Performance Evaluation of Disruption Tolerant Networks on Warships' Tactical Messages for Secure Transmissions

Davi Falcão, Ronaldo Salles, and Paulo Maranhão

***Abstract*—Disruption tolerant networks (DTN) are an evolution of mobile adhoc networks (MANET) working in scenarios where nodes are sparsely distributed, with low density, connections are intermittent and end-to-end infrastructure is not accessible. Therefore, DTNs are recommended for high latency applications that can last from hours to days. The maritime scenario has characteristics that would justify the use of DTN networks, but the concern with data security is also a relevant aspect in such scenarios. Thus, this paper proposes to evaluate the DTN approach in the maritime Scenario involving warships and helicopters, for sending tactical messages, taking into consideration security aspects at the perimeters where contacts occur. We set up a simulation experiment to compare the performance of Epidemic, Spray and Wait, and Direct Delivery protocols in three scenarios with different sizes. We also propose the application of discriminant analysis as a classification technique to select secure connections to improve the security of the DTN architecture.**

***Index Terms*—Discriminant function, DTN, epidemic protocol, security, tactical messages, warship scenario.**

I. INTRODUCTION

SHIPPING is responsible for about 90% of international trade, which justifies a large global investment in maritime commerce and port areas. This makes the sea a strategic area that generates wealth for countries that know how to correctly exploit their resources.

Along with the growing demand of maritime commerce, there is a need to keep these ships communicable and sharing information, such as geolocation, weather data, distress calls, etc. Communication solutions for maritime environments are generally slower and more expensive than land-based solutions [1]. They rely on conventional high frequency (HF), very high frequency (VHF) and ultra high frequency (UHF) technologies for near-shore communications and satellite systems for long-area coverage [2].

It is important to choose a network infrastructure that supports secure communication in scenarios where nodes are sparsely distributed, has an acceptable packet delivery rate and low costs. Knowing also that the data shared during missions has a high degree of confidentiality, it is mandatory to use techniques that restrict access to information, such as encryption-based solutions. Even knowing that there is no infallible security solution, it is necessary to adopt mechanisms that make it difficult for attackers.

Warships need to exchange tactical data during their missions and training. The tactical networks of warships are responsible for sharing data from the tactical subsystems. However, ships suffer from signal intermittency, making it difficult for their data to reach all destinations, what increases data retransmission rates on the network as a result of the many delivery errors. It is important to choose routing strategies that decrease retransmission rates and increase the probability of successful delivery [3], [4].

It should also be said that satellite communications are not always feasible due to the high cost of contracting this type of service, and sometimes leads to a strong technological dependence in a critical sector for defense purposes.

Traditional solutions, applied to terrestrial wireless scenarios, cannot be adopted for maritime communications due to the natural constraints of this type of environment. Some alternatives to minimize the problems include the installation of long distance modems with low transmission rates.

However, traditional routing strategies based on TCP/IP stack protocols require nodes to be within range of the wireless network's transmission point.

Therefore, delay or disruption tolerant networks (DTN) [5], [6] emerge as an appropriate technological alternative for scenarios that present long delays and frequent disconnections, thus it is possible to envision their use in the tactical message sharing of warships.

However, the security issue is not yet native to DTN networks and should be considered as a critical requirement for combat scenarios, where sensitive messages should only be transmitted in an encrypted form. However, this would not prevent crypto-analysis techniques being used to try to deduce the secret key and somehow decrypt the message using brute force, for example [7], [8].

The methodology followed by this work started with a review of the scientific literature on the subject of opportunistic networks in the maritime environment. To ensure the consistency of the simulations, real ship and helicopter route sections were used to compose the scenarios, which were edited using the open source tool known as OpenStreetMap. Some of

Manuscript received August 14, 2020; revised September 21, 2021; approved for publication by Heejo Lee, Division III Editor, November 18, 2021.

The authors gratefully acknowledge the following organizations that provided financial support and/or guidance for this project. Firstly, we thank the Brazilian Navy and the Brazilian Federal Government for having financed this research at the Instituto Militar de Engenharia (IME). It is also necessary to thank the IME for providing physical space and its professionals for guiding me during the period of two years.

D. Falcão, R. Salles and P. Maranhão are with Graduate Program in Defense Engineering (PGED), Instituto Militar de Engenharia (IME), Praça Gen. Tibúrcio, 80 - Urca, Rio de Janeiro - RJ, 22290-270, email: dmafalcao@gmail.com and {salles, maranhao}@ime.eb.br.

D. Falcão is the corresponding author.

Digital Object Identifier: 10.23919/JCN.2021.000043

the most cited DTN network protocols were selected for comparison in terms of performance, taking into consideration: message delivery rate, message delay, number of ships, impact of the number of high-speed vehicles (helicopters or drones) etc. This was made possible using a free opportunistic network simulation tool, The ONE [9].

The simulations were performed in three different scenarios, each varying in area, number of messages created, message size, distribution of nodes in the network, etc. From this point on, the work addressed the issue of security and proposed a new mechanism that contributes to the selection of secure connections, classifying them as a result of statistical analysis of the data obtained from the perimeter and that were chosen empirically, through a mathematical function that allows the classification of connections into two major groups: secure and insecure.

The main contributions of this work are:

- To evaluate the performance of some of the most cited DTN protocols (Epidemic, Spray and Wait and Direct Delivery) to find the best suitable for warship scenarios; and
- To develop and evaluate a security module for DTN networks based on a multivariate data analysis technique that allows the classification of connections as trusted or not. Such classification technique minimizes the sharing of confidential messages with untrusted nodes. This module constitutes the major contribution of this work regarding the security of the DTN architecture applied to warship tactical scenarios. Usually, these tactical scenarios feature few warships, sparsely distributed, and surrounded by a larger number of civilian vessels.

The structure of this paper is organized as follows, Section II presents the main works that relate to the current topic, Section III presents the main characteristics of DTN networks in maritime scenarios and describes the behavior of some of the DTN protocols, Section IV presents the concept of secure connection, Section V explains the connection classification technique adopted in this work, known as Discriminant Function. Section VI deals with information about the simulations and their results and finally in Section VII the paper is concluded.

II. Related Work

Mohsin and Woods [10] proposed the use of a mobile ad-hoc networks (MANET) [11], [12] as a low-cost alternative for ship-to-ship VHF radio communication. The work evaluated four MANET protocols for the maritime scenario: Ad-hoc on-demand distance vector protocol (AODV), ad-hoc on-demand multipath distance vector protocol (AOMDV), dynamic source routing protocol (DSR) and destination sequenced distance vector protocol (DSDV). The AOMDV was considered the most efficient protocol.

Mohsin *et al.* [13] also addressed the MANET issue in the maritime setting by simulating three different types of MANET protocols. He concluded that the routes that most ships develop tend to facilitate packet delivery over multiple hops. According to the text, the performance of MANET protocols had a positive relationship with density and an inverse relationship with mobility, losing performance in very sparse scenarios. This means that delivery rates increase with the number of ships in the area (density) and decrease as the mobility of the nodes in the network increases, making scenarios sparser. They also presented the application of MANET as a lower cost alternative for ships.

K. Youngbum [4] proposed to use a network similar to vehicular ad-hoc network (VANETS) in maritime environment called nautical ad-hoc network (NANET). NANET is a hybrid mesh-mode network architecture to increase communication capacity with ships. The observed simulations occurred in three different maritime scenarios located in the harbor, on the coast, and in the ocean. In all of them the NANET was simulated with the ships both inside and outside the coverage of the Base Radio Stations. However, a MANET needs to establish an end-to-end route before sending a message, but this requirement is not always possible in maritime scenarios due to the large number of connections and disconnections.

S and Viswanathan [14] talked about the main types of attacks that are used in DTN networks, such as denial of service (DOS) and distributed denial of service (DDoS) attack that are used to disrupt proper operation during message forwarding. In DTN networks, messages are shared when two nodes meet and remain within a range. The main goal is to get nodes to collaborate with each other so that messages reach their recipients. However, attacks on DTN networks are carried out by malicious nodes in order to restrict routing. The work advocated the use of methods to detect malfunctioning nodes so that they could be bypassed and excluded from the network, leaving only those nodes that actually contributed to message forwarding. Malicious nodes, at the time of the attack, present false forwarding metrics, but upon receiving messages simply discard them, even though there is still free buffer space. A well-known DOS attack for DTN networks is the Black Hole Attack, where malicious nodes lure as many messages as possible from the network and then purposely discard them without making any kind of real attempt to forward or deliver.

Chen and Shen [15] propose a new mechanism to keep the routing information of nodes confidential. This routing information, called routing utility, was used to calculate the probability of routing messages to their recipients. The routing information contains the records of encounters and the frequency of those encounters, and with it, it is possible to estimate which will be the best forwarders in the DTN network for a given recipient. However, in a malicious attack, it is possible to generate fake data to fool other nodes in the network; this allows malicious nodes to pretend to have the best routing metrics; however they will discard all messages instead of forwarding them. The proposed security mechanism advocated partial disclosure of routing information; the rest would remain protected by cryptologic features.

In Li *et al.* [16] a mechanism for exchanging encounter tickets is proposed to bring more reliability in the choice of routing nodes in the DTN network. The tickets act as a guarantee that the encounters really happened over time, preventing malicious users from creating false routing information to pretend to be good routers. This strategy became effective in combating the black hole attack, but was still fragile for the tailgating attack. Tailgating attacks generate fake encounters with the goal of accumulating tickets, so that later the malicious nodes can present themselves as good routers, but this type of attack is known to require a lot of mobility and energy consumption. It is said that the best strategy to combat black hole and tailgating attacks would be to use routing protocols that implement random propagation, i.e., without using probability.

Chrysostomou [2] recommended a hybrid network architecture approach involving conventional maritime communications and DTN technologies. The paper emphasized the benefits of DTN networks at sea when nodes are sparsely distributed, so it performed simulations in three different scenarios in terms of area, using different types of routing protocols: Epidemic, Prophet, MaxProp, Spray and Wait, and RAPID. It was concluded that the probabilistic routing protocols obtained a better use of available network resources, as well as presented a good performance in the delivery of packets, knowing that the more information about the future mobility of ships, the more efficient the system will be in detecting changes in network topology. However, as a disadvantage, probabilistic protocols rely heavily on a priori data that is usually used in routing decisions, making them more sensitive to sudden changes, such as the reallocation of nodes in the scenarios, these changes consequently generate decision errors and lost routing opportunities. Probabilistic protocols are usually adopted in scenarios that have a larger number of available nodes, which would normally result in an increase in the number of connections, these protocols aim to save resources and avoid network congestion. However, in scenarios where few nodes are sparsely distributed, a protocol that would encourage more message dissemination without generating network outages might be better.

In general, the works dealing with ad-hoc networks in the maritime scenario have been limited to comparing the performance of different types of protocols in challenging environments [17], but none of them have emphasized the use of DTN networks for warships. As for security, there are several approaches that focus on some strategies related to cryptography and public and private key distribution mechanisms [15], [16]. However, as far as we know, there is no approach that has proposed any technique for classifying connections as to security and applying them to tactical scenarios at sea, using parameters that can be obtained at the communication perimeters of warships through equipment such as radar, sonar, etc.

III. DTN in the Maritime Environment

The maritime scenario [18] has peculiar characteristics that make it suitable for the use of Disruption Tolerant Networks.

DTN networks are recommended in challenging environments [5], marked by intermittent connections, absence of an end-to-end infrastructure, and that is benefited by node mobility [6], as is the case in warships. Other characteristics that make DTN networks attractive for the maritime environment are [2]: The low density in the distribution of ships, an unlimited buffer and power capacity, and the speeds of ships favoring prolonged contacts between them [13].

In general, the DTN architecture [6] proposes an improvement in the communication of scenarios where there is no end-to-end infrastructure [19], [20].

A. DTN Routing Protocols

Routing in DTN networks is basically divided into two strategies [21]: The first one is the flooding strategy, which is based on replicating messages to a large number of nodes in order to reach the destination node. In this approach, multiple copies of the same message are created and sent through a set of nodes called relay nodes. These nodes store the messages until they reach the destination nodes [22], [23].

Protocols based on the Flooding strategy do not need a priori knowledge about the networks, because they are not probabilistic. The second strategy is routing, which uses a priori knowledge about the networks to select the best path to the recipient, because its protocols are probabilistic.

This strategy uses a priori knowledge of the network topology or about any other important information that allows the choice of the best path to the recipient. In this way, messages are not routed randomly, but based on previously available information. There are also hybrid approaches that combine Flooding and Forwarding strategies according to the need.

1) Single Hop Transition or Direct Delivery: It is considered the simplest algorithm, in which the source will transmit directly to the recipient, immediately when they make contact [21], so there are no retransmissions through intermediate nodes. In this type of protocol, each node carries only its own message, the big advantage of this is that it is not necessary to allocate large storage resources for this type of protocol. However, message delay times will be the highest compared to other protocols that perform routing. Another important detail is that this behavior decreases the probability of delivering messages to the recipients. This type of protocol is only recommended when you realize that there is a lot of movement in the network and that the source and destination nodes are a hop away, i.e., they are neighbors.

2) Two-Hop Relay: In this protocol, retransmissions will only occur between the source node and those nodes with which it has been in contact in the first moment. Then these nodes must cooperate, taking these messages with them until they reach the final recipient, without generating more retransmissions. This type of protocol significantly increases the probability of message delivery when compared to Direct Delivery, but still has the same limitations as the previous protocol, in addition to increased bandwidth and storage usage [21].

3) Epidemic Routing: Epidemic is considered the first DTN routing protocol. It assumes that each node has unlimited bandwidth and storage, this means that theoretically every node can store all messages received during established contacts. Each node keeps a list of messages in an internal database and may transmit entire messages to other nodes during contacts. In scenarios where the nodes are sparsely distributed and the messages exchanged are short, this may come to be considered a good protocol. However, the biggest problem with epidemic routing is that the message continues to propagate even when it reaches its destination. Another major disadvantage is that this type of routing consumes a large amount of resources [21]. It was called Epidemic because of its behavior, similar to the transmission of a contagious disease, since the node carrying a message will try to transmit it to all nodes in contact, without any criteria.

4) Spray and Wait: This protocol works in two phases, the first is called the Spray phase in which each node will flood the network with copies of the messages to a number of L relay node type nodes, and the value of L is configurable at the source node. If the message reaches the destination node, the transmission is interrupted; otherwise it will enter the Wait phase where relay nodes can transmit only during the contacts phase. The value of L is calculated taking into account node density, distribution and mobility profile [21].

IV. Connection Security

Radio communication takes place using electromagnetic waves that propagate between transmitting and receiving antennas. An electromagnetic wave has the ability to carry energy. The wave propagates through three wave phenomena: reflection, refraction, and diffraction. The transmitting antenna converts voltage and current variations into electromagnetic waves, while the receiver does the reverse work, transforming the energy carried by electromagnetic waves into voltage and current variations. Electromagnetic waves are represented by sine waves (one for the electric field and one for the magnetic field). In general, antennas can be classified as directional and omnidirectional.

A directional antenna increases the range in terms of distance, but the coverage angle decreases. Directional signals are stronger because they concentrate power in one direction. A directional antenna has the advantage of not spreading the signal into all directions, so it ends up naturally contributing to have more secure connections than an omnidirectional, which radiates its signal in all directions.

Omnidirectional antennas send the signal in all directions. They have the advantage of a 360° coverage angle. However, while omnidirectional antennas offer more possibilities for connectivity by radiating electromagnetic waves in all directions, they consequently offer security gaps. Before transmitting the data, the originating ship tests the receiver for authenticity, and there may be encrypted message exchanges in this procedure. However, there must also be other ships that, although not part of the same network, can pick up these electromagnetic waves through their antennas. For this reason, messages must be encrypted to protect their content, so that only those who have the keys can access their content. However, crypto-analysis techniques can always be applied in this context in order to discover the clear text. DTN networks work more efficiently in environments where nodes are sparsely distributed, because environments with large agglomerations favor deliveries by direct contact instead of routing through intermediate nodes, given that in denser scenarios there is a greater probability of source and destination nodes meet and exchange messages directly. Another problem that could occur in DTN architecture in highly concentrated environments would be the high consumption of routing resources, due to the large number of contacts, generating high energy and storage costs, especially when the routing protocol used is not probabilistic.

Among the issues pertinent to Disruption Tolerant Networks, security is a point that needs to be considered, because just as cyber-attacks can occur in conventional networks, versions can be adapted for DTN networks [24]. A DOS can be considered the most common for DTN networks, and a simple strategy to control this type of attack is the exclusion of infected nodes after they are detected. This detection is possible by monitoring the network. A faulty node behaves by discarding all the messages it should forward, yet it tries to look as if it is in perfect condition to perform the forwarding (Black Holes Attack) [25].

In some previous work, the system detected the malicious nodes through the message forwarding histories that were shared by the nodes, based on these histories, the nodes that were not working correctly would be excluded from the network [14]. The misbehavior of nodes in the DTN network will accuse those that are considered malicious and this is only possible by monitoring and sharing packet forwarding information across the network [26].

Another strong indication of a defective node is when it starts flooding the network with requests, leaving the rest of the nodes inoperable through a buffer overflow, for example. This pattern can also be analyzed by the shared history and, if any anomaly is detected, these nodes are excluded from the network. Uncertainty increases computational costs and decreases acceptability of communication and cooperation, so choosing a decision model that is reliable (reducing uncertainty) is important both for efficient use of available resources and for establishing secure communication [27]. A warship has on its perimeter a number of parameters that can be used to classify a connection as secure or insecure. Based on these parameters, you can create a function to classify connections allowing the DTN protocol to block a given connection.

V. Discriminant Analysis

Discriminant Analysis is a multivariate statistical technique that can be used to classify items from a sample or population. Its application requires prior knowledge of the groups to which the sample elements belong to, that is, the groups must be known a priori. The central idea of the method is to build a mathematical rule based on probabilistic foundations so that each new sample item is classified in the previously known groups.

A. Construction of the Classification Rule

To construct a classification rule, it is necessary to know the probability distributions of the characteristics of the population elements. In addition, the set of observations in each population must be independent. Thus, if these two requirements are met, the maximum likelihood method can be applied to develop the classification rule.

The maximum likelihood principle aims to estimate unknown parameters from the sample data minimizing the chance of misclassification of the new sample items, because although the probability distributions of the populations involved are known, in practice, their parameters are not known. Thus, through this principle, a function is initially created, called the discriminant function, given by the ratio between the density functions (probability functions in the discrete case) of the populations considered in the study. If there are only two populations in the study, say A and B, the discriminant function is given by (1), where x is an observation vector while $f_A(x)$ and $f_B(x)$ are the probability density functions of populations A and B respectively.

$$fd(x) = \frac{f_A(x)}{f_B(x)} \tag{1}$$

If populations A and B are drawn from a normal distribution with means μ_A and μ_B respectively and the same variance σ^2, the discriminant function is given by (2):

$$fd(x) = \frac{\frac{1}{\sigma\sqrt{2\pi}}e^{-(x-\mu_A)^2/2\sigma^2}}{\frac{1}{\sigma\sqrt{2\pi}}e^{-(x-\mu_B)^2/2\sigma^2}}. \tag{2}$$

In this way, for a fixed value of x, it is possible to calculate the value of the discriminant function. Thus, if $fd(x) > 1$ it is more likely that the element belongs to population A, otherwise, the highest probability would be that it belongs to population B. Still, if $fd(x) = 1$, the element could be classified in either A or B, which according to Mingoti [28], is equivalent to tossing a coin to decide whether the element would belong to groups A or B.

In the case where there are k populations to classify, the rule is to calculate the density function value for each population and again, for a fixed value of x, that population with the maximum density function value will be the population to which the new sample element belongs. Also, when formulating the classification rule, it is common to take into account more than one variable when calculating the discriminant function.

In this case, the discriminant function can be obtained as a linear combination of discriminant variables as follows in (3):

$$fd(x) = C + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_n x_n, \tag{3}$$

where C is a constant, the β's are the discriminant coefficients, the x_i's are the discriminant variables and n is the number of discriminant variables. To select these variables one can use the same techniques as in regression models, to learn more about variable selection, see Montgomery *et al.* [29].

B. Quality of Classification and Estimation of the Probabilities of Misclassification

In the previous subsection, the concern was to determine a classification rule for the new sample elements considering prior knowledge of the populations or groups in the study. However, it is possible to evaluate the quality of the classification performed and find the probabilities of misclassification. For the case of two populations, one of the rules for assess quality uses the calculation of the numerical score of the discriminant function for each population considered. Thus, if the function is adequate, the scores for each population are expected to be very different. In practice, this evaluation is equivalent to a mean comparison test. In the case where the populations are independent and normally distributed, the test is defined by the followed F-statistic (4) [30]:

$$F = \frac{(n_i + n_j - p - 1)}{p(n_i + n_j - 2)}T^2, \tag{4}$$

where n_i and n_j are respectively the sizes of the populations i and j, and p is the number of discriminant variables used in the classification. Besides, $T^2 = \frac{n_i n_j}{n_i + n_j}(\overline{Y}_i - \overline{Y}_j)$ and $\overline{Y}_i$ and $\overline{Y}_j$ are the discriminant function scores when applied to the sample means vectors of populations i and j, respectively.

Note that T^2 carries the information of the distance between the discriminant functions' scores, and it is represented by the difference between the averages of the samples of the discriminant functions' scores of populations i and j.

Furthermore, according to Anderson [31], it can be proved that under the assumption of normality of the populations, the F-statistic has Snedecor's F-distribution with p and $(n_i + n_j - p - 1)$ degrees of freedom.

Thus, for a defined significance level α, if the value of the F-statistic given by (3) is greater than the value tabulated by Snedecor's F-statistic, one can conclude the existence of a difference between the means, which implies the good quality of the classification.

Regarding the probabilities of incorrect classifications, two types of errors must be considered:

- Type 1 Error: When the sample element is classified as belonging to population i, when it actually belongs to population j.
- Type 2 Error: When the sample element is classified as belonging to population j, when it actually belongs to population i.

It is possible to determine the probabilities of both errors and there are several methods for this, among which we can mention: the Resubstitution Method, the Holdout Method and the Lachenbruch Method. For more on this subject, see Mingoti [28]. Obviously, the smaller these errors are, the better the classification rule will be.

C. Discriminant Connection Analysis

The objective to be achieved with discriminant analysis in this paper is to classify the connections of a DTN network as being safe or unsafe, based on parameters that are related to the node encounters in the network. For this, two types of antenna configuration were considered, either omnidirectional or directional, as shown in Figs. 1 and 2, respectively.

In this work, some security parameters were taken into account to compose the discriminant functions, such as: the number of allies and enemies nodes in the perimeter (the area covered by the antenna, it is about 10 to 13 km) , the distance

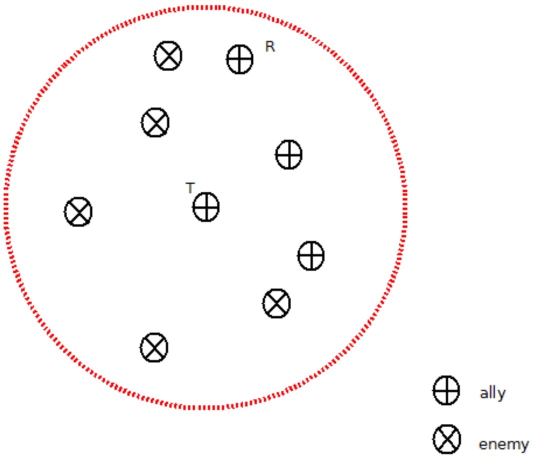


Fig. 1. Omnidirectional irradiation. Transmitter (T) needs to send the message to Receiver (R), but eventually radiates to the entire perimeter.

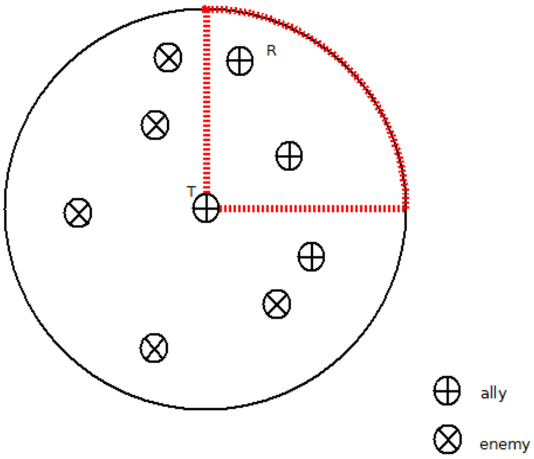


Fig. 2. Directional irradiation. The Transmitter (T) needs to send the message to the Receiver (R), so it radiates in the quadrant whose recipient is present, with a fixed angle of 90º degrees.

between the source and destination nodes, the distance from the nearest enemy node, the distance from the closest ally node and whether the closest and recipient nodes are allies (safe nodes) or enemies (unsafe nodes).

The specific security parameters used in the directional algorithm were the distance from the source node to the destination node, whether the recipient is an ally or enemy, the number of allies and enemies present in the antenna's line of sight and whether the host closest to the sight is an ally or enemy.

The directional function implemented in this work considered, as irradiation area, the specific quadrant (90º degrees) in which the recipient node is located, excluding the others. For this reason, the directional discriminant function received data obtained exclusively from the quadrant in which the recipient node was included, according to Fig. 2.

These parameters are important in deciding whether or not to transmit information within the perimeter during a given connection, taking into account issues of security involving the presence of unauthorized ships. For example, if at a given perimeter there are no enemies present, it can be said that the connection is totally safe to transmit. Similarly, if in the region of an encounter there are more allies than enemies, and if the destination (ally) node is the node closest to the origin node, there will be a greater possibility of considering this region as being safe.

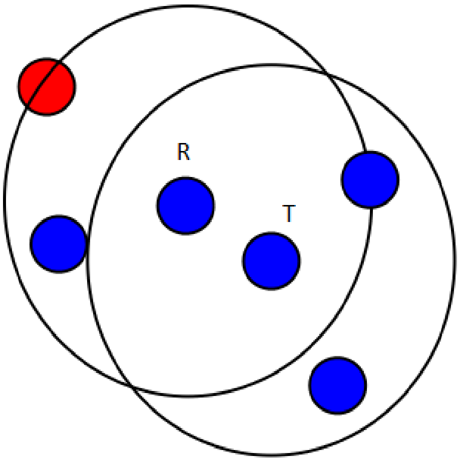


Fig. 3. Example of safe encounter between transmitter (T) and receiver (R).

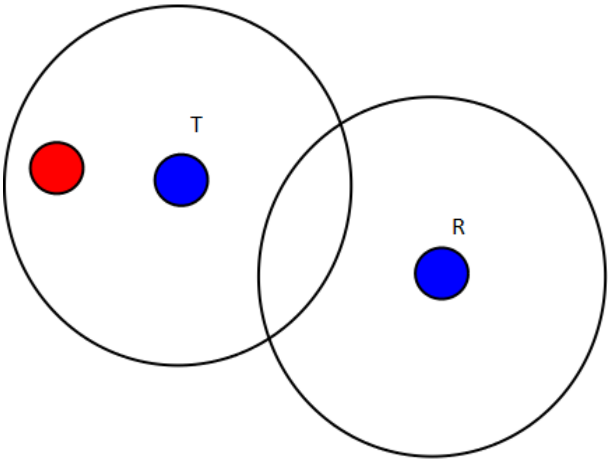


Fig. 4. Example 1 of unsafe encounter between transmitter (T) and receiver (R).

Fig. 3 shows a transmitter (T) and receiver (R) at a perimeter with more allies (in blue) than enemies (in red). In this case, the connection could be considered secure. However, if there are more enemies than allies at the perimeter of a connection, or if these enemies are too close to the source or the destination node, there is a high chance of signal interception, so this connection should be considered insecure by algorithm.

Figs. 4 and 5 show a transmitter (T) trying to forward messages to the receiver (R), both are allies, but there is an enemy at the perimeter (in red), so this connection should be classified as insecure. Thus, the discriminant analysis uses the same parameters that were used to classify a priori the elements that represent effective encounters as safe or insecure. Finally, to create a discriminant function that classifies, with an appropriate level of precision, the elements representing connections as safe or unsafe.

The software used to perform the discriminant analysis was

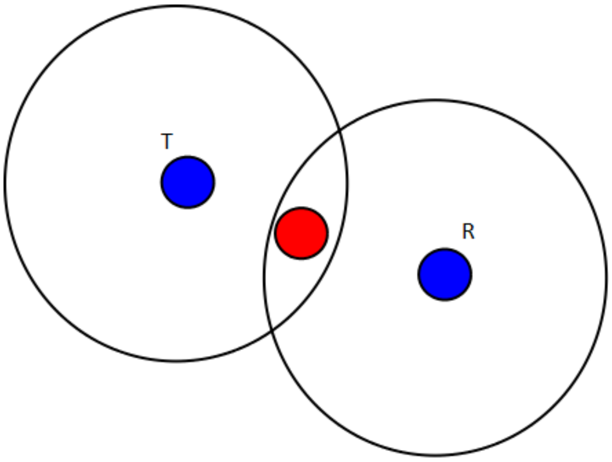


Fig. 5. Example 2 Unsafe encounter between transmitter (T) and receiver (R).

MINITAB, from Minitab Inc. The selection of the parameters for discriminant analysis was made empirically, taking into account those that were most relevant in the safety issue. In this process, parameters were added while others were removed (as they were of little relevance during the analysis), so that discriminant functions could reproduce results closer to those presented a priori. The a priori classification data was extracted from simulations.

The discriminant function would classify even a connection involving two allied nodes as unsafe, because the discriminant function takes into account other variables that represent important perimeter information about security.

VI. Simulations

This section is responsible for showing the results and explanations about what was observed during the simulations.

A. Simulations Setup

In this work, three different scenarios were used whose routes represented real movements of warships and helicopters in maritime environments. These routes were combined with the help of the OpenStreetMap tool resulting in the three scenarios that can be seen in Fig. 6.

The first one represented an area of 150 km^2, consisting of eight overlapping routes, two of which were used exclusively by helicopters. The second had an area of 400 km^2, consisting of two common routes for ships and helicopters. Finally, the third had an area of 600 km^2, consisting of three routes, one of which was exclusively for helicopters. In each scenario, about 200 simulations were performed, each corresponding to 12 hours of movement in a maritime environment. Initially it was considered that the amount of messages created would be few in a 12 hour interval, so in the first simulations only 16 messages were created.

However, additional simulations were performed with 346, 585 and 587 messages created. Message sizes ranged initially from 11 to 100 bytes and then from 11 to 1000 bytes. The transmission range of each node was defined with a radius ranging from 12 to 13 km, with transmission rates varying between 300, 600, 1200 and 4800 bits per second. The speeds of warships could reach 18 knots, while helicopters developed a speed between 100 and 300 km/h.

For comparison, in terms of message delivery performance, 3 most commonly cited DTN routing protocols were used: Direct Delivery, Epidemic and Spray and Wait; remembering that the Direct Delivery protocol represents the closest behavior to a network without the benefits of message retransmission, that is, similar to conventional non-DTN networks. This is why this configuration was used to represent a scenario without the benefits of DTN networks.

The simulation results will be presented in tables using the following parameters: Total number of nodes (N.Nodes), a flag indicating the existence or not of helicopters in the simulation (Helicopter), total number of messages (N.Messages), message size (Size), average deliveries (A.V.Deliveries) and average delays (A.V.Delays).

B. Simulation results for Epidemic, Spray and Wait and Direct Delivery protocols

1) Scenario 1: In this scenario the movement of about 36 ships was observed, and in some moments four of them were replaced by helicopters, in order to verify the impact of the influence of higher speed vehicles. According to the results in Table I, the Epidemic protocol showed better performance in the delivery of 16 messages in Scenario 1.

This superiority was 7.80% over Spray and Wait and 32.99% over Direct Delivery. The added helicopters, in Scenario 1, contributed a remarkable 45.27% decrease in message delivery delay time using the Epidemic protocol. Overall, the simulations in Scenario 1 showed the Epidemic protocol as the one that showed the best performance in message delivery, about 98.45%. Next came Spray and Wait, delivering 90.65% of the messages, and finally Direct Delivery, delivering about 65.46% of the messages.

2) Scenario 2: In the first simulations of Scenario 2, the configuration conditions of Scenario 1 were repeated, the results are presented in Table II.

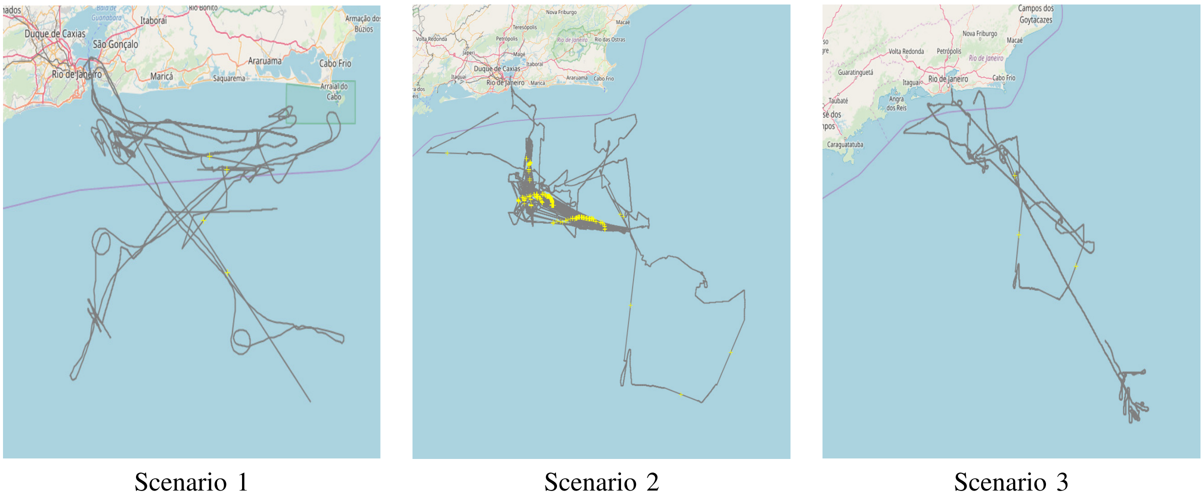
Scenario 2 presented a reduction in performance, in message delivery, in all protocols when compared to Scenario 1. This was due to the significant increase of $250km^2$ of area in the new scenario, while maintaining the same amount of 36 nodes.

Therefore, the message delivery rate for the Epidemic protocol was 61%, Spray and Wait was around 45%, and Direct Delivery was 17.55% of the 16 messages created. However, the Epidemic protocol continued to perform better, delivering 43.43% more than Direct Delivery and 16% more than Spray and Wait.

The helicopters caused an 11.20% reduction in the message delivery delay time of the Epidemic protocol.

Additional simulations were performed with the generation of 340 and 581 messages, but keeping the total number of 36 nodes, 4 of which were helicopters. The results of the new simulations in scenario 2 can be seen in Table III.

According to Table III, 67% of the messages were delivered



Scenario 1 Scenario 2 Scenario 3

Fig. 6. Scenarios of simulations represented on the OpenStreetMap Software.

TABLE I
SCENARIO 1 SIMULATIONS RESULT WITH 16 MESSAGES CREATED.

Protocol	**Epidemic**				**Direct Delivery**				**Spray And Wait**			
N.Nodes	36				36				36			
N.Messages	16				16				16			
Size(bytes)	100		1000		100		1000		100		1000	
Helicopter	Not	Yes	Not	Yes	Not	Yes	Not	Yes	Not	Yes	Not	Yes
Av. Deliveries	15,54	15,8	15,525	15,775	10,13	10,17	10,119	10,165	14,075	14,58	14,055	14,585
Av. Delays (Seconds)	633,55	338,15	716,46	415,92	4499,69	4340,85	4513,03	4349,62	2651,98	2396,01	2680,49	2400,02

TABLE II
SCENARIO 2 SIMULATIONS RESULT WITH 16 MESSAGES CREATED.

Protocol	**Epidemic**				**Direct Delivery**				**Spray And Wait**			
N.Nodes	36				36				36			
N.Messages	16				16				16			
Size(bytes)	100		1000		100		1000		100		1000	
Helicopter	Not	Yes	Not	Yes	Not	Yes	Not	Yes	Not	Yes	Not	Yes
Av. Deliveries	8,005	10,75	7,94	10,72	2,425	2,68	2,425	2,68	5,495	8,16	5,48	8,15
Av. Delays (Seconds)	6195,52	5513,56	6243,40	5593,83	5282,99	5563,86	5289,41	5599,31	6287,03	6285,76	6328,35	6305,29

via the Epidemic protocol, while the Spray and Wait protocol sent 53% and Direct Delivery only 18% of the 340 messages. However, in the simulations with 581 messages, Epidemic and Spray and Wait showed a tie around 64% of the delivered messages while Direct Delivery remained with 18% of the delivered messages.

3) Scenario 3: As expected, by increasing the scenario area and keeping the same amount of nodes, the rates of messages delivered to the recipient tend to decrease, because in this scenario the spacing between ships is greater, decreasing the probability of them meeting. To prove this hypothesis, in Scenario 3, simulations with 61 (25 new nodes) were subsequently performed. The results of the first simulation with 36 nodes, 16 messages of variable size up to 1000 bytes can be seen in Table IV.

In Scenario 3, the Epidemic protocol forwarded about 41.31% of the messages, the Spray and Wait protocol about 34.83% and the Direct Delivery about 15.81%. This showed that even with the sparse Scenario 3, the Epidemic protocol remained the best forwarder.

The helicopters contributed a 22% increase in message delivery in the Epidemic protocol. However, the simulator showed a 20% increase in average message delivery delays.

However, one explanation for this increase is in the time accounting of the messages delivered in the scenario with helicopters. That is, since these messages had not been delivered in the simulations without helicopters, their buffering time was disregarded by the simulator in the final calculation; giving a false impression that there was a drop in performance, when in fact more messages managed to reach the final recipient through the helicopters. Because it is the most extensive scenario, new simulations were performed with a larger number of ships and messages in Scenario 3. The number of nodes varied from 36 to 61 ships and messages varied from 346 to 585. The results of these new simulations can be seen in Table V.

There was a slight improvement of 4.21% in the delivery rate of the 346 messages created and of 2.81% in the delivery rate of the 585 messages created, in the Epidemic protocol, when the number of nodes was increased from 36 to 61.

TABLE III
SCENARIO 2 SIMULATIONS RESULT WITH THE CREATION OF 340 AND 581 MESSAGES, RESPECTIVELY.

Protocol	**Epidemic**		**Direct Delivery**		**Spray And Wait**	
N.Nodes	36		36		36	
Size (bytes)	1000		1000		1000	
Helicopter	Yes		Yes		Yes	
N.Messages	340	581	340	581	340	581
Av. Deliveries	220,62	360,85	57,325	97,88	174,355	360,3085
Av. Delays (Seconds)	6080,902	6429,012	5900,831	5978,24	6391,973	6424,89

TABLE IV
SCENARIO 3 SIMULATIONS RESULT WITH 16 MESSAGES CREATED.

Protocol	**Epidemic**				**Direct Delivery**				**Spray And Wait**			
N.Nodes	36				36				36			
N.Messages	16				16				16			
Size (bytes)	100		1000		100		1000		100		1000	
Helicopter	Not	Yes	Not	Yes	Not	Yes	Not	Yes	Not	Yes	Not	Yes
Av. Deliveries	5,05	8,65	5,05	8,625	2,57	2,455	2,57	2,455	4,415	7,135	4,41	7,125
Av. Delays (Seconds)	5441,96	6730,87	5494,54	6776,55	5534,78	5245,69	5542,84	5253,37	5839,78	6739,20	5875,18	6742,33

TABLE V
SCENARIO 3 SIMULATIONS RESULT WITH THE CREATION OF 346/585 MESSAGES, WITH THE PARTICIPATION OF 36/61 NODES AND THE INCLUSION OF HELICOPTERS.

Protocol	**Epidemic**				**Direct Delivery**				**Spray And Wait**			
Size (bytes)	1000				1000				1000			
Helicopter	Yes				Yes				Yes			
N.Nodes	36		61		36		61		36		61	
N.Messages	346	585	346	585	346	585	346	585	346	585	346	585
Av. Deliveries	115,475	192,7	130,535	203,26	55,885	95,285	53,565	76,25	100,815	171,16	103,005	160,85
Av. Delays (Seconds)	5856,344	5967,81	5228,19	5545,29	5754,15	5789,01	5483,66	5188,21	6002,00	6017,44	5790,32	5870,83

As the number of nodes in the network increased, the Epidemic and Spray and Wait protocols showed even a small performance improvement. This means that these new nodes, through mobility, filled some of the gaps in the new scenario, allowing a larger number of messages to reach their recipients.

Despite the good performance achieved by the Epidemic protocol in all scenarios, the strategy adopted for message forwarding, of this protocol, brought concerns about security issues. It can also be stated that the DTN protocols relied on collaboration from intermediate nodes that were not part of the network of the allied nodes, i.e., insecure collaboration. Excluding these collaborations coming from unsafe nodes would result in a performance loss of about 50% of the message delivery efficiency. This would mean that if these connections had simply been blocked, about half of the messages would not have reached the destination node, which is why there is a delicate balance between security and performance. So when one decides to block a connection that is deemed insecure, this action will affect the performance of the DTN network as a whole.

It is known that the messages of the tactical systems of warships are processed in encrypted mode. Even so, thinking about continuing the study, a security module for the Epidemic algorithm should be tested in order to add one more security layer for the tactical message traffic in warships. For this reason, new simulation results will be presented, in the same scenarios as before, but applying Omnidirectional and Directional Discriminant Functions to classify secure connections in the Epidemic protocol.

C. Epidemic protocol with Discriminant Function

The Epidemic protocol can cause network overload in high node concentration scenarios, resulting from the excessive amount of message forwarding and node buffer overflows, which leads to increased message discarding. However, in low density scenarios, with sparsely distributed nodes, the Epidemic protocol performed well in comparison with the Direct Delivery and the Spray and Wait protocols. Because it is non-deterministic, the Epidemic protocol tries to take advantage of every opportunity to transmit messages [23].

As seen earlier, the warship maritime environment exhibits characteristics of low node density and a large number of connections and disconnections over time. The Epidemic protocol aims to forward messages to all nodes that are in contact with each other, without any concern for the routing metrics of intermediate nodes. This type of protocol is recommended for networks that have few nodes and want to take advantage of as many contact opportunities as possible, but without any concern for the security issue.

In order to improve the security on DTN architecture communication, this work proposes the implementation of a security module that takes into account the configuration of the perimeter where the source and destination nodes are inserted, taking into consideration security indicator parameters such as:

TABLE VI
CONNECTIONS CLASSIFIED A PRIORI IN BOTH GROUPS.

Group	0	1
Total	2712	798

the quantity enemy ships present, the ally's proximity to the enemy, etc.

These parameters would be received as input and in return the system would classify the connection as being secure or insecure. This module would be used in the Epidemic protocol to detect secure connections and block unsafe ones. For the classification of these connections, a statistical technique called discriminant analysis [28] was used. As mentioned earlier, the Epidemic protocol has the ability to disseminate data during every connection opportunity. Thus the discriminant function could be applied to select secure connections from those ones detected by the Epidemic Protocol, based on the conditions of the communication perimeter. As you can see, comparing the two Diagrams (A and B) in the Fig. 7, the Epidemic protocol has been improved.

According to Diagram A, the Epidemic protocol is always looking for new connections, prioritizing the direct delivery to the recipient. However, if the source node is not in direct contact with any recipient, the protocol will prioritize a forwarding approach. A large amount of message forwardings is where the danger of insecurity lies.

According to Diagram B, at first is checked if there are any connections with the final recipients of the messages to be transmitted, if it is true, that connections will be accepted and the messages will be delivered to their respective recipients. Otherwise, the messages should be forwarded, but at this time, the discriminant function (generated during the discriminant analysis) will detect if a given connection is safe or not to transmit. Being considered secure, the data will be transmitted and the node (the warship) will carry on searching for new connection opportunities along its route, otherwise the connection will be blocked, so new connection opportunities will be sought by the node.

It is important to highlight that the discriminant function, in this work, was applied only over indirect message forwarding, therefore, it will not affect the performance of messages delivered directly. As stated before the large number of message forwardings can be considered the main weakness of the Epidemic protocol. The intention in this action was not to sacrifice the real opportunities to reach the final recipient. Next, the configurations of the omnidirectional and directional discriminant analysis will be shown.

1) Omnidirectional Discriminant Analysis Setup: A total of N, 3510 connections were simulated, of which 2712 were classified as unsafe connections (Group 0) and 798 secure connections (Group 1) a priori, as can be seen in Table VI.

TABLE VII
CONNECTIONS CLASSIFIED A POSTERIORI IN BOTH GROUPS.

		Predicted Class	
	Group	0	1
True Class	0	2680	30
	1	32	768
	Total of N	2712	798
	N correct	2680	768
	Proportion (Precision)	0,988	0,962

TABLE VIII
ACCURACY MEASUREMENT OF DISCRIMINANT FUNCTION.

Correct Classifications		
N	**Correct**	**Proportion (Accuracy)**
3510	3448	0,982

These data served as the basis for the multivariate discriminant analysis of connections to create a discriminant function, which is a mathematical expression that generates approximate results to those of a priori classification. It can be seen from Table VII that the approximation of the discriminant function generated with the results of a priori classification obtained a posteriori accuracy of almost 100% for both groups 0 and 1. The same can be seen in Table VIII which shows the measurement of the accuracy of the discriminant function results.

Finally there are linear discriminant functions for each of the groups. The values of the coeficients can be seen in the Table IX.

Through these functions it is possible to carry out a posteriori classification of the new connections using the perimeter safety parameters (discriminant variables). The coeficients of the discriminant functions are described in Table X.

Each discriminant function is calculated using the values of the combination of discriminant coeficients and variables representing the perimeter security, comparing the results of the fd_0 and fd_1, the discriminant functions of the groups 0 and 1, respectively. If $fd_0 > fd_1$ means that the connection was classified as belonging to group zero (insecure) because it scored higher for this group.

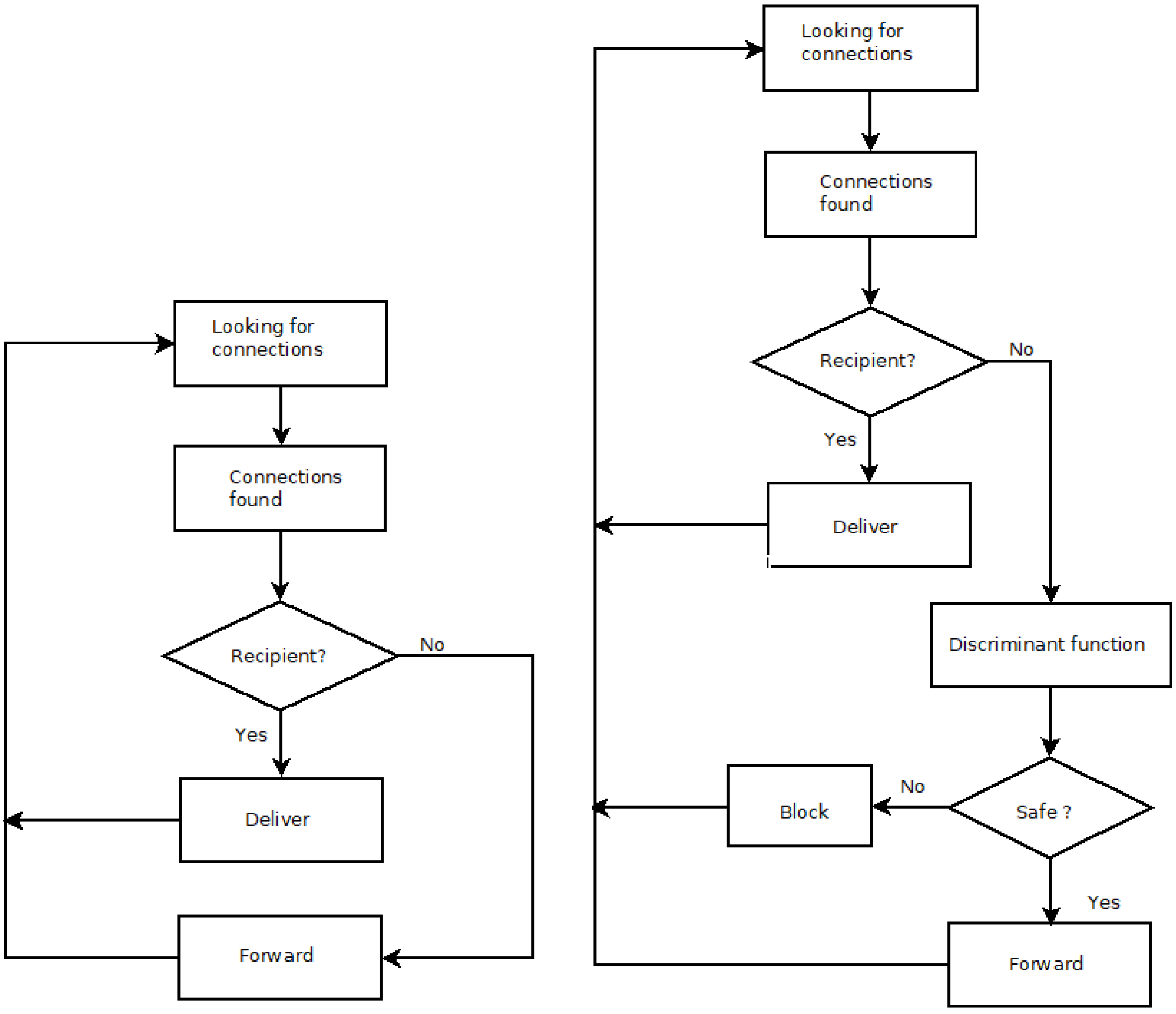
Otherwise, if $fd_0 < fd_1$ means that the connection has been classified in group one and so is a secure connection. The discriminant functions fd_0 and fd_1 are composed by the combination of discriminant coeficients and variables as can be showed in the following (5) and (6).

$$fd_0(x) = constant_0 + dist\_tr_0(x_1) + recipient_0(x_2) + \\ n\_enemies_0(x_3) + n\_allies_0(x_4) + nearest\_dist_0(x_5) + \\ plus_{prox_0}(x_6) + dist\_enemy_{prox_0}(x_7) + dist\_ally_{prox_0}(x_8), \tag{5}$$

$$fd_1(x) = constant_1 + dist\_tr_1(x_1) + recipient_1(x_2) + \\ n\_enemies_1(x_3) + n\_allies_1(x_4) + nearest\_dist_1(x_5) + \\ plus_{prox_1}(x_6) + dist\_enemy_{prox_1}(x_7) + dist\_ally_{prox_1}(x_8) \tag{6}$$

The vector x represents the discriminant variables, a posteriori, [$x_1, x_2, x_3, \cdots, x_8$], which will be used for the calculation of fd_0 and fd_1.

2) Directional Discriminant Analysis Setup: Following the same steps as the discriminant analysis performed for omnidirectional antennas, a discriminant analysis for safety in



(A) (B)

Fig. 7. (A) Basic description of Epidemic protocol and (B) Basic description of Epidemic protocol with discriminant function.

TABLE IX
DISCRIMINANT FUNCTION FOR BOTH GROUPS FOR OMNIDIRECTIONAL ANTENNA SAFETY.

Linear Discriminant Function for Omnidirectional Group		
Groups	0	1
constant	-10,8876777247	-25,2637851236
dist_tr	0,0006873730	0,0000562900
recipient	2,2006247937	11,9459910732
n_enemies	2,2603670023	1,7463959821
n_allies	2,3873702530	2,9789690743
nearest_dist	0,0007618536	0,0010964448
plus_prox	2,8212830847	11,5176646994
dist_enemy_prox	0,0000026170	0,0000180310
dist_ally_prox	0,0000070485	0,0000108450

directional antennas was also performed. A total of N,3510 connections, of which 2506 were classified as unsafe connections (Group 0) and 1004 secure (Group 1) a priori, as can be seen in Table XI.

It can be seen from Table XII that the approximation of the discriminant function generated with the results of the a priori classification obtained a posteriori accuracy of approximately 100% for both groups 0 and 1. The same can be seen in Table XIII, which shows the measurement of the accuracy of the discriminant function results.

Farther groups allow for more accurate classification with fewer intersecting elements. Through these functions it is possible to carry out a posteriori classification of the new connections using the perimeter safety parameters (discriminant variables). The coeficients of the discriminant functions are described in Table XIV.

Finally there are linear discriminant functions for each of the groups. The values of the coefficients can be seen in the Table XV. Each discriminant function is calculated using the values of the combination of discriminant coeficients and variables representing the perimeter security, comparing the results of the fd_0 and fd_1, the discriminant functions ofthe groups 0 and 1, respectively. If $fd_0 > fd_1$ means that the connection was classified as belonging to group zero (insecure)

TABLE X
DESCRIPTION OF THE DISCRIMINANT FUNCTIONS COEFICIENTS IN OMNIDIRECTIONAL ANTENNAS.

Parameters	**Description of linear discriminant functions coeficients for omnidirectional antennas**
constant	A constant value assigned by the analysis.
dist_tr	The distance between the transmitter and the receiver of the data.
recipient	Indicates whether the recipient node is an ally or an enemy, represented by one or zero values respectively.
n_enemies	Number of unsafe nodes in the perimeter.
n_allies	Number of safe nodes in perimeter.
nearest_dist	The distance from the nearest node to the source node.
plus_prox	Indicates who is the nearest node, if enemy is represented by zero, otherwise it will be represented by one.
dist_enemy_prox	It is the distance from the nearest unsafe node to the source node.
dist_ally_prox	Is the distance from the closest safe node to the source node.

TABLE XI
CONNECTIONS CLASSIFIED A PRIORI IN BOTH GROUPS.

Group	0	1
Total	2506	1004

TABLE XII
CONNECTIONS CLASSIFIED A POSTERIORI IN BOTH GROUPS.

		Predicted Class	
	Grupo	0	1
True Class	0	2506	0
	1	0	1004
	Total of N	2506	1004
	N correct	2506	1004
	Proportion (Precision)	1	1

because it scored higher for this group.

Otherwise, if $fd_0 < fd_1$ means that the connection has been classified in group one and so is a secure connection. The discriminant functions fd_0 and fd_1 are composed by the combination of discriminant coeficients and variables as can be showed in the following (7) and (8):

$$fd_0(x) = constant_0 + dist\_tr_0(x_1) + recipient_0(x_2) + n_{ene\_sight_0}(x_3) + n_{ally\_sight_0}(x_4) + enemy_{prox\_sight_0}(x_5) + ally_{prox\_sight_0}(x_6) + host_{dest\_prox\_sight_0}(x_7), \tag{7}$$

$$fd_1(x) = constant_1 + dist\_tr_1(x_1) + recipient_1(x_2) + n_{ene\_sight_1}(x_3) + n_{ally\_sight_1}(x_4) + enemy_{prox\_sight_1}(x_5) + ally_{prox\_sight_1}(x_6) + host_{dest\_prox\_sight_1}(x_7). \tag{8}$$

The x vector represents the discriminant variables a posteriori, [$x_1, x_2, x_3, \cdots, x_7$], which will be used for the calculation of fd_0 and fd_1.

TABLE XIII
ACCURACY MEASUREMENT OF DISCRIMINANT FUNCTION.

Correct Classifications		
N	**Correct**	**Proportion (Accuracy)**
3510	3510	1

TABLE XIV
DESCRIPTION OF THE DISCRIMINANT FUNCTIONS COEFICIENTS IN DIRECTIONAL ANTENNAS.

Parameters	**Description of the linear discriminant functions coeficients for directional antennas**
constant	A constant value assigned by the analysis.
dist_tr	The distance between the transmitter and the receiver of the data.
recipient	Indicates whether the recipient node is an ally or an enemy, represented by one or zero values respectively.
n_enemy_sight	Number of unsafe nodes present in 90° sight.
n_ally_sight	Number of safe nodes present in 90° sight.
enemy_prox_sight	The distance from the closest unsafe node in the sight.
ally_prox_sight	The distance from the closest safe node in the sight.
host_dest_prox_sight	Indicates who is the closest destination host in the sight. If it is an ally its value will be one, otherwise its value will be zero.

D. Analysis of the results of the Epidemic protocol simulations with and without Discriminant Function

At this point in the work, the simulations with the previous scenarios were repeated, but this time using discriminant functions with a modified Epidemic protocol.

Each scenario went through 200 simulations, but this time using different seeds from those used for discriminant analysis, in order to validate the efficiency of the discriminant functions. That is, in the discriminant analysis seeds ranging from 0 to 199 were used, but during the validation stage of Epidemic insurance seeds ranging from 200 to 399 were used.

1) Scenario 1: In the new simulations results of the Scenario 1, visible in Table XVI, a number of 61 ships were sufficient to deliver about 87% of messages via routing using the the pure Epidemic protocol (PE). However, PE protocol achieved an average of 57% routing through unsafe nodes.

These unsafe nodes could have affected the delivery of about 292 of the 511 messages delivered (through a black hole attack), what would reduce the performance of the PE protocol. Therefore, if 35 of these 61 nodes were malicious, there would be a performance reduction to 37% of the messages delivered, moreover, the unsafe nodes would be compromising the security because they would be sharing data with unsafe vessels.

The epidemic block connections (EBC) protocol simply tests for the presence of unsafe nodes in the perimeter, if there are any, that connection is blocked and nothing is transmitted. The EBC compared to the PE protocol showed a reduction of 8% in deliveries, because the strong blocking constraint causes the protocol to miss many connection opportunities.

On the other side, epidemic protocol with discriminant functions showed better performance than PE protocol, in Scenario

TABLE XV
DISCRIMINANT FUNCTION FOR BOTH GROUPS FOR SAFETY IN DIRECTIONAL ANTENNAS.

Linear Discriminant Function for Directional Group		
Groups	0	1
constant	-21,4730403378	-186204,8986442230
dist_tr	0,0003314234	-0,2248181938
recipient	10,9924666567	789,7466812982
n_enemy_sight	8,3006092303	510,3340114402
n_ally_sight	8,1523172741	-154,8431726991
enemy_prox_sight	0,0013972843	0,3754072552
ally_prox_sight	0,0000198844	-0,0003384868
host_dest_prox_sight	-1,4013761751	-1706,8102019036

TABLE XVI
RESULT COMPARISON OF EPIDEMIC PROTOCOLS IN SCENARIO 1.

Scenario 1				
Protocol	PE	EBC	OE	DE
N.Nodes	61	61	61	61
Helicopter	sim	sim	sim	sim
N.Messages	587	587	587	587
Size(bytes)	1000	1000	1000	1000
A.V.Deliveries	511,895	403,8	515,315	525,75
A.V.Delays (seconds)	2981,03	4363,974	3535,25	3237,02
Enemy Forwardings	57%	0%	0%	23%

TABLE XVII
RESULT COMPARISON OF EPIDEMIC PROTOCOLS IN SCENARIO 2.

Scenario 2				
Protocol	PE	EBC	OE	DE
N.Nodes	61	61	61	61
Helicopter	sim	sim	sim	sim
N.Messages	587	587	587	587
Size(bytes)	1000	1000	1000	1000
A.V.Deliveries	400,305	223,22	325,545	339,715
A.V.Delays (seconds)	5697,84	7860,831	7389,1	7053,1
Enemy Forwardings	58%	0%	0%	0%

TABLE XVIII
RESULT COMPARISON OF EPIDEMIC PROTOCOLS IN SCENARIO 3.

Scenario 3				
Protocol	PE	EBC	OE	DE
N.Nodes	61	61	61	61
Helicopter	sim	sim	sim	sim
N.Messages	587	587	587	587
Size(bytes)	1000	1000	1000	1000
A.V.Deliveries	220,075	125,32	151,1	159,12
A.V.Delays (seconds)	5433,81	6560,45	6679,213	6482,001
Enemy Forwardings	61%	0%	0%	0%

1 , about 1% for omnidirectional Epidemic (OE) and 2% for directional epidemic (DE). Maybe the nodes' movements, into the smallest scenario, have favored the amount of the effective encounters in that scenario.

As should be seen later, the performance of the discriminant functions decreases as the area of the scenarios increases. In the DE protocol, in Scenario 1, the directive discriminant function made some mistakes and thus allowed unsafe connections that reached 23% of the total forwardings, however, it still can be considered a sensible reduction in enemies forwardings when compared with PE protocol which was around 57%.

2) Scenario 2: In the new simulations results of the Scenario 2, visible in Table XVII, a number of 61 ships were sufficient to deliver about 70% of the messages by routing through the PE protocol. However, the PE protocol achieved an average of 58% routing through unsafe nodes.

These unsafe nodes could have affected the delivery of about 232 of the 400 messages delivered (through a black hole attack), what would reduce the performance of the PE protocol. Therefore, if 35 of these 61 nodes were malicious, there would be about a performance reduction to 28% of the messages delivered, moreover, the unsafe nodes would be compromising security because they would be sharing data with unsafe vessels.

The EBC compared to PE protocol, showed a 31% reduction in deliveries, because the strong blocking constraint causes the loss of many connection opportunities.

Regarding the Epidemic protocols with discriminant functions, a performance reduction of 13% could be observed for the OE protocol and only 10% for the DE protocol, compared to the PE protocol. These performance degradations were expected, as security constraints require blocking many unsafe connections. However, the Epidemic protocols with discriminant functions, both omnidirectional and directional, performed with a better performance when compared to EBC protocol.

Therefore, the Epidemic protocols with discriminant functions were allowed to filter out the riskiest connections, without missing so many connection opportunities as the simple EBC protocol. The DE protocol, for example, focused its constraint on just one perimeter quadrant, it allowed to happen more connections than the OE protocol, which imposed its constraint in all directions of the perimeter.

3) Scenario 3: In the new simulations results of the Scenario 3, visible in Table XVIII, a number of 61 ships were sufficient to deliver about 37% of the messages by routing through the PE protocol. However, the PE protocol achieved an average of 61% routing through unsafe nodes.

These unsafe nodes could have affected the delivery of about 134 of the 220 messages delivered (through a black hole attack), what would reduce the performance of the PE protocol. Therefore, if 35 of these 61 nodes were malicious, there would be about a performance reduction to 14% of the messages delivered, moreover, the unsafe nodes would be compromising security because they would be sharing data with unsafe vessels.

One more time, the EBC compared to the PE protocol showed a difference of 16% in deliveries, because the blocking restriction causes the protocol to miss many connection opportunities. Over again, as in Scenario 2, regarding to the Epidemic protocols with discriminant functions, it could be observed a performance reduction of 12% for the OE protocol and only 10% for the DE protocol, compared to the PE protocol.

The summary of evaluation results involving the different versions of the Epidemic protocol can be seen in Table XIX.

TABLE XIX
SUMMARY OF EVALUATION RESULTS.

Protocols	Description of the results
PE	• The PE was considered the most suitable protocol for all warship scenarios featured in this work when compared with Spray and Wait and Direct Delivery protocols, on the other hand, the security is not natively implemented in that pure DTN protocol; and • Thus, the PE was the chosen protocol to be tested with the proposed security module which implements discriminant analysis.
DE	• The scenario 1 was the only one where DE protocol showed a little better performance than the PE protocol, there DE was considered the best protocol in message delivering. Thereby, the discriminant function achieved a good aproximation; and • Despite of the DE protocol have presented a lower performance in message delivering than PE protocol, in scenarios 2 and 3, it was better than EBC and OE protocols in all scenarios. Furthermore, it also presented a sensitive reduction in messages forwarding through enemies contributions comparing to PE.
OE	• The scenario 1 was the only one where OE protocol showed a smooth better performance than the PE protocol, there OE was considered the second best after DE protocol; and • Despite of the OE protocol have presented a lower performance in message delivering than PE protocol, in scenarios 2 and 3, it was better than the EBC protocol and presented a reduction in messages forwarding through enemies contributions.

VII. CONCLUSIONS

The DTN architecture is useful in environments where there is no end-to-end network infrastructure. The ability to forward messages to recipient nodes, taking advantage of node mobility, makes the DTN approach compatible with filling the gaps left by conventional networks. Therefore, this work suggested a hybrid network infrastructure (conventional networks along with DTN).

The maritime scenarios of warships have characteristics that favor the use of DTN networks such as: unlimited buffering, high power capacity, constant connections and disconnections, and node speeds that contribute to prolonged contacts. The Epidemic protocol has the ability to spread information to as many nodes as possible without worrying about security issues.

Thus, the current work added a security module to the Epidemic protocol, which uses discriminant analysis functions to classify connections as secure or insecure. If a particular connection is considered insecure, it will be rejected, otherwise data will be transmitted.

The discriminant analysis technique, in this case, classified the connections into two groups: secure or insecure. This classification is based on perimeter parameters, chosen empirically, such as: number of enemy (insecure) and allied (secure) nodes present in the transmission radius, the comparison of distances from the allied recipient to the nearest enemy recipient, etc.

At the end of the process, a discriminant function is created to classify the connections, used to indicate to the Epidemic protocol whether a given connection is secure or not, depending only on the output of the discriminant function.

This security limitation, imposed on the Epidemic protocol, aims to reduce the sharing of sensitive data with unauthorized nodes. The Epidemic protocol with discriminant function was presented as being more efficient than the EBC approach to message delivery. The discriminant function was shown to perform better during warship encounter opportunities.

Some classification errors were found, around 23%, in the Epidemic protocol with directional discriminant function in Scenario 1, it was because a discriminant function is an approximation and, therefore, can generate outputs that lead to incorrect classification.

These mistakes allowed messages to be shared with unsafe nodes in the first Scenario. However, it is possible to improve the directional discriminant function by providing more accurate a priori data, or by making parameter adjustments to generate closer functions and reduce the number of mistakes.

In general, both OE and DE protocols contributed more message deliveries than EBC approach. This implies that applying the discriminant function to the Epidemic protocol is a way to combine the dissemination power of this protocol with a certain limitation of data transmission in areas that are considered insecure.

The security module stimulates more connections between safe nodes, which in turn resulted in more message deliveries to the recipient nodes. For more efficient message delivery, it is necessary to invest in secure collaboration, reducing the number of deadlocks by increasing the number of trusted vessels in the network. It would also be important to encourage the use of directional communication technologies for warships, because it is naturally more secure compared to omnidirectional transmissions.

The contributions of this work were to present DTN networks as a complementary network infrastructure and a low-cost solution in warship scenarios and to point out the Epidemic protocol as the best suited for routing tactical messages in maritime scenarios, in comparison with Spray and Wait and Direct Delivery.

In addition, it demonstrated that discriminant functions are useful to assist the Epidemic protocol in selecting secure connections, reducing the amount of information sharing with unauthorized nodes, improving the performance in delivering messages to end recipients when compared to more restrictive rules.

REFERENCES

[1] M. Zhou *et al.*, "Triton: High-speed maritime wireless mesh network," *IEEE Wireless Commun.*, vol. 20, pp. 134–142, Oct. 2013.

[2] L. Lambrinos, C. Djouvas, and C. Chrysostomou, "Applying delay tolerant networking routing algorithms in maritime communications in world of wireless mobile and multimedia networks," in *Proc. IEEE WoWMoM*, 2013.

[3] P. Kolios and L. Lambrinos, "Optimising file delivery in a maritime environment through inter-vessel connectivity predictions," *Cyprus University of Technology*, 2012.

[4] K. YoungBum, K. J. W. YuPeng, C. KyungHi, P. Jong, and L. YongKon, "Application scenarios of nautical ad-hoc network for maritime communications," in *Proc. IEEE OCEANS*, 2009.

[5] D. H. Job, M. A. N. Silva, W. A. Pinheiro, and R. M. Salles, "An architecture to implement the bundle layer function of delay tolerant networks," in *Proc. IWT*, May 2013.

[6] J. Ott, D. Kutscher, and C. Dwertmann, "Integrating DTN and MANET routing," in *Proc. ACM SIGCOMM*, 2006.

[7] K. Huang and R. Tso, "A commutative encryption scheme based on elgamal encryption," in *Proc. IEEE ISIC*, 2012.

[8] Y. Ding, X. Zhou, Z. mi Cheng, and W. lu Zeng, "Efficient authentication and key agreement protocol with anonymity for delay tolerant networks," *Wireless Personal Commun.*, vol. 70, pp. 1473–1485, Jun. 2013.

[9] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proc. ICST SIMUTools*, 2009.

[10] R. Mohsin and J. Woods, "Performance evaluation of manet routing protocols in a maritime environment," in *Proc. IEEE CEEC*, 2014.

[11] P. Puri and M. P. Singh, "A survey paper on routing in delay-tolerant networks," in *Proc. IEEE ISCON*, 2013.

[12] G. C. Sampaio, G. C. Sampaio, and R. M. Salles, "Avaliação de algoritmos dtn para ambiente operacional tático, um estudo de caso do esquadrão de cavalaria mecanizado," in *Proc. RMCT*, 2019.

[13] R. J. Mohsin, J. Woods, and M. Q. Shawkat, "Density and mobility impact on manet routing protocols in a maritime environment," in *Proc. SAI*, 2015.

[14] A. P. S and A. Viswanathan, "A survey on detection and mitigation of misbehavior in disruption tolerant networks," *IRACST - Int. J. Comput. Netw. Wireless Commun.*, vol. 2, Dec. 2012.

[15] K. Chen and H. Shen, "Distributed privacy-protecting dtn routing: Concealing the information indispensable in routing," in *Proc. IEEE ICNP*, 2016.

[16] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," in *Proc. IEEE INFOCOM*, 2009.

[17] Z. Guo, Z. Peng, B. Wang, J. Cui, and J. Wu, "Adaptive routing in underwater delay tolerant sensor networks," in *Proc. CHINACOM*, 2011.

[18] V. Friderikos, K. P. M. Dohler, and H. A. A. Gkelias, "Linked waters," *Commun. Engineer*, vol. 3, no. 2, pp. 24–27, Apr. 2005.

[19] C. T. de Oliveira, M. D. D. Moreira, M. G. Rubinstein, L. H. M. K. Costa, and O. C. M. B. Duarte, "Redes tolerantes a atrasos e desconexões," *Universidade Federal do Rio de Janeiro, Universidade do Estado do Rio de Janeiro*, 2007.

[20] A. T. C. C. Silva, "Redes tolerantes a atrasos, protocolos de disseminação e aplicações," *Universidade Federal do Rio de Janeiro, Universidade do Estado do Rio de Janeiro*, 2007.

[21] M. A. R.S. Mangrulkar, "Routing protocol for delay tolerant network: A survey and comparison," in *Proc. IEEE ICCCCT*, 2010.

[22] K. Fall and S. Farrell, "Dtn: An architectural retrospective," *IEEE J. Selected Areas Commun.*, vol. 26, no. 5, pp. 828–836, Jun. 2008.

[23] K. Fall, "A delay-tolerant network architecture for challenged internets," *Intel Research, Technical Report IRB-TR-03-003*, 2003.

[24] S. Farrell and V. Cahill, "Security considerations in space and delay tolerant networks," in *Proc. IEEE SMC-IT*, 2006.

[25] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in *Proc. ACM MobiHoc*, 2007.

[26] A. Kate, G. M. Zaverucha, and U. Hengartner, "Anonymity and security in delay tolerant networks," in *Proc. IEEE SecureComm*, 2007.

[27] F. Li and J. Wu, "Mobility reduces uncertainty in manets," in *Proc. IEEE INFOCOM*, 2007.

[28] S. Mingoti, *Análise de dados através de métodos de estatística multivariada: uma abordagem aplicada*. Editora UFMG, 2005.

[29] D. Montgomery, E. Peck, and G. Vining, *Introduction to linear regression analysis*. New York: John Wiley, 2001.

[30] J. Jobson, *Applied multivariate data analysis. v. I and II.* New York: Springer Verlag, 1996. 731p.

[31] T. Anderson, *An introduction to multivariate analysis*. New York: John Wiley, 2003.

Davi Falcão received his B.Sc. in Computer Engineering, in 2009, from University of Pernambuco (UPE-PE),Brazil. He also completed, in 2014, a specialization course in Cryptography at Fluminense Federal University (UFF-RJ) and received the M.Sc. in Defense Engineering, in 2019, from Military Institute of Engineering (IME-RJ), both in Brazil. Currently, he is working as an engineer at Brazilian Navy and his research interests are focused on intelligent computing, network architectures and cyber security.

Ronaldo Salles is appointed professor at the Military Institute of Engineering (IME-RJ), Brazil, in the Postgraduate Program of Defence Engineering. He received his master degree in Computer Science from IME in 1998, and his Ph.D. degree in 2004 from the Imperial College London, UK. His main research interests include performance analysis of computer networks, internet traffic engineering, delay and disruption tolerant networks, network resilience, network security, simulation and modeling. He received best paper awards at the following conferences: SBSeg´21, ACM LANC'09, IEEE/IFIP LANOMS'09 and SBRC'08. He has served on the technical program committees of many conferences and has published more than 90 papers in international journals and conference proceedings.

Paulo Maranhão received his B.Sc. in Statistics at Federal University of Ceará (UFC - CE), in 1994, the M.Sc. in Statistics at Federal University of Pernambuco (UFPE - PE), in 1998, a Ph.D in Production Engineering at Pontifical Catholic University of Rio de Janeiro (PUC-RJ) , in 2012, and a Post-Doctorate in Production Engineering at PUC- RJ, in 2020. Currently, is appointed professor at the Military Institute of Engineering (IME-RJ), Brazil, and his fields of interest are Statistical Process Control, Multivariate Statistics and Statistical Models.