Revista Angolana de Ciências

Vol. 8, Nº 1. e080117. Janeiro – Junho, 2026
(Publicação em Fluxo Contínuo)

Redes Ad Hoc Móveis sob Ataque Flooding: Avaliação de Desempenho de Protocolos de Roteamento

Mobile Ad Hoc Networks under Flooding Attack: Performance Evaluation of Routing Protocols

Redes Ad Hoc Móviles bajo Ataque de Flooding: Evaluación del Desempeño de Protocolos de Enrutamiento

Osvaldo Ló Nunes Sebastião[1]
Mateus Padoca Calado[2]

RESUMO

As Redes Ad Hoc Móveis (MANETs) têm aplicações críticas em cenários sem infraestrutura, como resgate, operações militares e IIoT temporário, mas sofrem com mobilidade, múltiplos saltos e vulnerabilidade a ataques. Este trabalho avalia comparativamente os protocolos de roteamento AODV (*Ad hoc On-Demand Distance Vector*), DSDV (*Destination-Sequenced Distance Vector*) e GPSR (*Greedy Perimeter Stateless Routing*) em condições normais e sob ataque *Flooding* extremo. Para isso, foram realizadas simulações no OMNeT++/INET com o padrão IEEE 802.11, em uma topologia de 600×600 m, com tráfego UDP-CBR de 256 bytes, quatro nós atacantes e dez repetições por cenário, coletando as métricas de Taxa de Entrega de Pacotes (PDR), Vazão (*Throughput*) e Latência (*Delay*). Em regime normal, AODV e DSDV alcançaram 98% de Taxa de Entrega de Pacotes, enquanto o GPSR atingiu 7,03%. Sob ataque Flooding, a Taxa de Entrega de Pacotes caiu para 31,13% no AODV, 18,63% no DSDV e 1,91% no GPSR. A Vazão reduziu de 10,14 para 2,76 kbps no AODV, de 4,06 para 1,65 kbps no DSDV e de 0,71 para 0,17 kbps no GPSR. Quanto à latência, o AODV manteve-se estável (≈528 para 560 ms), enquanto o DSDV e o GPSR apresentaram valores na ordem de 5×10^4–6×10^4 ms, inviáveis para aplicações de tempo real. Como contribuição, este trabalho oferece um pipeline de simulações reprodutível (NED/INI), padronização de métricas (PDR, *Delay*, *Throughput*) e estimativas com intervalos de confiança de 95%. O impacto do estudo reside em gerar evidências práticas para a seleção de protocolos conforme requisitos de robustez e latência, além de fornecer subsídios para o desenho de estratégias de detecção e mitigação de ataques em MANETs.

Palavras-chave: MANETs; Avaliação de Desempenho; Ataque Flooding; OMNeT++.

RECEBIDO: 15/09/2025
ACEITE: 15/01/2026
PUBLICADO: 30/06/2026

Como citar: Ló Nunes Sebastião, O. & Calado, M.P. (2026). Redes Ad Hoc Móveis sob Ataque Flooding: Avaliação de Desempenho de Protocolos de Roteamento. *RAC: Revista Angolana de Ciências*, 8(1), e080117. https://doi.org/10.54580/R0801.17

E-ISSN. 2664-259X

1. ISTM/USP. Luanda/São Paulo, Angola/Brasil
osvalnunes@usp.br / https://orcid.org/0009-0006-1000-5042
2. UAN. Luanda, Angola
padoca@padoca.org / https://orcid.org/0000-0002-2563-5593

Abstract

Mobile Ad Hoc Networks (MANETs) have critical applications in infrastructure-less scenarios such as rescue operations, military environments, and temporary Industrial Internet of Things (IIoT) deployments; however, they face challenges related to mobility, multi-hop communication, and vulnerability to security attacks. This study comparatively evaluates the routing protocols AODV (Ad hoc On-Demand Distance Vector), DSDV (Destination-Sequenced Distance Vector), and GPSR (Greedy Perimeter Stateless Routing) under normal conditions and under an extreme *Flooding* attack. To this end, simulations were conducted using OMNeT++/INET with the IEEE 802.11 standard, considering a 600×600 m topology, UDP-CBR traffic with 256-byte packets, four attacking nodes, and ten repetitions per scenario. The evaluated metrics include Packet Delivery Ratio (PDR), *Throughput*, and End-to-End Delay. Under normal conditions, AODV and DSDV achieved a PDR of 98%, whereas GPSR reached 7.03%. Under *Flooding* attack, the PDR dropped to 31.13% for AODV, 18.63% for DSDV, and 1.91% for GPSR. *Throughput* decreased from 10.14 to 2.76 kbps for AODV, from 4.06 to 1.65 kbps for DSDV, and from 0.71 to 0.17 kbps for GPSR. Regarding latency, AODV remained stable (approximately 528 to 560 ms), while DSDV and GPSR exhibited delays on the order of 5×10^4–6×10^4 ms, rendering them unsuitable for real-time applications. As a contribution, this work provides a reproducible simulation pipeline (NED/INI), standardized metrics (PDR, Delay, *Throughput*), and estimates with 95% confidence intervals. The impact of this study lies in delivering practical evidence for protocol selection based on robustness and latency requirements, as well as supporting the design of detection and mitigation strategies for attacks in MANETs.

Keywords: MANETs; Performance Evaluation; Flooding Attack; OMNeT++.

Resumen

Las Redes Ad Hoc Móviles (MANETs) presentan aplicaciones críticas en escenarios sin infraestructura, como operaciones de rescate, entornos militares y despliegues temporales del Internet Industrial de las Cosas (IIoT); sin embargo, enfrentan desafíos asociados a la movilidad, la comunicación multi-salto y la vulnerabilidad a ataques de seguridad. Este trabajo evalúa comparativamente los protocolos de enrutamiento AODV (*Ad hoc On-Demand Distance Vector*), DSDV (*Destination-Sequenced Distance Vector*) y GPSR (*Greedy Perimeter Stateless Routing*) en condiciones normales y bajo un ataque de *Flooding* extremo. Para ello, se realizaron simulaciones utilizando OMNeT++/INET con el estándar IEEE 802.11, considerando una topología de 600×600 m, tráfico UDP-CBR con paquetes de 256 bytes, cuatro nodos atacantes y diez repeticiones por escenario. Las métricas analizadas incluyen la Tasa de Entrega de Paquetes (PDR), el rendimiento de la red (*Throughput*) y la latencia extremo a extremo (*Delay*). En condiciones normales, AODV y DSDV alcanzaron un PDR del 98%, mientras que GPSR obtuvo un 7,03%. Bajo ataque *Flooding*, el PDR se redujo a 31,13% para AODV, 18,63% para DSDV y 1,91% para GPSR. El rendimiento de la red disminuyó de 10,14 a 2,76 kbps en AODV, de 4,06 a 1,65 kbps en DSDV y de 0,71 a 0,17 kbps en GPSR. En cuanto a la latencia, AODV se mantuvo estable (aproximadamente entre 528 y 560 ms), mientras que DSDV y GPSR presentaron valores del orden de 5×10^4–6×10^4 ms, resultando inviables para aplicaciones en tiempo real. Como contribución, este estudio ofrece un pipeline de simulaciones reproducible (NED/INI), la estandarización de métricas (PDR, *Delay*, *Throughput*) y estimaciones con intervalos de confianza del 95%. El impacto del trabajo radica en proporcionar evidencia práctica para la selección de protocolos según requisitos de robustez y latencia, además de aportar fundamentos para el diseño de estrategias de detección y mitigación de ataques en MANETs.

Palabras clave: MANETs; Evaluación del Desempeño; Ataque de Flooding; OMNeT++.

Introdução

As Redes Ad Hoc Móveis (*Mobile Ad Hoc Networks* – MANETs) representam um paradigma essencial na comunicação sem fio, caracterizado pela ausência de infraestrutura fixa, pela mobilidade dos nós e pela capacidade de auto-organização. Essas propriedades tornam as MANETs uma solução estratégica em cenários críticos, como operações militares, monitoramento de desastres, missões de resgate e, mais recentemente, aplicações da Internet das Coisas (*Internet of Things* – IoT) e da Internet Industrial das Coisas (*Industrial Internet of Things* – IIoT) (Darsena et al, 2022; Ryu e Kim, 2024). No entanto, a mesma flexibilidade que garante sua ampla aplicabilidade também amplia a vulnerabilidade a ataques, em razão do ambiente aberto e altamente dinâmico no qual os nós se comunicam. Além disso, as restrições de memória, energia e capacidade de processamento inerentes às redes sem fio agravam os riscos de segurança (Faris et al, 2023).

Entre os diferentes tipos de ameaças, destacam-se os ataques de Negação de Serviço (*Denial of Service* – DoS), que exploram diretamente essas fragilidades estruturais. Dentre esses ataques, sobressai o ataque *Flooding*, caracterizado pela inundação da rede com Pacotes de Requisição de Rota (*Route Request* – RREQ), o que resulta em sobrecarga de tráfego, consumo excessivo de energia e queda acentuada da Taxa de Entrega de Pacotes (Alghofaili et al, 2023). Pesquisas recentes confirmam que ataques como Sinkhole, Sybil, Wormhole e *Flooding* figuram entre os mais investigados, por impactarem parâmetros de Qualidade de Serviço (*Quality of Service* – QoS), tais como Taxa de Entrega de Pacotes (*Packet Delivery Ratio* – PDR), Latência (*Delay*) e Vazão (*Throughput*) (Jahangeer et al, 2023; Obaid et al, 2024).

No âmbito da investigação científica, observa-se uma variedade de estudos dedicados à análise de ataques sobre protocolos de roteamento ad hoc. Safdar et al. (2022), por exemplo, demonstraram os impactos dos ataques Blackhole e Wormhole em MANETs em Nuvem (*Cloud-Based Mobile Ad Hoc Networks – Cloud*-MANET), utilizando o protocolo de roteamento AODV (*Ad hoc On-Demand Distance Vector*), evidenciando a necessidade de análises comparativas que também considerem cenários de ataque *Flooding*. Por outro lado, Ismail et al. (2024), ao discutirem a integração de técnicas de aprendizado de máquina à segurança em redes sem fio, apontam que ainda são escassas metodologias robustas e padronizadas para avaliar o comportamento das redes sob diferentes tipos de ataque. De forma convergente, revisões sistemáticas como as de Pamarthi e Narmadha (2022) e Alzhrani e Alliheedi (2024) indicam que, embora existam diversas propostas de defesa, a detecção e a mitigação de ataques *Flooding* permanecem desafios em aberto.

A relevância deste estudo torna-se ainda mais evidente quando se considera a necessidade de avaliar o desempenho de protocolos de roteamento sob condições adversas de tráfego intenso e ataques deliberados, conforme discutido por Rao et al. (2023). Estruturas de simulação têm possibilitado a replicação de cenários realistas para a mensuração de métricas como Taxa de Entrega de Pacotes, Vazão e Latência, fornecendo subsídios práticos para a escolha de protocolos em ambientes críticos (Alghofaili et al, 2023). Estudos empíricos recentes corroboram que o ataque Flooding provoca degradações na Taxa de Entrega de Pacotes e acelera o esgotamento energético, comprometendo serviços essenciais de monitoramento e controle em Redes de Sensores sem Fio (RSSF) e MANETs (Bhatti et al, 2024). Diante das limitações identificadas na literatura, este estudo investiga como o ataque *Flooding* impacta o desempenho dos protocolos de roteamento AODV, DSDV (*Destination-Sequenced Distance Vector*) e GPSR (*Greedy Perimeter Stateless Routing*) em MANETs, considerando as métricas de Taxa de Entrega de Pacotes, Vazão e Latência. A questão de pesquisa que orienta este trabalho é: qual protocolo apresenta maior resiliência sob ataque *Flooding* e quais métricas são mais impactadas? A fundamentação teórica e a derivação dessa questão são detalhadas na seção seguinte, dedicada à Revisão da Literatura e ao Estado da Arte.

Revisão da Literatura e Estado da Arte

A literatura recente sobre segurança em MANETs e RSSF evidencia avanços relevantes, mas também revela lacunas persistentes. Estudos como os de Ryu e Kim (2024) e Malik e Sun (2020) analisam ataques clássicos, como Wormhole e Blackhole, enquanto trabalhos de Alghofaili et al. (2023) e Bhatti et al. (2024) concentram-se no ataque *Flooding*, demonstrando seus impactos negativos sobre métricas de desempenho. Revisões abrangentes, como as de Faris et al. (2023) e Obaid et al. (2024), sistematizam ameaças e mecanismos de defesa, mas apontam a carência de investigações comparativas entre diferentes protocolos de roteamento em cenários de ataque. Outros autores, como Ismail et al. (2024) e Malik e Sun (2020), exploram abordagens baseadas em aprendizado de máquina, enquanto Mohammed et al. (2025) ampliam a discussão para ambientes de Cloud-MANET, evidenciando a diversidade de contextos e metodologias existentes.

A análise conjunta desses estudos evidencia que a literatura sobre MANETs sob ataque *Flooding* tende a avaliar isoladamente um único protocolo de roteamento ou a empregar métricas e cenários não padronizados, o que dificulta comparações diretas entre abordagens. Essa limitação metodológica compromete a identificação de protocolos mais resilientes em condições adversas.

Além disso, embora haja avanços significativos em técnicas de detecção e classificação de ataques, poucos trabalhos investigam de forma sistemática o impacto do ataque *Flooding* sobre diferentes protocolos de roteamento, avaliando simultaneamente métricas de Qualidade de Serviço, como Taxa de Entrega de Pacotes, Vazão e Latência, em cenários realistas de mobilidade.

Com base nessas evidências, formula-se o seguinte **problema de pesquisa**:

> Como o ataque *Flooding* afeta o desempenho dos protocolos de roteamento AODV, DSDV e GPSR em MANETs, considerando métricas como Taxa de Entrega de Pacotes, Vazão e Latência?

A partir desse problema, estabelece-se a **hipótese principal**, segundo a qual o ataque *Flooding* provoca degradação significativa nas métricas de desempenho das MANETs, reduzindo a confiabilidade, a vazão e a responsividade da rede, independentemente do protocolo adotado.

Como **hipóteses específicas**, considera-se que:

> (i) protocolos proativos, como o DSDV, tendem a apresentar maior resistência ao ataque *Flooding* devido à manutenção periódica das tabelas de rotas, ainda que com aumento do atraso médio e do overhead de controle;
> (ii) protocolos reativos, como o AODV, são mais suscetíveis ao *Flooding*, uma vez que o ataque explora diretamente o mecanismo de requisição de rotas (RREQ); e
> (iii) protocolos geográficos, como o GPSR, apresentam comportamento intermediário, podendo equilibrar eficiência e robustez, porém com desempenho inferior em ambientes saturados pelo ataque.

O **objetivo geral** deste trabalho é avaliar comparativamente o impacto do ataque *Flooding* sobre os protocolos de roteamento AODV, DSDV e GPSR em MANETs, identificando seus efeitos sobre as métricas de desempenho.

Como **objetivos específicos**, busca-se:

(i) implementar cenários de simulação no ambiente OMNeT++;
(ii) analisar o desempenho dos protocolos AODV, DSDV e GPSR em condições normais e sob ataque *Flooding*;
(iii) comparar métricas como Taxa de Entrega de Pacotes, Vazão e Latência; e
(iv) identificar o protocolo mais resiliente e as métricas mais impactadas.

Dessa forma, este trabalho justifica-se pela necessidade de uma avaliação comparativa sistemática entre diferentes protocolos de roteamento sob ataque *Flooding*, contribuindo para a compreensão de seus impactos em métricas críticas de desempenho. Os resultados esperados podem subsidiar diretamente aplicações críticas em ambientes industriais, de saúde e militares, nos quais a segurança e a confiabilidade dos sistemas de comunicação são requisitos fundamentais.

O presente estudo adota uma abordagem experimental e quantitativa, baseada em simulação computacional,

Metodologia / Material e Métodos

com o objetivo de avaliar os impactos do ataque *Flooding* em MANETs. A opção pela simulação justifica-se pela necessidade de controlar de forma precisa variáveis da rede, tais como topologia, mobilidade, tráfego e parâmetros de rádio, além de permitir a observação reprodutível do comportamento de diferentes protocolos de roteamento sob cenários adversos. Essa escolha metodológica está alinhada com a literatura da área, que aponta a modelagem e a simulação como estratégias essenciais em pesquisas em Ciência da Computação, por possibilitarem controle de variáveis, reprodutibilidade e validação de hipóteses em ambientes complexos (Shaik e Kim, 2025; Wazlawick, 2021). A imagem 1 apresenta o fluxo lógico da pesquisa, destacando as principais etapas metodológicas, desde a definição do cenário de simulação até a análise dos resultados obtidos.

Cenário de Simulação

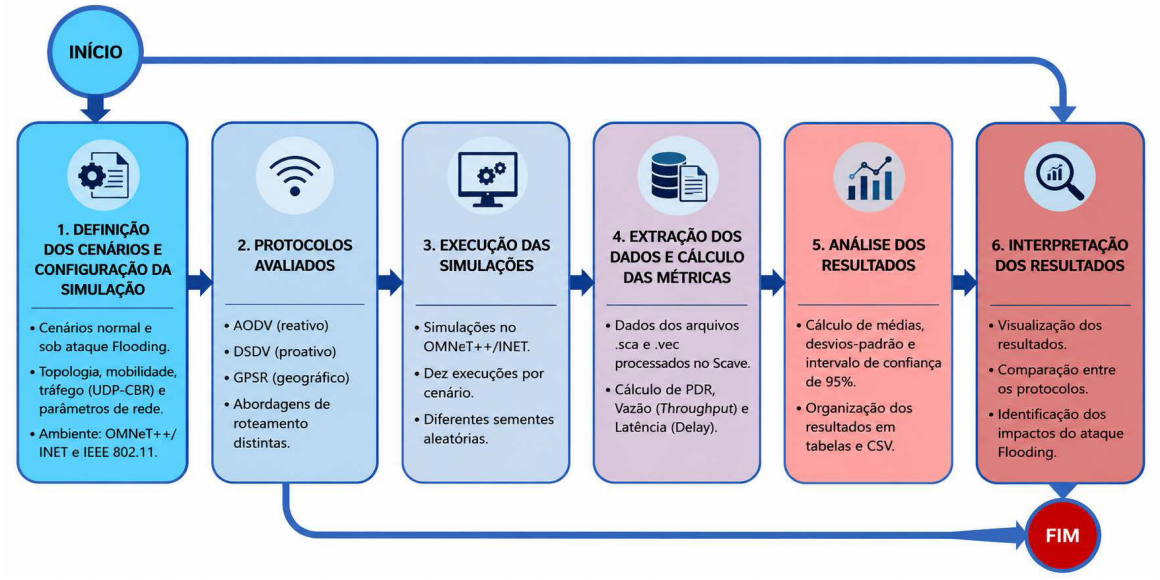

Imagem 1: Fluxo metodológico da pesquisa.
Fonte: Elaboração própria do autor.

Foram implementados dois cenários principais de simulação:

(i) um cenário normal, sem a presença de ataques, e
(ii) um cenário sob ataque *Flooding*, no qual quatro nós foram configurados como atacantes.

Esses cenários permitem comparar o desempenho dos protocolos de roteamento em condições regulares e sob uma situação extrema de sobrecarga da rede.

A topologia modelada é composta por 10 nós, sendo um nó fonte (*source*), oito nós intermediários e um nó destino (*destination*), distribuídos em uma área de 600 × 600 metros, conforme as restrições de mobilidade do simulador. A mobilidade padrão dos nós foi configurada como mobilidade linear, na qual cada nó se desloca em linha reta com velocidade constante, definida em aproximadamente 25 m/s. Nos cenários de ataque, o nó atacante e alguns nós intermediários foram configurados com mobilidade estacionária, de modo a representar pontos fixos de inundação de tráfego, caracterizando hotspots de *Flooding*.

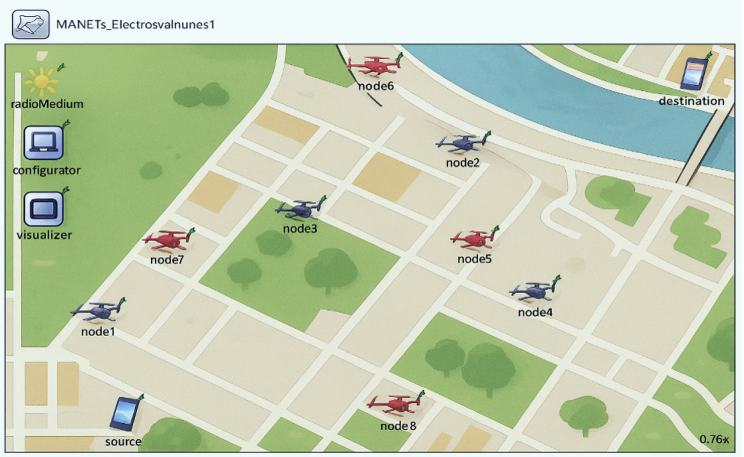

Imagem 2: Topologia da rede simulada.

Fonte: Elaboração própria do autor a partir dos dados de pesquisa simulados no OMNeT++/INET.

A simulação foi desenvolvida no ambiente OMNeT++, utilizando o *Framework INET*, que fornece módulos para modelagem das camadas de rede e enlace (OMNeT++ Community, 2025). A camada de controle de acesso ao meio (MAC) foi configurada com o módulo IEEE 802.11 MAC, responsável pelo acesso ao canal, retransmissões automáticas e controle de colisões, conforme o padrão IEEE 802.11. A camada física (PHY) utilizou o módulo IEEE 802.11 Radio, configurado de acordo com o padrão IEEE 802.11b, com taxa nominal de 2 Mbps e alcance aproximado de 100 metros, assegurando consistência dos parâmetros físicos empregados.

A aplicação legítima foi configurada utilizando os módulos UdpBasicApp e UdpSink, responsáveis, respectivamente, pela geração e recepção de tráfego via protocolo UDP (*User Datagram Protocol*). As mensagens legítimas possuem tamanho de 256 bytes e são enviadas a cada 0,2 segundos, utilizando a porta 5000, com início de transmissão distribuído uniformemente entre 150 e 152 segundos de simulação.

O ataque *Flooding* foi configurado para utilizar a porta 5001, com pacotes de 1500 bytes enviados em intervalos curtos (aproximadamente 0,0002 segundos), gerando tráfego intenso e contínuo de requisições falsas, conforme definido no arquivo de configuração do simulador. Essa configuração caracteriza um cenário de ataque de alta intensidade, representando uma condição de alto volume de tráfego e elevada concorrência pelo acesso ao canal, permitindo observar o comportamento dos protocolos sob situações críticas de congestionamento, conforme discutido na literatura (Bakade e More, 2023; Shaer et al, 2023).

Cada cenário foi executado 10 vezes, utilizando diferentes sementes aleatórias, e a duração de cada simulação foi de 300 segundos, assegurando a robustez estatística dos resultados obtidos. Os principais parâmetros de configuração da rede são apresentados na Tabela 1.

Tabela 1.
Parâmetros de configuração da rede.

PARÂMETRO	VALOR
Quantidade de nós	10 (1 source, 8 intermediários, 1 destination)
Topologia	Ad hoc móvel
Área total	600 m × 600 m
Tempo total de simulação	Sim_time_limit: 300 segundos
Bitrate PHY	24Mbps (normal); 2 Mbps (Flooding EXTREME)
Tamanho do pacote legítimo	256 B (legítimo); 1500 B (ataque)
Número de retransmissões	10
Número de nós atacantes	Nós 5 a 8

Fonte: Elaboração própria do autor a partir dos dados de pesquisa simulados no OMNeT++/INET.

Protocolos Avaliados

Foram avaliados três protocolos de roteamento utilizados em MANETs, selecionados de modo a representar as três abordagens predominantes na literatura: reativa, proativa e geográfica (Gupta e Seth, 2024). Essa escolha possibilita comparar como diferentes estratégias de descoberta e manutenção de rotas se comportam sob o impacto do ataque *Flooding*.

O protocolo AODV (*Ad hoc On-Demand Distance Vector*) é um protocolo reativo, que estabelece rotas sob demanda por meio da troca de mensagens de requisição (RREQ) e resposta (RREP). Embora reduza o tráfego de controle em condições normais, o AODV tende a ser vulnerável ao *Flooding*, uma vez que o ataque explora diretamente o mecanismo de descoberta de rotas (Safari et al, 2023).

O protocolo DSDV (*Destination-Sequenced Distance Vector*) é um protocolo proativo, baseado na manutenção periódica de tabelas de roteamento em cada nó. Essa característica promove maior previsibilidade das rotas, mas implica maior overhead de controle e consumo de largura de banda (Messabih et al, 2023). O DSDV foi incluído para analisar como protocolos com atualização contínua reagem à inundação de tráfego típica do ataque *Flooding*.

O protocolo GPSR (*Greedy Perimeter Stateless Routing*) é um protocolo geográfico, no qual as decisões de encaminhamento dependem da posição física dos nós, dispensando tabelas globais de rotas. Em geral, essa abordagem reduz overhead e pode melhorar a escalabilidade; entretanto, sob ataque *Flooding*, o elevado volume de tráfego falso pode interferir na tomada de decisão baseada em posição, degradando o desempenho (Zheng et al, 2023).

As configurações específicas de cada protocolo foram mantidas com os parâmetros padrão do *Framework INET*, assegurando reprodutibilidade e aderência a práticas de referência.

Métricas de Avaliação

Para quantificar o impacto do ataque Flooding sobre o desempenho dos protocolos de roteamento, foram analisadas três métricas clássicas de Qualidade de Serviço (QoS): Taxa de Entrega de Pacotes (*Packet Delivery Ratio* – PDR), Vazão (*Throughput*) e Latência (*Delay*). Essas métricas foram selecionadas por refletirem diretamente confiabilidade, eficiência de roteamento e responsividade da rede, sendo utilizadas na avaliação de MANETs em cenários adversos (Bhatti et al, 2024; Rashid et al, 2023; Wang et al, 2024).

Os dados necessários para o cálculo dessas métricas foram obtidos a partir dos arquivos escalares (.sca) e vetoriais (.vec) gerados pelo OMNeT++ durante as simulações. O processamento inicial dos dados foi realizado por meio do módulo Scave (*Simulation Control and Visualization Environment*), que permite a filtragem, o cálculo de médias e a exportação dos resultados para análises comparativas.

A Taxa de Entrega de Pacotes (PDR) foi calculada como a razão entre o número total de pacotes recebidos com sucesso no nó destino e o número total de pacotes enviados pelas fontes de tráfego, expressa em porcentagem. Essa métrica indica a confiabilidade do processo de roteamento, sendo que valores mais elevados representam melhor desempenho da rede.

$$PDR = \frac{P\_recebidos}{P\_enviados} * 100 \quad (1)$$

- **P_recebidos** representa o número total de pacotes entregues com sucesso ao nó destino;
- **P_enviados** representa o número total de pacotes gerados pelas fontes de tráfego.

A Vazão (*Throughput*) foi definida como a quantidade média de bits entregues com sucesso por segundo ao nó destino durante o tempo total de simulação, refletindo a capacidade efetiva da rede sob diferentes condições de carga e ataque.

$$Throughput = \frac{(T\_recebidos \times 8)}{T\_simulação} * 100 \quad (2)$$

- **T_recebidos** é o volume total de dados recebidos (em bytes);
- **T_simulação** é o tempo total de simulação (em segundos).

A Latência (*Delay*) corresponde ao tempo médio decorrido entre o envio e o recebimento de um pacote válido, considerando atrasos de propagação, enfileiramento, processamento e retransmissões. Valores elevados de latência indicam degradação do desempenho, geralmente associada à saturação do canal ou à sobrecarga causada pelo ataque *Flooding*.

$$Delay = \sum_{i=1}^{N} (t\_recebimento\_i - t\_envio\_i))/N \quad (3)$$

- **t_envio_i** e **t_recebimento_i** correspondem, respectivamente, ao instante de envio e de recepção do pacote i;
- **N** é o número total de pacotes válidos recebidos.

As médias e os desvios padrão de todas as métricas foram obtidos a partir de 10 execuções independentes de cada cenário, com diferentes sementes aleatórias, permitindo estimativas com intervalo de confiança de 95%, em consonância com estudos similares (Bhatti et al, 2024; Nasir et al, 2022).

Os resultados finais foram exportados em formato CSV (*Comma-Separated Values*) para análise comparativa e geração de gráficos e tabelas. Além da análise no Scave, os dados exportados dos arquivos .sca e .vec foram tratados e visualizados externamente em Python 3.10, utilizando a biblioteca Matplotlib, a fim de gerar os gráficos comparativos apresentados na seção de Resultados. Essa etapa complementar garante rastreabilidade, transparência e reprodutibilidade das análises realizadas.

Disponibilidade dos códigos e dados

Com o objetivo de garantir transparência e reprodutibilidade científica, os principais arquivos utilizados neste estudo foram organizados em um repositório público no GitHub. O repositório contém os códigos de simulação desenvolvidos no OMNeT++/INET, incluindo os arquivos .ned e .ini, bem como os cenários Normal e *Flooding* configurados para os protocolos AODV, DSDV e GPSR. Também são disponibilizadas as figuras da topologia, o fluxo lógico da pesquisa, os gráficos de resultados e os arquivos de apoio para análise das métricas de desempenho, como PDR, atraso médio e *Throughput*. Dessa forma, os materiais permitem a verificação, reprodução e ampliação dos experimentos por outros pesquisadores. O repositório está disponível em: https://github.com/Electrosvalnunes/MANET-Flooding-Attack-AODV-DSDV-GPSR-OMNeT.

Resultados e Discussão

Esta seção apresenta e analisa os resultados obtidos nos cenários simulados, considerando tanto a operação normal da rede quanto a presença do ataque *Flooding*. As métricas analisadas — Taxa de Entrega de Pacotes (*Packet Delivery Ratio* – PDR), Vazão (*Throughput*) e Latência (*Delay*) — foram calculadas a partir dos dados coletados nos arquivos escalares (.sca) e vetoriais (.vec) gerados pelo simulador OMNeT++/INET. O processamento dos dados foi realizado no módulo *Scave* (*Simulation Control and Visualization Environment*), que permitiu a filtragem, o cálculo de médias, desvios-padrão e a exportação dos resultados para o formato CSV, utilizado na geração dos gráficos comparativos. Cada valor apresentado nas tabelas e figuras corresponde à média de 10 execuções independentes, com diferentes sementes aleatórias, garantindo estimativas estatisticamente robustas e intervalo de confiança de 95%.

Tabela 2.
Desempenho médio dos protocolos em cenários normal e sob ataque *Flooding*.

PROTOCOLO / CENÁRIO	PDR(%)	THROUGHPUT (KBPS)	DELAY (MS)
AODV (Normal)	98,0	10,14	528,47
AODV (Flooding)	31,13	2,76	560,02
DSDV (Normal)	98,0	4,06	52.833,47
DSDV (Flooding)	18,63	1,65	59.560,33
GPSR (Normal)	7,03	0,71	61.560,12
GPSR (Flooding)	1,91	0,17	61.680,22

Fonte: Elaboração própria a partir dos resultados simulados no ambiente OMNeT++/INET. Os valores foram calculados com base nos arquivos .sca e .vec, utilizando o módulo Scave para extração de médias, desvios e exportação para formato .csv. Cada valor corresponde à média de 10 execuções independentes com intervalo de confiança de 95%.

Taxa de Entrega de Pacotes (PDR)

A Tabela 2 e a imagem 3 mostram o comportamento médio da Taxa de Entrega de Pacotes (PDR) para os protocolos AODV, DSDV e GPSR nos cenários normal e sob ataque *Flooding*. Observa-se que, em condições normais, os protocolos AODV e DSDV alcançam elevados níveis de confiabilidade, ambos com PDR de aproximadamente 98%, enquanto o GPSR apresenta desempenho inferior já nesse cenário, com PDR de 7,03%.

Sob ataque *Flooding*, ocorre uma redução acentuada do PDR em todos os protocolos avaliados. O AODV sofre queda de 98% para 31,13%, o DSDV de 98% para 18,63% e o GPSR de 7,03% para 1,91%. Essas reduções evidenciam a degradação elevada da confiabilidade da rede causada pela inundação de pacotes falsos de requisição de rota (RREQ), que saturam o canal de comunicação e comprometem o encaminhamento de pacotes legítimos.

O ataque *Flooding* ocupa grande parte da largura de banda disponível e sobrecarrega as estruturas de controle dos protocolos, aumentando a taxa de colisões, retransmissões e descartes de pacotes. Como consequência, as rotas válidas tornam-se instáveis ou indisponíveis, reduzindo drasticamente a quantidade de pacotes entregues com sucesso ao destino.

O protocolo AODV, por ser reativo, sofre impacto direto, uma vez que o ataque explora seu mecanismo de descoberta de rotas sob demanda. O DSDV, apesar de ser proativo, apresenta degradação ainda mais acentuada, pois suas atualizações periódicas de tabelas de roteamento tornam-se ineficientes em um ambiente congestionado. O GPSR, baseado em informações geográficas, apresenta o menor

PDR absoluto, tanto em condições normais quanto sob ataque, refletindo sua sensibilidade a perturbações no tráfego de controle e à perda de informações de vizinhança. Resultados semelhantes são reportados por estudos anteriores (Rao et al, 2023; Wang et al, 2024), que observaram reduções superiores a 60% no PDR de MANETs sob ataques Flooding, corroborando os achados deste estudo.

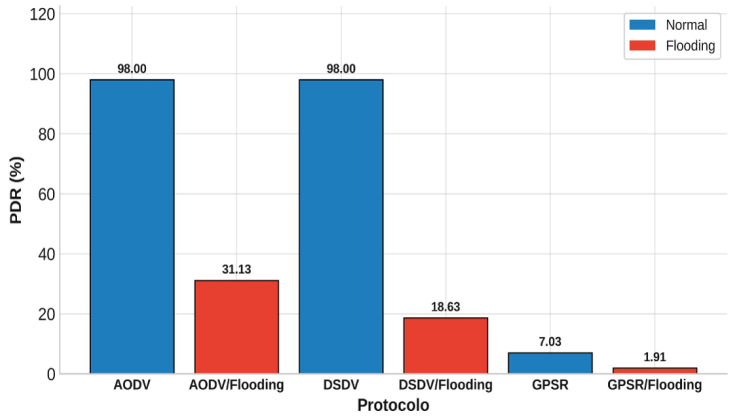

Imagem 3: Comparação da Taxa de Entrega de Pacotes (PDR) nos protocolos AODV, DSDV e GPSR em cenários Normal e sob *Flooding*.
Fonte: Elaboração própria do autor a partir dos resultados simulados no OMNeT++/INET e processados em Python matplotlib.

De forma geral, os resultados indicam que o ataque *Flooding* compromete fortemente a confiabilidade da rede, afetando todos os protocolos avaliados, com reduções superiores a 70% na eficiência de entrega de pacotes.

Vazão (*Throughput*)

A Tabela 2 e a imagem 4 mostram que a vazão apresenta comportamento consistente com os resultados observados para o PDR. Em condições normais, o AODV apresenta maior vazão média (10,14 kbps), seguido pelo DSDV (4,06 kbps) e pelo GPSR (0,71 kbps). Esses valores refletem a eficiência de cada protocolo na utilização do canal em cenários sem interferência maliciosa.

Sob ataque *Flooding*, observa-se uma redução expressiva da vazão em todos os protocolos. O AODV apresenta uma queda de aproximadamente 73%, passando de 10,14 kbps para 2,76 kbps. O DSDV sofre redução de cerca de 59%, de 4,06 kbps para 1,65 kbps, enquanto o GPSR apresenta a maior degradação relativa, com redução de aproximadamente 76%, de 0,71 kbps para 0,17 kbps.

O ataque *Flooding* provoca ocupação excessiva do canal por pacotes falsos de controle, reduzindo drasticamente a largura de banda disponível para o tráfego legítimo. Esse fenômeno aumenta a taxa de colisões e ativa mecanismos de backoff na camada MAC, resultando em maior número de retransmissões e atrasos, o que compromete a eficiência global da rede.

O AODV é particularmente afetado, pois sua dependência do mecanismo de descoberta de rotas é explorada pelo ataque, intensificando o tráfego de controle. O DSDV apresenta desempenho relativo superior sob ataque, pois mantém rotas previamente estabelecidas, ainda que com alto custo de controle. Já o GPSR, dependente de mensagens de beacon e de informações de localização, sofre forte degradação devido à competição entre tráfego legítimo, mensagens de controle e pacotes falsos.

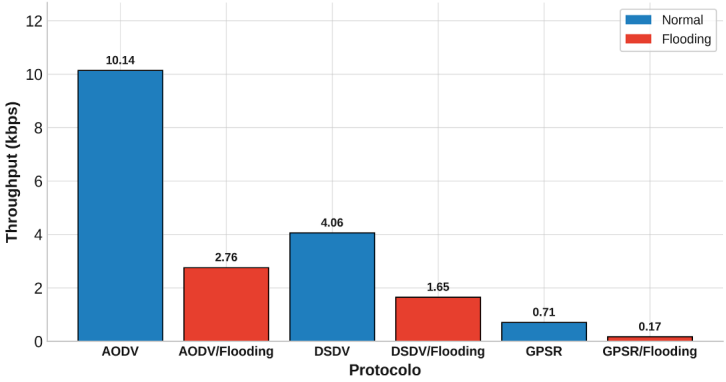

Imagem 4: Comparação da Vazão (*Throughput*) nos protocolos de roteamento AODV, DSDV e GPSR em cenários Normal e sob *Flooding*.
Fonte: Elaboração própria do autor a partir dos resultados simulados no OMNeT++/INET e processados em Python matplotlib.

Esses resultados estão em consonância com os achados de Naveen e Nirmaladevi (2025) e Wang et al. (2024), que relataram reduções entre 60% e 80% na vazão de MANETs sob ataques de inundação, reforçando a validade dos resultados obtidos.

Latência (*Delay*)

A análise da Latência Média (*Delay*) evidencia comportamentos distintos entre os protocolos avaliados, de acordo com Tabela 2 e a imagem 5. O AODV apresenta valores relativamente baixos de atraso tanto no cenário normal (528 ms) quanto sob ataque *Flooding* (560 ms). Em contraste, o DSDV e o GPSR apresentam latências significativamente mais elevadas, variando entre aproximadamente 52.000 ms e 61.000 ms, tanto em condições normais quanto sob ataque.

O aumento do *Delay* sob ataque está diretamente associado à saturação do canal causada pela inundação de pacotes RREQ falsos, o que gera filas extensas de retransmissão na camada MAC e aumenta o tempo de espera para o envio de pacotes legítimos. Entretanto, a intensidade desse impacto varia conforme a natureza do protocolo.

É importante destacar que a aparente estabilidade do *Delay* no AODV não indica necessariamente melhor desempenho. Esse comportamento ocorre porque pacotes excessivamente atrasados tendem a ser descartados antes da entrega, reduzindo a amostra de pacotes válidos considerados no cálculo da média e mascarando o impacto real do ataque. Assim, o atraso médio baixo no AODV deve ser interpretado com cautela.

O DSDV, por ser proativo, propaga atualizações periódicas de rotas, o que gera acúmulo de atrasos sob congestionamento intenso. O GPSR, por sua vez, apresenta latência elevada mesmo em condições normais, devido à troca frequente de mensagens de beacon e aos cálculos de vizinhança; sob ataque *Flooding*, esse custo é amplificado pela competição por acesso ao canal.

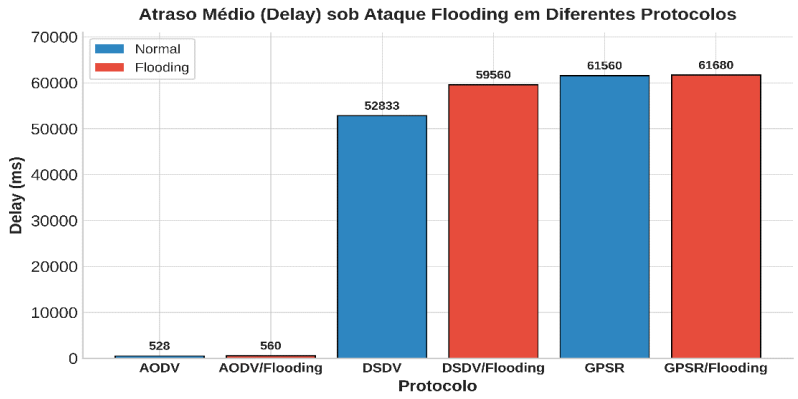

Imagem 5: Comparação da Latência (*Delay*) nos protocolos AODV, DSDV e GPSR em cenários Normal e sob *Flooding*.
Fonte: Elaboração própria do autor a partir dos resultados simulados no OMNeT++/INET e processados em Python matplotlib.

Resultados semelhantes foram observados por Khalid et al. (2023) e Rao et al. (2023), que associam o aumento da latência em MANETs à saturação do canal e à degradação das rotas em cenários de tráfego malicioso.

Discussão Geral

A análise integrada das métricas de desempenho confirma o impacto do ataque *Flooding* sobre os protocolos AODV, DSDV e GPSR. Em todos os casos, verificou-se degradação na confiabilidade, eficiência e responsividade da rede, caracterizando um cenário típico de Negação de Serviço (*Denial of Service* – DoS) em MANETs.

A Taxa de Entrega de Pacotes (PDR) apresentou reduções superiores a 70%, evidenciando que o *Flooding* compromete diretamente a confiabilidade do roteamento, comportamento que se alinha aos levantamentos de Rao et al. (2023) e Wang et al. (2024). A Vazão foi reduzida devido à sobrecarga de pacotes falsos que limitam a capacidade efetiva de transmissão da rede, conforme observado empiricamente por Naveen e Nirmaladevi (2025). Já a Latência foi afetada nos protocolos proativos e geográficos, refletindo o impacto do congestionamento e das retransmissões sucessivas na camada MAC, dinâmica detalhada por Khalid et al. (2023) em cenários de alta saturação de canal por tráfego malicioso.

De modo geral, o AODV apresentou melhor desempenho em condições normais, mas mostrou-se vulnerável sob ataque, uma vez que a inundação explora diretamente seu mecanismo reativo de descoberta de rotas por mensagens RREQ (Safari et al, 2023). O DSDV demonstrou maior robustez relativa em termos de vazão, embora com latência elevada, enquanto o GPSR apresentou o menor desempenho global, sendo o mais impactado nas três métricas analisadas devido à perda de informações de vizinhança necessárias para o encaminhamento geográfico (Zheng et al, 2023).

Esses resultados reforçam a necessidade de mecanismos adaptativos de mitigação, como a limitação dinâmica de requisições de rota e o desenvolvimento de arquiteturas de detecção baseadas em aprendizado de máquina e inteligência artificial em tempo real, conforme sugerido na literatura recente para a identificação e isolamento de nós maliciosos (Bhatti et al, 2024; Nasir et al, 2022; Rashid et al, 2023).

Conclusões

- Este trabalho avaliou comparativamente o impacto do ataque *Flooding* sobre os protocolos de roteamento AODV, DSDV e GPSR em MANETs, utilizando o ambiente OMNeT++/INET e as métricas de Qualidade de Serviço Taxa de Entrega de Pacotes (PDR), Vazão (*Throughput*) e Latência (*Delay*). Os resultados das simulações demonstraram que o ataque *Flooding* degrada significativamente todas as dimensões de desempenho analisadas.
- Em termos de confiabilidade, o PDR foi reduzido de 98% para 31,13% no AODV, de 98% para 18,63% no DSDV e de 7,03% para 1,91% no GPSR. Na métrica de vazão, observaram-se quedas expressivas, passando de 10,14 para 2,76 kbps no AODV, de 4,06 para 1,65 kbps no DSDV e de 0,71 para 0,17 kbps no GPSR. Quanto à latência, o AODV manteve valores aparentemente estáveis (aproximadamente 528–560 ms), enquanto o DSDV e o GPSR apresentaram atrasos excessivos, na ordem de 5×10^4 a 6×10^4 ms, inviáveis para aplicações sensíveis a tempo.
- Os resultados confirmaram parcialmente as hipóteses formuladas. O DSDV apresentou maior resistência relativa em termos de vazão, corroborando a expectativa de que protocolos proativos preservam parte do desempenho sob ataque, embora à custa de latência elevada. O AODV mostrou-se eficiente em cenário normal, mas altamente vulnerável ao *Flooding*, enquanto o GPSR não apresentou o equilíbrio esperado entre eficiência e robustez, sendo o protocolo mais afetado globalmente.
- Como principais contribuições, este estudo ofereceu uma avaliação comparativa padronizada entre três classes de protocolos de roteamento — reativo, proativo e geográfico — sob condições experimentais idênticas, permitindo identificar diferenças claras de comportamento frente ao ataque *Flooding*. Foi desenvolvido um pipeline reprodutível de simulação e análise, integrando os arquivos .sca e .vec do OMNeT++ com o módulo Scave e exportação para CSV, assegurando transparência, rastreabilidade e reprodutibilidade científica.
- Entre as limitações do estudo, destacam-se a análise restrita ao ataque *Flooding*, o uso de modelos específicos de mobilidade e tráfego, e a consideração de um conjunto limitado de métricas de desempenho. Trabalhos futuros podem expandir a análise para outros ataques, como *Blackhole*, *Wormhole* e *Rushing*, bem como incorporar métricas adicionais, diferentes modelos de mobilidade, novos perfis de tráfego e protocolos de roteamento alternativos. A disponibilização pública dos scripts e dados utilizados também pode contribuir para a replicação dos experimentos e futuras meta-análises.
- Em síntese, o estudo forneceu evidências quantitativas e reprodutíveis sobre os efeitos do ataque *Flooding* em MANETs, oferecendo subsídios relevantes para a seleção de protocolos em ambientes adversos e para o desenvolvimento de mecanismos eficazes de detecção e mitigação de ataques em redes móveis sem infraestrutura.

Referências

Alzhrani, R., & Alliheedi, M. (2024). Enhancing IoT Security in 5G Networks: Mitigating DDoS Attacks with Deep Learning. *Journal of Information Security and Cybercrimes Research*, 7(2), 156-166. https://doi.org/10.26735/MVMP8068

AlGhofaili, R., Albinali, H., & Azzedin, F. A. (2023). Impact of *Flooding* Attack on Wireless Sensor Networks: Framework and Toolkit. Preprints. Disponível em: https://doi.org/10.20944/preprints202312.1356.v1

Bakade, K.V., More, A. (2023). Performance Analysis of UAV Routing Protocol Based on Mobility Models. In: Pundir, A.K.S., Yadav, A., Das, S. (eds) Recent Trends in Communication and Intelligent Systems. ICRTCIS 2023. Algorithms for Intelligent Systems. Springer, Singapore, (pp 1–13). Disponível em: https://doi.org/10.1007/978-981-99-5792-7_1

Bhatti, D. S., Saleem, S., & Imran, A. (2024). Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions. *Scientific Reports*, 14, 3428. https://doi.org/10.1038/s41598-024-53938-9

Darsena, D., Gelli, G., Iudice, I., & Verde, F. (2022). Detection and Blind Channel Estimation for UAV-Aided Wireless Sensor Networks in Smart Cities Under Mobile Jamming Attack. *IEEE Internet of Things Journal*, 9(14), 11932-11950. https://doi.org/10.1109/JIOT.2021.3132381

Faris, M., Mahmud, M. N., Salleh, M. F. M., & Alnoor, A. (2023). Wireless sensor network security: A recent review based on state-of-the-art works. *International Journal of Engineering Business Management*, 15, https://doi.org/10.1177/18479790231157220

Gupta, V., Seth, D. (2024). Unmanned Aerial Vehicles (UAVs): Performance Analysis of Routing Protocols for Optimized Operations. In: Tavares, J.M.R.S., Pal, S., Gerogiannis, V.C., Hung, B.T. (eds) Proceedings of Second International Conference on Intelligent System. ICIS 2023. Algorithms for Intelligent Systems. Springer, Singapore, pp 139–156. Disponível em: https://doi.org/10.1007/978-981-99-8976-8_13

Ismail, S., Dawoud, D. W., & Reza, H. (2024). A Comparative Study of Datasets for Cyber-attacks Detection in Wireless Sensor Networks. IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI) (pp. 1-6). Disponível em: https://doi.org/10.1109/ICMI60790.2024.10586154

Jahangeer, A., Bazai, S. U., Aslam, S., Marjan, S., Anas, M., & Hashemi, S. H. (2023). A Review on the Security of IoT Networks: From Network Layer's Perspective. *IEEE Access*, 11, 71073-71087. https://doi.org/10.1109/ACCESS.2023.3246180

Khalid, W., Ahmed, N., Khan, S., Ullah, Z., & Javed, Y. (2023). Simulative Survey of Flooding Attacks in Intermittently Connected Vehicular Delay Tolerant Networks. *IEEE Access*, 11, 75628-75656. https://doi.org/10.1109/ACCESS.2023.3297439

Malik, S., & Sun, W. (2020). Analysis and Simulation of Cyber Attacks Against Connected and Autonomous Vehicles. IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroCAD) (pp. 62-70). Disponível em: https://doi.org/10.1109/MetroCAD48866.2020.00018

Messabih, H., Kerrache, C. A., Cheriguene, Y., Calafate, C. T., & Bousbaa, F. Z. (2023). An Overview of Game Theory Approaches for Mobile Ad-Hoc Network's Security. *IEEE Access*, 11, 107581-107604. https://doi.org/10.1109/ACCESS.2023.3321082

Mohammed, A., Deb Nath, A., & Bin Sharif, N. (2025). AODV Routing in Industrial IoT MANETs Under Dynamic Topology and Traffic Conditions. 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), (pp. 708-711). Disponível em: https://doi.org/10.1109/ICIMIA67127.2025.11200709

Nasir, M. H., Khan, S. A., Khan, M. M., & Fatima, M. (2022). Swarm intelligence-inspired intrusion detection systems — A systematic literature review. *Computer Networks*, 205, 108708. https://doi.org/10.1016/j.comnet.2021.108708

Naveen, N., & Nirmaladevi, J. (2025). Otimização bioinspirada segura com roteamento sob demanda com reconhecimento de intrusão em MANETs. *Scientific Reports*, 15, 25335. https://doi.org/10.1038/s41598-025-99269-1

Obaid, A. K., Rusli, M. E. B., & Yussof, S. (2024). Cache Improvement Based on Routing Protocol for Ad-Hoc Networks: Systematic Literature Review. *IEEE Access*, 12, 170754-170779. https://doi.org/10.1109/ACCESS.2024.3455993

OMNeT++ Community (2025). OMNeT++ Simulation Manual. Disponível em: https://doc.omnetpp.org/omnetpp/manual/. Acessado em 03/ 08/2025

Pamarthi, S., & Narmadha, R. (2022). Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, 10(4), 482–506. https://doi.org/10.1108/IJIUS-05-2021-0028

Rao, M., Chaudhary, P., Sheoran, K., & outros. (2023). A secure routing protocol using hybrid deep regression based trust evaluation and clustering for mobile ad-hoc network. *Peer-to-Peer Networking and Applications*, 16, 2794–2810. https://doi.org/10.1007/s12083-023-01560-3

Rashid, K., Saeed, Y., Ali, A., Jamil, F., Alkanhel, R., & Muthanna, A. (2023). An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). *Sensors*, 23(5), 2594. https://doi.org/10.3390/s23052594

Ryu, J., & Kim, S. (2024). Trust system-based method and multiple verification technique for wormhole attack detection in MANETs. *IEEE Access*, 12, 16266-16275. https://doi.org/10.1109/ACCESS.2024.3355467.

Safari, F., Kunze, H., Ernst, J., & Gillis, D. (2023). A Novel Cross-Layer Adaptive Fuzzy-Based Ad Hoc On-Demand Distance Vector Routing Protocol for MANETs. *IEEE Access*, 11, 50805-50822. https://doi.org/10.1109/ACCESS.2023.3277817

Safdar, T., Siddiqui, M. N., Mateen, M., Malik, K., Sun, S., & Wen, J. (2022). Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring. *Security and Communication Networks*. 2022(1) 1-18. https://doi.org/10.1155/2022/4943218

Shaer, I., Haque, A., & Shami, A. (2023). Availability-aware multi-component V2X application placement. *Vehicular Communications*, 43, 100653. https://doi.org/10.1016/j.vehcom.2023.100653

Shaik, M., Kim, S.W. (2025). Security in Wireless Sensor Networks Using OMNET++: Literature Review. *Sensors*. 25(10) 2972. https://doi.org/10.3390/s25102972

Wang, G., Zhang, J., Zhang, Y., Liu, C., & Chang, Z. (2024). Performance Evaluation of Routing Algorithm in Satellite Self-Organizing Network on OMNeT++ Platform. *Electronics*, 13(19), 3963. https://doi.org/10.3390/electronics13193963

Wazlawick, R. S. (2021). Metodologia de Pesquisa para Ciência da Computação. Rio de Janeiro: GEN | LTC

Zheng, H., Huang, Y., & Chen, L. (2023). The Regional Protocol for Local Communications Among Maritime Autonomous Surface Ships Based on VDES. Em 2023 7th International Conference on Transportation Information and Safety (ICTIS) (pp. 2223-2229). Disponível em: https://doi.org/10.1109/ICTIS60134.2023.10243992