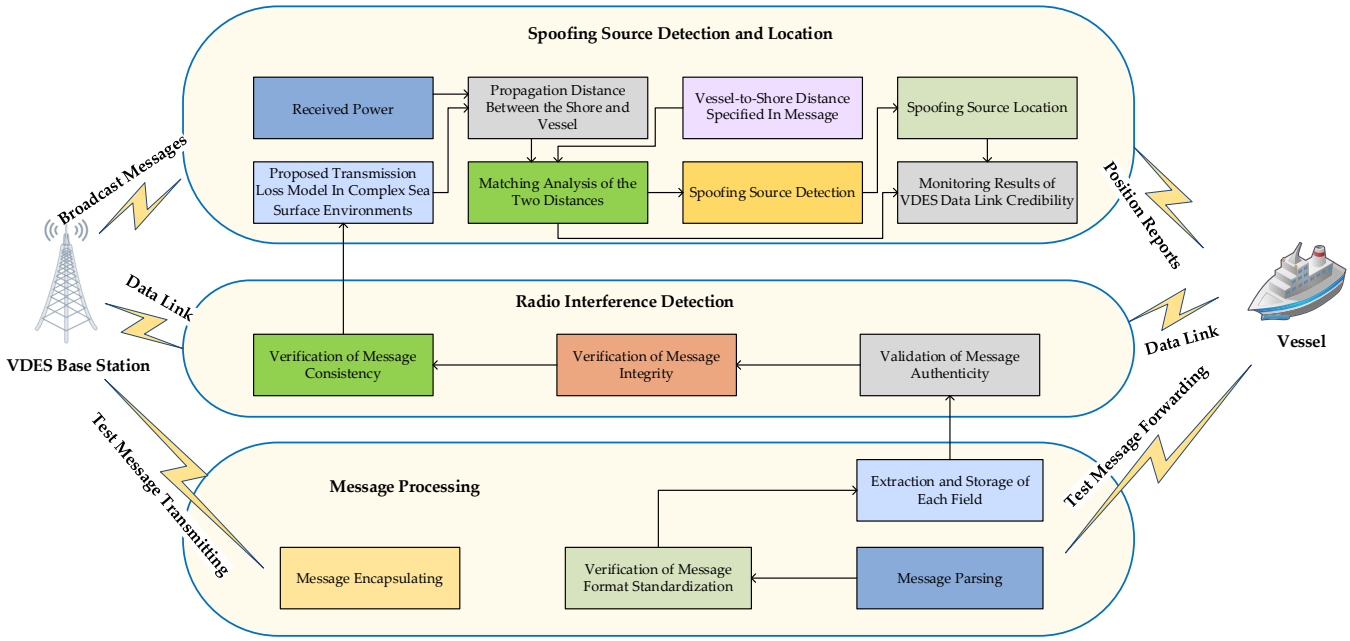


Figure 3. Main structural diagram of VDES data link credibility monitoring approach based on a combined detection method.

2.1. Radio Interference Detection Based on Message Characteristics

The presence of radio interference within VDES data links impedes the accurate demodulation of VDES messages by equipment, resulting in transmission errors that pose risks to maritime navigation safety. To facilitate the prompt identification of these errors by traffic managers or crew members, detecting radio interference in VDES data links is imperative. This study adopts a radio interference detection methodology based on message characteristics. It entails a meticulous examination of message format adherence, message parameter legitimacy, message content integrity, and message transmission and reception consistency to assess the potential impact of radio interference on the faithful transmission of VDES messages. In scrutinizing message content integrity, the MD5 algorithm is employed to pad and segment parsed VDES messages. Each segment undergoes cyclic processing to yield a 128-bit hash value for the VDES message. Simultaneously, the MD5 algorithm is used to compute the hash value of authenticated messages received from ship stations by the base station in the original VDES message repository. Subsequently, the hash values of these two messages are compared for congruence. A congruent hash value suggests the integrity of the received VDES message content, thereby confirming the integrity assessment. Conversely, incongruent hash values indicate the potential presence of radio interference. VDES base stations disseminate link management messages through TDB statements, which VDES ship stations automatically forward via VEM statements upon receipt. Verifying message transmission and reception consistency involves utilizing the initial seven characters of link management messages broadcast by VDES base stations in TDB statements as a shared key. This key is extended to 64 bytes using the HMAC algorithm, the required fixed length for the hash function, to generate the HMAC value for the entire message. Concurrently, the HMAC value of the message received by VDES base stations through VEM statements relayed by VDES ship stations is computed, and the HMAC values of both messages are compared. A match in HMAC values indicates identical transmitted and received message contents, affirming adherence to the consistency check. Conversely, disparate HMAC values suggest inconsistencies in transmitted and received message contents, signaling potential deviations caused by radio interference. Thus, the precise detection of radio interference can be achieved through the methodologies outlined above.

2.1.1. VDES Message Integrity Verification Method Based on the MD5 Algorithm

During the communication process between VDES base stations and ship stations, incomplete message content transmission due to radio interference within the data link can significantly impact the safety of vessel navigation. Consequently, assessing message content integrity is imperative for identifying potential threats posed by this interference. The use of hash algorithms, recognized as robust methods for validating message integrity, provides a viable mechanism for scrutinizing the integrity of VDES message content. The MD5 algorithm, a prevalent hashing technique, can transform messages of varying lengths into uniform 128-bit hash values, uniquely characterizing each message. By employing this algorithm to compute the hash value of parsed messages and comparing it with the hash value of authentic messages dispatched by ship stations and received by the base station within the VDES original message repository, discrepancies in the hash values signal deficiencies in message completeness attributable to radio interference during transmission. Thus, by juxtaposing the hash values of messages, the integrity of VDES messages during transmission can be effectively corroborated. The schematic representation of the MD5 algorithm utilized in this study is illustrated in Figure 4, offering a visual depiction of the computational process involved in ensuring the integrity of VDES messages amid potential radio interference challenges.

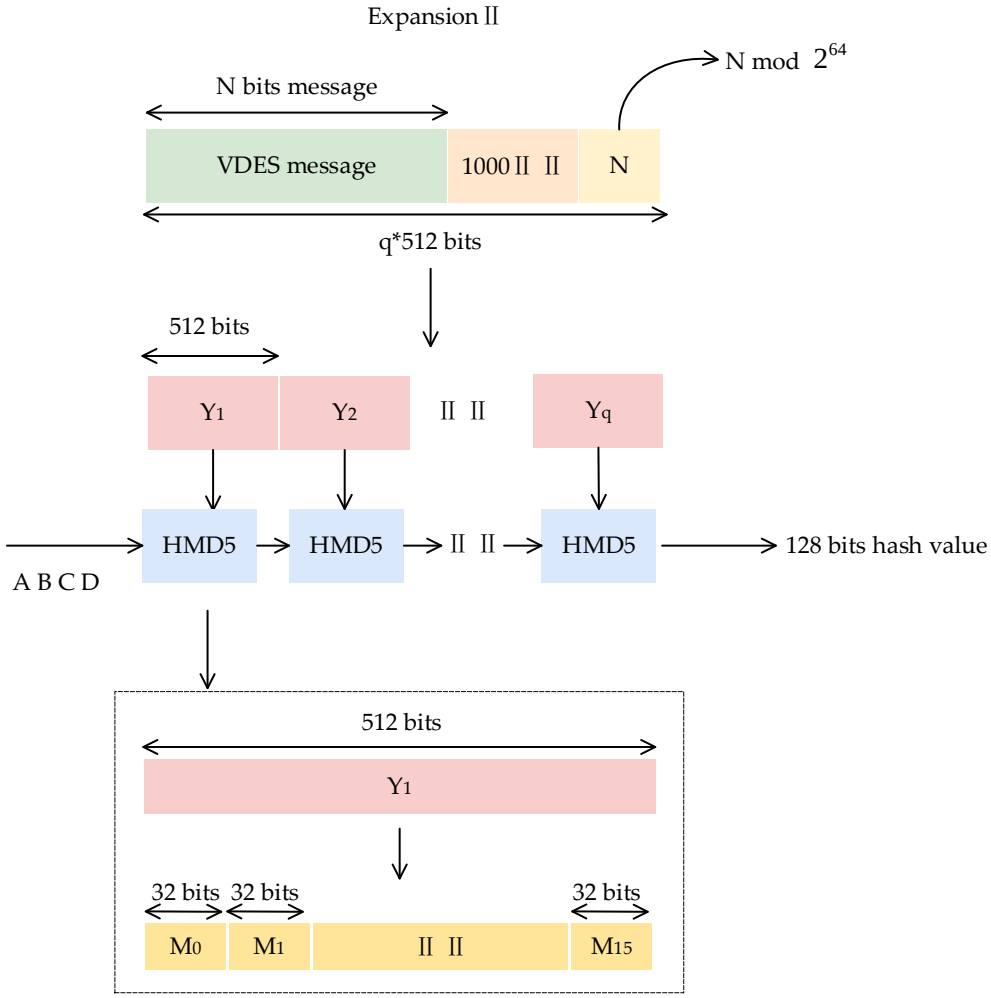


Figure 4. Flowchart of the MD5 algorithm computation.

Initially, the data parsed from VDES messages undergo padding and segmentation by the MD5 algorithm. Subsequently, each block is subjected to iterative processing, ultimately yielding a 128-bit hash value for the VDES message. The specific computational process is outlined as follows:

Step 1 VDES Message Padding: A digit "1" is appended to the end of the VDES message to signal its conclusion, followed by the addition of "0" to ensure that the message length is congruent to 448 when divided by 512. At this stage, the message length is N × 512 + 448, where N is a positive integer.

Step 2 Appending Message Length: Following the initial step, 64 bits of the original message data are added after the final "0". If the length of the original message data exceeds the limit, it is adjusted using modulo. Consequently, the padded VDES message achieves a length of N × 512 + 448 + 64 = (N + 1) × 512N × 512 + 448 + 64 = (N + 1) × 512N × 512 + 448 + 64 = (N + 1) × 512 bits.

Step 3 Initialization of Chaining Variables: After the preceding two steps, the VDES message is effectively partitioned into q groups of 512-bit message blocks. Simultaneously, four 32-bit registers, denoted as A, B, C and D, are internally defined within the algorithm. These registers serve the purpose of storing and updating intermediate values and final outcomes during the computation process. The initial chaining variable values for these four registers are set as $A = 0X01234567$, $B = 0X89ABCDEF$, $C = 0XFEDCBA98$, and $D = 0X76543210$.

Step 4 Message Grouping and Four-Round Iterative Computation: Following the aforementioned procedures, the message is segmented into individually processed 512-bit blocks. Each VDES message block is then subdivided into sixteen 32-bit blocks, with each group processed through the compression function HMD5. HMD5 consists of four rounds of iterative processes, each involving the calculation of logical function values denoted as F, G, H, and I. Each round includes 16 iterations, necessitating a total of 64 iterations for each VDES message block.

Initially, four fundamental logical functions are defined, where *X*, *Y*, and *Z* are 32-bit integers [37].

$$\begin{cases} F(X,Y,Z) = (X \ and \ Y) \ or \ \left(\left(not(X)\right) and \ Z\right) \\ G(X,Y,Z) = (X \ and \ Z) \ or \ \left(Y \ and \ \left(not(Z)\right)\right) \\ H(X,Y,Z) = X \ xor \ Y \ xor \ Z \\ I(X,Y,Z) = Y \ xor \ \left(X \ or \ \left(not(Z)\right)\right) \end{cases} \quad (1)$$

Let M_j represent the *j*-th message block of the VDES message, where j ranges from 0 to 15, $<<<s$ denotes a circular left shift by s bits; then, the logical function for each round of computation is as follows [37]:

$$\begin{aligned} &FF\left(a,b,c,d,M_j,s,t_i\right): a = b + \left(\left(a + F\left(b,c,d\right) + M_j + t_i\right) <<< s\right) \\ &GG\left(a,b,c,d,M_j,s,t_i\right): a = b + \left(\left(a + G\left(b,c,d\right) + M_j + t_i\right) <<< s\right) \\ &HH\left(a,b,c,d,M_j,s,t_i\right): a = b + \left(\left(a + H\left(b,c,d\right) + M_j + t_i\right) <<< s\right) \\ &II\left(a,b,c,d,M_j,s,t_i\right): a = b + \left(\left(a + I\left(b,c,d\right) + M_j + t_i\right) <<< s\right) \end{aligned} \quad (2)$$

Step 5 Outputting the Hash Value: Once all message blocks in the original VDES message have undergone computation, the calculated value from the iteration of the final HMD5 output message block serves as the VDES message hash value. The pseudocode implementation of the MD5 algorithm utilized in this paper is presented in Algorithm 1.

Algorithm 1 MD5 algorithm

Initialize variables:
A ← 0X67452301
B ← 0XEFCDAB89
C ← 0X98BADCFE
D ← 0X10325476
Pre-processing:
append "1" bit to message
append "0" bits until message length in bits ≡ 448 (mod 512)
append bit length of message as 64 bits little-endian integer to message
for each 512 bits chunk of message **do**
    break chunk into sixteen 32 bits little-endian words $w[i]$, 0 ≤ i ≤ 15
    Initializa hash value for this chunk:
    a ← A
    b ← B
    c ← C
    d ← D
    for i from 0 to 63 **do**
        if 0 ≤ i ≤ 15 **then**
            f ← (b & c)|(~ b & d)
            g ← i
        else if 16 ≤ i ≤ 31 **then**
            f ← (d & b)|(~ d & c)
            g ← (5×i+1) mod 16
        else if 32 ≤ i ≤ 47 **then**
            f ← b ⊕ c ⊕ d
            g ← (3 × i+5) mod 16
        else if 48 ≤ i ≤ 63 then
            f ← c ⊕ (b|(~ d))
            g ← (7 × i) mod 16
        end if
        temp ← d
        d ← c
        c ← b
        b ← $leftrotate\left(\left(a + f + k[i] + w[g]\right), r[i]\right) + b$
        a ← temp
    end for
    Add this chunk's hash to result so far:
    A ← A + a
    B ← B + b
    C ← C + c
    D ← D + d
end for
digest ← *AappendBappendCappend* //(expressed as little-endian)

In conclusion, following the procedural sequence encompassing Steps 1 through 5, the computation of the hash value for the deciphered message from the VDES base station is compared with the hash value of legitimate messages dispatched by ship stations and

received by the base station within the VDES original message repository. If the hash values of these messages align, verification of message completeness occurs, thereby affirming the integrity of the message content. Conversely, a discrepancy in hash values implies potential tampering with the contents of VDES messages during transmission, resulting in incomplete message data. By adhering to the evaluative criteria outlined above, a robust mechanism for effectively monitoring the integrity of VDES message content is established.

To corroborate the efficacy of the VDES message integrity validation technique reliant on the MD5 algorithm in overseeing the integrity of VDES message content, this section undertakes validation and scrutiny of the design methodology utilizing authentic link management messages received by the VDES base station. For instance, in an illustrative scenario, the VDES base station may receive a message such as "!AIVEM,1,1,0,A,403sooQvMSfR0`JAhH=Tdp400D0E,0*5D", while the legitimate message sent by a ship station and received by the base station in the VDES original message database is "!AIVEM,1,1,0,A,403sooQvLohh<`dD=LF?M3U00D0G,0*3C".

Initially, the received VDES message is decoded, and its conformity to the prescribed message format stored in the VDES original message database is verified for successful parsing and consistency, thus confirming adherence to the message format. Subsequent validation involves cross-referencing the AIS/VDES message distributed database to ascertain alignment between the parameters of the various message fields in the VDES message and those of legitimate messages previously transmitted by the base station and stored in the AIS/VDES message distributed database, thereby guaranteeing compliance with message parameter authenticity. Ultimately, the hash values of the received message and the legitimate message received by the base station in the VDES original message database are computed using the MD5 algorithm, with the results illustrated in Figure 5.

The simulation environments in Figure 5 employs the C# language within Visual Studio 2019 in Windows11 operating system environment. As depicted in Figure 5, the two message hash values highlighted by the red box differ, indicating that the messages did not pass the integrity check for message content. The discrepancies in the VDES messages are attributed to radio interference during the data link transmission process, resulting in transmission errors. This observation underscores the effectiveness of the MD5 algorithm in detecting data integrity issues within VDES messages.

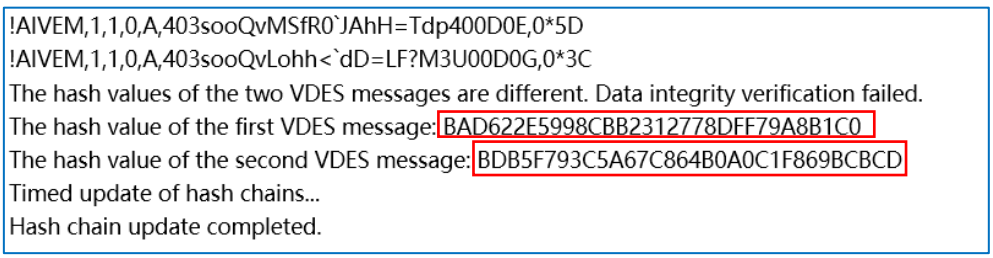


Figure 5. Results of failed message content integrity verification detection.

For instance, if a VDES base station receives the message "!AIVEM,1,1,0,A,403sooQvN7AgR`df;nF>BSW00D0c,0*67", and a legitimate message previously sent by a ship station is "!AIVEM,1,1,0,A,403sooQvN7AgR`df;nF>BSW00D0c,0*60", the hash values of both messages are computed using the MD5 algorithm after verifying compliance with the message format and the legitimacy of message parameters. The calculation results are illustrated in Figure 6.

```
!AIVEM,1,1,0,A,403sooQvN7AgR`df;nF>BSW00D0c,0*67
!AIVEM,1,1,0,A,403sooQvN7AgR`df;nF>BSW00D0c,0*60
The hash values of the two VDES messages are the same. Data integrity verification passed.
The hash value of VDES message: B286DA103A03514F0A6335BF9A49EC20
Timed update of hash chains...
Hash chain update completed.
```

Figure 6. Results of successful message content integrity verification detection.

The simulation environments in Figure 6 employs the C# language within Visual Studio 2019 in Windows11 operating system environment. As shown in Figure 6, the hash values of the two messages are congruent, both represented as B286DA103A03514F0A6335BF9A49EC20. This congruence signifies the resilience of VDES message transmission against data link radio interference, validated through meticulous scrutiny of message integrity. This experimental endeavor affirms the efficacy of the MD5 algorithm in discerning the integrity of VDES message content.

Moreover, within the realm of algorithmic evaluation, computational time serves as a pivotal benchmark. To further explore the processing efficiency advantage of the MD5 algorithm, this study compared the processing durations of the MD5 algorithm with three other prominent hashing algorithms, namely SHA-256, SHA-384 and SHA-512, in handling a single instance of the same VDES message. The VDES message under consideration for this comparative analysis is "!ABTDB,1,1,0,A,403t?j1vLohh<`JAhH=Tdp500D0G,0*6E", with the outcomes of this verification detailed in Figure 7.

```
VDES Message: !ABTDB,1,1,0,A,403t?j1vLohh<`JAhH=Tdp500D0G,0*6E
MD5 Hash Value: 0851f7443a2eae5ac4f0a50df3ddfe17
MD5 Hash Time: 9.8928 ms
SHA-256 Hash Value: 7ba8cb2527bb670b4d80e08aaa3babfa2ab2ca4bd8d1b8f53bd150e3bd79c490
SHA-256 Hash Time: 12.4144 ms
SHA-384 Hash Value: 311240a1af04f9d66c7166692697480b1fbfbf4583c0a1a2f18d0cdadbb04f5c50b6f211826699dd0d0f6296e352c7e9
SHA-384 Hash Time: 13.6527 ms
SHA-512 Hash Value: 237354c5be93f2cceb905484ab64c7afc30b9ce377714a3addece7db599127a6d353cb474380bd2a2646b3e7f12f25d6d9debe9e5f6452e61f6ab3430c52107c
SHA-512 Hash Time: 16.4384 ms
```

Figure 7. Comparison chart of computational speed of message digest algorithms.

The simulation environment in Figure 7 runs using the Java language in the Windows 11 operating system under the IDEA2022 configuration environment with JDK17. According to Figure 7, the processing of the identical VDES message revealed that the MD5 algorithm demonstrated the shortest processing time, at 9.8928 ms. The SHA-256 algorithm followed with a processing time of 12.4144 ms, while the SHA-384 algorithm recorded the longest processing time of 13.6527 ms. The SHA-512 algorithm recorded the longest processing time of 16.4384 ms. This finding highlights that the MD5 algorithm, as applied in this investigation, effectively validates the integrity of VDES message content while also offering the swiftest computational efficiency. This proficiency facilitates the effective monitoring of potential radio interference threats to the VDES data link, thereby enhancing the overall robustness of the system.

The complexity of the MD5 algorithm can be classified into birthday search, near-collision, and computation time. Among these, birthday search represents a birthday attack, which is the application of probabilistic modeling to lower the complexity of identifying MD5 hash function conflicts, as well as to assess the approximate risk of a hash conflict within an MD5 hash of a given overall scale.

The complexity of birthday search $C_b(r,k,w)$ is dictated by two principal factors, namely the search space $|V| = 2^{64+k}$ and the probability $P_{r,k,w}$. The probability $P_{r,k,w}$

refers to the probability of attaining a birthday collision that is not a pseudo-collision within the aforementioned search space and that the collision can be materialized given the selected parameter w as well as the requirement of approximating the number of collisions up to r times [37]. Hence, the complexity of the birthday search is $C_b(r,k,w)=\sqrt{2^{64+k}\pi/2P_{r,k,w}}$. In 2009, Stevens et al. provided a theoretically optimal attack complexity of 2^{39} [38].

Near-collision denotes the presence of two distinct input data having the same MD5 hash value, for the differential path construction and finding the near-collision block two components. Regarding near-collision complexity $C_{nc}(r,k,w)$, it consists of differential path construction complexity C1 and finding near-collision block complexity C2. The computation of differential path construction complexity C1 is relatively independent, and the average complexity of constructing such differential paths is $\bar{C}_1 \approx 2^{35}$ [38].

The complexity C2 of identifying each pair of collision blocks, conversely, relies predominantly on the parameter w, the strength of the tunnel, and the number of conditions in the last 2.5 rounds of the differential path [39]. For w = 0, 1, 2 and the aforementioned differential path constructed above, the average complexity of identifying each pair of collision blocks is $\bar{C}_2 \approx 2^{34}$ [38].

Based on the foregoing analysis, the collision complexity of the MD5 algorithm when w = 2, k = 0 and r = 9 is $2^{39.1}$ [38]. The complexity of the birthday search and r near-collisions at this juncture are 2^{37} and $2^{38.8} = 2^{38.8} = 9\times(2^{34}+2^{35})$ [38]. This complexity is the optimal outcome obtained by weighing the parameters and the equilibrium relationship between the two components of the complexity, whereas in practice, the number of near-collision blocks amounts to 3; thus, the actual attack complexity is approximately $2^{49.9}$ when w = 5, k = 8 and r = 3 [38]. Regarding the analysis of the computational time complexity, the paper conducts the time complexity analysis of the MD5 algorithm on page 13, that is, it computes the time for the MD5 algorithm and the other three typical hash algorithms, SHA256, SHA384 and SHA512 algorithms, to process the same VDES message once, and the VDES message utilized is "!ABTDB,1,1,0,A,403t?j1vLohh<`JAhH=Tdp500D0G,0*6E". For the processing of the same VDES message, the MD5 algorithm consumed the least time at 9.8928 ms, followed by the SHA256 algorithm at 12.4144 ms, the SHA384 algorithm at 13.6527 ms, and the SHA512 algorithm, which consumed the most time, at 16.4384 ms.

2.1.2. VDES Message Consistency Detection Method Based on the HMAC Algorithm

The VDES base station broadcasts link management messages in TDB format, which are automatically relayed by VDES ship stations using VEM statements. However, due to radio interference in the data link, the content of messages relayed by VDES ship stations and subsequently received again by the VDES base station may be tampered with, resulting in inconsistencies and posing safety risks to maritime navigation. Therefore, it is essential to verify the consistency of the content between the link management messages broadcast by the VDES base station in TDB format and the messages received again by the base station after being relayed. The Hash-based Message Authentication Code (HMAC) is a message authentication code that utilizes a hash function as part of its authentication algorithm. In wireless communication, the HMAC algorithm is employed to verify data integrity, playing a crucial role in safeguarding data security and preventing tampering. The HMAC algorithm generates HMAC values by combining a key with VDES messages. By comparing the HMAC value of the link management messages broadcast in TDB format with the HMAC value of the messages received via VEM statements, any discrepancies in the HMAC values indicate content tampering due to radio interference during transmission. Thus, comparing the HMAC values of TDB and VEM messages allows for the verification of data integrity in the transmission of messages between VDES base stations. The process flow diagram of the HMAC algorithm is illustrated in Figure 8.

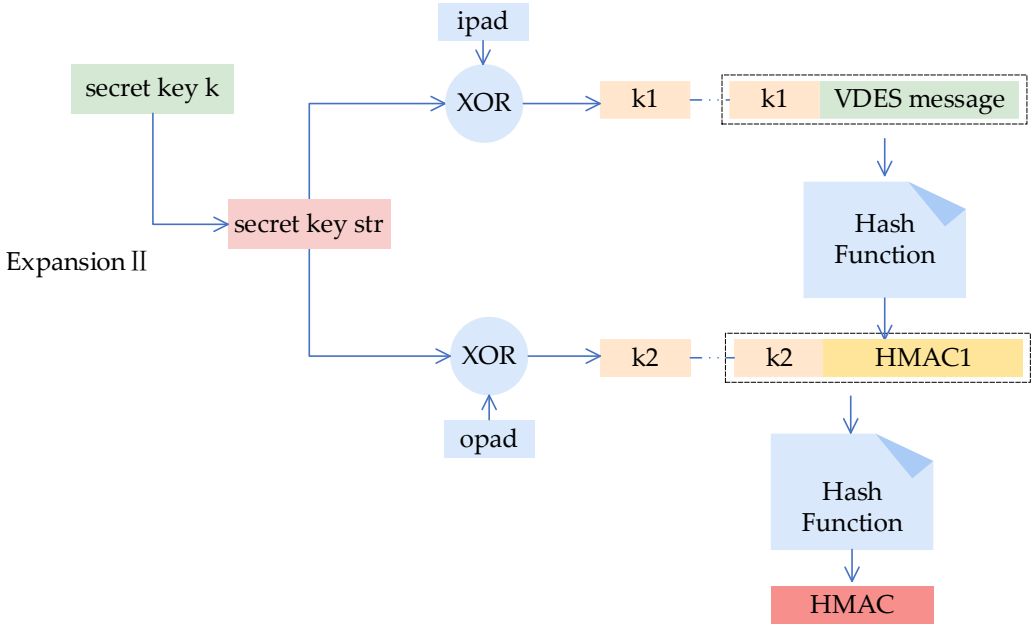


Figure 8. Diagram of the HMAC algorithm computation process.

As crucial fields of the VDES message, such as the MMSI code and message ID, are contained within the first 7 characters of the message, this paper utilizes these characters as the shared key. Subsequently, this key, along with the VDES message, serves as input for the HMAC algorithm. The specific computation process for HMAC is outlined as follows:

Step 1: Input the key k and the VDES message.

Step 2: Pad the key k to obtain a new key, str. Initially, preprocess the key length; if the key length is less than 64 bytes, append zeros to extend it to 64 bytes, forming the new key str. If the key length exceeds 64 bytes, utilize the hash value of key k as the new key k, then append zeros to the hash value until it reaches 64 bytes, resulting in the new key str.

Step 3: Perform internal hash operations. XOR the new key str obtained in Step 2 with the hexadecimal constant ipad (i.e., 0X36) to derive the string k1. Append the VDES message to the string k1 and hash the concatenated result to generate HMAC1.

Step 4: XOR the new key str obtained in Step 2 with the hexadecimal constant opad (i.e., 0X5c) to obtain the string k2. Append HMAC1 to k2 and hash the combined result to produce the final HMAC value for the VDES message.

Following these procedures, calculate the HMAC value for the link management messages broadcast by the VDES base station in TDB format and for the messages received again by the base station after being automatically relayed by VDES ship stations using VEM statements. If the two values match, it indicates that the VDES message remained unaffected by radio interference in the data link, ensuring message integrity verification. Conversely, if the values differ, it suggests that radio interference during transmission led to inconsistencies in the message content. By employing these criteria, consistency checks for the transmission of messages between VDES base stations can be facilitated.

Building upon the verification of data integrity in VDES messages, potential radio interference in the VDES data link can be detected by assessing the consistency of message exchanges between base stations. In this section, the VDES base station broadcasts link management messages in TDB format, such as "!ABTDB,1,1,0,A,403sooQvMSfR0W`0B4@qWO400D0E,0*34". After being automatically relayed by ship stations using VEM statements, this message was received again by the VDES base station as "!AIVEM,1,1,0,A,403sooQvMSfR0`JAhH=Tdp400D0E,0*5D". The HMAC algorithm was employed to calculate the HMAC values of these two messages,

revealing the consistency of message exchange between VDES base stations, as depicted in Figure 9.

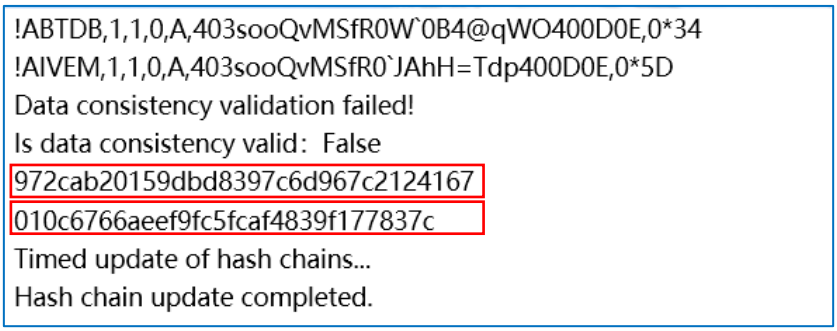


Figure 9. Results of failed verification of message consistency between VDES base stations.

The simulation environments in Figure 9 employs the C# language within Visual Studio 2019 in Windows11 operating system environment. From Figure 9, it is evident that the HMAC value of the link management message broadcast by the VDES base station in TDB format is 972cab20159dbd8397c6d967c2124167, while the HMAC value of the message received again by the base station is 010c6766aeef9fc5fcaf4839f177837c. The inconsistency between these HMAC values indicates that the VDES messages encountered transmission errors due to radio interference in the data link. This demonstrates the effectiveness of the HMAC algorithm in verifying the consistency of message content exchanged by VDES base stations.

At a particular moment, if the message received again by the VDES base station after being relayed by a ship station is "!AIVEM,1,1,0,A,403sooQvMSfR0W`0B4@qWO400D0E,0*33", the HMAC value for this message can be calculated using the HMAC algorithm to yield the results of the consistency check for message exchanges, as shown in Figure 10.

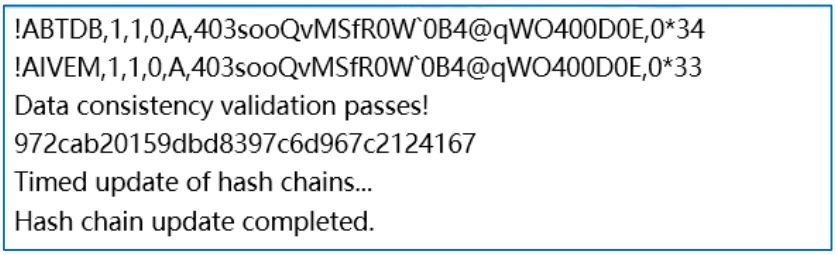


Figure 10. Results of successful verification of message consistency between VDES base stations.

The simulation environments in Figure 10 employs the C# language within Visual Studio 2019 in Windows 11 operating system environment. Illustrated in Figure 10, the congruence of HMAC values between link management messages originating from the VDES base station via TDB statements and those relayed by VDES ship stations using VEM statements—subsequently re-captured by the base station—underscores a uniformity represented by the value 972cab20159dbd8397c6d967c2124167. This consistency serves as evidence that VDES communications endure unscathed amidst the challenges posed by wireless radio interference in the data link, a conclusion substantiated through meticulous assessments of message coherence. Consequently, this outcome affirms the efficacy of the HMAC algorithm in fortifying message integrity throughout VDES base station transmissions.

In summary, employing a wireless radio interference detection mechanism grounded in message attributes facilitates a robust surveillance framework designed to pinpoint vul-

nerabilities associated with radio interference within the VDES data network. By rigorously scrutinizing message format adherence, parameter validity, content integrity, and the uniformity of messages during transit and reception, latent risks stemming from radio interference within the VDES data conduit can be efficiently exposed and vigilantly monitored.

2.2. Spoofing Source Identification and Localization Method Based on Distance Matching Analysis

Due to the lack of encryption in the messages broadcast by VDES base stations and the absence of an identity verification mechanism within VDES itself, malicious entities could deceive vessels within the signal coverage area by illicitly sending false VDES messages using the MMSI code stolen from a legitimate base station. This deceptive practice can mislead vessel navigation decisions, posing a significant threat to maritime safety. Therefore, to ensure the safety of vessel operations, it is imperative to identify and locate any spoofing sources present in the VDES data link. This paper employs a method for spoofing source detection based on distance matching analysis. Specifically, it involves calculating the distances between VDES base stations and vessels by analyzing the message parsing of vessel position coordinates and base station location information. Simultaneously, it utilizes a model for VHF signal propagation loss and receiver power calculations under complex sea surface conditions to determine the propagation distance of VDES signals. By analyzing whether the ship-to-shore distance falls within the tolerance range of the propagation distance, a matching analysis is conducted. If the ship-to-shore distance is within this range, no spoofing source is present; if it exceeds this range, the presence of a spoofing source is inferred. In cases where a spoofing source is identified within the VDES data link, a spoofing source identification algorithm is employed to determine the position or range of the deceptive entity. Thus, through the described methodology, accurate identification and localization of spoofing sources can be achieved.

2.2.1. Method for Calculating VDES Signal Propagation Distance and Ship-to-Shore Distance

VDES is a maritime communication and data exchange system operating within the VHF frequency band. When VHF signals propagate over the sea surface, they typically follow a two-ray model. However, the complexity of the marine environment introduces various factors that influence the transmission loss of VHF signals, including sea surface wind speed, tidal effects, and evaporation ducting. These factors lead to varying degrees of attenuation during signal propagation, subsequently affecting the transmission distance. Therefore, this section considers the complexity of VHF signal propagation in maritime environments and utilizes a model for VHF signal propagation loss under complex sea surface conditions to calculate the transmission distance of VDES signals [36].

Sea surface wind speed primarily affects the transmission loss of VHF reflected signals by altering the sea surface reflection coefficient. When considering sea surface wind speed, the transmission loss of VHF signals is determined as follows [40]:

$$L_W = 32.45 + 20\log r_1 + 20\log f - 10\log\left\{1 + \Gamma_R{}^2 - 2\left|\Gamma_R\right|\cos\left[\frac{\left(8h_t d_2 \mathrm{R} + 8h_r d_1 \mathrm{R} - 3d_1 d_2 d\right)^2}{64\lambda d_1 d_2 d \mathrm{R}^2}\pi\right]\right\} \quad (3)$$

In the equation, r_1 represents the length of the direct wave propagation path; f denotes the frequency in MHz; Γ_R stands for the reflection coefficient; h_t and h_r, respectively, indicate the heights of the transmitting and receiving antennas in meters; d_1 is the horizontal distance from the transmitter to the reflecting point; d_2 is the horizontal distance from the receiver to the reflecting point; E_0 represents the electric field strength at the transmitter; R is the radius of the Earth; d is the propagation distance of the VHF signal; and λ is the wavelength of the VHF signal in meters.

Tidal effects impact the transmission loss of VHF signals by altering both the reflection path length of these signals and the antenna heights of vessels. When considering tidal effects, the transmission loss of VHF signals can be expressed as follows [41]:

$$L_T = 20\log\left\{\frac{2\pi df/c}{\left|\sin\left[2\pi h_t\left(h_r+\Delta h\right)/\left(cd/f\right)\right]\right|}\right\} \tag{4}$$

In the equation, h_t and h_r represent the heights of the transmitting and receiving antennas, respectively, in meters; f denotes the frequency in MHz; Δh is the height change caused by tidal effects; d is the propagation distance of the VHF signal; and c is the speed of light.

Evaporation ducts affect the transmission loss of VHF signals by capturing electromagnetic waves within the duct layer. When considering evaporation ducts, the transmission loss of VHF signals can be expressed as follows [42]:

$$L_{\mathrm{E}} = -10\log 10\left\{\left(\frac{\lambda}{4\pi d}\right)^2\left[2\left(1+\Delta\right)\right]^2\right\} \tag{5}$$

In the equation, λ represents the wavelength of the VHF signal in meters; d denotes the propagation distance of the VHF signal in meters. The expression of Δ in the equation is as follows [42]:

$$\Delta = 2\sin\left(\frac{2\pi h_t h_r}{\lambda d}\right)\sin\left[\frac{2\pi\left(h_e-h_t\right)\left(h_e-h_r\right)}{\lambda d}\right] \tag{6}$$

In the equation, h_t and h_r represent the heights of the transmitting and receiving antennas, respectively, in meters; h_e is the effective duct height; and d is the propagation distance of the VHF signal.

Therefore, considering the influence of hydro-meteorological factors such as sea surface wind speed, tidal water level changes, and evaporation duct height on the transmission of VDES signals, the expression for the transmission loss of VHF signals can be formulated as follows:

$$L_{bR}\left(\left[p_1,p_2,\cdots,p_n\right],d\right) = f\left[L_{bu}\left(d,u\right),L_{b\Delta h}\left(d,\Delta h\right),L_{bh_e}\left(d,T_a,T_s,U,RH\right)\right] \tag{7}$$

In the equation, $\mathrm{P}=[p_1,p_2,\cdots,p_n]$ represents the environmental factor vector, $p_1,p_2,\cdots,p_n$ describes the various parameters of the environmental factors, and $L_{bu}(d,u)$ signifies the transmission loss influenced by sea surface wind speed. u denotes the sea surface wind speed in meters per second. $L_{b\Delta h}(d,\Delta h)$ indicates the transmission loss affected by tidal water level changes. Δh stands for the tidal water level change in meters. $L_{bh_e}(d,T_a,T_s,U,RH)$ represents the transmission loss influenced by evaporation duct height. T_a refers to air temperature in Kelvin. T_s denotes sea surface temperature in Kelvin. U signifies sea surface wind speed in meters per second. RH represents relative humidity, and d is the propagation distance.

To obtain an accurate expression for the propagation loss model, actual measurements of VHF signal reception power were utilized for data fitting using the least squares method. These data were obtained from real experiments conducted by the author's team in the Dalian coastal area, with detailed experimental results available in reference [43]. The propagation loss model for VHF signals in complex sea surface environments, after fitting, is as follows:

$$L_{bR}\left(\left[p_1,p_2,\cdots,p_n\right],d\right) = 0.4873L_{bu}\left(d,u\right)+0.3671L_{b\Delta h}\left(d,\Delta h\right)+0.1417L_{bh_e}\left(d,T_a,T_s,U,RH\right) \tag{8}$$

According to the conclusion in reference [36], the goodness of fit for Equation (8) is 0.9675, indicating a deviation of only 3.3% between the complex sea surface VHF signal transmission loss calculated by this equation and the actual data. This meets the criteria for a good fit, making it suitable for calculating the propagation distance of VDES signals.

As VDES stations regularly report their vessel positions via telegrams, and the location of the VDES base station is known, the calculation of ship-to-shore distance can be accomplished using the Haversine formula. This formula is used to determine the distance between two given latitude and longitude points on Earth, typically measured in nautical miles, kilometers, or miles. This revision improves clarity and coherence while maintaining the original content. Assuming the specific coordinates of the ship and base station are ($lat1$, $lon1$) and ($lat2$, $lon2$), respectively, the expression is as follows:

$$d = 2\mathrm{R}\arctan\left[\frac{\sqrt{hav(lat2-lat1)+\cos(lat1)\cos(lat2)hav(lon2-lon1)}}{\sqrt{1-[hav(lat2-lat1)+\cos(lat1)\cos(lat2)hav(lon2-lon1)]}}\right] \quad (9)$$

In the equation, R represents the radius of the Earth.

2.2.2. Spoofing Sources Localization Method

In this paper, the approach for locating the spoofing sources existing in the VDES data link is to employ the VDES communication signals, and the localization method based on this is the land-based positioning method. When a VDES ship station receives messages from three VDES base stations, the positions of each base station can be considered the centers of circles, with the coverage range of each signal serving as the radius. These circles intersect pairwise. Line MN denotes the common chord formed by the signal coverage circles of Base Stations A and B, and Line EF denotes the common chord formed by the signal coverage circles of Base Stations A and C. By connecting the intersection points of any two circles, three common chords can be derived from the intersections of the three pairs of circles, all converging at a single point, which represents the location of the VDES ship station, as shown in Figure 11.

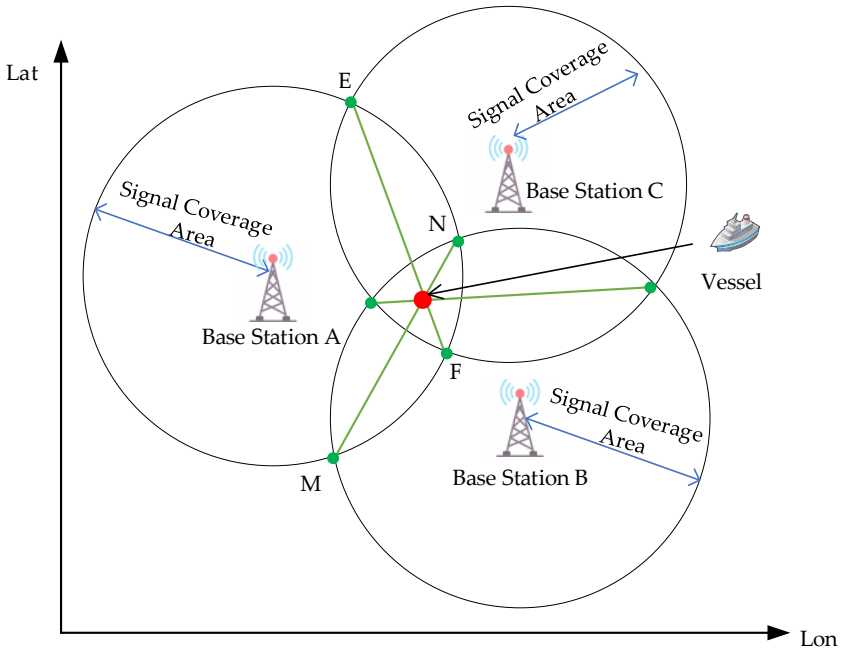


Figure 11. Positioning the vessel by using VDES shore station signals.

Subsequently, the distances between the VDES ship station and each VDES base station are calculated. Using a model for VHF signal propagation loss and received power

under complex sea surface conditions, the propagation distances of the signals from each VDES base station are determined. The analysis then checks whether the ship-to-shore distance falls within the tolerance range of the propagation distance from each base station. If all distances are within this range, there is no indication of a spoofing source; however, if any propagation distance exceeds this range, it suggests the presence of a spoofing source, implying that one of the base station messages is being broadcast by an unauthorized source, as shown in Figure 12.

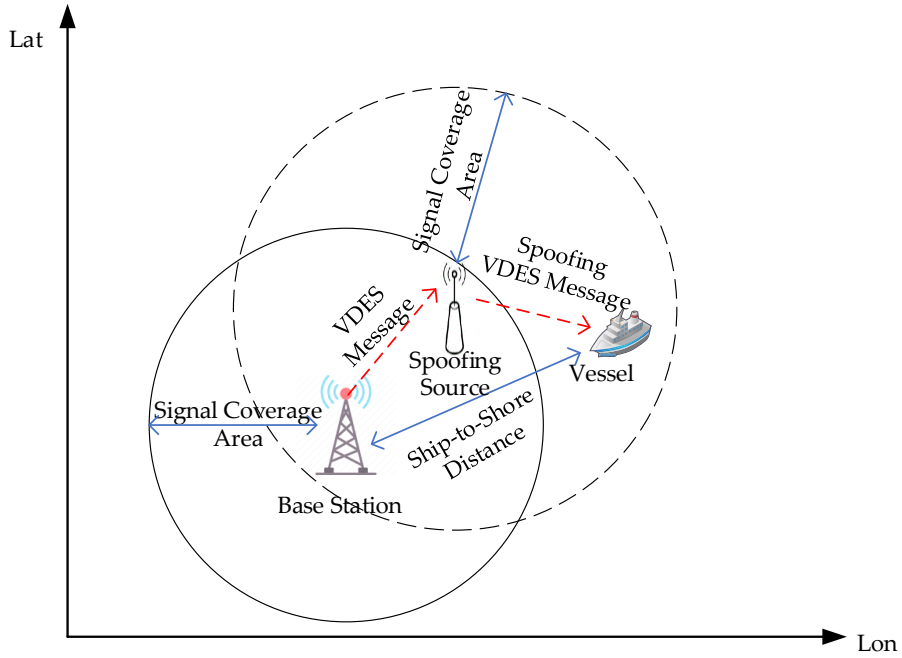


Figure 12. The spoofing source broadcasting the spoofing VDES message.

Upon detecting a spoofing source while monitoring the VDES data link, the VDES ship station, as known information, is used to locate the spoofing source based on the vessel position reported by the VDES shipborne terminal and the two base station positions received by the ship station within the tolerance range. By utilizing the positions of each monitoring station as circle centers with the coverage range of each station's signal as the radius, similar pairwise circle intersections occur. Line EF denotes the common chord formed by the signal coverage circles of Base Stations A and B. Connecting the intersection points of any two circles yields three common chords that converge at a single point, indicating the location of the spoofing source. Therefore, this method accurately identifies the position of the spoofing source, as shown in Figure 13.

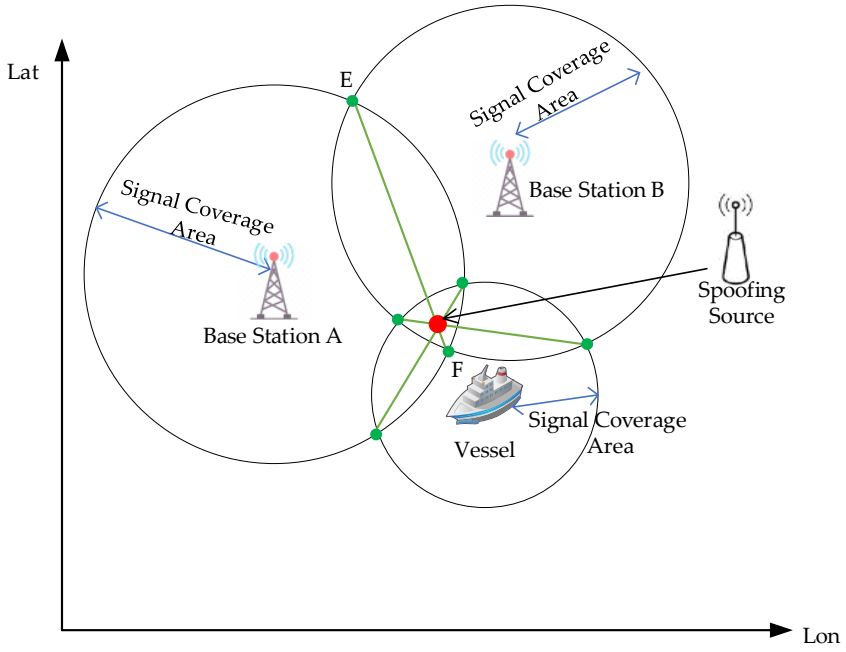


Figure 13. Positioning the spoofing source.

The formula for estimating the location of a spoofing source using a land-based positioning method is as follows:

$$(y_s, x_s) = f_N\left[r_i, i, s_i(y_i, x_i, t)\right]|_{N=1,2,3} \tag{10}$$

In the equation, r_i represents the propagation distance of the *i*-th VDES signal monitoring station, where $i = 1 \ldots N$, with N denoting the number of VDES signal monitoring stations, and s_i indicating the position and timing information of the *i*-th monitoring station.

When $N = 1$, indicating that only one monitoring station receives the message from the spoofing source. The VDES signal propagation distance is calculated using a model for VHF signal propagation loss and received power under complex sea surface conditions. The ship-to-shore distance is then analyzed to determine if it falls within the tolerance range of this propagation distance. If it does, no spoofing source is present in the VDES data link; however, if it exceeds this range, the message from that VDES base station is deemed to originate from a spoofing source, which is uniformly distributed within a circle defined by the VDES signal propagation distance as the radius. The single monitoring station positioning scenario is shown in Figure 14.

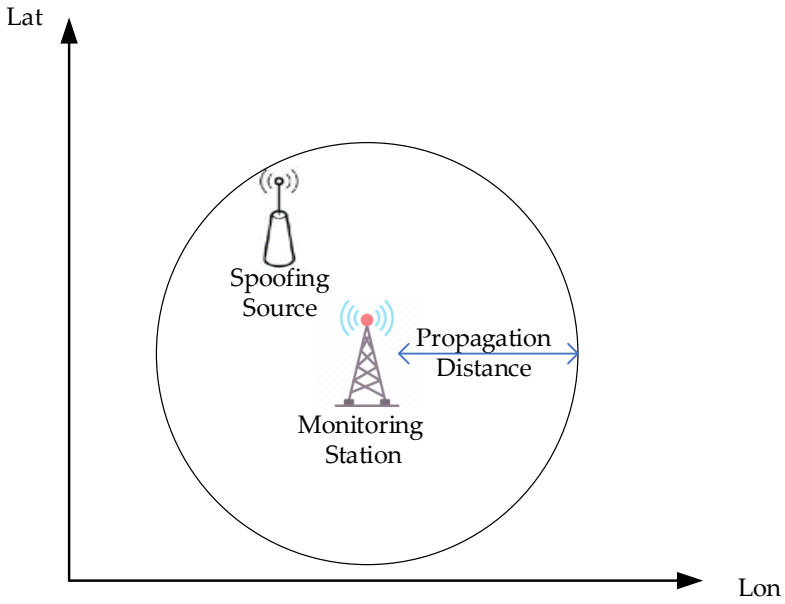


Figure 14. The single monitoring station positioning scenario.

When N = 2, meaning two monitoring stations receive the message from the spoofing source. The propagation distances of the signals from each base station are calculated using the same model for VHF signal propagation loss and received power under complex sea surface conditions. The ship-to-shore distance is analyzed to determine if it falls within the tolerance range of the propagation distance from each base station. If all distances are within this range, no spoofing source exists; if any distance exceeds this range, it indicates that a message from one base station originates from a spoofing source. Upon detecting a spoofing source in the VDES data link, the VDES ship station is used as known information to locate the spoofing source. This is based on the vessel position information reported by the VDES shipborne terminal and the position of one VDES base station within the tolerance range. Considering the positions of the VDES base station and ship station, along with the time difference in message arrival, the spoofing source can be localized uniformly along the circumference of a circle with the VDES base station's position as the center. The two monitoring stations positioning scenario is shown in Figure 15.

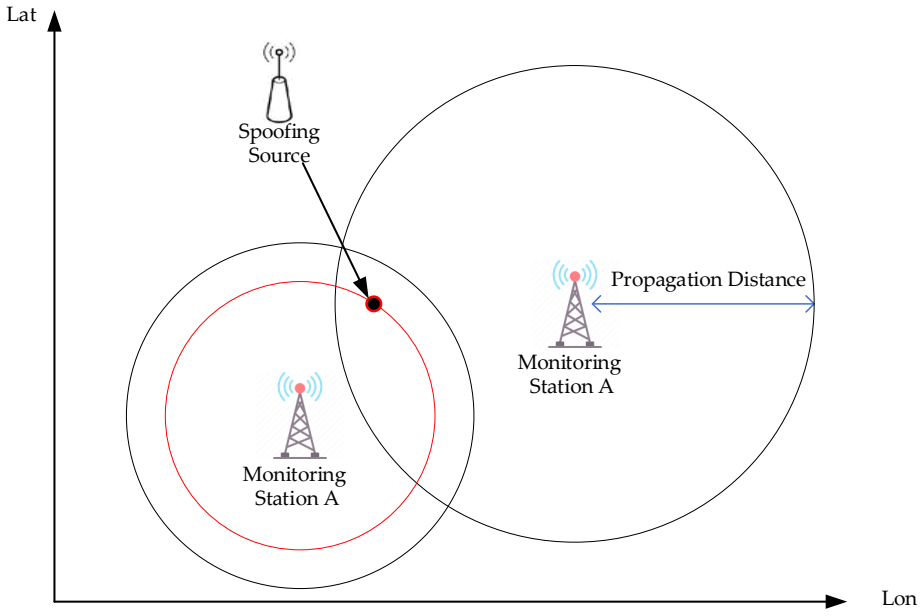


Figure 15. The two monitoring stations positioning scenario.

Assuming the coordinates of monitoring station A are (x_A, y_A), those of monitoring station B are (x_B, y_B), and the coordinates of the spoofing source S are (x_S, y_S); the time difference between the arrival of the VDES message sent by station B to station A and the arrival of the VDES message sent by source S to station A is given by:

$$\Delta t = t_{AS} - t_{AB} \tag{11}$$

In the equation, t_{AS} represents the time at which the VDES message sent by spoofing source S arrives at monitoring station A, and t_{AB} denotes the time at which the VDES message sent by monitoring station B arrives at monitoring station A.

Consequently, the difference Δd between the distance from monitoring station A to monitoring station B and the distance from monitoring station A to spoofing source S is given by:

$$\Delta d = (t_{AS} - t_{AB}) \times c \tag{12}$$

In the equation, t_{AS} represents the time at which the VDES message sent by spoofing source S arrives at monitoring station A, while t_{AB} denotes the time at which the VDES message sent by monitoring station B arrives at monitoring station A, with c representing the speed of light.

The distance Δd_{BS} between monitoring station B and spoofing source S is:

$$\Delta d_{BS} = \sqrt{(x_S - x_B)^2 + (y_S - y_B)^2} \tag{13}$$

In the equation, x_B represents the horizontal coordinate of monitoring station B, y_B represents the vertical coordinate of monitoring station B, x_S represents the horizontal coordinate of spoofing source S, and y_S represents the vertical coordinate of spoofing source S.

In accordance with the definition of a hyperbola, the following is derived:

$$\frac{x_A^2}{\left(\frac{\Delta d}{2}\right)^2} - \frac{y_A^2}{\left(\frac{\Delta d_{BS}}{2}\right)^2 - \left(\frac{\Delta d}{2}\right)^2} = 1 \tag{14}$$

Substituting Equations (12) and (13) into Equation (14) yields the equation for the positional range curve of the spoofing source:

$$\frac{x_A^2}{c^2 (t_{AS} - t_{AB})^2} - \frac{y_A^2}{(x_S - x_B)^2 + (y_S - y_B)^2 - c^2 (t_{AS} - t_{AB})^2} = \frac{1}{4} \tag{15}$$

As per Equation (15), it is evident that the range of the spoofing source's location lies on the circumference with monitoring station B as the center, expressed as follows:

$$(x_S - x_B)^2 + (y_S - y_B)^2 = \frac{(\Delta d)^2 \left[4x_A^2 + 4y_A^2 - (\Delta d)^2 \right]}{4x_A^2 - (\Delta d)^2} \tag{16}$$

When $N \geq 3$, it indicates that three or more monitoring stations are simultaneously receiving the spoofing source message. By treating the positions of each monitoring station as centers and drawing circles with the signal coverage radius of each station, these circles intersect pairwise. The intersection points of two circles form common chords. From the intersections of three pairs of circles, three common chords can be derived, all intersecting at a single point, which represents the location of the spoofing source. The three monitoring stations positioning scenario is shown in Figure 16.

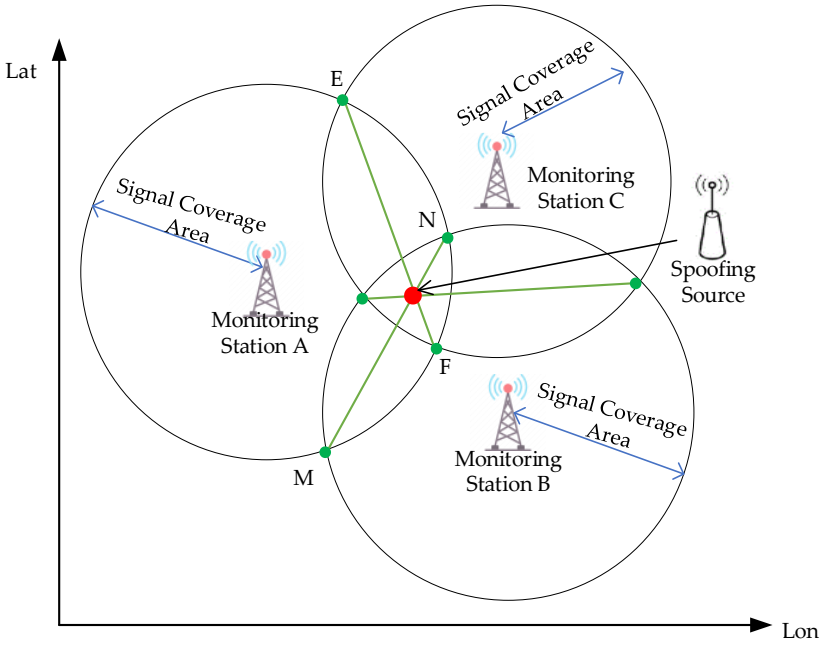


Figure 16. The three monitoring stations positioning scenario.

We assume the coordinates of monitoring station A are (x_A, y_A), monitoring station B are (x_B, y_B), and monitoring station C are (x_C, y_C), with O (x_O, y_O) being the midpoint of stations A and B, where $x_O = \frac{x_A + x_B}{2}$ and $y_O = \frac{y_A + y_B}{2}$, and r represents the signal coverage radius of the VDES monitoring stations. Consequently, the intersections of the signal coverage circles of stations A and B result in two points, E (x_E, y_E) and F (x_F, y_F). The line connecting intersection point E and intersection point F is termed the common chord EF. The half-length r_{ef} of the common chord EF is determined as follows:

$$r_{ef} = \sqrt{r^2 - \left[\frac{\sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}}{2}\right]^2} \tag{17}$$

The slope $k_{AB} = \frac{y_A - y_B}{x_A - x_B}$ of the line connecting monitoring stations A and B can be used to determine the slope k_{EF} of the common chord EF.

$$k_{EF} = -\frac{1}{k_{AB}} \tag{18}$$

According to the theorem of intersecting circles, the line connecting the centers of two intersecting circles bisects the common chord of the two circles. Therefore, the distance between point E and point O is equal to half the length of the common chord, expressed as follows:

$$\sqrt{(x_E - x_O)^2 + (y_E - y_O)^2} = r_{ef} \tag{19}$$

The coordinates of the intersection points E and F of the two monitoring stations can be derived from Equation (19) and the slope $k_{EF} = \frac{y_E - y_O}{x_E - x_O}$ of the common chord EF as follows:

$$\begin{cases} x_E = x_O + \sqrt{\dfrac{r_{ef}^2}{1+k_{EF}^2}} \\ y_E = y_O + k_{EF}\left(x_E - x_O\right) \end{cases}, \quad \begin{cases} x_F = x_O - \sqrt{\dfrac{r_{ef}^2}{1+k_{EF}^2}} \\ y_F = y_O + k_{EF}\left(x_F - x_O\right) \end{cases} \tag{20}$$

This yields the expression for the common chord EF between monitoring stations A and B as follows:

$$y = -\frac{1}{k_{AB}}x + y_E + \frac{1}{k_{AB}}x_E \tag{21}$$

By utilizing the method for determining the common chord EF between monitoring stations A and B, the expression for the common chord MN between monitoring stations B and C can be derived as follows:

$$-\frac{x_B - x'}{y_B - y'} \times x_C + \frac{y_B + y'}{2} + \frac{x_B - x'}{y_B - y'} \times \frac{x_B + x'}{2} = y_C \tag{22}$$

In the equation, x' represents the abscissa of any point on the common chord MN between monitoring stations B and C, y' denotes the ordinate of any point on MN, x_B represents the abscissa of monitoring station B, y_B signifies the ordinate of B, x_C stands for the abscissa of monitoring station C, and y_C denotes the ordinate of C.

With Equations (21) and (22), the position (x_S, y_S) of the spoofing source S can be determined as follows:

$$\begin{aligned} x_S &= \frac{-a + \sqrt{a^2 - 4\times\left[1-\left(\dfrac{x_A - x_B}{y_A - y_B}\right)^2\right]\times\left[\dfrac{4y_B\left(y_A - y_B\right)\left(x_A^2 - x_B^2\right) - \left(y_A^2 - y_B^2 + x_A^2 - x_B^2\right)^2}{4\left(y_A - y_B\right)^2} - 2x_C x_B - x_B^2 + y_A y_B\right]}}{2\left[1-\left(\dfrac{x_A - x_B}{y_A - y_B}\right)^2\right]}, \\ y_S &= \frac{-b + \sqrt{b^2 - 4\left[\left(\dfrac{y_A - y_B}{x_A - x_B}\right)^2 - 1\right]\left[-3x_B x_C - x_A x_C - x_B^2 - y_B^2 - \dfrac{4x_C\left(x_A - x_B\right)\left(y_A^2 - y_B^2\right) + y_A^2 - y_B^2 + x_A^2 - x_B^2}{4\left(x_A - x_B\right)^2}\right]}}{2\left[\left(\dfrac{y_A - y_B}{x_A - x_B}\right)^2 - 1\right]} \end{aligned} \tag{23}$$

where $a = \dfrac{\left[-\left(y_A - y_B\right)^2 - x_A^2 + x_B^2\right]\left(x_A - x_B\right)}{\left(y_A - y_B\right)^2} + 2x_C$, $b = \dfrac{\left[\left(2x_C - x_A - x_B\right)\left(x_A - x_B\right) - y_A^2 + y_B^2\right]\left(y_A - y_B\right)}{\left(x_A - x_B\right)^2} + 2y_B$.

2.2.3. Experimental Testing and Results Analysis

To assess the detection capability of the spoofing source identification and localization method based on distance matching analysis against deceptive threats in the VDES data link, various experimental scenarios were conducted in this section to validate and analyze the proposed design method.

I. Spoofing Source Detection Experiment

(a) No Spoofing Source Detected

At a certain moment, the VDES ship station received a message from a VDES base station, which read: "!ABTDB,1,1,0,A,403sooQvN<?W<`Gtj0FG9hG00D0c,0*5C". Upon

decoding, the location information of the VDES base station was identified as (39°4.8′ N, 117°4.8′ E), as illustrated in Figure 17, according to the experimental results.

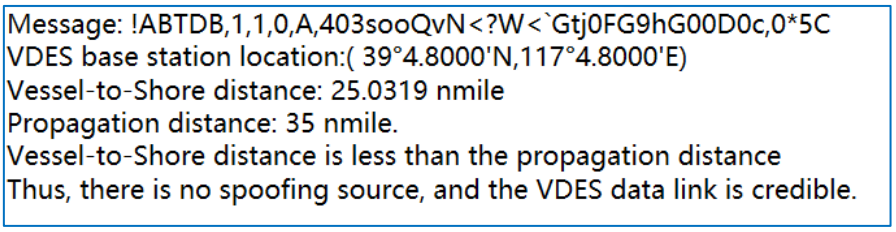


Figure 17. Simulation results of testing for the absence of spoofing sources based on Visual Studio 2019.

The simulation environment in Figure 17 employs the C# language within Visual Studio 2019 in a Windows 11 operating system environment. As shown in Figure 17, when the VDES ship station is located at (38°54.594′ N, 117°34.146′ E), the ship-to-shore distance calculated using Equation (9) is 25.0319 nautical miles. At this moment, with a wind speed of 10 m/s, a sea surface temperature of 15 °C, a tidal level of 0.3 m, and relative humidity of 50%, the received signal power at the VDES ship station is −70 dBm. Consequently, the VDES signal propagation distance, calculated using Equation (8), is 35 nautical miles. Since the ship-to-shore distance is less than the VDES signal propagation distance, the VDES ship station can successfully receive messages from the VDES base station, indicating the absence of a spoofing source in the VDES data link. Therefore, at this point, the VDES data link can be considered credible.

(b) Spoofing Source Detected

At a certain moment, the VDES ship station received a message from a VDES base station, which read: "!ABTDB,1,1,0,A,403sooQvN<?W<`Gtj0FG9hG00D0c,0*5C". Upon decoding, the location information of the VDES base station was identified as (39°4.8′ N, 117°4.8′ E), as illustrated in Figure 18, according to the experimental results.

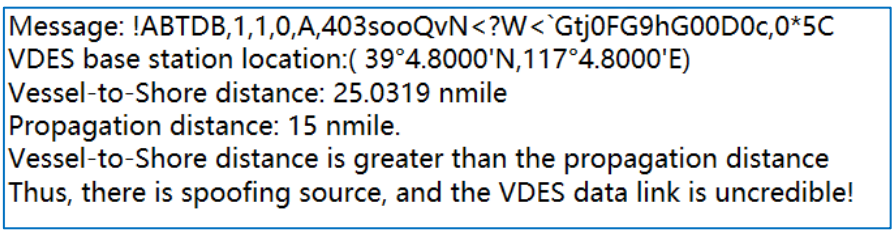


Figure 18. Simulation results of spoofing source detection based on Visual Studio 2019.

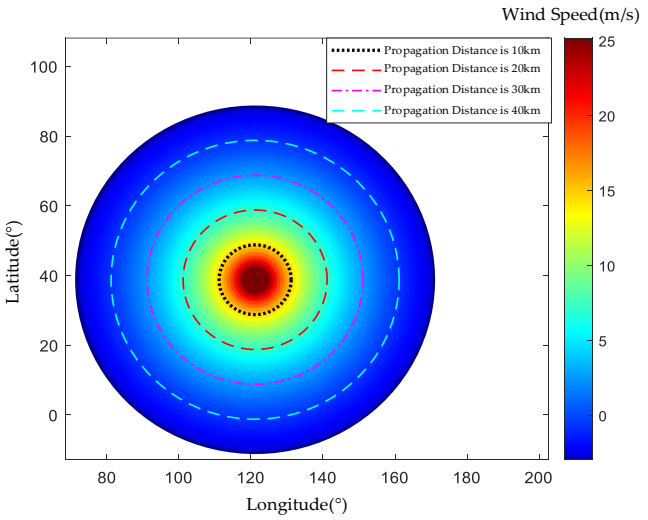
The simulation environments in Figure 18 employs the C# language within Visual Studio 2019 in a Windows 11 operating system environment. As shown in Figure 18, when the VDES ship station is located at (38°54.594′ N, 117°34.146′ E), the ship-to-shore distance calculated using Equation (9) is 25.0319 nautical miles. At this moment, with a wind speed of 15 m/s, a sea surface temperature of 16 °C, a tidal level of 0.1 m, and relative humidity of 67%, the received signal power at the VDES ship station is −70 dBm. Consequently, the VDES signal propagation distance, calculated using Equation (8), is 15 nautical miles. Since the ship-to-shore distance exceeds the VDES signal propagation distance, the VDES ship station is unable to receive the message sent by the VDES base station. This establishes that the VDES message received by the VDES ship station originates from a spoofing source, indicating the presence of a spoofing threat in the VDES data link. Therefore, at this point, the VDES data link is not considered credible.

II. Spoofing Source Localization Experiment

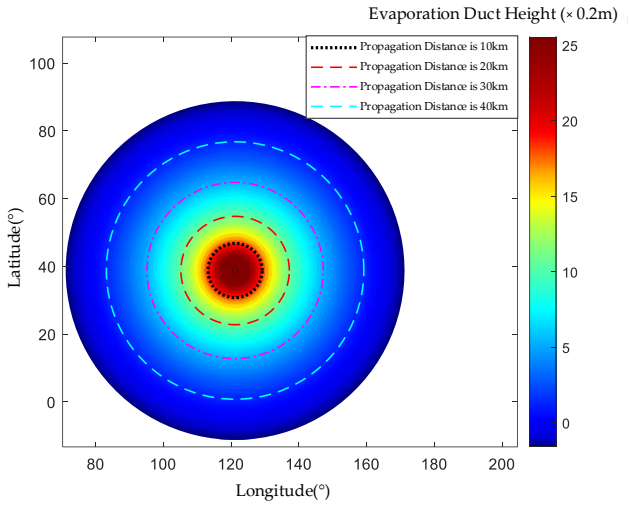
In this section, the range and position of the spoofing source were determined using a localization algorithm that analyzes the reception of deceptive messages by one, two, and three monitoring stations. For the case of a single monitoring station, variations in the coverage of VDES signals under different sea conditions were examined to establish the potential location range of the spoofing source. In the scenario involving two monitoring stations, the positions of each station and the time differences in signal arrival were utilized, along with the coverage of VDES signals, to track the position trajectory of the spoofing source. When three monitoring stations were employed, a cross-location method was used to accurately pinpoint the position of the spoofing source.

(1) Localization of Spoofing Sources by Single Monitoring Stations

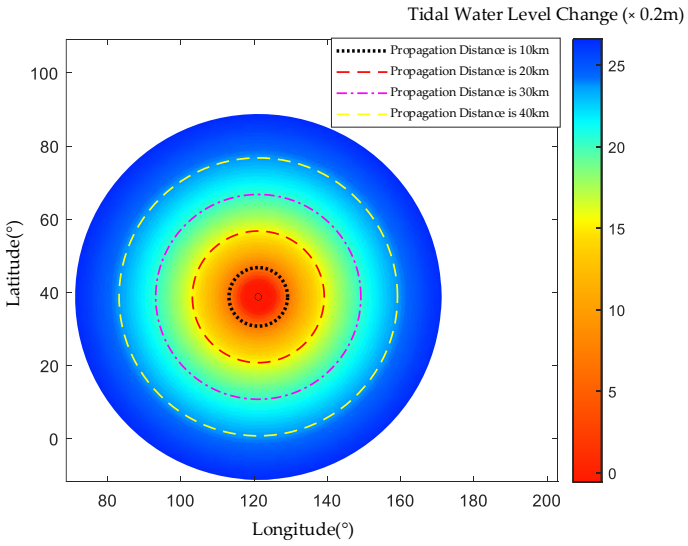
When only one monitoring station receives a deceptive message, the spoofing source is uniformly distributed within a range defined by the propagation distance of the VDES signal. Taking into account the influence of hydro-meteorological factors—such as sea surface wind speed, tidal level variations, and evaporation duct height—on the signal propagation distance from the VDES base station, the positions of the spoofing source were determined under different sea conditions for received powers of −83 dBm, −77 dBm, −69 dBm, and −60 dBm. The results, indicating the possible locations of the spoofing source, are illustrated in Figure 19.



(**a**) Wind speed: 1 m/s, 5 m/s, 10 m/s, 15 m/s



(**b**) Evaporating duct height: 1 m, 2 m, 3 m, 4 m



(**c**) Tidal water level change: 1 m, 2 m, 3 m, 4 m

Figure 19. Results of spoofing source localization by a single monitoring station.

Figure 19a shows the equal probability distribution of the spoofing source in a circle with varying propagation distances as the radius, under different wind speed conditions. It also depicts the variation of the spoofing source location across different VDES signal propagation distances when the wind speeds are 1 m/s, 5 m/s, 10 m/s, and 15 m/s, respectively. When the wind speed is 1 m/s and the received signal power is −83 dBm, the VDES signal propagation distance is 40 km; thus, the spoofing source is located within a circle centered on the VDES monitoring station, with a radius of 40 km, reflecting an equal probability distribution. When the wind speed increases to 5 m/s and the received signal power is −77 dBm, the propagation distance decreases to 30 km, resulting in the spoofing source being located within a circle of 30 km radius centered on the monitoring station. For a wind speed of 10 m/s and a received signal power of −69 dBm, the VDES signal propagation distance is 20 km, placing the spoofing source within a circle of 20 km radius centered on the monitoring station. Finally, when the wind speed reaches 15 m/s and the received signal power is −60 dBm, the propagation distance is 10 km, and the spoofing source is located within a circle of 10 km radius centered on the VDES monitoring station, maintaining an equal probability distribution.

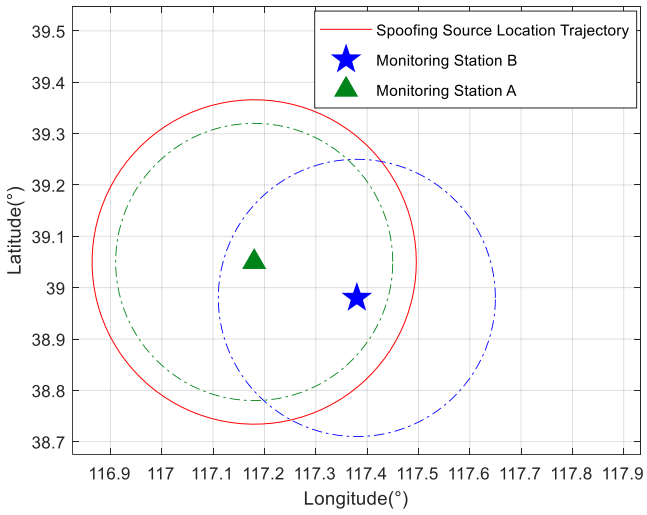
Figure 19b illustrates that, under different evaporating waveguide heights, the spoofing source is distributed with equal probability in a circle with varying propagation distances as the radius. It also shows the variation of the spoofing source location across different VDES signal propagation distances for evaporating waveguide heights of 1 m, 2 m, 3 m, and 4 m. When the evaporating waveguide height is 1 m and the received signal power is −83 dBm, the VDES signal propagation distance is 40 km; at this time, the spoofing source is located in a circle centered on the VDES monitoring station, with an equal probability distribution within a radius of 40 km. When the evaporating waveguide height is increased to 2 m and the received signal power is −77 dBm, the propagation distance decreases to 30 km, placing the spoofing source in a circle with a radius of 30 km centered on the monitoring station. At an evaporating waveguide height of 3 m and a received signal power of −69 dBm, the VDES signal propagation distance is 20 km, which means the spoofing source is located within a circle of 20 km radius centered on the VDES monitoring station. Finally, when the evaporating waveguide height is 4 m and the received signal power is −60 dBm, the propagation distance remains 10 km, positioning the spoofing source in a circle centered on the monitoring station with a radius of 10 km, maintaining an equal probability distribution.

Figure 19c illustrates the equal probability distribution of the spoofing source within a circle defined by varying propagation distances under different tidal water level heights. It also shows the changes in the spoofing source location across different VDES signal propagation distances when the tidal water level is 1 m, 2 m, 3 m, and 4 m, respectively. When the tidal water level is 1 m and the received signal power is −60 dBm, the VDES signal propagation distance is 10 km; at this time, the spoofing source is located within a radius of 10 km, centered on the VDES monitoring station. When the tidal water level rises to 2 m and the received signal power is −69 dBm, the propagation distance increases to 20 km, placing the spoofing source in a circle of 20 km radius centered around the VDES monitoring station. For a tidal water level of 3 m and a received signal power of −77 dBm, the VDES signal propagation distance is 30 km, which means the spoofing source is located within a circle of 30 km radius centered on the monitoring station. Finally, when the tidal water level reaches 4 m and the received signal power is −83 dBm, the VDES signal propagation distance is 40 km, positioning the spoofing source within a circle of 40 km radius centered on the VDES monitoring station, maintaining an equal probability distribution.

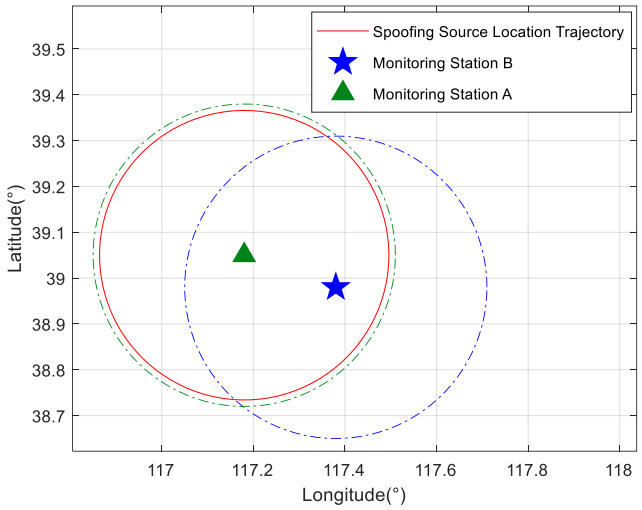
(2) Spoofing Source Localization Using Two Monitoring Stations

When two monitoring stations simultaneously receive signals from the spoofing source, the position trajectory of the spoofing source can be determined based on the positional information of both monitoring stations and the time difference in signal arrival. Assuming monitoring station A is located at (38°58.8′ N, 117°22.8′ E) and monitoring station B is at (39°3′ N, 117°10.8′ E), the trajectory of the spoofing source can be established. Under conditions of a sea surface wind speed of 10 m/s, a tidal water level variation of 0.2 m, an evaporation duct height of 0.1 m, and received powers of −61 dBm, −68 dBm, −75 dBm, and −82 dBm, the positioning results of the spoofing source at VDES signal propagation distances of 10 km, 20 km, 30 km, and 40 km calculated using Equation (8) are depicted in Figure 20.

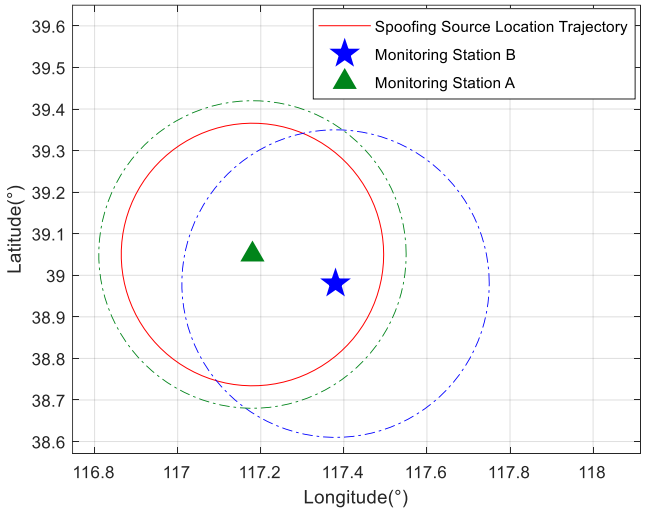
From Figure 20, it is evident that at VDES signal propagation distances of 10 km, 20 km, 30 km, and 40 km, the range of the spoofing source's location exhibits an equal probability distribution along the circumference, with monitoring station A (38°58.8′ N, 117°22.8′ E) as the center.



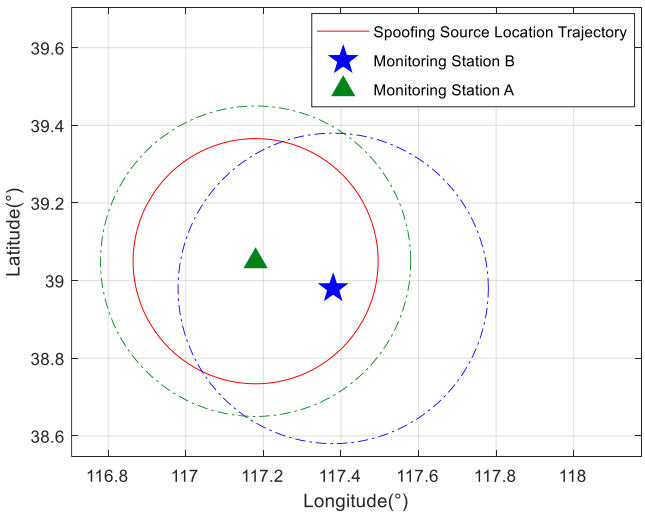
(**a**) The VDES signal propagation distance is 10 km



(**b**) The VDES signal propagation distance is 20 km



(**c**) The VDES signal propagation distance is 30 km



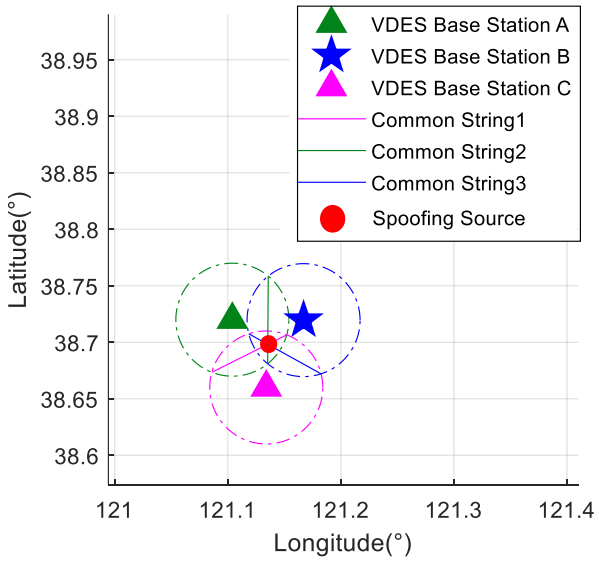
(**d**) The VDES signal propagation distance is 40 km

Figure 20. Results of spoofing source localization by a two monitoring stations.

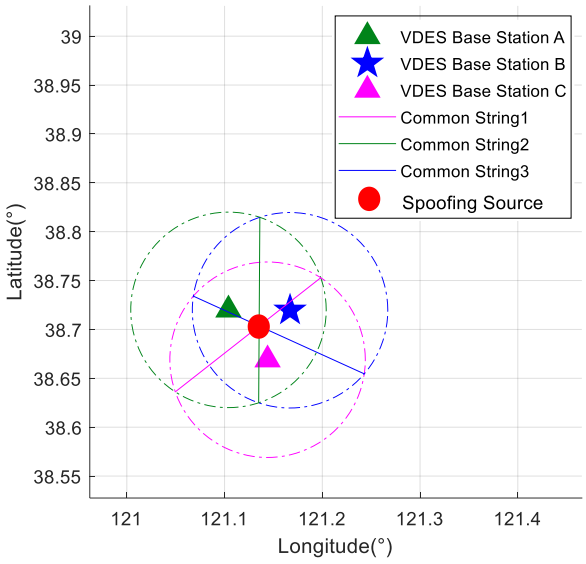
(3) Spoofing Source Localization with Three Monitoring Stations

When three or more monitoring stations simultaneously receive signals from the spoofing source, circles are constructed with the positions of each monitoring station as centers and the VDES signal coverage ranges as radii. These circles intersect pairwise, and the common chord of two intersecting circles is used to determine the location of the spoofing source. Assuming monitoring station A is positioned at (38°43.2′ N, 121°6.24′ E) and monitoring station B is located at (38°43.176′ N, 121°10.02′ E), under conditions of a sea surface wind speed of 10 m/s, a tidal water level variation of 0.2 m, an evaporation duct height of 0.1 m, and received powers of −61 dBm, −68 dBm, −75 dBm, and −82 dBm, the positioning results of the spoofing source at VDES signal coverage ranges of 10 km, 20 km, 30 km, and 40 km calculated using Equation (8) are illustrated in Figure 21.

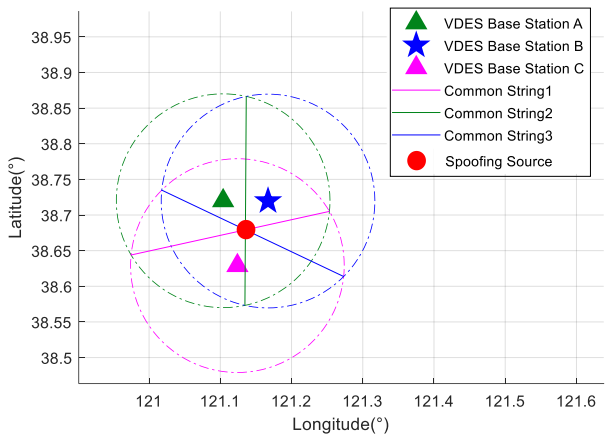
In Figure 21a, the position of monitoring station C is (38°39.6′ N, 121°8.04′ E). With a VDES signal coverage range of 10 km, the location of the spoofing source determined based on the positions of each monitoring station and the signal coverage range is (38°41.8909′ N, 121°8.1217′ E). In Figure 21b, with monitoring station C at (38°40.14′ N, 121°8.64′ E) and a VDES signal coverage range of 20 km, the spoofing source location is (38°42.2063′ N, 121°8.1238′ E). In Figure 21c, when monitoring station C is at (38°37.74′ N, 121°7.44′ E) with a coverage range of 30 km, the spoofing source is located at (38°40.7501′ N, 121°8.1145′ E). Finally, in Figure 21d, with monitoring station C at (38°36.54′ N, 121°8.04′ E) and a coverage range of 40 km, the spoofing source is determined to be at (38°40.1323′ N, 121°8.1106′ E).



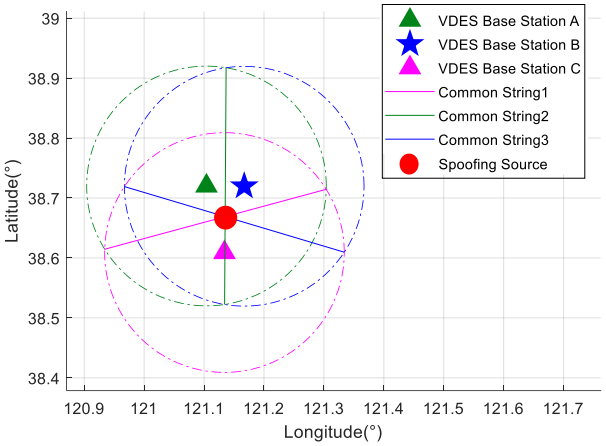
(**a**) The VDES coverage range is 10 km



(**b**) The VDES coverage range is 20 km



(**c**) The VDES coverage range is 30 km



(**d**) The VDES coverage range is 40 km

Figure 21. Results of spoofing source localization by a three monitoring stations.

In summary, the method of spoofing source identification and localization based on distance matching analysis effectively detects threats from spoofing sources in the VDES data link. It enables the determination of the range and location of spoofing sources based on the varying number of monitoring stations capable of receiving deceptive signals.

3. Design of Software for Monitoring VDES Data Link Credibility

Based on the analysis of the VDES data link integrity monitoring method, a VDES data link integrity monitoring system was constructed in this study. The implementation process of the system algorithm is illustrated in Figure 22, and the effectiveness of this system in practical scenarios was validated through various interference setups.

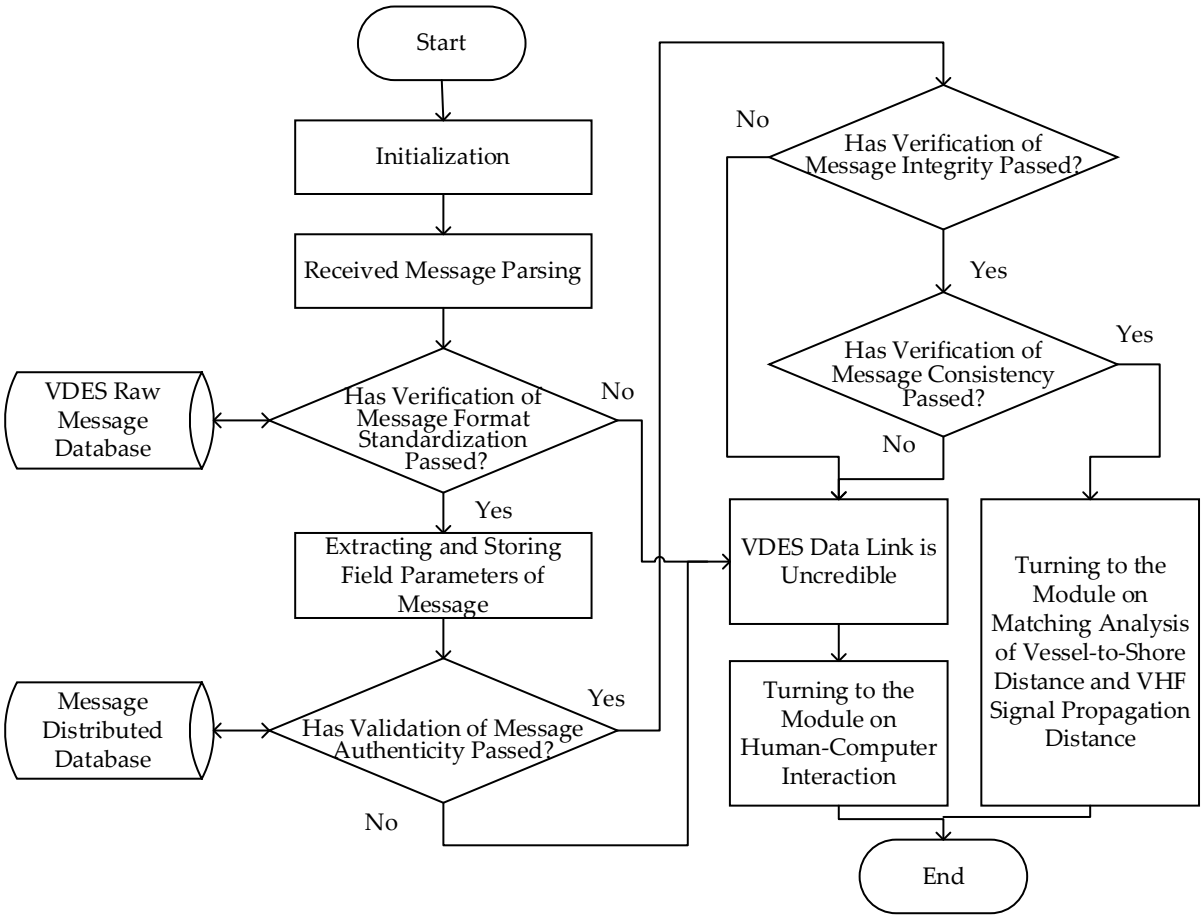


Figure 22. Algorithmic flowchart for a VDES data link credibility monitoring system based on a combined detection method.

According to Figure 22, the VDES data link integrity monitoring system initiates the initialization of system parameters. Subsequently, the system parses the messages received by the VDES base station and verifies the conformity of the message format with the VDES raw message database. If the received message format does not align with the stored formats in the database, leading to unsuccessful parsing, it is determined that the content of the VDES message is corrupted due to radio interference. This results in an output indicating an untrusted monitoring result for the VDES data link. Conversely, if the formats match, allowing for successful parsing of the received message, the system proceeds to verify the legitimacy of the message parameters. It extracts and stores the message field parameters, then cross-references these with the legitimate message parameters previously sent by the base station and stored in the AIS/VDES message distributed database. If discrepancies exist between the VDES message parameters and the legitimate AIS/VDES message parameters, it is concluded that the content of the VDES message has been disrupted by interference, resulting in an untrusted monitoring outcome for the VDES data link. Should all parameters align, the system verifies the integrity of the message content. This integrity verification process utilizes the MD5 algorithm to calculate the hash values of the received VDES message and the legitimate messages previously received from the ship station, as stored in the VDES raw message database. If the hash values do not match, indicating incomplete content in the VDES message due to radio interference, the system outputs an untrusted monitoring result. Conversely, if the hash values match, the system proceeds to verify the consistency of the message content, entering the subsequent step of checking consistency between sent and received messages. This consistency check utilizes the HMAC algorithm to calculate the HMAC values of the TDB statement message and the VEM statement broadcast message. If the HMAC values do

not match, it is inferred that the message content has been tampered with due to interference, indicating the presence of radio interference in the VDES data link, and resulting in an untrusted monitoring outcome. Conversely, if the HMAC values match, the system continues to the consistency check of sent and received messages, initiating the spoofing source identification process. Spoofing source identification employs an analysis method comparing the distance between ships and shore with the propagation distance of VDES signals. The ship-to-shore distance is calculated using the Haversine formula, based on the vessel position information reported by the VDES onboard terminal and the base station's position. Simultaneously, the VDES signal propagation distance is calculated using a model of VHF signal propagation losses in complex maritime environments and received power calculations. The analysis determines if the ship-to-shore distance falls within the tolerance range of the propagation distance. If it is within this range, it signifies the absence of a spoofing source in the VDES data link, resulting in a trusted monitoring outcome. If it exceeds this range, the presence of a spoofing source within the VDES data link is concluded, leading to an untrusted monitoring result and initiating the spoofing source localization process. Through the spoofing source localization algorithm, the position or range of the spoofing source is determined.

Following the algorithmic processes outlined above, this study utilized Visual Studio 2019 as the development software, based on the SQL Server database, and employed C# as the primary programming language to design the VDES data link integrity monitoring system. Built on the C/S model, the system features a layered architecture comprising the data acquisition layer, business logic layer, and frontend display layer, as depicted in Figure 23.

As illustrated in Figure 23, the C/S model facilitates communication between VDES base stations and ship stations. The data acquisition layer integrates components such as web crawlers, power detectors, VDES receivers, and communication networks, forming the entire data collection segment. At the core of the system is the business logic layer, which encompasses modules for data storage, data processing, and VDES data link integrity monitoring. Specifically, the VDES data processing module operates on the raw VDES message data stored in the SQL Server database, parsing and extracting relevant field parameters, categorizing them into different data tables, and managing message encapsulation for data exchange and communication with VDES ship stations. The VDES data link integrity monitoring module consists of two key components: first, the radio interference detection module, which includes four sub-modules VDES message format conformity verification, VDES message parameter legitimacy verification, VDES message content integrity verification, and consistency checks of sent and received messages—aimed at monitoring radio interference in the VDES data link. Second, the spoofing source identification and localization module comprises sub-modules for spoofing source identification based on ship-to-shore distance and propagation distance matching analysis, as well as for spoofing source localization using specialized algorithms. This enables the identification of spoofing sources within the VDES data link. Finally, the frontend display layer visualizes user login information, received messages, parsed message parameters, message verification results, distance matching analysis results, spoofing source localization records, and VDES data link integrity monitoring results. This allows users to observe and understand the status of VDES data link integrity and receive timely alerts.

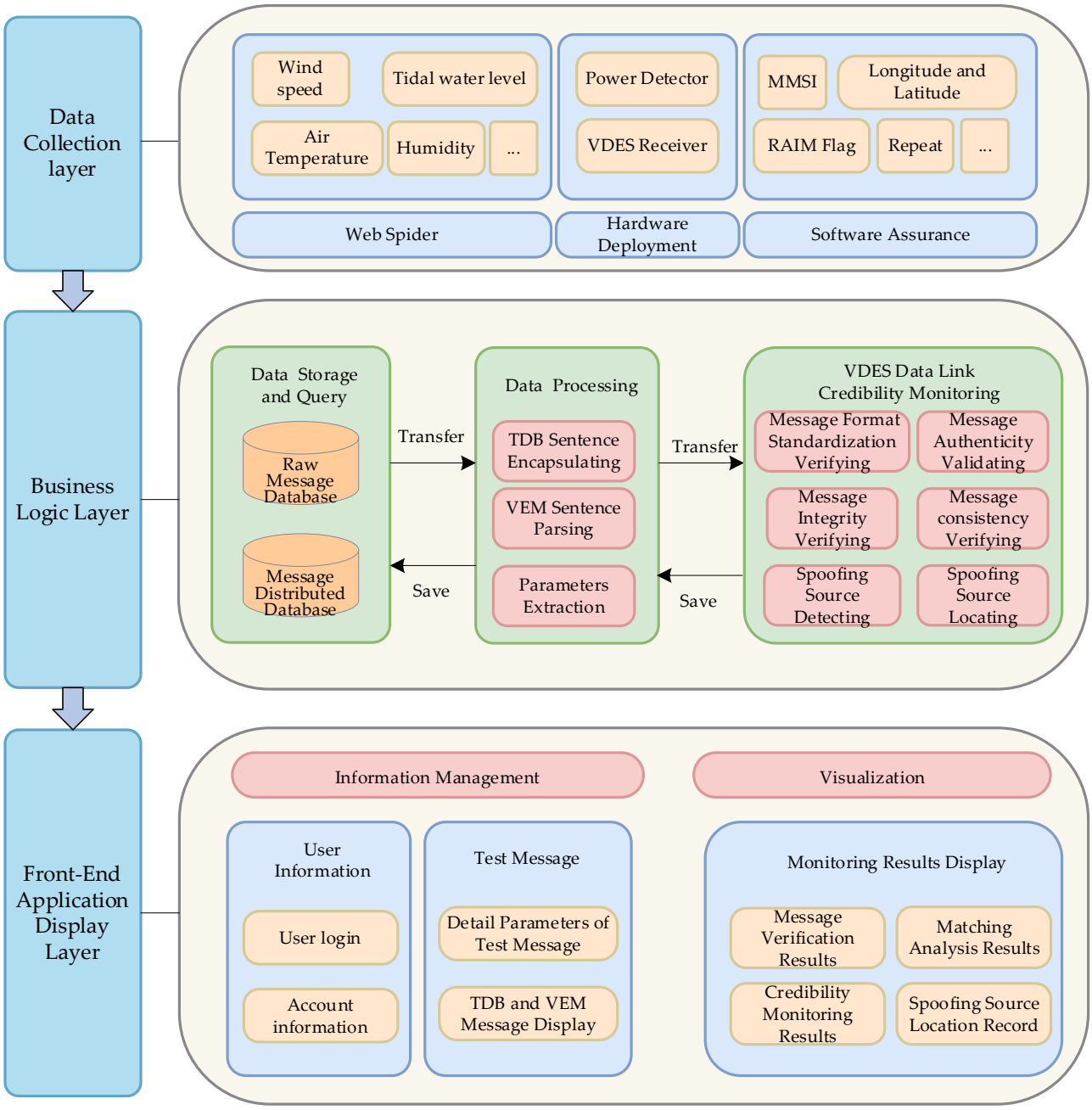


Figure 23. Architectural overview of the VDES data link monitoring system.

Figure 24 depicts the user login interface of the VDES data link integrity monitoring software system.

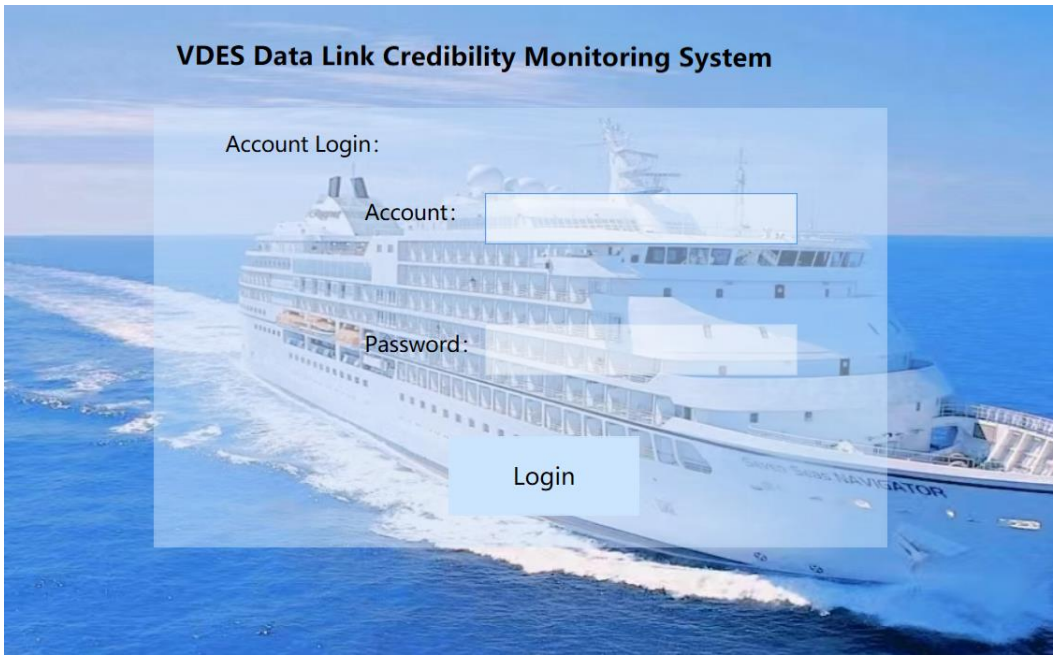


Figure 24. User login interface for the software system.

3.1. Design of Key Modules

The algorithmic process and overall architecture of the VDES data link integrity monitoring system, as shown in Figures 25 and 26, necessitate the implementation of functions such as communication, message processing, and data link integrity monitoring. This section provides a detailed exposition of the design process for the key modules of the system.

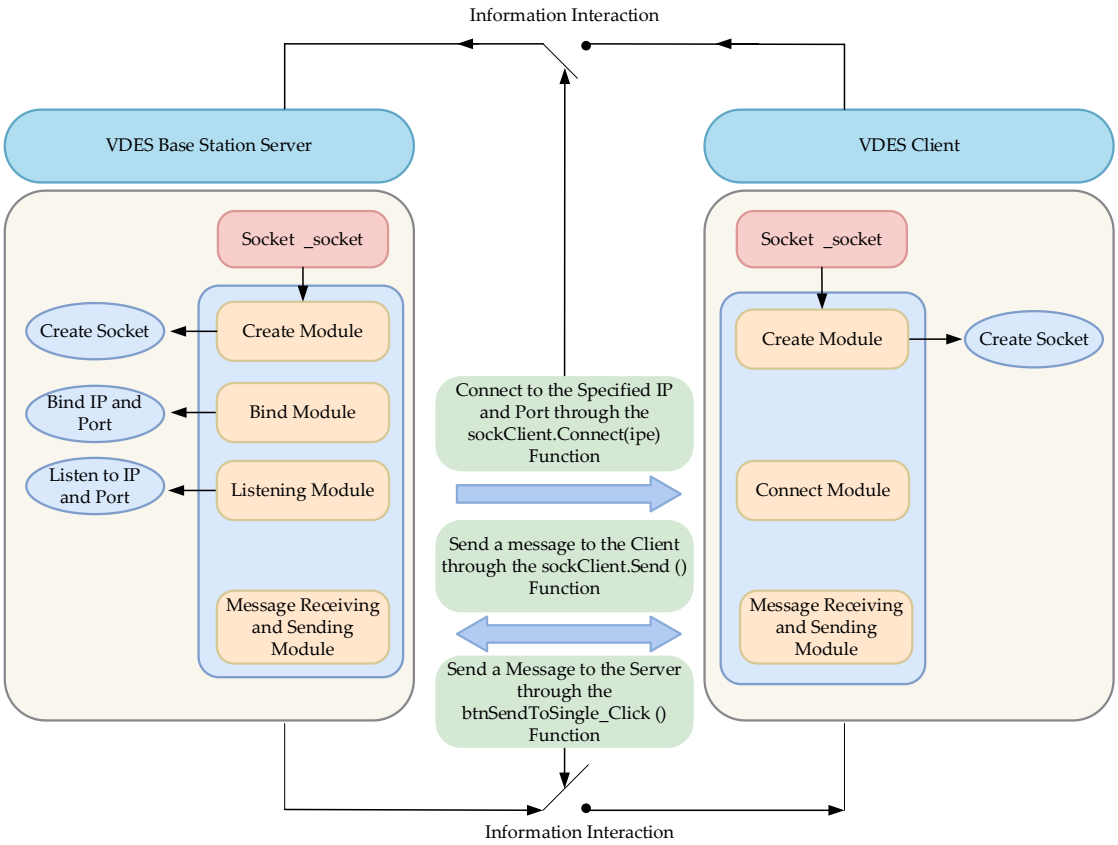
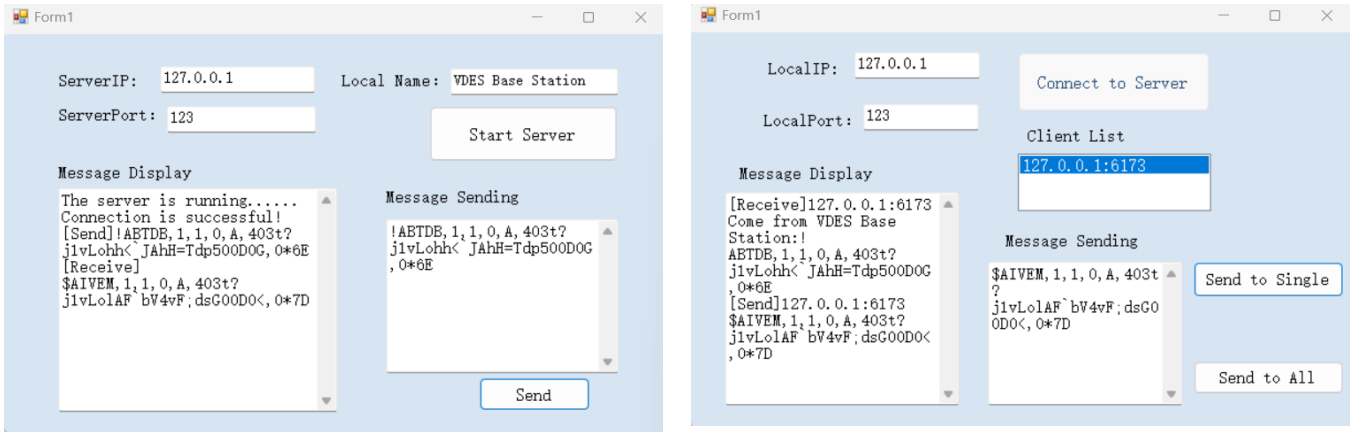


Figure 25. Structural block diagram of the VDES communication module.



(**a**) Verification of Server Communication Function (**b**) Verification of Client Communication Function

Figure 26. Functionality verification results of the VDES communication module.

3.1.1. VDES Communication Module

Based on the C/S model, this paper designed a VDES communication module, which facilitates the connection between the server and client for data transmission between systems. The structural diagram of the VDES communication module is illustrated in Figure 25.

The VDES communication module, as illustrated in Figure 25, utilizes socket communication based on the System.Net.Sockets namespace. On the client side, upon clicking the StartService button, a Socket object named _socket is created and bound to a specified IP address and port to begin listening for connection requests from the VDES base station server. Once the client is initiated, the ListenFunction() is invoked to continuously accept connection requests, adding information about the connected VDES base station to the dicSocket dictionary. A new thread is then launched to receive message data from the VDES base station server. Messages are sent from the client to the VDES base station server via the btnSendToSingle_Click() function. On the server side, when the Connect button is clicked, the VDES base station server connects to the client at the designated IP address and port using the sockClient.Connect(ipe) function. Once the connection is established, the VDES base station server can communicate with the client through the sockClient.Send() function. Upon completion of communication, the socket is closed using the close() function to terminate the connection.

To validate the functionality of the VDES communication module, a C/S model is employed as the foundational structure in Visual Studio 2019. The client initiates requests through socket connections, which are received and responded to by the server. A graphical user interface is created using C# and the WPF framework to facilitate communication between the server and client, with the verification results depicted in Figure 26.

As shown in Figure 26, with the listening port set to 123, the client and server display specific message information for transmission and reception in their respective message exchange areas: "!ABTDB,1,1,0,A,403t?j1vLohh<`JAhH=Tdp500D0G,0*6E" and "$AIVEM,1,1,0,A,403t?j1vLolAF`bV4vF;dsG00D0<,0*7D". This signifies successful communication between the client and server, validating the functionality of the VDES communication module.

3.1.2. VDES Message Processing Module

The VDES message processing module accomplishes the parsing and encapsulation of VDES messages. VDES message parsing involves dissecting received messages to extract various field parameters. Conversely, VDES message encapsulation packages outgoing information in a fixed data format to facilitate data exchange and communication between systems.

(1) VDES Message Encapsulation

The process of VDES message encapsulation is illustrated in Figure 27. The VDES message encapsulation module transforms outgoing information into messages that include cyclic redundancy check (CRC) codes, following the ITU-R M.2092 international standard. These messages consist of a header, payload data, and a checksum, along with the message length, VDES channel number, and additional relevant information. The payload data contains encoded navigational safety-related information. The VDES checksum is a two-digit hexadecimal number calculated by CRC to ensure the integrity and accuracy of the received messages.

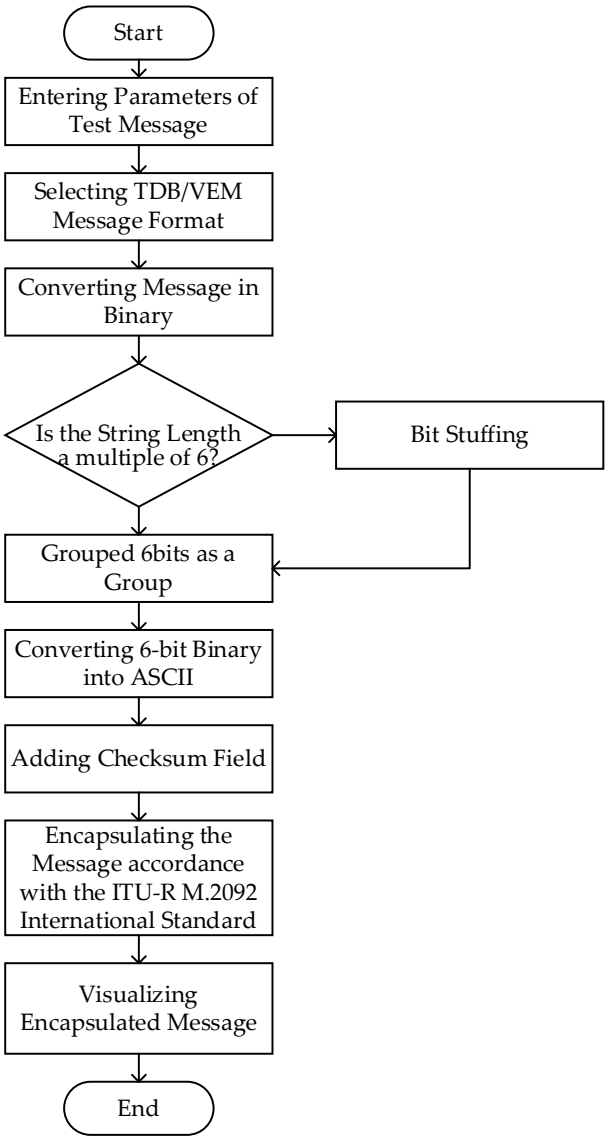


Figure 27. Flowchart for VDES message encapsulation.

As depicted in Figure 27, the VDES message encapsulation submodule initially inputs data such as the Maritime Mobile Service Identity (MMSI) code, Coordinated Universal Time (UTC), and latitude–longitude coordinates into the VDES message encapsulation information exchange interface. The DecimalToBinary() function is then invoked to convert decimal numbers into binary, followed by partitioning the binary numbers into groups of six bits each. In cases where the data points are less than six bits, zero-padding is applied to reach the required length. Subsequently, using a conversion table that maps

six-bit binary to ASCII characters, each group of binary data is transformed into the corresponding ASCII code. Finally, the CalculateChecksum() function is called to compute the message checksum, completing the encapsulation process. The pseudocode implementation of the VDES message encapsulation algorithm utilized in this paper is presented in Algorithm 2.

Algorithm 2 VDES message encapsulation algorithm

```
procedure MESSAGE-ENCAPSSULATION (sender, e)
    String DecimalToBinary(int decimalNumber,int Length)
      return binaryNumber ""
    String finalMessage ← ""
    String strr ← ""
    String id ← ID
    switch(Convert.ToInt32(id))
    case 4:
      //When the id is 4, the string value is obtained from the input and a series of processing is performed
    end switch
    int srl ← strr.Length
    int zerosToAdd ← 0
    if (srl % 6 ≠ 0)
      zerosToAdd ← 6 -(srl % 6)
      strr ← strr + new string('0', zeresToAdd)
    int Size ← 6
    int nums ← strr.Length/Size
    String binaryChunkk[nums]
    for i ← 0 to nums do
      binaryChunkk[i] ← strr.Substring(i * Size, Size)
    end for
    for all binaryChunk in binaryChunkk do
      int asciiValue ← Convert.ToInt32(binaryChunk, 2)
      if asciiValue < 0x28 then
        asciiValue ← asciiValue + 0x30
        finalMessage ← finalMessage + Convert.ToChar(asciiValue)
      else if asciiValue < 0x80 then
        asciiValue ← asciiValue + 0x38
        finalMessage ← finalMessage + Convert.ToChar(asciiValue)
      else
        asciiValue ← 0
        finalMessage ← finalMessage + Convert.ToChar(asciiValue)
    end if
    end for
    VDES_Message ← finalMessage
    int CalculateChecksun(String sentence)
      return Convert.ToInt32(checksun.ToString("X2"), 16)
    String st ← TextBox22.Text + finalMessage + "," + zerosToAdd
    Console.WriteLine("Checksun: " + st)
    int ccc ← CalculateChecksun(st)
end procedure
```

To validate the functionality of the VDES message encapsulation module, a message ID of 4, a forwarding indicator of 0, UTC time set to 15 March 2023, at 16:48:12, position accuracy of 1, and electronic position-fixing device type 5 are utilized. Additionally, there

are five time slots, 23 other stations currently received by this station, and all transmission control bits and RAIM flags are set to 0. The module encapsulates a base station with an MMSI code of 004132808 and position coordinates of (38°52.18692′ N, 121°31.74228′ E) into a VDES message compliant with the ITU-R M.2092 protocol standard. The resulting encapsulated message is: "!ABTDB,1,1,0,A,403t?j1vLohh<`dD=LF?M3U00D0G,0*0E". As illustrated in Figure 28, this module successfully accomplishes the VDES message encapsulation functionality.

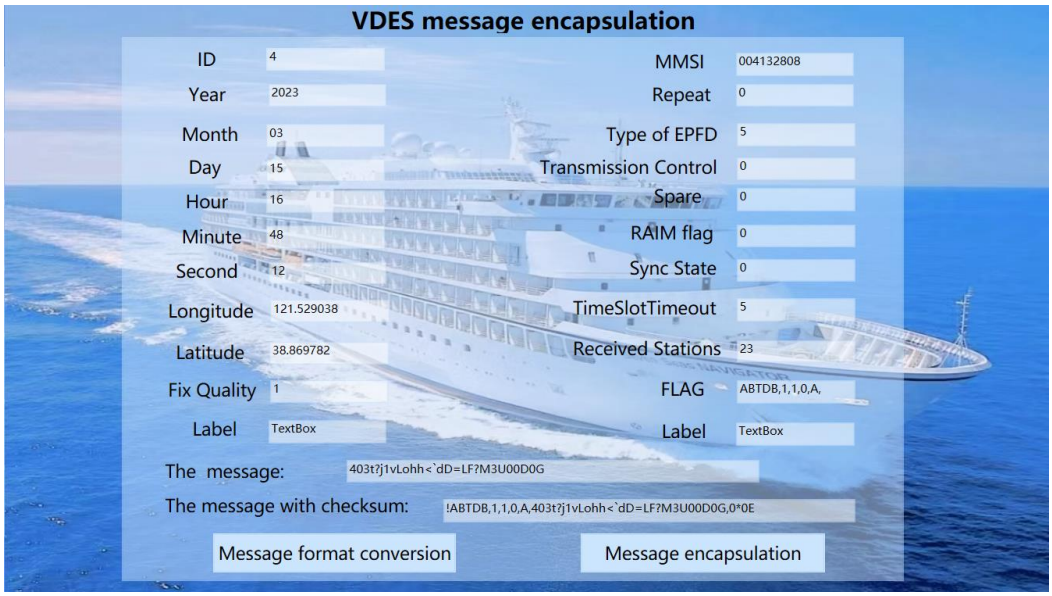


Figure 28. Functionality verification results for the VDES message encapsulation module.

(2) VDES Message Parsing

To acquire station, vessel dynamic, static, and navigational safety information from VDES messages, the VDES data link integrity monitoring system incorporates a VDES message parsing submodule, as illustrated in the UML diagram in Figure 29.

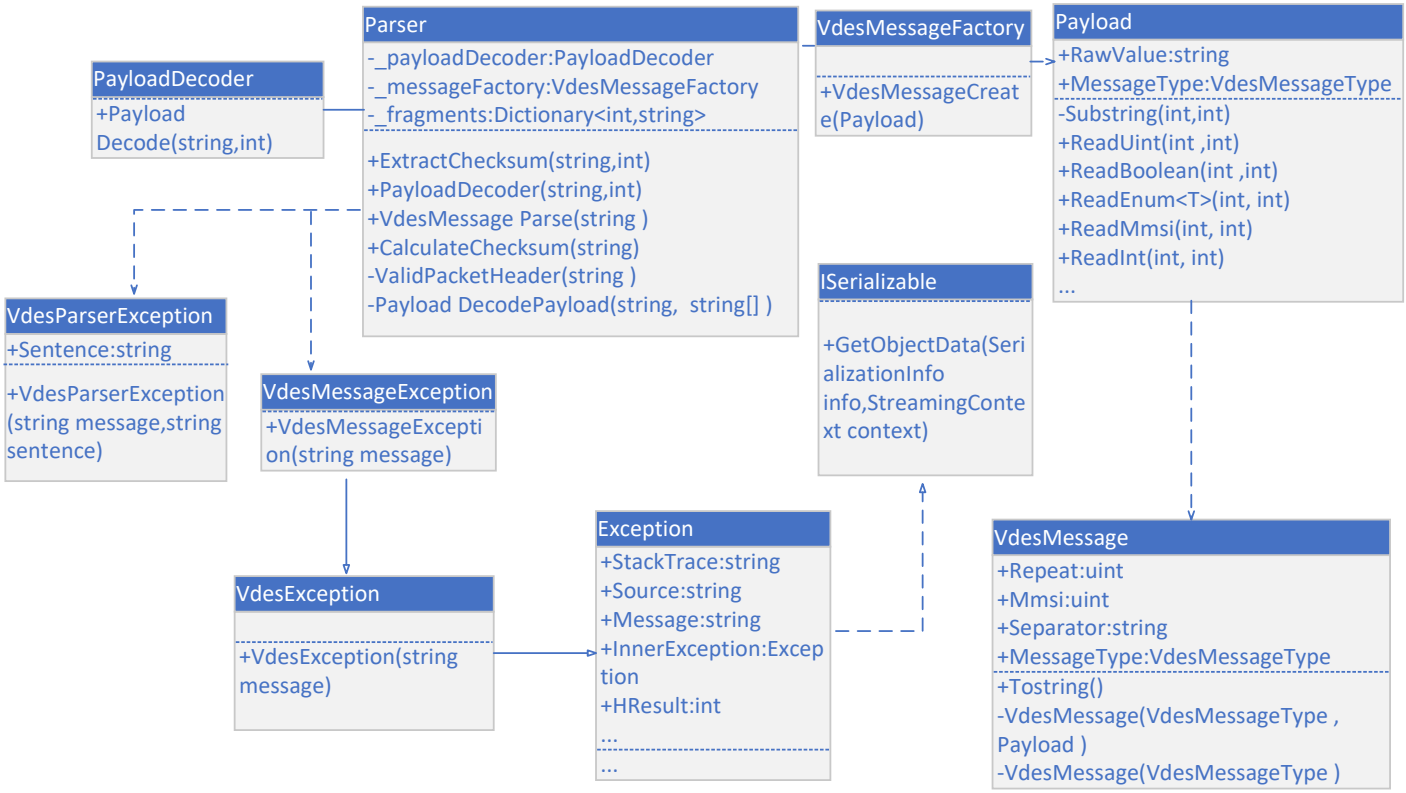


Figure 29. UML diagram for VDES message parsing.

As illustrated in Figure 29, during the VDES message parsing process, the received VDES message is first subjected to checksum computation using the CalculateChecksum() function. The computed checksum is then compared with the checksum extracted from the original message via the ExtractChecksum() function. If the checksums match, the verification process is deemed successful; if not, verification fails, and an appropriate error message is generated. Upon successful verification, the ASCII codes in the message are converted to 6-bit binary codes using the Decode() function. Following the specific bit count regulations outlined in the ITU-R M.2092 international standard, grouping is performed using the DecodePayload() function. Finally, by utilizing the payloadDecoder.Decode() function, the grouped information is converted from binary to decimal, thereby revealing the parsed content of the VDES message.

To validate the functionality of the VDES message parsing module, the message "!ABTDB,1,1,0,A,403t?j1vLohh<`dD=LF?M3U00D0G,0*0E" is parsed, with the results depicted in Figure 30.

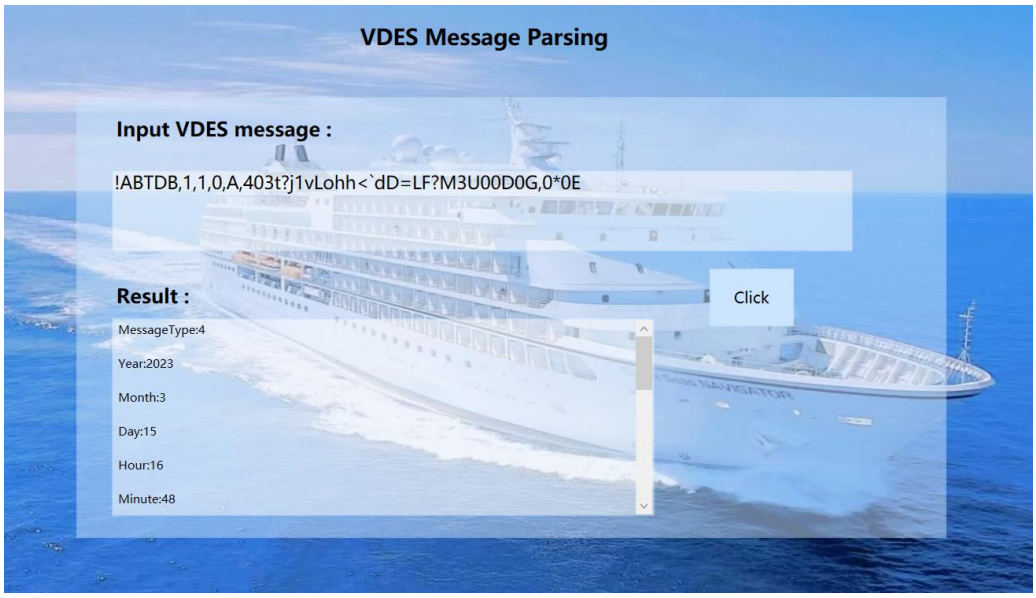


Figure 30. Functionality verification results for the VDES message parsing module.

As depicted in Figure 30, the MMSI code of the VDES base station is 004132808. The longitude, converted to 121.529038, corresponds to 121°31.74228′ E, while the latitude, converted to 38.869782, corresponds to 38°52.18692′ N. The VDES base station has a position accuracy of 1, a message type of 4, a forwarding indicator of 0, and UTC time set to 15 March 2023, at 16:48:12. Additionally, the electronic position fixing device type is 5, with all transmission control bits and RAIM flags set to 0. This information is consistent with the content sent by the base station and encapsulated in the VDES message by the VDES message encapsulation module, as shown in Figure 30. This validation confirms the functionality of the VDES message parsing module.

3.1.3. VDES Data Link Credibility Monitoring Module

The VDES data link integrity monitoring module comprises two key components: the radio interference detection module, which monitors radio interference within the VDES data link, and the ship-to-shore distance and propagation distance matching analysis module, which aims to identify and locate spoofing sources within the VDES data link. The radio interference detection module includes four submodules: VDES message format compliance verification, VDES message parameter validity verification, VDES message content integrity verification, and transmit-receive message consistency verification. This section primarily focuses on the VDES message content integrity verification and transmit–receive message consistency verification submodules, while the VDES message format compliance verification and VDES message parameter validity verification have been extensively discussed in reference [36].

(1) VDES Message Integrity Verification Module

The VDES message integrity verification module utilizes the MD5 algorithm to compare the received VDES message with the legitimate message content previously sent by ships and stored in the VDES original message database. This process verifies the integrity of the received message content. First, the ProcessVDESMessage(string VDESMessages) function calls the DivideIntoBlocksByField(string data) function to divide the parsed message into multiple blocks. Next, the ValidateIntegrity() function performs an integrity check on the message. This function calculates the hash values of the received VDES message and the legitimate message from the VDES original message database using the MD5 algorithm through the CalculateHash() subfunction. It then updates the hash chain and compares the two hash values. If the hash values do not match, indicating potential radio interference in the data link, the VDES data link integrity monitoring system outputs an

unreliable monitoring result. If the hash values match, the integrity of the message content is confirmed.

(2) VDES Transmission and Reception Message Consistency Verification Module

The VDES message consistency verification module employs the HMAC algorithm to verify the consistency of TDB statement messages and VEM statement messages, ensuring that data integrity is maintained during the transmission of VDES messages. The ComputeHMAC(receivedVDES, sharedKey) function calculates the HMAC values for both the TDB and VEM statement messages. A discrepancy in the HMAC values indicates the presence of radio interference in the data link, resulting in unreliable monitoring results for the VDES data link. If the HMAC values match, the module proceeds with the transmit–receive message consistency verification.

Through the verification of VDES message integrity and consistency, the VDES data link integrity monitoring system effectively detects data anomalies caused by radio interference. To facilitate this process and serve as a precursor to module programming, the following pseudocode is designed as shown in Algorithm 3:

Algorithm 3 VDES message integrity and consistency monitoring

```
Step 1: Connect database
sever = (local); database = DBTESTB; integrated security = true
Step 2: Calculate hash value
function CALCULATEHASH(data)
    using MD5 md5 = MD5.Create()
    hashBytes ← md5.ComputeHash(Encoding.UTF8.GetBytes(data))
    return BitConverter.ToString(hashBytes).Replace("-", "")
end function
Step 3: Message integrity verification
vdesMessage ← concatenatedValues
valuesString ← Join values11 and replace spaces
ProcessVDESMessagel(vdesMessage)
dataBlocksForMessage1 ← new List()
ProcessVDESMessage2(vuluesString)
dataBlocksForMessage2 ← new List()
hashValue1 ← CalculateHash(Join dataBlocksForMessage1)
hashValue2 ← CalculateHash(Join dataBlocksForMessage2)
areHashesEqual ← hashValue1 = = hashValue2
if areHashesEqual then
    shuchu1 ← "The hash values of the two VDES messages are the same.
Data integrity verification passed."
else
    shuchu1 ← "The hash values of the two VDES messages are different.
Data integrity verification failed."
end if
Step 4: Message consistency verification
function computeHMAC(data, key)
    using HMACMD5 hmac = new HMACMD5(Encoding.UTF8.GetBytes(key))
    hashBytes ← hmac.ComputeHash(Encoding.UTF8.GetBytes(data))
    return BitConverter.ToString(hashBytes).Replace("-", "").ToLower()
end function
data1 ← TDB Message
vdesMessage ← data1[5]
sharedKey ← Substring(0,7) of data1[5]
```

```
generatedHMAC1 ← ComputeHMAC(vdesMessage, sharedKey)
ReceivedVdes.Split(',')
receivedVdes← data [5]
generatedHMAC2 ← ComputeHMAC(receivedVdes, sharedKey)
if generatedHMAC1 = = generatedHMAC2 then
    shuchu2 ← "Data consistency validation passes!"
else
    shuchu2 ← "Data consistency validation failed!"
end if
```

To validate the functionality of the VDES message integrity verification module, a verification of message content integrity was conducted at a specific moment. The module compared a message received by a VDES base station at that time: "!AIVEM,1,1,0,A,403sooQvMSfR0`JAhH=Tdp400D0E,0*5D", with a legitimate message previously sent by ships and stored in the VDES original message database: "!AIVEM,1,1,0,A,403t?i1vLohh<`dD=LF?M3U00D0G,0*0A". The verification results are illustrated in Figure 31.

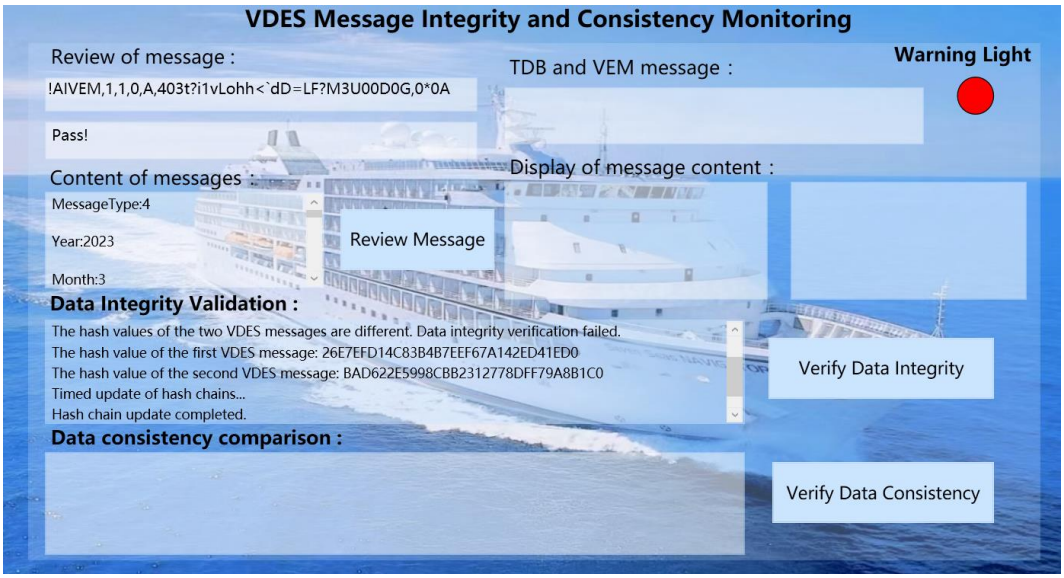


Figure 31. Functionality verification results for the VDES message integrity module.

As shown in Figure 31, the VDES base station received a VDES message with a hash value of BAD622E5998CBB2312778DFF79A8B1C0, while the hash value of the legitimate message from the VDES original message database was 26E7EFD14C83B4B7EEF67A142ED41ED0. The discrepancy between these two hash values indicates that the VDES message was affected by radio interference, leading to incomplete message content and confirming the functionality of the VDES message integrity verification module.

To validate the functionality of the VDES message consistency verification module, a scenario was set in which a link management message was broadcast by a VDES base station using the TDB statement "!ABTDB,1,1,0,A,403t?j1vLohh<`JAhH=Tdp500D0G,0*6E". This message was then received by a VDES ship station, automatically forwarded using the VEM statement, and subsequently re-received by the VDES base station as: "!AIVEM,1,1,0,A,403sooQvMSfR0W`0B4@qWO400D0E,0*33". The consistency of these two messages was verified, with the results presented in Figure 32.

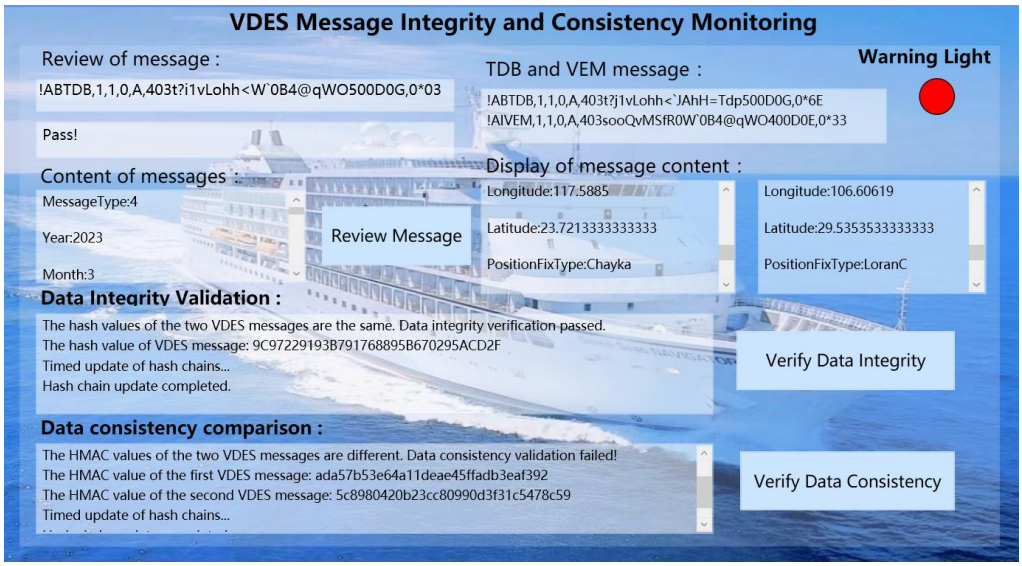


Figure 32. Verification results of the VDES communication consistency checking module.

As depicted in Figure 32, the HMAC value of the message broadcast by the VDES base station using the TDB statement was ada57b53e64a11deae45ffadb3eaf392, while the HMAC value of the VEM statement message, relayed by the ship station and then re-received by the VDES base station, was 5c8980420b23cc80990d3f31c5478c59. The discrepancy in these HMAC values indicates that the VDES message was compromised by radio interference at that moment, leading to alterations in the message content. This module successfully fulfills the functionality of the VDES message consistency verification module.

(3) Module for Analyzing the Matching of Ship-to-Shore Distance and Propagation Distance

Upon confirming the absence of radio interference in the VDES data link, the VDES data link integrity monitoring system proceeds to monitor for the presence of spoofing sources within the link. This module initially invokes the GetDistance(double, double, double, double) function to calculate the ship-to-shore distance using the Haversine formula, based on the vessel position reported by the VDES shipborne terminal and the base station's location. It incorporates current hydro-meteorological information, such as sea surface wind speed and sea surface temperature. Subsequently, the CalculateRange(double, double, double, double, double) function computes the propagation distance of the VDES signal in the current maritime environment. The analysis then determines whether the ship-to-shore distance falls within the tolerance range of the propagation distance. If the distance is within this tolerance range, it signifies the absence of spoofing sources in the VDES data link at that moment. Conversely, if the distance exceeds this tolerance range, it indicates the presence of a spoofing source within the VDES data link. An algorithm for spoofing source messages is employed to ascertain the location or range of the spoofing source. The Ship-to-Shore Distance vs. Propagation Distance Matching Analysis module can effectively monitor anomalous data resulting from spoofing source interference in the VDES data link. To facilitate this process and serve as a preliminary step for module programming, the pseudocode designed for this purpose is provided as shown in Algorithm 4:

Algorithm 4 Matching monitoring between ship-to-shore distance and propagation distance

Step 1: Calculate the distance between the base station and the ship
function GETDISTANCE(lng1,lat1,lng2,lat2)
radLat1 ← Rad(lat1)
radLng1 ← Rad(lng1)
radLat2 ← Rad(lat2)

radLng2 ← Rad(lng2)
a ← radLat1 ← radLat2
b ← radLng1 ← radLng2

$$result \leftarrow 2\times\sin^{-1}\left(\sqrt{\sin^2\left(\frac{a}{2}\right)+\cos(radLat1)\times\cos(radLat2)\times\sin^2\left(\frac{b}{2}\right)}\right)\times 6378$$ ◁ Haversine formula

return result
end function

Step 2: Calculate the service radius of the base station

function SERVICERADIUS(d, u, h, Ta, Ts, Rh)

$$L \leftarrow 0.4873\times Lbu(d,u)+0.3671\times Lbh(d,h)+0.1417\times Lbhe(d,Ta,Ts,u,RH)$$ ◁ Transmission loss

S ← A − L
if S = 0 **then**
return d
end if
end function

When the system margin is greater than 0, the maximum transmission distance d corresponds to the propagation distance R of the VDES base station.

Step 3: Matching monitoring

if R ≥ D **then**
shuchu3 ← "located within the propagation distance of the VDES base station"
else
shuchu3 ← "beyond the propagation distance of the VDES base station"
end if

To verify the functionality of the Ship-to-Shore Distance vs. Propagation Distance Matching Analysis module, consider a scenario in which the VDES base station is positioned at (38°58.14′ N, 121°2.46′ E). The sea surface wind speed is 10.88 m/s, the sea surface temperature is 16 °C, the tidal water level is 0.2 m, and the relative humidity is 75%. The VDES ship station is located at (38°43.176′ N, 121°10.02′ E). Given a VDES signal reception power of −67 dBm, the results of spoofing source detection in the VDES data link are illustrated in Figure 33.

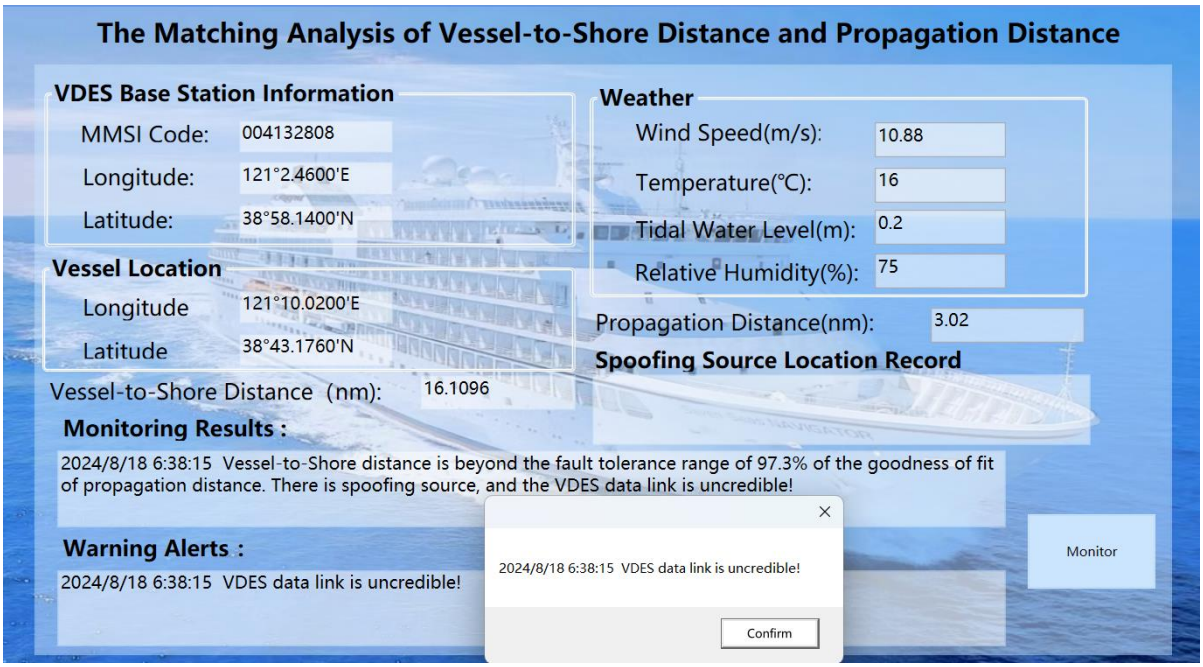


Figure 33. Functional verification results of the ship-to-shore distance and propagation distance matching analysis module.

As shown in Figure 33, based on the sea surface meteorological conditions, the calculated coverage range of the VDES signal is 27.1623 nautical miles. Simultaneously, using Equation (9) to compute the ship-to-shore distance based on the VDES ship station location yields a value of 16.1096 nautical miles. Since this ship-to-shore distance is less than the VDES signal coverage range, it indicates that the information broadcast by the base station can be received by the ship station. Considering the received power, the calculated propagation distance of the VDES signal, using Equation (8), is 3.02 nautical miles. At this point, the ship-to-shore distance exceeds the tolerance range of 97.3% of the propagation distance, indicating that the received VDES message was not transmitted by the base station. This suggests the presence of spoofing source interference in the VDES data link at that moment, thereby validating the functionality of the Ship-to-Shore Distance vs. Propagation Distance Matching Analysis module.

4. Verification and Analysis of Experimental Results

The VDES data link integrity monitoring software system is a human–computer interaction system based on the C/S model, designed to effectively monitor the presence of radio interference or spoofing sources within the VDES data link. In this section, various interference scenarios are simulated to test the functionality and monitoring effectiveness of the software system.

4.1. Testing of Radio Interference Vulnerability and Threats

In this section, the effectiveness of the radio interference detection method based on message characteristics is validated through tests that assess vulnerabilities to radio interference within the VDES data link. These tests include the verification of VDES message format compliance, legality of VDES message parameters, completeness of VDES message content, and consistency between transmitted and received messages. This validation demonstrates the method's capability to effectively detect radio interference vulnerabilities in the VDES data link.

I. Compliance Testing of VDES Message Formats

We assuming the message received by the VDES base station is "!AIVEM,1,1,0,A,46:tkW1vLohh<`dD=LF?M3U00D0G,0*6F". Upon parsing this message using the VDES raw message database, the test results are illustrated in Figure 34.

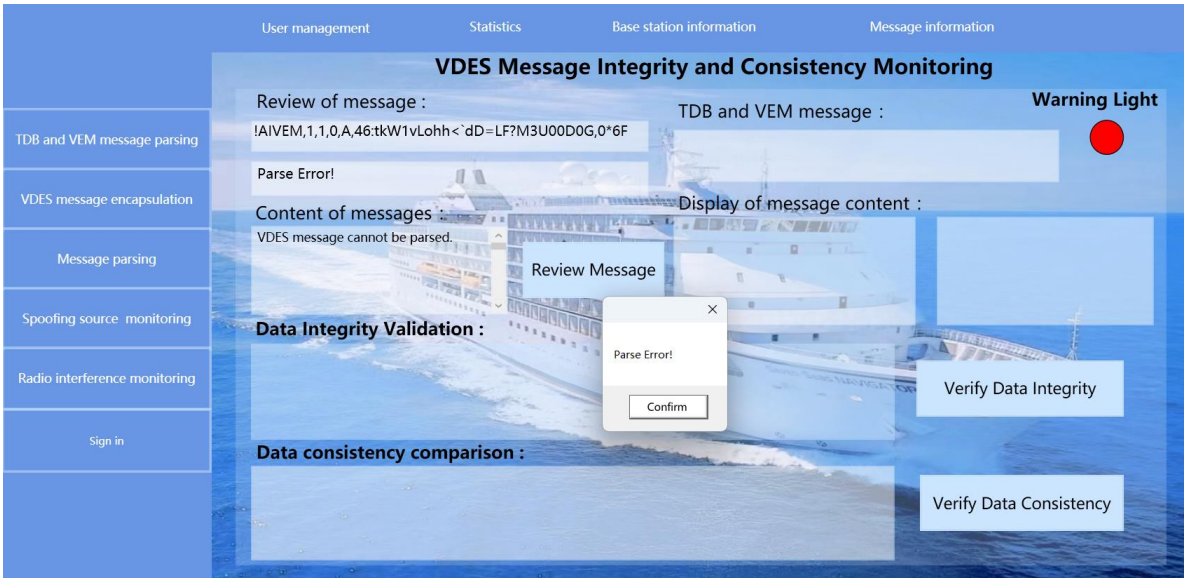


Figure 34. Results and figures of VDES message format compliance testing.

As shown in Figure 34, querying the VDES raw message database confirmed that the format of the message is inconsistent with the format stored in the database, preventing the message from being parsed correctly. Consequently, the verification of VDES message format compliance failed, indicating the presence of radio interference within the VDES data link at that time.

II. Verification Testing of VDES Message Parameter Legitimacy

We assuming the message received by the VDES base station is "!AIVEM,1,1,0,A,403t?j1vN2hkR`dKu<F?IAG02D0O,0*62". Following a query to the VDES raw message database for parsing this specific message and extracting parameter information from each field of the message, the parameters are detailed in Table 1. A comparison is then made between the parameters listed in Table 1 and the parameters of legitimate messages previously sent by this base station in the AIS/VDES message distributed database. The test outcomes are presented in Figure 35.

Table 1. Parameter table for VDES message parameter legitimacy verification testing.

Parameters	Explain
MMSI Code	004132808
Longitude	121°33.32862′ E
Latitude	38°52.09008′ N
Repeat	0
Position accuracy	1
Types of electronic positioning devices	7
Transmission control of long-range broadcast messages	0
Spare	0
Sync State	0
RAIM flag	1
Time slot timeout	5
Received Stations	31

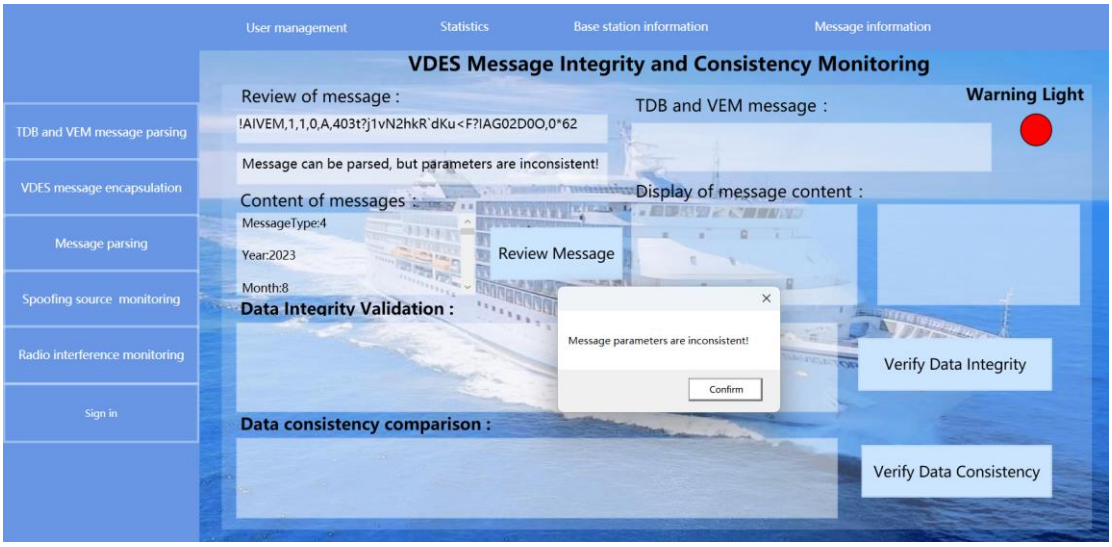


Figure 35. Results and figures of VDES message parameter legitimacy verification testing.

As illustrated in Figure 35, querying the VDES raw message database confirmed that the format of the message aligns with the stored format, allowing for successful parsing. The verification of message format compliance passed. However, upon consulting the

AIS/VDES message distributed database, it was revealed that previously sent legitimate messages from this base station identified the Electronic Positioning Device type as 5, with an RAIM flag of 0. In contrast, the Electronic Positioning Device type in the received VDES message, as listed in Table 1, was 7, with an RAIM flag of 1. This presents inconsistencies with the parameters of legitimate messages. Consequently, the validation of the legitimacy of VDES message parameters failed, indicating the presence of radio interference within the VDES data link at that time.

III. Verification of VDES Message Content Integrity

Assuming the message received by the VDES base station is "!AIVEM,1,1,0,A,403t?i1vLohh<`dD=LF?M3U00D0G,0*0A", upon querying the VDES raw message database, it was found that a legitimate message previously sent by the ship station received by this base station was "!AIVEM,1,1,0,A,403t?i1vLohh<W`0B4@qWO500D0G,0*04". The parameters of this message retrieved from the VDES raw message database are detailed in Table 2. Following the parsing and parameter comparison of the received message using the VDES raw message database, the test results are depicted in Figure 36.

Table 2. Parameter table for VDES message content integrity verification testing.

Parameters	Explain
MMSI Code	004132804
Longitude	106°36.3714′ E
Latitude	29°32.1212′ N
Repeat	0
Position accuracy	1
Types of electronic positioning devices	5
Transmission control of long-range broadcast messages	0
Spare	0
Sync State	0
RAIM flag	0
Time slot timeout	5
Received Stations	23

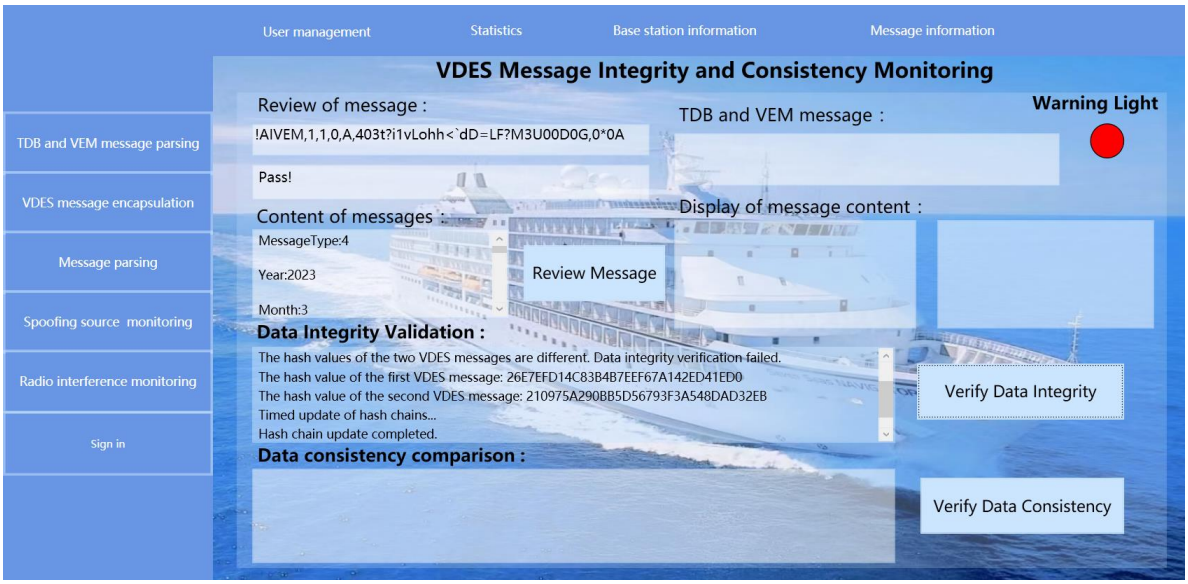


Figure 36. Results of VDES message content integrity verification testing.

As shown in Figure 36, querying the VDES raw message database confirmed that the format of the message aligns with the stored format, enabling successful parsing. The verification of message format compliance passed. Following parsing, a query to the AIS/VDES message distributed database revealed that all parameters of this message matched those of previously sent legitimate messages, thereby passing the validation of message parameter legitimacy. However, upon computing the hash values of the received message and the hash value of a legitimate message previously received by this base station using the MD5 algorithm, the software interface indicated a discrepancy between the two hash values. This integrity check failure of the message content suggests the presence of radio interference within the VDES data link at that time.

IV. VDES Transmission and Reception Messages Consistency Check Test

Assuming the link management message broadcast by the VDES base station in TDB format is "!ABTDB,1,1,0,A,403t?j1vLohh<`JAhH=Tdp500D0G,0*6E", the message received by the VDES shipborne unit after automatic forwarding by VEM, and subsequently re-received by the VDES base station, is "!AIVEM,1,1,0,A,403sooQvMSfR0W`0B4@qWO400D0E,0*33". Upon querying the VDES raw message database for parsing the received message and comparing parameters in the AIS/VDES message distributed database, the test results are depicted in Figure 37.

As depicted in Figure 37, querying the VDES raw message database confirmed that the message format aligns with that stored in the database, enabling successful parsing. The verification of message format compliance was successful. Following this, a query to the AIS/VDES message distributed database revealed that all parameters of the message matched those of previously sent legitimate messages, thus validating the legitimacy of the message parameters. By utilizing the MD5 algorithm to compute the hash value of the received message and comparing it to the hash value of the legitimate message previously received by this base station, the computed results were consistent; both hashes were 9C97229193B791768895B670295ACD2F, confirming the integrity of the message content. Additionally, by applying the HMAC algorithm to compute the HMAC values of the TDB statement message and the VEM statement message separately, the software interface indicated a discrepancy between the HMAC values of the two messages. Consequently, the consistency check of the VDES transmission and reception messages failed, suggesting the presence of radio interference within the VDES data link at that time.

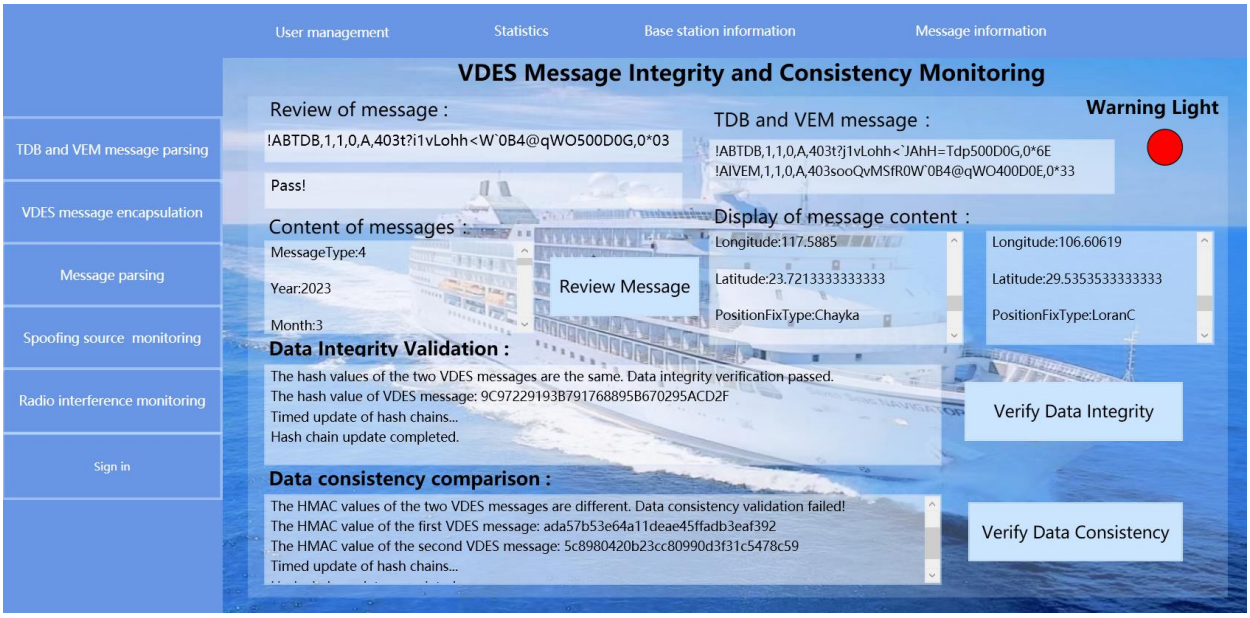


Figure 37. Results of VDES transmission and reception messages consistency check test.

V. Testing of Radio Interference Vulnerability and Threats

Assuming that the VDES base station broadcasts a link management message in TDB format as follows, "!ABTDB,1,1,0,A,403sooQvMSfR0W`0B4@qWO400D0E,0*34", the message received by the VDES shipborne unit—after automatic forwarding by VEM and then re-received by the VDES base station—is "!AIVEM,1,1,0,A,403sooQvMSfR0W`0B4@qWO400D0E,0*33". Upon querying the VDES raw message database to parse the received message and compare parameters in the AIS/VDES message distributed database, the test results are depicted in Figure 38.

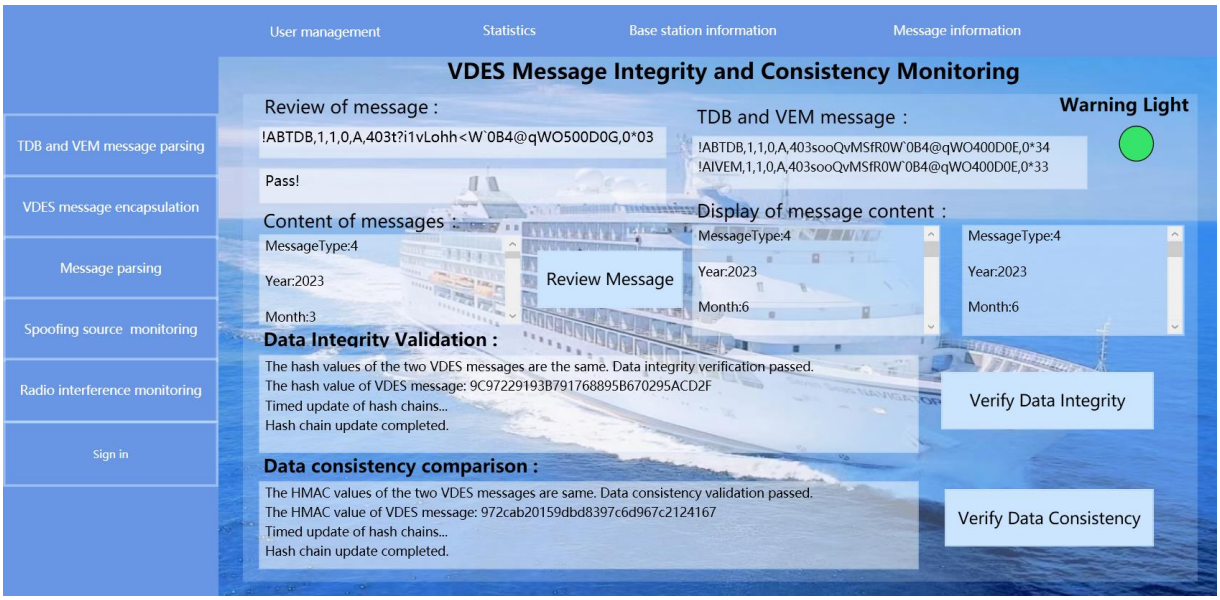


Figure 38. Results of radio interference vulnerability and threat testing.

As shown in Figure 38, it was confirmed that the format of the message aligns with that stored in the VDES raw message database, enabling successful parsing. The verification of message format compliance was successful. Following this, a query to the AIS/VDES message distributed database revealed that all parameters of the message matched those of previously sent legitimate messages, validating the legitimacy of the message parameters. By utilizing the MD5 algorithm to compute the hash value of the received message and comparing it to the hash value of the legitimate message previously received by this base station, the computed results were consistent; both hashes were 9C97229193B791768895B670295ACD2F, confirming the integrity of the message content. Additionally, by applying the HMAC algorithm to compute the HMAC values of the TDB statement message and the VEM statement message separately, the results were also consistent, both being 972cab20159dbd8397c6d967c2124167, thereby passing the consistency check of the transmission and reception messages. In conclusion, at this point, the VDES messages were not vulnerable to threats of radio interference in the data link, allowing for subsequent spoofing source identification.

4.2. Testing of Spoofing Source Vulnerability and Threats

Building upon the completion of radio interference detection in the VDES data link, this section employs a method that matches ship-to-shore distance with propagation distance to validate the effectiveness of the VDES data link integrity monitoring system in detecting spoofing sources within the data link.

I. Testing of Ship-to-Shore Distance and Propagation Distance Matching

To validate the effectiveness of the ship-to-shore distance matching analysis method in detecting spoofing sources within the VDES data link, this section simulates various interference scenarios to verify the functionality of the algorithm.

(a) Match Test Passes the Experiment

Assuming the coordinates of the VDES base station are (38°46.0398′ N, 121°9.1872′ E), with a sea surface wind speed of 10.88 m/s, a sea surface temperature of 16 °C, a tidal water level of 0.2 m, and a relative humidity of 75%. When the VDES ship station is located at (38°43.176′ N, 121°10.02′ E), the monitoring results are shown in Figure 39.

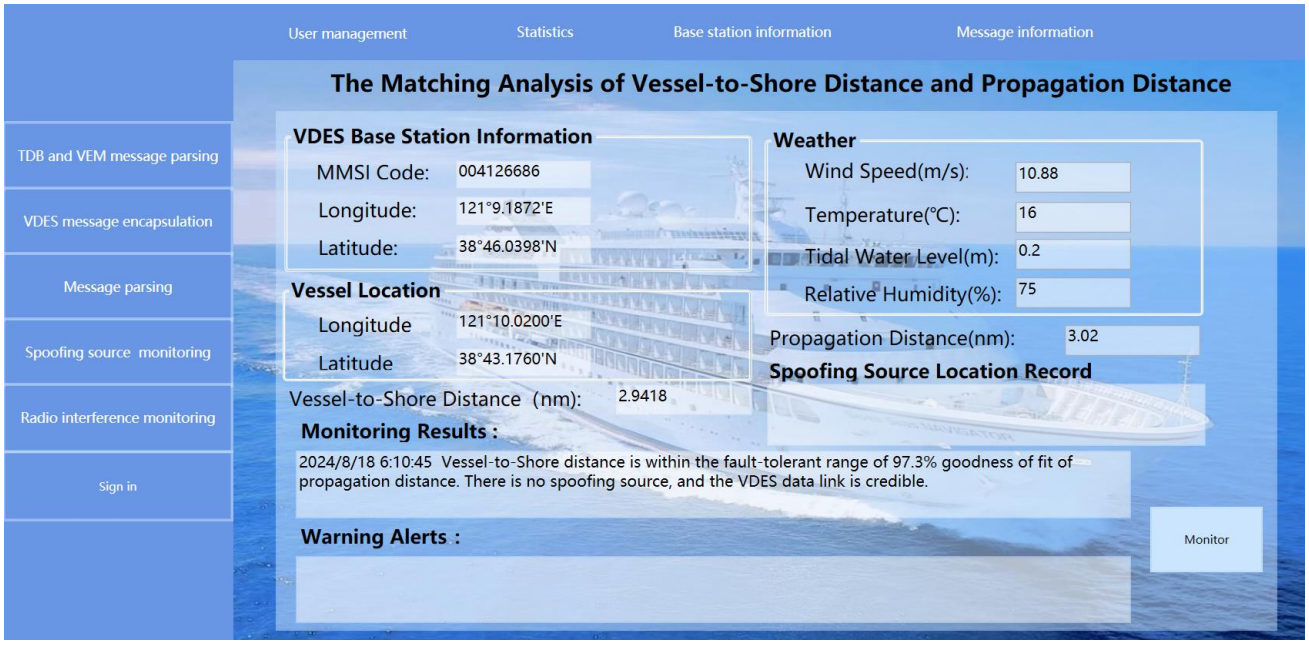


Figure 39. Results of testing for the absence of spoofing sources based on the Credibility Monitoring Software.

As shown in Figure 39, it was confirmed that the format of the message aligns with that stored in the VDES raw message database, enabling successful parsing. The verification of message format compliance was successful. Following this, a query to the AIS/VDES message distributed database revealed that all parameters of the message matched those of previously sent legitimate messages, validating the legitimacy of the message parameters. By utilizing the MD5 algorithm to compute the hash value of the received message and comparing it to the hash value of the legitimate message previously received by this base station, the computed results were consistent; both hashes were 9C97229193B791768895B670295ACD2F, confirming the integrity of the message content. Additionally, by applying the HMAC algorithm to compute the HMAC values of the TDB statement message and the VEM statement message separately, the results were also consistent, both being 972cab20159dbd8397c6d967c2124167, thereby passing the consistency check of the transmission and reception messages. In conclusion, at this point, the VDES messages were not vulnerable to threats of radio interference in the data link, allowing for subsequent spoofing source identification. The VDES signal coverage range calculated based on sea surface meteorological conditions is 27.1623 nautical miles. Concurrently, using the Haversine formula with the VDES base station coordinates, the ship-to-shore distance is determined to be 2.9418 nautical miles, which is less than the VDES signal coverage range. Considering a received signal power of −67 dBm at the VDES ship station and a calculated VDES signal propagation distance of 3.02 nautical miles—based on a complex sea surface environment VHF signal propagation loss model—this ship-to-shore distance falls within the tolerance range of 97.3%, fitting the propagation distance. This

alignment indicates that the signal emitted from the base station matches the received signal power at the receiving end, suggesting the absence of spoofing source interference in the VDES data link.

(b) Experimental Analysis of Matching Testing Failures

At a specific moment, the coordinates of the VDES base station are (38°58.14′ N, 121°2.46′ E), with a sea surface wind speed of 12.23 m/s, a sea surface temperature of 17 °C, a tidal water level of 0.1 m, and a relative humidity of 69%. The VDES ship station is positioned at (38°43.62′ N, 121°9.66′ E), with a received power of −67 dBm. The results of the ship-to-shore distance matching with the propagation distance test are depicted in Figure 40.

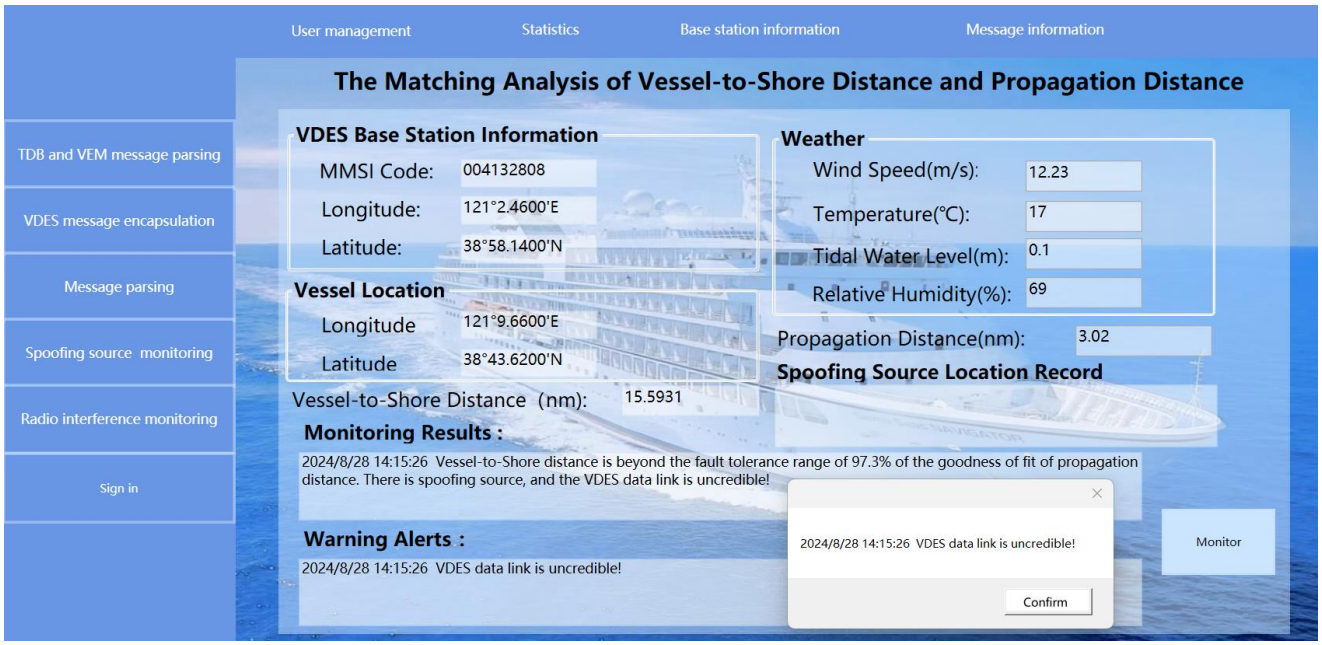


Figure 40. Results of spoofing source detection based on the Credibility Monitoring Software.

As shown in Figure 40, it was confirmed that the format of the message aligns with that stored in the VDES raw message database, enabling successful parsing. The verification of message format compliance was successful. Following this, a query to the AIS/VDES message distributed database revealed that all parameters of the message matched those of previously sent legitimate messages, validating the legitimacy of the message parameters. By utilizing the MD5 algorithm to compute the hash value of the received message and comparing it to the hash value of the legitimate message previously received by this base station, the computed results were consistent; both hashes were 9C97229193B791768895B670295ACD2F, confirming the integrity of the message content. Additionally, by applying the HMAC algorithm to compute the HMAC values of the TDB statement message and the VEM statement message separately, the results were also consistent, both being 972cab20159dbd8397c6d967c2124167, thereby passing the consistency check of the transmission and reception messages. In conclusion, at this point, the VDES messages were not vulnerable to threats of radio interference in the data link, allowing for subsequent spoofing source identification. The VDES signal coverage is calculated to be 27.1623 nautical miles based on sea surface meteorological conditions. Simultaneously, the ship-to-shore distance computed using Equation (9) from the VDES ship station position is 15.5931 nautical miles, which is less than the VDES signal coverage range, indicating that the information broadcast by the base station can be received by the ship station. Considering the received power, the VDES signal propagation distance calculated using Equation (8) is 3.02 nautical miles. At this point, the ship-to-shore distance exceeds the tolerance range of 97.3% fitting the propagation distance, suggesting that the received

VDES message is not from the base station. It is inferred that spoofing source interference exists in the VDES data link at this instance, leading to subsequent engagement with the spoofing source localization module.

II. Testing of Spoofing Source Localization

Assuming the coordinates of VDES monitoring station A are (38°43.2′ N, 121°6.24′ E) and those of VDES monitoring station B are (38°40.14′ N, 121°8.64′ E), with a sea surface wind speed of 10.88 m/s, a sea surface temperature of 16 °C, a tidal water level of 0.2 m, and a relative humidity of 75%, the VDES ship station is located at (38°43.176′ N, 121°10.02′ E) with a received power of −67 dBm. The results of the detection of spoofing sources in the VDES data link are presented in Figure 41.

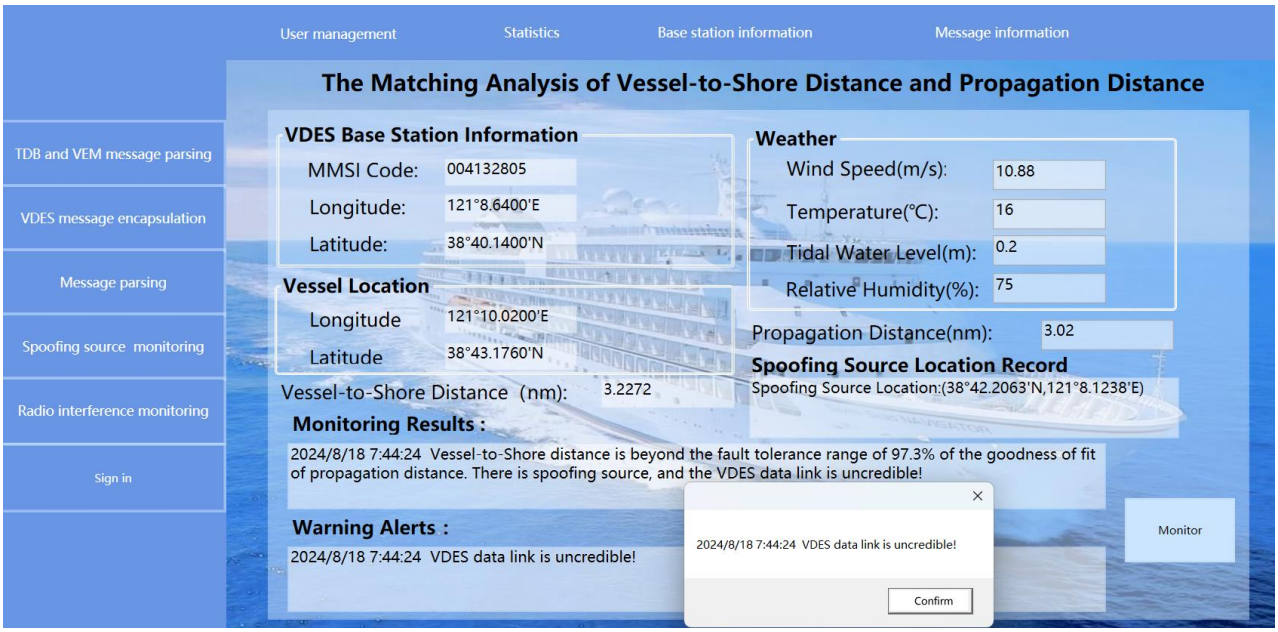


Figure 41. Results of spoofing source localization testing.

As shown in Figure 41, it was confirmed that the format of the message aligns with that stored in the VDES raw message database, enabling successful parsing. The verification of message format compliance was successful. Following this, a query to the AIS/VDES message distributed database revealed that all parameters of the message matched those of previously sent legitimate messages, validating the legitimacy of the message parameters. By utilizing the MD5 algorithm to compute the hash value of the received message and comparing it to the hash value of the legitimate message previously received by this base station, the computed results were consistent; both hashes were 9C97229193B791768895B670295ACD2F, confirming the integrity of the message content. Additionally, by applying the HMAC algorithm to compute the HMAC values of the TDB statement message and the VEM statement message separately, the results were also consistent, both being 972cab20159dbd8397c6d967c2124167, thereby passing the consistency check of the transmission and reception messages. In conclusion, at this point, the VDES messages were not vulnerable to threats of radio interference in the data link, allowing for subsequent spoofing source identification. The VDES signal coverage is calculated to be 27.1623 nautical miles based on sea surface meteorological conditions. Additionally, the distances between VDES monitoring station A and the ship station, calculated using Equation (9), is 2.9513 nautical miles, while the distance between VDES monitoring station B and the ship station is 3.2272 nautical miles. Both ship-to-shore distances are less than the VDES signal coverage range, indicating that the information broadcast by both monitoring stations can be received by the VDES ship station at this time. However, when considering the received power and the VDES signal propagation distance calculated using a

complex VHF signal propagation loss model in the intricate sea surface environment, the distance between monitoring station A and the ship station falls within the tolerance range of 97.3%, fitting the propagation distance. Conversely, the distance between monitoring station B and the ship station exceeds this tolerance range, suggesting that the received VDES message does not originate from monitoring station B. This inference indicates the presence of a spoofing source in the VDES data link. The spoofing source localization algorithm determines the coordinates of the spoofing source to be (38°42.2063′ N, 121°8.1238′ E), validating the capability of the VDES data link integrity monitoring software system to successfully detect and locate spoofing sources within the data link.

5. Conclusions

This paper proposes a credibility monitoring approach based on radio interference detection incorporating spoofing source identification and localization, in the context of the two major classes of data link vulnerabilities outlined in the IALA G1181 VDES VDL Integrity Guide. Initially, the system parses received messages using its VDES message database to verify their compliance with the VDES message format. Next, the parameters extracted from these parsed VDES messages are compared with the legitimate parameters previously sent by the VDES base station and stored in the AIS/VDES message distributed database to validate their authenticity. The integrity of the message content is then verified using the MD5 algorithm, which is more efficient for ensuring message integrity compared to SHA1 and SHA256 algorithms. Further, the consistency of the link management messages sent by the VDES base station in TDB statements and the VEM message statements received by VDES via shipborne automatic retransmission is checked using the HMAC algorithm to detect radio interference threats. Upon detecting radio interference, the VDES signal propagation distance is calculated using a VHF signal transmission loss model in complex sea surface environments. The ship-to-shore distance is then computed based on the location information in the messages, and a comparative analysis is conducted between this ship-to-shore distance and the propagation distance to identify potential spoofing sources. If spoofing sources are detected, a spoofing source identification algorithm is employed to accurately locate these sources, thereby ensuring the integrity of the VDES data link. To support automated monitoring of the VDES data link, we have developed VDES data link monitoring software based on the C/S model. This software includes a VDES communication module, a VDES message processing module, and a link integrity monitoring module. It facilitates the visualization of the VDES link monitoring status, alerts, and records of spoofing source locations. However, this paper has not taken into account other VHF data link vulnerability threats mentioned in the IALA G1181 guide, including unauthorized signaling, misbehaving devices, incorrect device configuration and installation, DOS attack and protocol attack. In the future, the VDES data link trustworthiness monitoring methodology will further enhance the monitoring of unauthorized signaling, misbehaving devices, incorrect device configuration and installation, DOS attack and protocol attack, and the VDES data link vulnerability monitoring methodology will further intensify the monitoring of VHF data link vulnerability threats. The research findings are significant for enhancing maritime traffic safety, improving shipping efficiency, and preventing maritime accidents.

Author Contributions: X.W. and Q.H. supervised the work, arranged the architecture, and contributed to the writing of the paper; L.F. and X.W. designed the measurement scheme, carried out the simulations, and wrote the paper; W.W. analyzed and compiled the data. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No. 62301106) and the National Key Research and Development Program of China (No. 2021YFB3901502).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data have been provided in this paper. Further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following is a comprehensive list of all abbreviations utilized in the text:
AIS: Automatic Identification System
AODV: Ad Hoc On-demand Distance Vector
ASM: Application Specific Messages
A-VDL: Advanced Very-High-Frequency Data Link
FBTDMA: Feedback based Time Division Multiple Access
IALA: The International Organization for Marine Aids to Navigation
IGO: Intergovernmental Organization
IMO: International Maritime Organization
ITU: The International Telecommunication Union
mARF: Maritime Automatic Rate Fallback
MCS: Modulation and Coding Scheme
MMSI: Maritime Mobile Service Identity
NCSR11: 11th session of the IMO Sub-Committee on Navigation, Communications, and Search and Rescue
NGO: Non-governmental Organization
SOLAS: Safety of Life at Sea
SOTDMA: Self-Organizing Time Division Multiple Access
VDE: Wideband Very-High-Frequency Data Exchange
VDES: Very-High-Frequency Data Exchange System
VDL: Very-High-Frequency Data Link

References

1. Lázaro, F.; Raulefs, R.; Wang, W.; Clazzer, F.; Plass, S. VHF Data Exchange System (VDES): An enabling technology for maritime communications. *CEAS Space J.* **2019**, *11*, 55–63.
2. International Telecommunication Union. *Technical Characteristics for a VHF Data Exchange System in the VHF Maritime Mobile Band*; Recommendation ITU-R M.2092-0; ITU: Geneva, Switzerland, 2015.
3. International Maritime Organization. Sub-Committee on Navigation, Communications and Search and Rescue (NCSR), 11th session[EB/OL]. Available online: https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/NCSR-11th-session.aspx (accessed on 5 August 2024).
4. Raulefs, R. Overview of the VHF Data Exchange System. In Proceedings of the OCEANS 2022, Hampton Roads, VA, USA, 17–20 October 2022; pp. 1–4.
5. Alagha, N.; Løge, L. IJSC&N Special Issue "Opportunities and challenges of maritime VHF data exchange systems": Guest editorial message. *Int. J. Satell. Commun. Netw.* **2023**, *41*, 99–101.
6. Dong, H.; Song, L.; Hua, C.Q.; Liu, L.Y.; Tang, J.H. Survey of The Research and Development on The Maritime Communication Technology. *Telecommun. Sci.* **2022**, *38*, 1–17.
7. Kim, W; Lee, M.S.; Shin, G; Kim, H; Lee, C.H.; Kim, Y; Yoon, I.J. Ferrite-Loaded, Low-Profile Grounded Bowtie-Loop Antenna for VHF Communication, in IEEE Antennas and Wireless Propagation Letters, vol. 22, no. 12, pp. 3132-3136.
8. Chen, X.Q.; Ma, D.F.; Liu, R.W. Application of Artificial Intelligence in Maritime Transportation. Journal of Marine Science and Engineering 12(3): 439.
9. Gong, G. The Research and Validation on Influencing Factor of AlS Slot Collision. Master's Thesis, Dalian Maritime University, Dalian, China, 2013.
10. D'andreagiovanni, F.; Mett, F.; Nardin, A.; Pulaj, J. Integrating LP-guided variable fixing with MIP heuristics in the robust design of hybrid wired-wireless FTTx access networks. *Appl. Soft Comput.* **2017**, *61*, 1568–4946.
11. Kennington, J.; Olinick, E.; Rajan, D. *Wireless Network Design: Optimization Models and Solution Procedures*; Springer: Berlin/Heidelberg, Germany, 2010.
12. Nace, D.; Pióro, M.; Poss, M.; D'Andreagiovanni, F.; Kalesnikau, I.; Shehaj, M.; Tomaszewski, A. An optimization model for robust FSO network dimensioning. *Opt. Switch. Netw.* **2019**, *32*, 25–40.
13. D'Andreagiovanni, F.; Mannino, C.; Sassano, A. Negative Cycle Separation in Wireless Network Design. In *Network Optimization, Proceedings of the 5th International Conference, INOC 2011, Hamburg, Germany, 13–16 June 2011*; Springer: Berlin/Heidelberg, Germany, 2011.

14. D'Andreagiovanni, F.; Gleixner, A. Towards an accurate solution of wireless network design problems. *Comput. Sci.* **2016**, *9849*, 135–147.
15. Lehto, A.; Sestorp, I.; Khan, S.; Gurtov, A. Controller Pilot Data Link Communication Security: A Practical Study. In Proceedings of the 2021 Integrated Communications Navigation and Surveillance Conference (ICNS), Dulles, VA, USA, 19–23 April 2021; pp. 1–11.
16. International Association of Lighthouse Authorities. *VDES VHF Data Link (VDL) Integrity Monitoring*; Guideline G1181, Saint Germain en Laye, France: IALA, 2023.
17. Li, M.M.; Shi, H.P.; Han, R.; Zhang, X.Y. Study on Co-Channel interference between VDE-Sat System and Land Mobile Communication System. *China Radio* **2021**, *4*, 38–42.
18. Quintana-Diaz, G.; Birkeland, R.; Loge, L.; Andersen, E.; Bolstad, A.; Ekman, T. In-orbit Interference Measurements and Analysis in the VDES-band with the NorSat-2 Satellite. In Proceedings of the 2022 IEEE Aerospace Conference (AERO), Big Sky, MT, USA, 5–12 March 2022; pp. 1–8.
19. Fei, C.; Zhao, B.; Yu, W.; Wu, C. A routing strategy for software defined satellite networks considering control traffic. *J. Beijing Univ. Aeronaut.* **2018**, *44*, 2575–2585.
20. Yang, Y. Research on Civil Maritime VDES Equipment Authentication and Broadcast Encryption Scheme. Master's Thesis, Sichuan University, Chengdu, China, 2021.
21. d'Afflisio, E.; Braca, P.; Willett, P. Malicious AIS Spoofing and Abnormal Stealth Deviations: A Comprehensive Statistical Framework for Maritime Anomaly Detection. *IEEE Trans. Aerosp. Electron. Syst.* **2021**, *57*, 2093–2108.
22. Frasconi, M.; Mando, G. Authentication mechanisms for VHF Data Exchange System (VDES). 2022. Available online: https://www.researchgate.net/publication/364410997_Authentication_mechanisms_for_VHF_Data_Exchange_System_VDES (accessed on 5 August 2024).
23. Louart, M.; Szkolnik, J.J.; Boudraa, A.O.; Le Lann, J.C.; Le Roy, F. Detection of AIS messages falsifications and spoofing by checking messages compliance with TDMA protocol. *Digit. Signal Process.* **2023**, *136*, 1051–2004.
24. Wimpenny, G.; Šafář, J.; Grant, A.; Bransby, M. Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *J. Navig.* **2021**, *75*, 333–345.
25. Zhang, F.; Wang, M.H.; Zhu, L.H. Design of an OFDM－based VDES Ground Subsystem. *Telecommun. Eng.* **2018**, *58*, 826–832.
26. Li, W.Y.; Liu, C.; Ji, X.Y.; Li, J.H. Virtual navigation aids and its message design based on VDE-SAT. *China Harb. Eng.* **2021**, *41*, 8–11.
27. Hu, X.; Lin, B.; Wang, Z. VDES-based Space, Air, Ground and Sea Integrated Communication Networks: Architecture and Key Technologies. *Mob. Commun.* **2019**, *43*, 2–8.
28. Jing, Q.; Sha, J. The Use of SNN for Ultralow-Power RF Fingerprinting Identification with Attention Mechanisms in VDES-SAT. *IEEE Internet Things J.* **2023**, *10*, 15594–15603.
29. Jamal, H.; Matolak, D.W. Advanced Physical-Layer Technologies in VHF Data Link Communications. In Proceedings of the 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 11–15 October 2020; pp. 1–8.
30. Hu, X.; Lin, B.; Wang, P.; Wang, Y. A Novel MAC Protocol for VDES in Space-Air Ground-Sea Integrated Networks. In Proceedings of the 2020 International Conference on Space-Air-Ground Computing (SAGC), Beijing, China, 4–6 December 2020; pp. 60–61.
31. Zeng, Y.; Qing, X.; See, T.S.P.; Peng, X. Circularly Polarized Turnstile Antenna for VHF Data Exchange System (VDES) on Satellite. In Proceedings of the 2020 IEEE International Conference on Computational Electromagnetics (ICCEM), Singapore, 24–26 August 2020; pp. 252–253.
32. Zheng, H.; Huang, Y.; Chen, L. The Regional Protocol for Local Communications Among Maritime Autonomous Surface Ships Based on VDES. In Proceedings of the 2023 7th International Conference on Transportation Information and Safety (ICTIS), Xi'an, China, 4–6 August 2023; pp. 2223–2229.
33. Ma, S.; Shi, K.; Meng, X.; Li, X. Frequency Offset Estimation Algorithm of VDES Signals Based on Cross-Correlation. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 1234–1238.
34. Shim, W.; Kim, B.; Kim, E.-J.; Kim, D. A New Link Adaptation Technique for Very High Frequency Data Exchange System in Future Maritime Communication. *Electronics* **2024**, *13*, 323.
35. Zhang, L.; Lin, B.; Zhang, S.; Zhao, T.; Zhang, Y. An Improved MAC Protocol Design in VHF Data Exchange System (VDES) For Internet of Vessels. *Procedia Comput. Sci.* **2018**, *129*, 1877–0509.
36. Wang, X.; Wang, Y.; Fu, L.; Hu, Q. An AIS Base Station Credibility Monitoring Method Based on Service Radius Detection Patterns in Complex Sea Surface Environments. *J. Mar. Sci. Eng.* **2024**, *12*, 1352.
37. Zhong, L.; Wan, W.; Kong, D. Java Web Login Authentication Based on Improved MD5 Algorithm. In Proceedings of the IEEE International Conference on Audio Language and Image Processing (ICALIP), Shanghai, China, 11–12 July 2016; pp. 131–135.
38. Stevens, M.; Sotirov, A.; Appelbaum, J.; Lenstra, A.; Molnar, D.; Osvik, D.A.; De Weger, B. Short Chosen-Prefix Collisions for MD5 and The Creation of A Rogue CA Certificate. In Proceedings of the CRYPTO 2009: Proceedings of the 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2009; pp. 55–69.
39. Cheng, K.; Han, W.B. Improvement on chosen-prefix collisions for MD5 and complexity analysis. *J. Comput. Appl.* **2014**, *34*, 2650–2655, 2682.

40. Huai, S.H. Research on the Theory and Key Technology of Real-time Detection of AIS Autonomous Positioning Information. Doctor's thesis, Dalian Maritime University, Dalian, China, 2020.
41. Gaitan, M.G.; D'Orey, P.M.; Santos, P.M.; Ribeiro, M.; Pinto, L.; Almeida, L.; De Sousa, J.B. Wireless Radio Link Design to Improve Near-Shore Communication with Surface Nodes on Tidal Waters. In Proceedings of the OCEANS 2021: San Diego–Porto, San Diego, CA, USA, 20–23 September 2021; pp. 1–8.
42. Habib, A.; Moh, S. Wireless Channel Models for Over-the-Sea Communication: A Comparative Study. *Appl. Sci.* **2019**, *3*, 443.
43. Yang, Q. The Characteristics Analysis of Costal VHF Signal Propagation. Master's Thesis, Dalian Maritime University, Dalian, China, 2017.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.