Detecção de Nó Malicioso em Redes de Dispositivos com Dois Rádios

Luisa Vasconcelos de Castro Toledo
Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
Belo Horizonte, Brasil
luisatoledo@dcc.ufmg.br

Luiz Filipe Menezes Vieira
Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
Belo Horizonte, Brasil
lfvieira@dcc.ufmg.br

***Abstract*—Este trabalho apresenta um protocolo simples e eficiente para detecção de nós maliciosos em redes sem fio com dispositivos com dois rádios. A solução utiliza sondas (*probes*) ativas enviadas por uma interface de rádio para identificar atrasos, ausência de resposta e respostas incorretas, evitando interferência no tráfego principal. O protocolo foi implementado no Mininet-WiFi e avaliado em cenários com diferentes tipos de comportamento malicioso. Os resultados mostram que a abordagem alcança baixa sobrecarga, rápido tempo de detecção e maior precisão quando comparada a mecanismos tradicionais como Watchdog, Pathrater e CONFIDANT.**

I. Introdução

As redes sem fio têm um papel cada vez mais central em aplicações distribuídas, sistemas de IoT, redes veiculares e infraestruturas descentralizadas que demandam comunicação eficiente e confiável. Nesse cenário, a presença de nós maliciosos ou não cooperativos representa uma ameaça significativa à integridade, disponibilidade e desempenho global da rede. Ataques como *blackhole, sinkhole*, atraso proposital, omissão e manipulação seletiva de pacotes e falsificação de comportamento podem comprometer completamente protocolos de roteamento e mecanismos de coordenação. Assim, detectar comportamentos anômalos de forma rápida, leve e precisa é um desafio de grande importância.

Dentro desse contexto amplo, este trabalho concentra-se no problema específico da detecção de comportamento malicioso em redes de dispositivos com dois rádios, nas quais cada nó possui duas interfaces operando de maneira independente. A maior parte dos mecanismos clássicos de detecção presume apenas uma interface por nó, o que limita a eficácia de técnicas baseadas em monitoramento passivo, análise de tráfego ou avaliação cooperativa, já que um atacante pode alternar seu comportamento entre as interfaces, ocultando ações maliciosas na interface principal enquanto mantém comportamento benigno na secundária. Assim, existe uma lacuna na literatura em relação a mecanismos de detecção propostos para cenários *dual-radio*.

Neste trabalho, apresentamos um protocolo leve e simples, proposto especificamente para redes de dispositivos de dois rádios, que funciona a partir de mensagens *probe* de sondagem enviadas por um dos rádios, enquanto o outro mantém seu comportamento normal. O método proposto utiliza medições de tempo da resposta e consistência entre mensagens esperadas e recebidas para identificar anomalias como omissão, atraso proposital e respostas incorretas. Os resultados obtidos mostram que essa abordagem permite detectar rapidamente alguns comportamentos maliciosos, com baixa sobrecarga na rede principal e sem depender de modelos complexos de reputação ou de tráfego.

Em um nível mais amplo, a principal diferença entre este trabalho e os métodos tradicionais está na forma como a existência de duas interfaces é explorada: em vez de tentar adaptar mecanismos originalmente pensados para observação passiva ou cooperação entre nós, este estudo utiliza diretamente a interface secundária como um canal para verificação, eliminando suposições que deixam técnicas clássicas vulneráveis a atacantes que alternam comportamento entre rádios. Enquanto os métodos existentes têm sido eficazes em redes de dispositivos com apenas um rádio, a abordagem aqui proposta preenche uma lacuna importante em ambientes com mais de uma interface de comunicação, tornando o processo de detecção mais robusto.

O restante deste artigo está organizado da seguinte forma: a Seção II apresenta o referencial teórico e discute os principais mecanismos de detecção presentes na literatura. A Seção III descreve em detalhes o protocolo proposto, incluindo sua arquitetura, operação e características de detecção. A Seção IV apresenta o ambiente experimental, os cenários avaliados, os parâmetros utilizados e os resultados obtidos. Por fim, a Seção VI apresenta as conclusões e sugestões para trabalhos futuros.

II. Referencial Teórico

A. Redes sem Fio e Segurança

As redes sem fio desempenham um papel central na conectividade moderna, sendo utilizadas em aplicações que vão desde a comunicação pessoal até sistemas industriais e a Internet das Coisas (IoT, do inglês, *Internet of Things*). Diferentemente das redes com fio, essas redes utilizam canais abertos para transmissão de dados, o que aumenta a exposição a interferências, interceptações e falhas deliberadas. Além disso, os nós que compõem essas redes frequentemente possuem recursos limitados de energia, processamento e memória, o

que restringe a implementação de mecanismos de segurança robustos.

A natureza dinâmica das topologias e a ausência de uma infraestrutura fixa tornam as redes sem fio suscetíveis a diversos tipos de ataques. Exemplos incluem:

- Escuta (*eavesdropping*), em que um invasor coleta dados confidenciais interceptando pacotes transmitidos pela rede;
- Injeção de mensagens falsas, que podem comprometer a integridade das informações trocadas;
- Falsificação de identidade (*spoofing*), onde um nó malicioso se passa por um nó legítimo para enganar vizinhos;
- Ataque *Sybil*, no qual um mesmo nó simula múltiplas identidades para, por exemplo, influenciar algoritmos de roteamento e de votação;
- Ataque *Sinkhole*, em que um nó malicioso atrái tráfego ao se passar pelo melhor caminho, podendo assim descartar, manipular ou atrasar mensagens;
- Ataque *Flooding*, no qual um nó malicioso envia uma quantidade excessiva de mensagens com o objetivo de sobrecarregar a rede.

Esses exemplos evidenciam que a segurança em redes sem fio é um desafio complexo, que podem afetar tanto a integridade quanto a disponibilidade de uma rede, exigindo mecanismos capazes de lidar com a diversidade de ataques e com as limitações intrínsecas aos nós da rede. Nesse contexto, a detecção de nós maliciosos surge como uma estratégia essencial para identificar comportamentos anômalos e proteger a rede contra falhas e ataques direcionados.

B. Redes Dual-Radio

Redes *dual-radio* consistem redes formadas por dispositivos equipados com duas interfaces de comunicação sem fio que podem operar simultaneamente, permitindo transmitir e receber mensagens de forma independente em cada rádio. Essa abordagem possibilita a separação de funções de comunicação, a redução de interferências e o aumento da vazão. Em alguns casos, os rádios operam em frequências diferentes (como 2,4 GHz e 5 GHz), permitindo que o dispositivo utilize uma interface para troca de dados e outra para controle, encaminhamento ou serviços auxiliares. Essa separação contribui para reduzir congestionamentos e melhorar significativamente a *performance* geral da rede.

No entanto, a presença de múltiplas interfaces também acrescenta complexidade ao monitoramento e à segurança da rede. Enquanto mecanismos tradicionais de detecção de comportamento malicioso pressupõem que todas as mensagens relevantes circulem por um único canal, arquiteturas com dois rádios permitem que um nó apresente comportamentos distintos em cada rádio. Dessa forma, um dispositivo pode atuar corretamente em uma interface, enviando mensagens legítimas, enquanto compromete o funcionamento da rede pela outra, introduzindo atrasos, omitindo respostas ou retornando informações manipuladas. Essa assimetria torna muitos mecanismos clássicos de detecção insuficientes ou imprecisos quando aplicados diretamente a ambientes multi-interface.

Diante dessas particularidades, soluções de detecção projetadas especificamente para redes dual-radio são necessárias, levando em conta a independência entre as interfaces, a possibilidade de caminhos diferenciados para mensagens de monitoramento e a dificuldade adicional de correlacionar o comportamento observado entre rádios distintos.

C. Técnincas de Detecção

Diversas técnicas têm sido propostas na literatura para detectar nós maliciosos em redes sem fio, explorando diferentes modelos de observação e análise do comportamento dos dispositivos. Entre as abordagens clássicas, destacam-se aquelas baseadas em monitoramento do encaminhamento de pacotes, reputação e confiança, análise de tráfego e mecanismos dependentes de variações de atraso. Cada uma dessas estratégias busca capturar indícios de comportamento anômalo, embora se diferenciem consideravelmente quanto às métricas utilizadas, aos requisitos computacionais e à adequação a ambientes com múltiplas interfaces de rádio.

Uma técnica conhecida é o mecanismo *Watchdog* [1], que monitora passivamente se um nó encaminha corretamente os pacotes que recebe. Caso o dispositivo vizinho deixe de retransmitir mensagens conforme esperado, ele é classificado como suspeito. Complementar ao *Watchdog*, o mecanismo Pathrater utiliza o histórico de cooperação dos nós para selecionar caminhos mais confiáveis. Embora eficazes contra ataques de descarte deliberado de pacotes, esses mecanismos assumem que todos os dispositivos podem observar o tráfego do vizinho, o que não se sustenta em ambientes dual-radio, onde pacotes relevantes podem circular em apenas uma das interfaces.

Outro conjunto de métodos amplamente utilizados envolve mecanismos baseados em reputação, como CONFIDANT [2] e CORE [3], nos quais cada nó avalia o comportamento dos vizinhos a partir de interações diretas e relatórios compartilhados. Essa abordagem busca criar um ecossistema em que dispositivos cooperativos são recompensados enquanto comportamentos suspeitos reduzem a reputação do nó. No entanto, reputações construídas sobre observações parciais se tornam frágeis quando um atacante alterna comportamentos entre rádios distintos, aparentando normalidade em uma interface enquanto realiza ataques pela outra.

As técnicas baseadas na análise de tráfego constituem outra estratégia importante. Elas monitoram padrões de envio e recepção de pacotes, avaliando taxas de perda, volumes incomuns de mensagens ou inconsistências estruturais. Esses métodos podem identificar ataques como *Flooding, Sinkhole* e *Blackhole*, mas dependem de janelas de observação maiores e de instrumentos de correlação que, novamente, se tornam menos eficientes quando o tráfego se distribui de forma assimétrica entre dois rádios independentes.

Os modelos de detecção baseados em atraso, por outro lado, são relevantes para este trabalho, pois consideram a latência de resposta ou o tempo de ida e volta (RTT) como métrica principal. Esses mecanismos assumem que variações significativas de atraso podem indicar manipulação, interferência proposital

ou sobrecarga artificial introduzida por nós maliciosos. Esse tipo de abordagem se mostra especialmente adequado para redes em que o objetivo é detectar comportamentos de omissão, atraso proposital ou resposta incorreta.

Por fim, métodos mais recentes exploram técnicas de aprendizado de máquina para classificar nós como benignos ou maliciosos com base em múltiplas métricas, incluindo atraso, intensidade de sinal, padrões de tráfego e frequência de retransmissões. Embora promissores, esses métodos exigem conjuntos de dados maiores e podem apresentar sobrecarga significativa, o que limita sua aplicação em ambientes de menor capacidade ou em protótipos simples.

Ao comparar essas técnicas à proposta por este projeto, observa-se que mecanismos clássicos, embora eficientes em redes de interface única, apresentam limitações estruturais quando aplicados diretamente a arquiteturas *dual-radio*. O protocolo desenvolvido neste trabalho se destaca justamente por adotar uma abordagem de monitoramento entre rádios, usando a interface secundária exclusivamente para sondas de verificação, o que permite identificar inconsistências entre comportamento esperado e comportamento observado de forma mais precisa. Além disso, ao utilizar métricas simples, o protocolo mantém baixo custo computacional e reduz sobrecarga na rede. A tabela a seguir apresenta uma comparação qualitativa entre o protocolo proposto e algumas das principais técnicas de detecção descritas na literatura. O objetivo é destacar como cada método se comporta diante de cenários relevantes, incluindo presença de múltiplas interfaces, atrasos artificiais e falhas de resposta. Uma comparação entre o protocolo proposto e os existentes na literatura pode ser vista na Tabela A, localizada no Apêndice.

III. Protocolo de Detecção Proposto

Este trabalho propõe um protocolo baseado em mensagens *probe* para a detecção de nós maliciosos em redes de dispositivos com dois rádios, aproveitando a interface de rádio secundária do dispositivo para realizar o monitoramento sem impactar o tráfego de dados que ocorre na interface principal. A ideia consiste em permitir que o rádio *A* permaneça responsável pelas funções tradicionais da rede, enquanto o rádio *B* é utilizado para sondar os nós, enviando e recebendo mensagens *probe*. Com isso, é possível fazer a detecção de nós maliciosos com impacto menor na *performance* da rede, já que o rádio *A* (o rádio principal) não é afetado pelo protocolo.

As mensagens *probe* agem como sondas, são enviadas periodicamente a partir do rádio *B* para cada vizinho da rede. Cada *probe* enviada carrega um pequeno conjunto de informações que o nó vizinho deve devolver ou confirmar. Entre esses campos podem estar, por exemplo, o endereço declarado do próprio nó, identificadores de interface ou outras informações básicas que permitem verificar a coerência entre o que o vizinho afirma ser e o que a rede realmente observa. Assim, a resposta não consiste apenas na devolução mecânica dos dados recebidos, mas numa confirmação explícita de atributos que podem ser checados pelo remetente. Ao receber a resposta correspondente, o nó calcula o tempo de ida e volta (RTT, do inglês *round trip time*) e verifica se os campos retornados coincidem com os valores esperados ou previamente conhecidos. A partir dessas verificações, o protocolo avalia o comportamento de cada vizinho.

Quando o RTT ultrapassa um limiar pré-definido, ou seja, quando a resposta não chega dentro de um intervalo aceitável, ou quando o conteúdo da resposta difere do esperado, o nó emissor interpreta esse evento como possível indício de comportamento malicioso. Esses eventos, quando observados de maneira isolada ou repetida, permitem identificar nós que atrasam, modificam ou descartam pacotes de forma deliberada, ou seja, nós maliciosos.

O uso do rádio *B* para essa troca de mensagens exploratórias reduz significativamente o impacto do processo de detecção no desempenho geral da rede, uma vez que o rádio *A* permanece exclusivamente dedicado ao tráfego principal. Dessa forma, o protocolo consegue realizar monitoramento contínuo com pouca interferência na operação normal da rede e com sobrecarga mínima em termos de largura de banda e processamento.

A. Exemplo de Detecção

Para ilustrar o funcionamento do protocolo proposto, consideremos um cenário simples composto por três nós: 1, 2 e 3, cada um com dois rádios, denominados *A* e *B*, sendo os nós 1 e 2 legítimos, e o nó 3 malicioso. A comunicação segue o modelo proposto: os nós utilizam o rádio *A* para realizar a comunicação principal, e mensagens de sondagem (as *probes*) são enviadas periodicamente através do rádio *B*. Nesse cenário, todos os nós aparentam comportamento normal quando analisamos apenas o tráfego dos respectivos rádios *A*. Vamos avaliar a situação do ponto de vista do nó 1. Ele envia, pelo rádio *B*, *probes* periódicas para os outros nós da rede, e observa as respostas recebidas, avaliando corretude e o RTT (o tempo de ida e volta da mensagem). No caso do nó 2, que é legítimo, as respostas chegam de forma consistente, dentro do tempo esperado e com conteúdo correto, refletindo o comportamento normal. Já o nó 3, por ser malicioso, pode adotar diferentes estratégias adversariais, cada uma com efeitos distintos.

No primeiro caso, o nó 3 não responde às sondas. Isso pode ocorrer, por exemplo, em um ataque de negação de serviço, onde o nó malicioso apenas envia uma grande quantidade de mensagens para sobrecarregar a rede. Nesse caso, o nó 1 não obtém resposta e, após o limite de tempo de espera definido, considera o nó 3 como malicioso. No segundo caso, o nó 3 envia respostas incorretas. Isso pode acontecer caso ele esteja se passando por outro nó, ou caso o nó originalmente legítimo tenha sido infectado. Nesse caso, o nó 1 recebe a resposta, mas ao verificar o conteúdo, encontra divergências com o que era esperado, e classifica o nó 3 como malicioso. Por fim, no terceiro caso, o nó 3 responde às mensagens, mas com um atraso introduzido. Isso pode ocorrer em um ataque no qual o objetivo é deteriorar a qualidade da rede. Diferentemente do primeiro cenário, o nó 1 recebe as respostas, mas observa valores de RTT significativamente superiores ao comportamento normal.

Quando esses atrasos ultrapassam o limite estabelecido, ele detecta o nó 3 como malicioso.

IV. Experimentos

Os experimentos foram realizados no Mininet-Wifi [4], uma plataforma de emulação voltada para redes sem fio, que permite flexibilidade na criação de topologias customizadas e no controle dos parâmetros de rede. Foi definido um comportamento padrão para os nós, que enviam mensagens ”HELLO” a cada 5 segundos via ambos os rádios (para simular o tráfego padrão), e as mensagens *probe* são enviadas pelo rádio *B* a cada 8 segundos. Para a detecção, foi definido, arbitrariamente, um limite de RTT de 22 segundos, ou seja, se a resposta da *probe* não for recebida nesse intervalo de tempo, o nó é considerado malicioso. Além disso, foram considerados 3 tipos de nós maliciosos: o nó que gera um atraso na rede (*delay*), o nó que não responde mensagens, e o nó que responde, mas não de maneira correta. Esses cenários representam, respectivamente, ataques de degradação de desempenho (como *greyhole* e *delay attacks*), ataques de interrupção do fluxo da rede (como ataques de negação de serviço e ataques *blackhole*, e ataques de integridade (como *spoofing*).

A. Topologia

Inicialmente, foi definida uma topologia composta por 3 nós, todos com duas interfaces de rede, sendo um deles um nó com comportamento malicioso. Esses nós foram integrados a duas redes diferentes: a interface de rádio *A* (ou, como definida pelo simulador, *wlan0*) foi conectada à uma rede por meio de um ponto de acesso, e a interface *B* (definida como *wlan1*) foi conectada a uma rede *ad hoc*, ou seja, uma rede descentralizada, para que o protocolo fosse testado em um cenário mais realista. Os experimentos com essa topologia foram usados para a validação inicial do protocolo. Em seguida, a topologia foi modificada para conter 5 nós, adicionando 2 nós com comportamento normal na rede, da mesma forma que os anteriores, resultando em 4 nós legítimos e um nó malicioso. Essa modificação foi feita para analisar o comportamento do protocolo com o aumento do número de nós na rede, e para realizar os experimentos em um cenário menos trivial.

A Figura 1 ilustra a topologia utilizada. Nela, as conexões feitas pelo rádio *A*, associadas ao ponto de acesso, estão representadas pelas linhas azuis, enquanto as conexões do rádio *B*, que formam a rede *ad hoc*, são representadas pelas linhas pretas. O nó malicioso está destacado na cor vermelha.

O nó malicioso foi configurado de três formas distintas, representando 3 tipos contemplados. No cenário de atraso deliberado (*delay*), o nó enviava respostas corretas, mas com um atraso. No cenário de não resposta, ele simplesmente ignorava todas as *probes* recebidas, ou seja, nunca enviava uma resposta, apesar de continuar enviando as mensagens ”HELLO” periodicamente. Por fim, no cenário de alteração de conteúdo, o nó respondia às sondas, mas com informações incorretas.

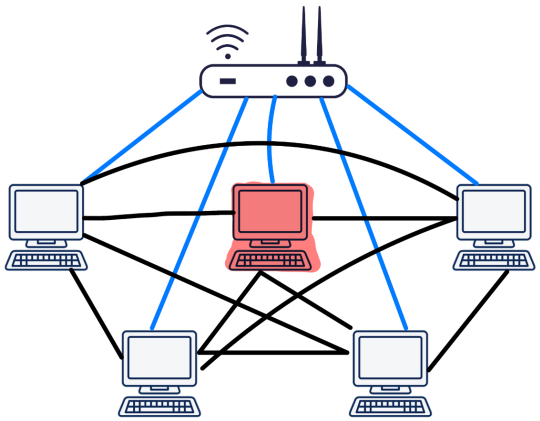

Fig. 1. Topologia utilizada nos experimentos

B. Resultados

Os resultados obtidos mostram que o protocolo foi capaz de detectar corretamente nós maliciosos nos cenários de resposta incorreta e de ausência de resposta, mas apresentou resultados diferentes nos cenários de atraso. Nos casos em que o nó respondia a *probe* com dados incorretos, a detecção ocorreu imediatamente no momento da recepção da resposta, evidenciando que a verificação de integridade das sondas é eficiente e confiável. Nos cenários de ausência de resposta, o nó malicioso foi detectado após a decorrência do tempo definido no limiar.

Já no caso de resposta atrasada, houve uma variação maior. Quando o atraso imposto é maior que o limiar do *timeout*, a detecção funciona como nos cenários de ausência de resposta, ou seja, o nó malicioso é detectado após a passagem do tempo limite. Porém, em casos onde o *delay* é menor que o limite, o nó foi classificado como legítimo, mas apresentava RTT sistematicamente mais elevado. Nesse cenário, o protocolo não marca o nó como malicioso, o que aponta para limitações da abordagem simples baseada em limiares fixos.

Além dos resultados de classificação correta, foi possível perceber, com a mudança da topologia inicial de 3 nós para a de cinco, que o aumento da quantidade de ispositivos na rede leva a um aumento da taxa de falsos positivos, ou seja, de nós legítimos sendo classificados como maliciosos. O maior número de vizinhos implica em maior volume de mensagens circulando simultaneamente, o que contribui para variações naturais nos tempos de resposta e para perdas ocasionais. Como consequência, nós legítimos podem falhar temporariamente no envio ou recepção das respostas, eventualmente ultrapassando o limite de tempo definido.

A Figura 2 apresenta a distribuição dos tempos de ida e volta (RTTs) medidos para cada um dos cinco nós durante os experimentos. Observa-se que os nós *sta1* e *sta2* exibem RTTs praticamente nulos, com variações mínimas e concentradas próximas de zero, indicando comunicação estável e ausência

de comportamento suspeito. O nó *sta3*, configurado como malicioso (nesse caso específico, ignorando as *probes*), não produz valores de RTT porque não responde às mensagens. Nos nós sta4 e *sta5*, observa-se que existem alguns pontos com RTT mais alto. Esses atrasos não são causados por comportamento adversário, mas sim pela maior carga gerada pelo aumento do número de nós na rede. À medida que o tráfego cresce, cresce também a latência e a probabilidade de colisões no canal, o que leva a eventuais atrasos. Esse fenômeno explica o aumento observado na taxa de falsos positivos, especialmente em cenários com maior quantidade de nós.

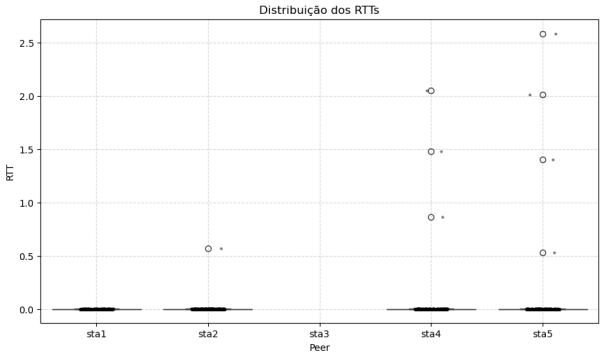

Fig. 2. Distribuição dos RTTs

Diante dos resultados observados, embora o protocolo tenha mostrado boa capacidade geral de detectar o nó malicioso na maioria dos cenários, a tendência de crescimento nos falsos positivos sugere que topologias mais densas exigem ajustes dinâmicos nos limiares ou abordagens mais sofisticadas de classificação.

V. Conclusão

Neste trabalho, propusemos um protocolo simples de detecção de nós maliciosos para redes de dispositivos com dois rádios. Mostramos que mecanismos tradicionais, como *Watchdog, Pathrater* e *CONFIDANT e CORE*, embora amplamente utilizados em redes de interface única, apresentam limitações estruturais quando aplicados a ambientes onde o tráfego é distribuído entre mais de uma interface. Em particular, a incapacidade de observar o comportamento completo do nó vizinho compromete a confiabilidade de métodos baseados em monitoramento passivo ou em reputação.

Os experimentos realizados no Mininet-WiFi demonstraram que o protocolo proposto é capaz de identificar de forma consistente dois tipos de comportamento malicioso: ausência de resposta e respostas incorretas, sendo que a detecção ocorre de maneira imediata nos casos de respostas inválidas e dentro dos limites configurados para cenários de ausência de resposta. Além disso, o uso de métricas simples e troca de mensagens restrita à interface secundária resultou em baixa sobrecarga sobre a rede principal, preservando o tráfego legítimo. Apesar disso, o protocolo não foi capaz de identificar nós maliciosos em cenários de atraso pequeno, enquanto, com atrasos maiores apresentou o mesmo comportamento do cenário de ausência de resposta.

Embora os resultados indiquem a efetividade da abordagem, este trabalho também evidencia oportunidades de evolução. A escolha do limiar de detecção pode ser refinada, possivelmente incorporando modelos adaptativos. Além disso, a ampliação da topologia e a inclusão de cenários com mobilidade também representam possíveis caminhos futuros. Por fim, integrar mecanismos de correlação com múltiplos vizinhos ou combinar a proposta com técnicas de aprendizado de máquina pode ampliar sua capacidade de identificar ataques mais sofisticados.

Em síntese, o protocolo apresentado demonstra que é possível detectar comportamentos maliciosos em ambientes dual-radio sem grande complexidade e com impacto mínimo na rede principal, oferecendo uma alternativa prática e adaptável para cenários em que técnicas clássicas deixam de ser eficazes.

References

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255–265.

[2] G. Milanez, L. Vieira, M. Vieira, and J. Miranda Nacif, "Drds: Comunicação dois-rádios para redes ieee 802.15.4 tsch," 11 2024, pp. 13–16.

[3] P. Michiardi and R. Molva, *Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks*. Boston, MA: Springer US, 2002, pp. 107–121. [Online]. Available: https://doi.org/10.1007/978-0-387-35612-9$_9$

[4] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. E. Rothenberg, "Mininet-wifi: Emulating software-defined wireless networks," in *Network and Service Management (CNSM), 2015 11th International Conference on*, Nov 2015, pp. 384–389.

[5] N. R. Júnior, M. Vieira, and L. Vieira, "Multipath routing for dual-radio wireless sensor networks," in *Anais Estendidos do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre, RS, Brasil: SBC, 2018. [Online]. Available: https://sol.sbc.org.br/index.php/sbrc$_e$$stendido/article/view/$14182

[6] G. Luz, N. Ribeiro Júnior, L. Vieira, M. Vieira, and O. Gnawali, "Latency minimizing in two paths dual radio networks," *Wireless Networks*, vol. 30, pp. 1–10, 12 2023.

[7] O. A. Khashan, "Dual-stage machine learning approach for advanced malicious node detection in wsns," *Ad Hoc Networks*, vol. 166, p. 103672, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S157087052400283X

[8] S. Y. Lim and Y.-H. Choi, "Malicious node detection using a dual threshold in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 2, no. 1, pp. 70–84, 2013. [Online]. Available: https://www.mdpi.com/2224-2708/2/1/70

[9] I. Butun, R. H. Morris, and O. Sankur, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[10] M. A. Farooqi and S. U. Khan, "Intrusion detection systems for wireless sensor networks: A survey," in *International Conference on Communication and Networking*, ser. Lecture Notes in Computer Science, vol. LNCS 5935. Springer, 2009, pp. 234–241.

[11] G. Kibirige and C. Sanga, "A survey on detection of sinkhole attack in wireless sensor network," *arXiv preprint*, vol. arXiv:1505.01941, 2015. [Online]. Available: https://arxiv.org/abs/1505.01941

[12] Y. Qiu, X. Xu, M. Zhu, and K.-C. Li, "An adaptive intrusion detection method for wireless sensor networks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 11, pp. 28–34, 2017. [Online]. Available: https://thesai.org/Downloads/Volume8No11/Paper$_4$ − $An_Adaptive_Intrusion_Detection_Method.pdf$

[13] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE communications surveys tutorials*, vol. 12, no. 2, pp. 159–170, 2010, eemcs-eprint-18041.
[14] N. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: A review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, 2013.
[15] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

APPENDIX

COMPARAÇÃO ENTRE DIFERENTES MECANISMOS DE DETECÇÃO DE NÓS MALICIOSOS

Protocolo	**Tipo de detecção**	**Sobrecarga na rede principal**	**Detecta atraso?**	**Detecta resposta incorreta?**	**Falsos positivos**	**Tempo de detecção**
Protocolo proposto	Probe ativo	Baixíssima (rádio B)	Parcialmente	Sim	Moderado em redes grandes	Baixo/Médio
Watchdog	Observação passiva	Alta	Não	Não	Alto (interferência)	Alto
Pathrater	Reputação baseada no Watchdog	Média	Não	Não	Alto	Alto
CONFIDANT	Reputação + avisos	Média/Alta	Não	Não	Médio	Médio
Probing tradicional single-radio	Probe ativo	Alta	Sim	Sim	Baixo	Baixo