Revista Brasileira de Computação Aplicada, November, 2025

DOI: 10.5335/rbca.v17i3.16484
Vol. 17, Nº 3, pp. 41–51
Homepage: seer.upf.br/index.php/rbca/index

ORIGINAL PAPER

Evaluation of Routing Protocols in Mobile Ad-Hoc Networks Applied to Military Scenarios: Challenges and Research Guidelines

Cláudia Rödel Bosaipo Sales da Silva[1], Ronaldo Ribeiro Goldschmidt[1], Ronaldo Moreira Salles[1]

[1]Instituto Militar de Engenharia

*rodel.claudia@ime.eb.br; ronaldo.rgold@ime.eb.br; salles@ime.eb.br. · · ·

Received: 2024-11-16. **Revised:** 2025-11-14. **Accepted:** 2025-11-29.

Abstract

Ad-hoc networks, widely studied by institutions such as the Internet Engineering Task Force, have gained prominence in military contexts due to their rapid deployment and the use of dynamic and adaptive routing protocols, which are essential for agile operations and training. Simulation-based studies have made it possible to identify the protocols best suited to different operational conditions, providing valuable guidance for their selection and use in military environments. Although the literature extensively addresses Ad-hoc networks, there is a noticeable lack of studies that jointly examine a set of protocols capable of supporting a complete service infrastructure tailored to military communication needs. The distinctive contribution of this work lies precisely in filling this gap: rather than analyzing isolated protocols, it proposes an integrated structure that takes into account the specificities of military networks—distinct from civilian and commercial networks—thus contributing to the development of a more robust and efficient technological framework to support military operations.

Keywords: Performance; MANET; Ad-hoc protocols; Military network; Ad-hoc routing.

Resumo

As redes Ad-hoc, amplamente estudadas por instituições como o *Internet Engineering Task Force*, têm ganhado destaque em cenários militares devido à sua rápida implantação e ao uso de protocolos de roteamento dinâmicos e adaptativos, essenciais para operações e treinamentos ágeis. Pesquisas baseadas em simulações vêm permitindo identificar os protocolos mais adequados a diferentes condições operacionais, fornecendo subsídios valiosos para sua seleção e emprego no contexto militar. Apesar de a literatura tratar extensivamente das redes Ad-hoc, observa-se uma carência de estudos que avaliem, de forma articulada, um conjunto de protocolos capaz de sustentar uma infraestrutura completa de serviços voltada às necessidades das comunicações militares. O diferencial deste trabalho está justamente em preencher essa lacuna: em vez de analisar apenas protocolos isolados, propõe-se uma estrutura integrada que considere as especificidades das redes militares — distintas das redes civis e comerciais — contribuindo para a consolidação de um arcabouço tecnológico mais robusto e eficiente para apoio às operações militares.

Palavras-Chave: Desempenho; MANET; Protocolos Ad-hoc; Rede militar; Roteamento Ad-hoc.

1 Introduction

When addressing networks with military characteristics, which can be structured with Ad-hoc technology, it is crucial to discuss routing protocols, essential for the success of military operations. In military networks, node distribution differs from civilian networks due to varying

levels of penetration and the influence of terrain and geography on technical connections. The connectivity bases of military networks include radio networks aligned with the chain of command and base stations using Ad-hoc technologies. In order to analyze these networks, The "Mobile Ad-Hoc Network" (MANET) group of the "Internet Engineering Task Force" (IETF), is responsible for verifying the challenges of these networks, such as: support for dynamic topology, bandwidth constraints, energy efficiency, and limited security.

In military environments, where needs are unpredictable, the choice and performance of routing protocols are critical. The literature focuses on works about ad-hoc networks, but as far as could be observed, there is a lack of studies investigating a collection of protocols aimed at meeting the demands of an infrastructure for military network services.

Therefore, this research aims to investigate a comparative study of protocols that can provide valuable insights into addressing specific operational challenges. This research aims to evaluate routing protocols in Ad-hoc networks, with a special focus on their use in military contexts. The goal of this approach is to investigate the efficiency and security of these protocols in critical environments, such as those involving military operations. Therefore, it is relevant to elucidate how these protocols adapt and respond to the demands of combat environments. The article is structured into the following sections: Section 2 explores studies related to the evaluation of routing protocols for Mobile Ad-Hoc Networks in military and civilian scenarios. The research methodology is detailed in Section 3. Section 4 discusses the essential fundamentals of military networks, their distinctive characteristics, the functional technical requirements that differentiate them from civilian networks, as well as the use of Mobile Ad-Hoc Networks in military operations and their main routing protocols. The performance evaluation of MANET protocols applied to military scenarios is presented in Section 5, describing the metrics considered, the protocols simulated in the studies, and presenting the results achieved in this research.The final considerations are presented in Section 6, along with an overview of future activities and new research possibilities.

2 Related Studies

In battlefield environments, selecting and implementing routing protocols that meet the specific requirements of military networks presents a complex challenge. A promising approach is the use of self-sufficient systems, such as Ad-hoc networks with delay-tolerant "Ad-Hoc Delay Tolerant Network" and failure-tolerant characteristics (MANETs-DTN). Protocols have been proposed with the aim of achieving optimal performance with minimal resource allocation. For example, the Spray-and-Wait protocol has demonstrated adequate performance in military networks, showing scalability and adaptability to combat environments (Medeiros, 2010).

Evaluating protocols considering energy resource limitations, as described in the study by (Sampaio and Salles, 2019) was crucial for ensuring operational efficiency in military networks.

It is essential to emphasize the importance of security in Ad-hoc networks, as attacks are one of the main causes of link failures and vulnerable points. Protocols such as "Secure Efficient Ad-hoc Distance-vector" (SEAD) (Hu et al., 2003) and "Authenticated Routing for Ad-hoc Networks" (Ariadne) (Hu et al., 2005) implement robust security mechanisms to protect against malicious nodes and logical attacks, using cryptographic keys derived from the "Timed Efficient Stream Loss-tolerant Authentication" (TESLA protocol) (Vivian and Westphall, 2006).

Focusing on security, as pointed out in the study by Quy et al. (2020), attacks constitute the primary cause of failures in links and are points of vulnerability in Ad-hoc networks. It also reports that the implementation of security mechanisms and primitives in MANET protocols has been extensively researched over the past ten years. This highlights the importance of metrics related to tolerance for physical and logical attacks, which contributed to the evaluative metrics used in the development of this article. This study compared SEAD (Hu et al., 2003; Hu, B.Johnson and Perrig, 2002; G., 2011), Ariadne (Hu, Perrig and Johnson, 2002), "Selective Acknowledgment Retransmission" (SAR) (Mathis et al., 1996; Hu and Perrig, 2004), "Authenticated Routing for Ad-hoc Networks" (ARAN) (Sanzgiri et al., 2002) and "Secure Ad-hoc On-demand Distance Vector" (SAODV) protocols (Ran et al., 2021; Guerrero-Zapata, 2002).

Additionally, comparative research between reactive and proactive protocols, such as "Ad-hoc On-demand Distance Vector" (AODV) (Perkins and Royer, 1999; C. E. Perkins, 2003), "Dynamic Source Routing" (DSR) (Johnson and Maltz, 1996; D. B. Johnson and Hu, 2007), and "Destination-Sequenced Distance Vector" (DSDV) (Perkins and Bhagwat, 1994), includes analyses in dynamic scenarios with constant mobility, which is crucial for investigating effective routing without resource loss, especially in military environments. The work by Herek (2011) depicts an evaluation between the reactive AODV and DSR protocols and the proactive DSDV protocol, illustrating a comparison between protocols within the same class. The context simulated a dynamic environment where nodes were in constant movement, reflecting changes in their routing tables. This characteristic is strongly present in military scenarios, where effective routing without resource loss is desired.

The study focused on the "Optimized Link State Routing" (OLSR) protocol (Schmidt and Trentin, 2007) concentrated on a specific military operations scenario, aiming to reach the enemy position. In this scenario, units were organized as follows: 1 command center (combat vehicle), 2 forward units (observers), and 8 groups of 4 members each, totaling 35 mobile units. The OLSR protocol showed results indicating its potential application in warfare environments due to its demonstrated effectiveness. It proved useful in the context of military operations, standing out as a relevant option for routing in such environments. Unlike the previously mentioned research, this study is characterized

by its approach to evaluating a set of specific Ad-hoc protocols for military networks through metric analysis. It is important to highlight that the results and focuses of previous research played a crucial role in the foundation and understanding of the evaluation proposed in this research.

The characteristics of the works are shown in **Table 1**. It depicts, among the related works, those in which the protocols were applied in military scenarios. The *Reference* column indicates the bibliographic reference, and the *Protocols* column shows which protocol was studied in that work. If the *Military Scenarios* column is marked with the symbol "•", it denotes that the protocol was used in military networks. Otherwise, it was not employed in a military scenario.

Table 1: Application of the protocols in the studies.

Reference	Protocols	Military Cenarios
(Medeiros, 2010)	DTN	•
(Sampaio and Salles, 2019)	DTN	•
(Vivian and Westphall, 2006)	SEAD,Ariadne	
(Quy et al., 2020)	SEAD,Ariadne SAR,ARAN SAODV	
Herek (2011)	AODV,DSR DSDV	
(Schmidt and Trentin, 2007)	OLSR	

We observe a lack of studies on Ad-hoc networks applied to military scenarios. This highlights a research gap. Therefore, this study aims to propose a set of protocols that may be more suitable form military network infrastructure.

3 Research Methodology

The procedures for the comparative study and evaluation of MANET protocols in military scenarios are detailed in this section. Initially, the research establishes the investigation question and the strategy for searching studies on the topic, as presented in **Table 2** , following selection criteria defined in **Table 3**. The central research question is: *"How can the performance of MANET routing protocols be evaluated for use in military scenarios"*? Based on this question, the aim is to understand how Ad-hoc network routing protocols are evaluated in terms of efficiency, security, and applicability in military environments.This involves considering metrics such as scalability, adaptability, resource consumption, fault tolerance, and delays, as well as the ability to ensure the integrity and confidentiality of communications in the face of potential threats and cyberattacks. Answering this question guides the selection of suitable protocols to provide optimal performance and security for communication operations in challenging military scenarios.

Table 2: Research Parameters.

Parameters	Content
Research Bases	ACM Digital Library, IEEE Xplore, Scopus, Science Direct, and Scholar
Context of Interest	Studies published in journals and conferences, Doctoral Theses and/or Master's Dissertations
Applied Search	Scope defined by the search string: "routing protocols" AND (("mobile ad-hoc network") OR ("MANET")) AND "military network" AND "performance" AND "functional requirements"
Languages	Portuguese and English
Period	2006-2023

Table 3: Inclusion and Exclusion Criteria.

Inclusion Criteria	Exclusion Criteria
Relevant studies on the topic based on title and abstract (I1)	Non-relevant studies based on title and abstract (E1)
Studies published in journals or conferences and/or doctoral theses and/or master's dissertations (I2)	Studies not available for full view (E2)
Studies published in Portuguese or English (I3)	Studies published before 2006 (E3)
Studies published from 2006 onward (I4)	

4 Theoretical Foundation

This section introduces essential concepts to clearly understand the performance evaluation mechanism of routing protocols in MANETs. The following subsections present the definition and characteristics of military networks, as well as the differences between military e civilian networks. Finally, the Ad-hoc technology adapted for war scenarios is explained, highlighting the main protocols.

4.1 Military Networks - Characteristics

At the core of modern conflicts, where the speed and accuracy of information are as crucial as physical force on the battlefield, military networks emerge as vital foundations of military operations. Structured as interconnected nodes forming a robust computational environment, these networks are designed to withstand the rigors of war scenarios, particularly in "Command and Control"(C2) environments related to military capability. The work by Arias and Salles (2016) highlights that the main issues related to the resilience of C2 topologies involve determining the ability to defend and maintain an acceptable level of service in the presence of failures.

Unlike civilian networks, which operate in relatively stable environments, military networks face unique challenges imposed by the combat scenario, as highlighted in the study by Papakostas et al. (2016). This includes the presence of adversaries, time constraints, and a range of hostile conditions that can induce instabilities and interruptions in data transmission.

The topology of these networks is equally complex and adaptive, as outlined by Katre et al. (2018). The structure is based on the connection between central nodes, usually located at the Headquarters, and tactical nodes, forming the backbone of the network. This configuration is vital for maintaining field operability, where nodes, characterized by their mobility or semi-mobility, must adjust to dynamic operational scenarios. They move according to the advance or retreat of forces, ensuring that the network reconfigures and remains robust regardless of external circumstances.

Furthermore, military networks are distinguished by their hierarchical structure and need for resilience in the face of adversities, including direct threats of interference and destruction by opposing forces. This hierarchical structure allows the tactical core of the network, composed of primary nodes, to support users and equipment on the ground, often through wireless connections that, despite being susceptible to fluctuations and high error rates, are essential for communication continuity (Katre et al., 2019).

The ability to collect, disseminate, and act based on accurate, timely, and relevant information about an adversary force is the goal of a military network. This capability involves information superiority, assisting in making correct decisions within time constraints, and contributing to operations (Cirincione et al., 2010). This aspect enhances real-time decision-making but also increases the responsiveness and adaptability of forces amid the chaos of combat. Thus, military networks have transcended their role as mere communication mechanisms to become key components in military strategy and tactics, essential for strategic decision-making and maintaining operational advantage. Amid the complexity of modern warfare, the importance of these networks intensifies, demanding continuous investments and innovations to ensure they remain resilient, adaptable, and ahead of emerging threats.

4.2 Differentiation between Functional Requirements of Military and Civilian Networks

Military networks, defined by unique characteristics and inherent complexity, play a crucial role in the digitalization and operationalization of the battlefield space. These networks support applications and services under a dynamic scope and extremely volatile conditions, where the ability to adapt and respond to chaotic situations is critical. The information and communications infrastructure supports and represents various aspects of the military scenario, making them key to operational capability.

Unlike civilian networks, military networks require real-time connectivity with extremely variable traffic demands, as pointed out in the study by Andrade et al. (2018). Such demands are essential for generating and transmitting information that directly influences critical decisions during military operations. The need for high-availability connections is emphasized by the continuous nature of these operations; thus, constant communication between different command levels is vital for effective mission execution.

Moreover, facing adversities such as data overloads, poorly adjusted configurations, and external interferences requires exceptional robustness to ensure operational continuity. The ability to sustain operations under abnormal conditions reiterates the importance of resilience in military networks, dealing with challenges in hostile and unpredictable environments subject to constant enemy attacks. Strategies to mitigate risks and potential failures, including implementing redundancies, highlight the stringent need to maintain stable quality and performance. Security in transmissions plays a fundamental role in military networks, especially given the sensitivity of the data and strategic information in circulation. The operational peculiarities of these networks, particularly extreme mobility in tactical environments, pose significant challenges in ensuring the protection and integrity of information. The heightened focus on security in military networks, compared to civilian networks, arises from the high risk of interception, intrusion, and other types of attacks, underscoring the importance of authentication and confidentiality of communications.

In MANET environments, security vulnerabilities are considerably high, exposing them to tampering and espionage attempts. In this context, maintaining anonymity, which is essential in military applications, stands out as a preventive measure against communication interception and tracking of units in the field. The need for anonymous routing protocols, as identified in the study by Quy et al. (2020), highlights the importance of concealing identities, locations, and data routes, a concern practically nonexistent in civilian networks.

The juxtaposition between military and civilian networks reveals fundamental distinctions in purpose and design. While civilian networks are characterized by the immutability and locational stability of nodes, military networks must accommodate frequent topological changes, maintaining service quality despite these dynamic alterations. The hierarchical nature of the military network, intended for integrated delivery of data, voice, and video services, is structured to facilitate communication across different command levels, following specific policies that define interaction protocols between nodes (Papakostas et al., 2016).

As prescribed by the Military Command and Control Doctrine (Estado-Maior do Exército, 2015), a military network must adhere to operational requirements such as simplicity, security, flexibility, and speed, characteristics that distinguish it from conventional networks. The capability for data transmission and support for real-time decision-making are fundamental for superiority in operations. In summary, military networks are built on

a wireless topology, incorporating radio links to maximize connectivity, especially under adverse conditions. The critical mission of these networks, unlike civilian ones, goes beyond productivity or profit, encompassing survival and strategic effectiveness. Thus, they are shaped by specific functional requirements that enable them to succeed in extremely challenging, demanding, and unpredictable military operations. **Table 4** summarizes some of these requirements to be provided by military networks.

Table 4: Functional Requirements of Military Networks. Source: Adapted from (Estado-Maior do Exército, 2015).

Attribute	Source or Dimension
Confidentiality	Information available only to authorized recipients/decoders
Provenance	Origin and operations on data from source through its transfer to destination, including authenticity and non-repudiation properties
Availability	Accessible via a given network and capable of providing critical functions
Intrusion Resilience	Measures how well a system withstands attacks, especially intrusion
Flexibility	Ability to adapt technology
Security	Implementation of priority levels
Amplitude	Geographic range
Integrity	Complete delivery of messages
Reliability	Redundancy and trust in usage

4.3 Employment of Ad-hoc Networks in Military Scenarios

Historically, in military scenarios, the concept of Ad-hoc networks dates back to the early 1970s when the United States "Defense Advanced Research Projects Agency" (DARPA), initiated the "Packet Radio Network" (PRNET) project, investigating the use of packet radio networks in a tactical environment for data communication. In the 1980s, the "Survivable Adaptive Network" (SURAN) program continued the PRNET's objectives, focusing on large networks and developing protocols to adapt rapidly to changes in a tactical environment. In the 1990s, the "Global Mobile Information Systems"(GloMO) program was expanded, and it was used to simulate complex environments of Ad-hoc networks (Defense Advanced Research Projects Agency (DARPA), 2022).

The use of this type of network is associated with scenarios where rapid deployment is needed. Typically, these are environments without a established network infrastructure. It is a beneficial technology in terms of flexibility, fault tolerance (able to reestablish routes), connectivity between nodes, and mobility. In battlefields, where the terrain is unknown and obscure, wired infrastructure setup is impractical. Thus, the most suitable technology is MANET, as it allows military personnel to utilize a local network technology to maintain information networks among soldiers, vehicles, and headquarters.

In military scenarios, typical transmission methods include radio links (through programmed contacts), messengers (through predictable contacts), and mobile Ad-hoc networks, which feature opportunistic contacts (Medeiros, 2010). It is important to note that regarding Ad-hoc technology, a new architecture called "Delay and Disruption Tolerant Networks" (DTN) was introduced, characterized by its ability to handle failures, delays, and interruptions effectively.

This architecture, even in the face of long delays or interruptions due to periods without connectivity, provides flexible, efficient, and robust communication between origin and destination. The scenarios for MANET-DTN are deterministic and stochastic. It is emphasized that the military scenario is initially a deterministic scenario, but during conflict, it can transform into a stochastic scenario.

In mobile Ad-hoc networks, the dynamics of conditioning with mobility are characterized by a set of wireless mobile nodes that establish direct communication, forming a temporary dynamic network (Gupta et al., 2011). Thus, they can change their topology unpredictably. They have the capability to self-configure, establish connections, and communicate with each other, independently of a base station. They possess relative autonomy and self-sufficiency (Cirincione et al., 2010) .

Regarding the dynamic structure of nodes, routing algorithms aim to find the best path for packets using calculations and metrics. This search is driven by the need for devices to transmit information from the source node to the destination node, making the routing process challenging and intensely dynamic (Herek, 2011). Due to the importance of dynamic topology reconstruction and randomness, the study by Firmino et al. (2021) highlights the relevance of using Ad-hoc networks in military operations.

4.4 Main Ad-hoc Routing Protocols

The IETF, through its MANET working group, has defined metrics for routing protocols aimed at quality and efficiency (Internet Engineering Task Force (IETF), 2022). These metrics include qualitative aspects such as distributed operation and security, and quantitative aspects such as message delivery time and efficiency. They are relevant when considering the functioning of Ad-hoc networks, as nodes act as routers, receiving and processing packets to make decisions based on network information, forwarding them to the destination. In MANETs, both conventional data and sensitive information, such as audio, video, and military data, can be transmitted, requiring that routing protocols be adapted to each type of traffic. The mechanism involves exchanging information between nodes to obtain network knowledge and select the best route. The effectiveness of this process depends on the routing protocol and its specific algorithm, which play a significant role in the operation and performance of the Ad-hoc network.

There are various routing protocols for MANETs, each with its specific actions, such as route selection and maintenance of routing tables. The use of these protocols directly impacts the average route length to transmit information optimally. The goal in Ad-hoc networks is to find the correct and efficient route for message delivery, with continuous node availability being essential for this operation, making energy consumption a crucial issue (Verma and Soni, 2017).

In the absence of connectivity between the source and destination nodes, routing protocols must reestablish the connection or seek alternatives, a challenging task,especially in military operations where routing is critical for network balance. Ad-hoc networks require effective protocols, categorized into reactive, proactive, and hybrid, classified according to their route discovery policies.

"Reactive" protocols are triggered as needed, minimizing network overhead, while proactive protocols keep routing information updated to allow immediate use of the route when sending a packet. The study by Gupta et al. (2011) reports that routing protocols classified as "reactive" aim to minimize network traffic to avoid overhead. In this task, periodic updates are not necessary for this type of protocol. Route creation is only performed when a node desires to initiate communication. In this case, the time to be evaluated is the route discovery time. According to Thakur and Kaur (2019), the characteristic of this protocol classification is to propagate the route only on demand. Once the route is established on demand, it is maintained until the destination becomes unreachable, traversing the outlined path possibilities from the source, or until the route is no longer used.

Regarding the study by Herek (2011), routing protocols classified as "Proactive" have the characteristic of keeping routing information updated. Therefore, they have the advantage of immediately using the route when sending a packet, as the routes of all possible destinations are listed in routing tables. Referring back to the approach presented by Gupta et al. (2011), it is emphasized that this group of routing protocols continuously learns the network topology. Consequently, each node is required to maintain tables with updated routing information. In this way, they seek to preserve node communication and preemptively design routes, even before they are needed. As reinforced by Thakur and Kaur (2019), these types of protocols maintain tables that represent the entire network topology. Protocols of this class are derived from well-known protocols such as Distance Vector and Link State.

This nomenclature arises from the fact that these protocols, in trying to continuously keep information updated and consistent in routing tables, proactively propagate them. These protocols are scalable in relation to network topology changes but not with respect to the increase in nodes.

"Hybrid" protocols utilize both of the strategies described. Reactive or proactive characteristics are adopted in different ways. This protocol group is typically used to provide hierarchical routing. Due to their incorporation of both classifications, they require higher energy and memory consumption. They perform a task associated with minimizing the overhead of route discoveries (Gupta et al., 2011).

Since routing protocols require an end-to-end path between the source and the destination, they address the fault tolerance mechanism. This refers to the ability of the Ad-hoc network to withstand communication interruptions by using temporary message storage and forwarding. Such a characteristic is well-suited to the dynamics of a military network. Moreover, fault tolerance is a metric included in the current performance evaluation of the protocols (Medeiros, 2010).

Still focusing on the fault tolerance mechanism, two basic principles are used in DTN networks: forwarding (tends to reduce buffer usage, has high delays, and low delivery rate) and message copying (utilizes the buffer, has low delays, higher delivery rate, and message discarding). Furthermore, the Ad-hoc DTN network employs specific protocols, not relying on traditional routing protocols.

Based on the context presented in Section 4.1, a selection was made regarding the set of routing protocols employed in the Ad-hoc network for this comparative study. The protocols selected for evaluation, in terms of their use in military scenarios, were those that met certain functional requirements of the military network.

5 Evaluation of Results

At this stage, the evaluation of the set of Ad-hoc protocols is performed, identifying the best alternatives for use, considering the encountered environment and the studies selected according to the methodology adopted in Section 3.

5.1 Evaluative Metrics

Ad-hoc networks have attracted military interest due to their dynamic topology, suitable for operational war scenarios. Various studies have been conducted to assess the performance of routing protocols in simulated environments designed to represent military situations with communication loss due to node mobility and interference. These studies focus on reactive, proactive, hybrid, and failure-tolerant protocols, analyzing their characteristics, strengths, and limitations. However, for a more accurate assessment, it is essential to conduct a comparative study based on relevant metrics considering the specific needs of military environments. Each protocol is evaluated based on fundamental metrics such as "Delivery Ratio" (*DR*) and "Fault Tolerance" (*FT*). The *DR* metric, indicating the proportion of packets received relative to those sent, is crucial for ensuring effective communication (Luo et al., 2023; Mohapatra and Kanungo, 2012). The *FT* metric relates to the ability to recover in case of route failures, supporting the concept of adaptive routing (Avizienis et al., 2004; Pelc, 1996).

In the military context, network reliability is crucial for the continuity of operations. The *DR* and *FT* metrics provide relevant data for evaluation, measuring packet delivery and response to failures. Interpreting the results of these metrics, as presented in the specific tables, is fundamental to determining the viability of the studied

protocols in demanding military environments.

Below are the descriptions of the *DR* scale and *FT* scale metrics, as described in **Table 5** and **Table 6**, based on the results obtained from the evaluated studies.

Table 5: Delivery Ratio Percentage Scale.

Percentage Scale	DR Categorization
Up to 50%	Low
51% to 85%	Medium
86% to 100%	High

Table 6: Fault Tolerance Degree Scale.

Fault Tolerance Degree	Observation
High	Instantaneous recovery
Medium	Low time recovery
Low	High time recovery or unable

Information security is a fundamental requirement in military networks, involving the implementation of measures to protect the confidentiality, integrity, and availability of data transmitted, processed, and stored in communication and information systems (Vivian and Westphall, 2006). The metric of tolerance to physical and logical attacks is essential to evaluate the network's security level against challenges during military operations. It is important to consider that Ad-hoc networks are susceptible to malicious nodes that can compromise routing protocols and affect network integrity. The potential interference of these malicious nodes highlights the need for innovation in secure routing protocols, incorporating mechanisms to ensure communication security in military environments. In this context, investigating secure and resilient routing protocols becomes a priority, with the introduction of security mechanisms designed to mitigate various types of cyberattacks (Yang et al., 2004). In the present study, protocols are evaluated regarding their satisfaction of secure mechanisms tolerant to physical and logical attacks. They have been categorized as: low, medium, and high as described in **Table 7**.

Table 7: Security Degree Scale.

Security Degree	Observation
High	Has several mechanisms tolerant to physical or logical attacks
Medium	Has some mechanism tolerant to physical or logical attacks
Low	Does not have mechanisms tolerant to physical or logical attacks

At this point, another distinctive characteristic of military networks, their dynamic nature, is addressed as they unpredictably change during field operations. In this context, the mobility metric was introduced to assess which routing protocols are capable of handling different levels of mutability, classified as high, medium, or low, providing an analysis of the network's adaptation in dynamic environments.

Additionally, the "Total Delivery Time" (*TT*) was introduced as an essential metric to evaluate the effectiveness of the main routing protocols. The *TT* represents the time it takes for a message to be generated at the source node and reach the destination node, which is particularly crucial in real-time operations (Xiao and Rosdahl, 2002). Long delivery times can result in service discontinuity, quality degradation, or even interruption, unacceptable scenarios in military tactical operations. The assessment of *TT* is relevant to understand network interactivity and ensure the continuity and efficiency of communications in dynamic environments (Li et al., 2001). Based on the studies analyzed in this paper, the *TT* metric was categorized based on the results obtained from bibliographic research. They are described in **Table 8**.

Table 8: Packet Delivery Time Scale.

TT Categorized	Framework
High	TT > 0.5 sec
Medium	0.05 sec < TT $\leq$ 0.5 sec
Low	0 sec < TT $\leq$ 0.05 sec

Table 9 illustrates the set of metrics used to evaluate the protocols specified in the studies. It describes the constituent metrics as well as the functional requirements covered.

Table 9: Set of Evaluative Metrics.

Functional Requirement	Metric
Reliability	*DR*, *FT*
Variable Traffic Management	*TT*
Security	Security Degree
Adaptability	Mobility

5.2 Simulated Routing Protocols

This study investigates the performance of various routing protocols in Ad-hoc networks, focusing on scenarios with high mobility and the need for robust security. Through simulations replicating real field conditions, it was observed that Epidemic, PROPHET, and MaxProp protocols exhibited superior performance in terms of packet delivery rate, closely followed by the Spray-and-Wait protocol. These protocols showed effectiveness in handling the increase in the number of nodes and movement variability, which is relevant for operations in dynamic environments.

Constant mobility revealed that the OLSR protocol is particularly efficient due to its proactive route update nature. In contrast, DSDV, despite showing improvements as it updates its routing tables, struggled to adjust to high mobility scenarios, proving less adaptable than OLSR and "Multipath TCP-based Ad hoc On-Demand Distance Vector" (MT-AODV). The latter, an optimization of AODV, stood out for exploring multiple routes on-

Table 10: Comparative Table of Ad-hoc Routing Protocols.

Protocol	DR	FT	Security Degree	TT	Mobility
DSR	Medium	Low	Low	Medium	Low
AODV	Low	Low	Low	Medium	Medium
OLSR	High	Medium	Medium (MPR use)	Low	High
DSDV	Medium	Medium	Low	Medium	Low
MT-AODV	Medium	Medium	Low	Low	Medium
Ariadne	Medium	Low	Medium (Prevents DDoS)	High	Low
SEAD	Low	Medium	Medium (Prevents DDoS and Wormhole)	Medium	Low
WRP[13]	Medium	Medium	Medium (Prevents Loop)	High	Medium
ZRP[14]	Low	Medium	Low	High	Low
PROPHET	Medium	High	Low (Prevents Black Hole Attack)	Low	High
Epidemic	Medium	High	Medium (Makes copies)	Low	High
MaxProp	High	High	Low (Prevents Black Hole Attack)	Low	High
Spray-and-Wait	High	High	Medium (Makes copies)	Low	High
Direct Delivery	Medium	High	Low	Low	Medium

[13] Wireless Routing Protocol.
[14] Zone Routing Protocol.

demand, showing promise in enhancing fault tolerance.

However, concerning this approach, AODV's reduced capability to maintain packet delivery in adverse situations and its increased total delivery time highlight its vulnerability. On the other hand, both OLSR and DSDV, using multiple paths and proactive update strategies, were noted for their resilience, as was MT-AODV for its ability to effectively discover alternative routes.

In terms of security, protocols must be robust against attacks. In this aspect, SEAD and Ariadne protocols, both implemented with cryptographic solutions, provided an adequate level of protection, with SEAD demonstrating better performance regarding total delivery time, maintaining synchronization.

For mutability purposes, OLSR is noted as especially effective for maintaining connectivity in high mobility environments, although MT-AODV also proves to be a promising alternative due to its ability to combine routing efficiency with fault tolerance.

5.3 Discussion and Results

The study on the performance of routing protocols in military scenarios allows identifying those that best meet a set of metrics for use in war environments. The considered metrics include operational message traffic with classification and priorities.In military operations, the presence of a command center sending movement instructions to units is common.

The comparative evaluation is presented in **Table 10**, illustrating the behavior of each protocol based on the set of evaluation metrics.

The goal is to coordinate and guide allied troop movements towards the enemy. In this context, the military network must provide technical support for the troops, combat, and defeat the enemy in battle (Schmidt and Trentin, 2007). The ability to report troop locations to the commander in real-time allows for rapid and precise execution of commands.

By combining a high delivery rate with a reduced packet delivery time, the network gains fundamental robustness (Estado-Maior do Exército, 2015). Optimizing routing helps reduce the amount of data transmitted in the war network, minimizing the chances of enemy attacks due to lower exposure and detection.

OLSR stands out for offering multiple routes between destination nodes, ensuring redundancy and adaptability to changes in network topology. Additionally, the "Multipoint Relay" (MPR) node selection mechanism helps prevent malicious attacks and reduce network load (Schmidt and Trentin, 2007).

The DTN Epidemic and Spray-and-Wait protocols, with their specific algorithms, already have fault tolerance mechanisms and meet the metrics of packet rate and delivery time, being resilient to the increase in mobile nodes (Medeiros, 2010). Additional techniques, such as user authentication and content verification, are recommended to reinforce security.

MaxProp and PROPHET protocols, aimed at DTN networks, meet most metrics, although they present vulnerabilities to some types of attacks (Medeiros, 2010). To enhance their security, it is advisable to complement their use with additional measures, such as user authentication, content verification, and gateways, to prevent unauthorized and unwanted traffic.

The evaluation of metrics revealed that none of the protocols achieved a "high" level of security, highlighting the inherent vulnerabilities of Ad-hoc networks. This finding underscores the continuous need to seek improvements and solutions to ensure secure communication in military and other critical applications.

6 Final Considerations

In wartime situations, the ability to coordinate and direct military forces is crucial to enhancing the effectiveness of combat actions, strategically combining resources and movements.

Through studies based on simulations, the investigation focused on identifying routing protocols

suitable for military environments. This work provided an in-depth understanding of military networks, highlighting their specific requirements and the relevance of Ad-hoc technology in such environments.

The literature focuses on works about ad-hoc networks, but as far as could be observed, there is a lack of studies investigating a collection of protocols aimed at meeting the demands of an infrastructure for military network services. The goal was not only to identify an isolated protocol but also to establish the ideal structure to meet the peculiarities of military networks and their applications, considering the differences compared to civilian and commercial networks.

For future research, in light of the dynamic nature of military operations, it is proposed to explore the implementation of self-configuration mechanisms in routing protocols to adapt to variations in the scenario. For instance, in stable scenarios with reduced mobility, protocols such as DSDV and MT-AODV may prove to be more suitable, while more complex contexts might require different solutions.

An additional research approach could involve integrating artificial intelligence into network nodes, enabling dynamic transitions between protocols based on real-time operational demands, providing greater adaptability to the military network. Furthermore, it is suggested to conduct studies that subject all protocols to standardized testing to validate or adjust the results of previous simulations, contributing significantly to scientific advancements in this field.

References

Andrade, B. M., P., S. C., Oliveira, A. M., Santos, A. F. and Maniçoba, R. H. C. (2018). Análise de desempenho dos protocolos de roteamento dsr e aodv em redes ad hoc, *VIII Conferência Nacional em Comunicações, Redes e Segurança da Informação – ENCOM 2018*, Salvador–BA, Brasil, pp. 159–160. Available at http://www.encom.org.br/.

Arias, R. P. and Salles, R. M. (2016). Resiliência em redes militares de comando e controle, *Revista Militar de Ciência e Tecnologia* **33**(2): 32–41.

Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing* **1**(1): 11–33. DOI: https://doi.org/10.1109/TDSC.2004.2.

C. E. Perkins, E. M. Royer, S. R. D. (2003). Ad hoc on-demand distance vector (aodv) routing, *RFC 3561, IETF* . Available at https://doi.org/10.17487/RFC3561.

Cirincione, G., Krishnamurthy, S. and Porta, T. F. L. (2010). Impact of security properties on the quality of information in tactical military networks, *The 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management* . Available at https://milcom2010.com/, accessed on 16 November 2024.

D. B. Johnson, D. A. M. and Hu, Y. C. (2007). The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4, *RFC 4728, IETF* . https://doi.org/10.17487/RFC4728.

Defense Advanced Research Projects Agency (DARPA) (2022). Darpa – defense advanced research projects agency. Available at https://www.darpa.mil/.

Estado-Maior do Exército (2015). *EB20-MC-10.205 Manual de Campanha – Comando e Controle*, Exército Brasileiro, Estado-Maior do Exército. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/12348.

Firmino, R. M., Mattos, D. M. F. and Medeiros, D. S. V. (2021). Mt-aodv: Provendo resiliência em redes ad-hoc móveis militares através de múltiplas tabelas de roteamento sob demanda, *XXXIX Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, Fortaleza-CE, Brasil. http://dx.doi.org/10.14209/sbrt.2021.1570727284.

G., P. V. (2011). Sead-fhc: Secure efficient distance vector routing with fixed hash chain length, *Global Journal of Computer Science and Technology* **11**(20): 43–51. Available at https://computerresearch.org/index.php/computer/article/view/1039, accessed on 16 November 2025.

Guerrero-Zapata, M. (2002). Secure ad hoc on-demand distance vector routing, *ACM Mobile Computing and Communications Review* **6**(3): 106–107. https://doi.org/10.1145/581291.581312.

Gupta, A. K., Sadawarti, H. and Verma, A. K. (2011). A review of routing protocols for mobile ad hoc networks, *WSEAS Transactions on Communications* **10**: 331–340. https://doi.org/10.1016/S1570-8705(03)00043-X.

Herek, T. A. (2011). Análise comparativa de desempenho dos protocolos de roteamento em redes móveis ad hoc, *Technical report*, Universidade Tecnológica Federal do Paraná, Departamento Acadêmico de Eletrônica, Curitiba, Brasil. Monografia de Especialização. Disponível em https://riut.utfpr.edu.br/jspui/bitstream/1/20020/2/CT_TELEINFO_XX_2012_13.pdf.

Hu, Y., B.Johnson, D. and Perrig, A. (2002). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks, *4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002)*, pp. 3–13. https://doi.org/10.1109/MCSA.2002.1017480.

Hu, Y., B.Johnson, D. and Perrig, A. (2003). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks, *Ad Hoc Networks* **1**(1): 175–192. https://doi.org/10.1016/S1570-8705(03)00019-2.

Hu, Y.-C., Perrig, A. and Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks, *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02)*, ACM, pp. 12–23. https://doi.org/10.1145/513800.514204.

Hu, Y.-C., Perrig, A. and Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks,

Wireless Networks **11**(1-2): 21–38. https://doi.org/10.1007/s11276-004-4744-y.

Hu, Y. and Perrig, A. (2004). A survey of secure wireless ad hoc routing (inclui sack / arq em redes "perdidas"), *IEEE Security & Privacy* **2**(3): 28–39. https://doi.org/10.1109/MSP.2004.14.

Internet Engineering Task Force (IETF) (2022). Internet engineering task force. Available at https://www.ietf.org/.

Johnson, D. B. and Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks, *in* T. Imielinski and H. Korth (eds), *Mobile Computing*, Kluwer Academic Publishers, pp. 153–181. Available at https://doi.org/10.1007/978-0-585-29603-6_5.

Katre, S., Goswami, A. and Mishra, P. (2018). Improved connectivity using differential priority assignments in military network, *5th IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2018)*, Solan, India, pp. 381–386. https://doi.org/10.1109/PDGC.2018.8745890.

Katre, S., Goswami, A., Mishra, P., Bapat, J. and Das, D. (2019). Impact of variable mtu size of voice packet to reduce packet loss in bandwidth constraint military network, *5th International Conference for Convergence in Technology*, Pune, India. https://doi.org/10.1109/I2CT45611.2019.9033868.

Li, J., Blake, C., Couto, D. S. J. D., Lee, H. I. and Morris, R. (2001). Capacity of ad hoc wireless networks, *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 61–69. https://doi.org/10.1145/381677.381684.

Luo, S., Lai, Y. and Liu, J. (2023). Selective forwarding attack detection and network recovery mechanism based on cloud-edge cooperation in software-defined wireless sensor network, *Computers & Security* **126**: 103083. DOI: https://doi.org/10.1016/j.cose.2022.103083, accessed on 16 November 2024.

Mathis, M., Mahdavi, J., Floyd, S. and Romanow, A. (1996). Tcp selective acknowledgment options, RFC 2018, IETF. https://doi.org/10.17487/RFC2018.

Medeiros, M. V. B. (2010). *Emprego de redes tolerantes a atrasos e desconexões em sistemas de comunicações militares*, Master's thesis, Instituto Militar de Engenharia. Available at http://rmct.ime.eb.br/arquivos/RMCT_3_quad_2009/emprego_redes_tolerantes.pdf.

Mohapatra, S. and Kanungo, P. (2012). Performance analysis of aodv, dsr, olsr and dsdv routing protocols using ns2 simulator, *Procedia Engineering* **30**: 69–76. Available at https://www.sciencedirect.com/science/article/pii/S187770581200325X, accessed on 16 November 2024.

Papakostas, D., Basaras, P., Katsaros, D. and Tassiulas, L. (2016). Backbone formation in military multi-layer ad hoc networks using complex network concepts, *35th Military Communications Conference (MILCOM)*, Baltimore, MD, USA. https://doi.org/10.1109/MILCOM.2016.7795434.

Pelc, A. (1996). Fault-tolerant broadcasting and gossiping in communication networks, *Networks: An International Journal* **28**(3): 143–156. DOI: https://doi.org/10.1002/(SICI)1097-0037(199610)28:3<143::AID-NET3>3.0.CO;2-N, accessed on 16 November 2024.

Perkins, C. E. and Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers, *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*, pp. 234–244. https://doi.org/10.1145/190314.190336.

Perkins, C. E. and Royer, E. M. (1999). Ad-hoc on-demand distance vector routing, *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, New Orleans, LA, USA, pp. 90–100. Available at https://doi.org/10.1109/MCSA.1999.749281.

Quy, V. K., Chuan, P. M., Nam, V. H. and Linh, D. M. (2020). A review on security-aware routing protocols for mobile ad hoc network, *International Journal of Advanced Trends in Computer Science and Engineering* **9**(3): 3655–3661. https://doi.org/10.30534/ijatcse/2020/175932020.

Ran, C., Yan, S. and Zhang, L. (2021). An improved aodv routing security algorithm based on blockchain technology in ad hoc network, *EURASIP Journal on Wireless Communications and Networking* . https://doi.org/10.1186/s13638-021-01938-y.

Sampaio, G. C. and Salles, R. M. (2019). Avaliação de algoritmos dtn para ambiente operacional tático: um estudo de caso do esquadrão de cavalaria mecanizado, *Revista Militar de Ciência e Tecnologia* **36**(4): 17–28. Available at http://rmct.ime.eb.br/.

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C. and Belding-Royer, E. M. (2002). Authenticated routing for ad hoc networks (aran), *Proceedings of the 8th Annual International Conference on Network Protocols (ICNP '02)*, pp. 152–163. https://doi.org/10.1109/ICNP.2002.1181388.

Schmidt, R. O. and Trentin, M. A. S. (2007). Desempenho de protocolos de roteamento para manets em um cenário de operação militar, *Revista Hífen (PUCRS campus Uruguaiana)* **31**(59/60): 16–22.

Thakur, M. and Kaur, M. (2019). Ad-hoc network routing protocols for wireless body area network, *Proceedings of the Third International Conference on Advanced Informatics for Computing Research (ICAICR)*, pp. 1–7. https://doi.org/10.1145/3339311.3339339.

Verma, N. and Soni, S. (2017). Efficiency comparison of routing protocols for locating nearby nodes in manet, *International Journal of Advanced Research in Computer Science* **8**(3): 324–329. Available at https://www.ijarcs.info/.

Vivian, D. and Westphall, C. B. (2006). Comparação de desempenho de protocolos de roteamento seguro para redes sem fio ad hoc, *Anais do XXVI Congresso da SBC*, Campo Grande-MS, Brasil, pp. 82–96. Available at https://www.sbc.org.br/.

Xiao, Y. and Rosdahl, J. (2002). Throughput and delay limits of ieee 802.11, *IEEE Communications Letters* **6**(8): 355–357. https://doi.org/10.1109/LCOMM.2002.802035.

Yang, H., Luo, H., Ye, F., Lu, S. and Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions, *IEEE Wireless Communications* **11**(1): 38–47. DOI: https://doi.org/10.1109/MWC.2004.1269716.